Aljabar Abstrak

Teori dan Penerapan — Edisi Bahasa Indonesia

Aljabar Abstrak

Teori dan Penerapan — Edisi Bahasa Indonesia

Thomas W. Judson
Stephen F. Austin State University

Latihan Sage untuk Aljabar Abstrak

Robert A. Beezer
University of Puget Sound

Terjemahan bahasa Spanyol

Antonio Behn
Universidad de Chile

Entitas penanggung jawab versi modifikasi dan penerbit edisi Bahasa Indonesia

Interlanguage

4 Agustus 2026

Edisi: Edisi Bahasa Indonesia 2026, berdasarkan Annual Edition 2026 (versi modifikasi tidak resmi)

Situs Web: github.com/KokunoYumeto/abstract-algebra-theory-and-applications-id

©1997–2026 Thomas W. Judson, Robert A. Beezer

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the appendix entitled "GNU Free Documentation License." Modified-version notice: This modified version is distributed under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the appendix entitled "GNU Free Documentation License." No additional copyright is claimed for the machine-generated translation.

Ucapan Terima Kasih

Saya ingin menyampaikan penghargaan kepada para penelaah berikut atas komentar dan saran mereka yang bermanfaat.

- David Anderson, University of Tennessee, Knoxville
- Robert Beezer, University of Puget Sound
- Myron Hood, California Polytechnic State University
- Herbert Kasube, Bradley University
- John Kurtzke, University of Portland
- Inessa Levi, University of Louisville
- Geoffrey Mason, University of California, Santa Cruz
- Bruce Mericle, Mankato State University
- Kimmo Rosenthal, Union College
- Mark Teply, University of Wisconsin

Saya juga ingin berterima kasih kepada Steve Quigley, Marnie Pommett, Cathie Griffin, Kelle Karshick, dan seluruh staf PWS Publishing lainnya atas arahan mereka selama proyek ini berlangsung. Bekerja bersama mereka merupakan pengalaman yang menyenangkan.

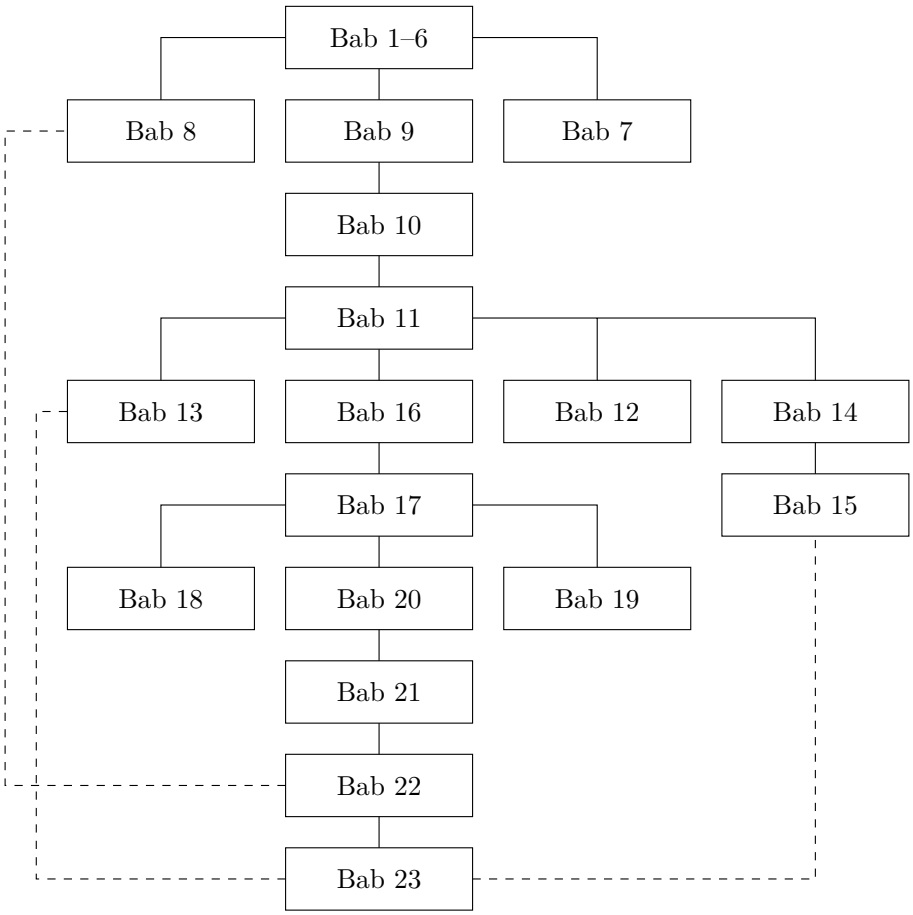
Robert Beezer mendorong saya untuk menyediakan *Aljabar Abstrak: Teori dan Penerapan* sebagai buku ajar sumber terbuka, suatu keputusan yang tidak pernah saya sesali. Dengan bantuannya, buku ini telah ditulis ulang dalam PreTeXt (pretextbook.org), sehingga versi cetak, web, PDF, dan versi lainnya dapat dihasilkan dengan cepat dari sumber yang sama. Versi sumber terbuka buku ini telah menerima dukungan dari National Science Foundation (Hibah #DUE-1020957, #DUE–1625223, dan #DUE–1821329).

Prakata

Teks ini ditujukan untuk mata kuliah aljabar abstrak tingkat sarjana selama satu atau dua semester. Secara tradisional, mata kuliah semacam ini membahas aspek teoretis dari grup, gelanggang, dan lapangan. Namun, seiring berkembangnya komputasi dalam beberapa dasawarsa terakhir, penerapan yang melibatkan aljabar abstrak dan matematika diskret menjadi semakin penting, dan kini banyak mahasiswa sains, teknik, dan ilmu komputer memilih program minor matematika. Meskipun teori tetap menempati peran sentral dalam aljabar abstrak dan tidak seorang pun mahasiswa sepatutnya menempuh mata kuliah semacam ini tanpa pemahaman yang baik mengenai apa itu pembuktian, arti penting penerapan seperti teori pengodean dan kriptografi telah meningkat secara berarti.

Hingga belum lama ini, kebanyakan teks aljabar abstrak hanya memuat sedikit penerapan, jika ada. Namun, salah satu masalah utama dalam mengajarkan mata kuliah aljabar abstrak ialah bahwa bagi banyak mahasiswa, inilah perjumpaan pertama mereka dengan lingkungan yang menuntut pembuktian secara ketat. Mahasiswa seperti ini sering kesulitan memahami manfaat belajar membuktikan teorema dan proposisi; contoh-contoh penerapan membantu pengajar memberikan motivasi.

Teks ini memuat lebih banyak materi daripada yang mungkin dibahas dalam satu semester. Tentu terdapat materi yang memadai untuk mata kuliah dua semester, bahkan mungkin lebih; namun, untuk mata kuliah satu semester, beberapa bab pilihan dapat dengan mudah ditiadakan dan teks ini tetap bermanfaat. Urutan penyajian topiknya mengikuti urutan baku: grup, kemudian gelanggang, dan akhirnya lapangan. Penekanan dapat diberikan pada teori ataupun penerapan. Mata kuliah satu semester yang lazim dapat membahas grup dan gelanggang sambil menyinggung teori lapangan secara singkat, dengan menggunakan Bab 1 sampai 6, 9, 10, 11, 13 (bagian pertama), 16, 17, 18 (bagian pertama), 20, dan 21. Bagian-bagian dari bab tersebut dapat ditiadakan dan diganti dengan penerapan sesuai minat mahasiswa dan pengajar. Mata kuliah dua semester yang menekankan teori dapat membahas Bab 1 sampai 6, 9, 10, 11, 13 sampai 18, 20, 21, 22 (bagian pertama), dan 23. Sebaliknya, jika penerapan hendak ditekankan, mata kuliah dapat membahas Bab 1 sampai 14, serta 16 sampai 22. Dalam mata kuliah terapan, beberapa hasil yang lebih teoretis dapat diterima tanpa pembuktian atau ditiadakan. Bagan ketergantungan bab ditampilkan di bawah ini. (Garis putus-putus menunjukkan ketergantungan parsial.)



Meskipun tidak ada prasyarat khusus untuk mata kuliah aljabar abstrak, mahasiswa yang pernah mengambil mata kuliah matematika tingkat lanjut lainnya pada umumnya akan lebih siap daripada mereka yang belum pernah, karena mereka memiliki kematangan matematis yang lebih tinggi. Sesekali, kami akan mengasumsikan beberapa pengetahuan dasar aljabar linear; dengan kata lain, kami akan menganggap pengetahuan dasar tentang matriks dan determinan telah dikuasai. Hal ini seharusnya tidak menimbulkan masalah berarti, sebab kebanyakan mahasiswa yang mengambil mata kuliah aljabar abstrak telah diperkenalkan dengan matriks dan determinan pada tahap lain dalam pendidikan mereka, jika mereka belum mengambil mata kuliah aljabar linear pada tahun kedua atau ketiga.

Bagian latihan merupakan inti setiap teks matematika. Serangkaian latihan terdapat di akhir setiap bab. Latihan-latihan tersebut mencakup beberapa kategori; di dalamnya terdapat soal komputasional, konseptual, dan teoretis. Bagian yang menyajikan petunjuk dan penyelesaian untuk banyak latihan terdapat di akhir teks. Dalam penyelesaian, suatu pembuktian sering kali hanya diberikan garis besarnya, dan mahasiswalah yang perlu melengkapi perinciannya. Tingkat kesulitan latihan terbentang dari sangat mudah hingga sangat menantang. Banyak soal yang lebih mendalam memerlukan pemikiran saksama, sehingga mahasiswa hendaknya tidak berkecil hati jika penyelesaiannya belum ditemukan setelah beberapa menit mencoba.

Idealnya, mahasiswa membaca materi yang relevan sebelum menghadiri kelas. Pertanyaan bacaan telah ditambahkan pada setiap bab sebelum latihan. Untuk mempersiapkan diri mengikuti kelas, mahasiswa hendaknya membaca bab tersebut sebelum kelas dimulai, lalu menjawab pertanyaan bacaan pada

tiap bagian.

Di akhir banyak bab terdapat latihan tambahan atau proyek komputer. Proyek komputer biasanya memerlukan pengetahuan pemrograman. Semua latihan dan proyek ini bersifat lebih mendalam dan memungkinkan mahasiswa mengeksplorasi hasil serta teori baru.

Sage (sagemath.org) adalah sistem perangkat lunak sumber terbuka gratis untuk matematika tingkat lanjut yang sangat sesuai untuk membantu mempelajari aljabar abstrak. Sage dapat digunakan pada komputer Anda sendiri, pada peladen lokal, atau melalui CoCalc (cocalc.com). Robert Beezer telah menulis pengantar Sage yang menyeluruh dan pilihan latihan relevan yang terdapat di akhir setiap bab, termasuk sel Sage aktif dalam versi web buku ini. Seluruh kode Sage telah menjalani pengujian ketepatan secara otomatis menggunakan versi terbaru yang tersedia pada saat ini: SageMath Versi 10.6 (dirilis pada 31 Maret 2025).

Thomas W. Judson
Massat, Prancis 2026

Riwayat (History)

Dokumen sumber adalah *Abstract Algebra: Theory and Applications*, Annual Edition 2026, karya Thomas W. Judson, dengan kontribusi Sage oleh Robert A. Beezer. Halaman judul sumber tidak mencantumkan penerbit; Judson Books merupakan proyek dan situs buku. Sumber transparan hulu dipatok pada commit 043274d5dead03ff007a461ffe4c2b8477be1248.

Versi modifikasi ini berjudul *Aljabar Abstrak: Teori dan Penerapan — Edisi Bahasa Indonesia*, tahun 2026. Terjemahan mesin Bahasa Indonesia dan backend modular tidak diklaim sebagai karya berhak cipta tambahan. Interlanguage adalah entitas penanggung jawab versi modifikasi sekaligus penerbit edisi ini. Versi modifikasi tidak resmi ini diterbitkan sebagai proyek Interlanguage dan tidak menyiratkan dukungan dari OpenAI maupun penulis hulu. Sumber transparan edisi ini tersedia di github.com/KokunoYumeto/abstract-algebra-theory-and-applications-id. Arsip permanen edisi ini memiliki DOI 10.5281/zenodo.22044963.

Daftar Isi

Ucapan Terima Kasih iv

Prakata v

Riwayat (History) viii

1 Pendahuluan 1

1.1 Catatan Singkat tentang Pembuktian . . . 1
1.2 Himpunan dan Relasi Ekuivalensi . . . 3
1.3 Pertanyaan Bacaan . . . 15
1.4 Latihan . . . 15
1.5 Referensi dan Bacaan yang Disarankan . . . 18

2 Bilangan Bulat 19

2.1 Induksi Matematis . . . 19
2.2 Algoritma Pembagian . . . 22
2.3 Pertanyaan Bacaan . . . 26
2.4 Latihan . . . 26
2.5 Latihan Pemrograman . . . 29
2.6 Referensi dan Bacaan yang Disarankan . . . 30

3 Grup 31

3.1 Kelas Ekuivalensi Bilangan Bulat dan Simetri . . . 31
3.2 Definisi dan Contoh . . . 36
3.3 Subgrup . . . 41
3.4 Pertanyaan Bacaan . . . 43
3.5 Latihan . . . 44
3.6 Latihan Tambahan: Mendeteksi Kesalahan . . . 48
3.7 Referensi dan Bacaan yang Disarankan . . . 49

4 Grup Siklik 51

4.1 Subgrup Siklik . . . 51

4.2 Grup Perkalian Bilangan Kompleks 54
4.3 Metode Kuadrat Berulang 59
4.4 Pertanyaan Bacaan 61
4.5 Latihan 61
4.6 Latihan Pemrograman 65
4.7 Referensi dan Bacaan yang Disarankan 65

5 Grup Permutasi **66**

5.1 Definisi dan Notasi 66
5.2 Grup Dihedral 73
5.3 Pertanyaan Bacaan 77
5.4 Latihan 77

6 Koset dan Teorema Lagrange **82**

6.1 Koset 82
6.2 Teorema Lagrange 84
6.3 Teorema Fermat dan Euler 86
6.4 Pertanyaan Bacaan 87
6.5 Latihan 87

7 Pengantar Kriptografi **90**

7.1 Kriptografi Kunci Privat 91
7.2 Kriptografi Kunci Publik 93
7.3 Pertanyaan Bacaan 96
7.4 Latihan 96
7.5 Latihan Tambahan: Keprimaan dan Faktorisasi 98
7.6 Referensi dan Bacaan yang Disarankan 99

8 Teori Pengodean Aljabar **101**

8.1 Kode Pendeteksi dan Pengoreksi Kesalahan 101
8.2 Kode Linear 109
8.3 Matriks Pemeriksa Paritas dan Matriks Pembangkit 112
8.4 Pendekodean Efisien 117
8.5 Pertanyaan Bacaan 120
8.6 Latihan 121
8.7 Latihan Pemrograman 126
8.8 Referensi dan Bacaan yang Disarankan 126

9 Isomorfisma **127**

9.1 Definisi dan Contoh 127
9.2 Hasil Kali Langsung 131
9.3 Pertanyaan Bacaan 135
9.4 Latihan 135

10 Subgrup Normal dan Grup Hasil Bagi **140**

10.1 Grup Hasil Bagi dan Subgrup Normal 140
10.2 Kesederhanaan Grup Alternasi 142
10.3 Pertanyaan Bacaan 146
10.4 Latihan 146

11 Homomorfisma **149**

11.1 Homomorfisma Grup 149
11.2 Teorema-Teorema Isomorfisma 151
11.3 Pertanyaan Bacaan 154
11.4 Latihan 154
11.5 Latihan Tambahan: Automorfisme 156

12 Grup Matriks dan Simetri **158**

12.1 Grup Matriks 158
12.2 Simetri 165
12.3 Pertanyaan Bacaan 171
12.4 Latihan 172
12.5 Referensi dan Bacaan yang Disarankan 174

13 Struktur Grup **175**

13.1 Grup Abelian Hingga 175
13.2 Grup Solvabel 180
13.3 Pertanyaan Bacaan 183
13.4 Latihan 183
13.5 Latihan Pemrograman 185
13.6 Referensi dan Bacaan yang Disarankan 185

14 Aksi Grup **186**

14.1 Grup yang Beraksi pada Himpunan 186
14.2 Persamaan Kelas 189
14.3 Teorema Pencacahan Burnside 191
14.4 Pertanyaan Bacaan 197
14.5 Latihan 197
14.6 Latihan Pemrograman 200
14.7 Referensi dan Bacaan yang Disarankan 200

15 Teorema Sylow **202**

15.1 Teorema Sylow. 202
15.2 Contoh dan Penerapan 205
15.3 Pertanyaan Bacaan 208
15.4 Latihan 208
15.5 Proyek. 210
15.6 Referensi dan Bacaan yang Disarankan 211

16 Gelanggang **212**

16.1 Gelanggang 212
16.2 Daerah Integral dan Lapangan 216
16.3 Homomorfisma Gelanggang dan Ideal 217
16.4 Ideal Maksimal dan Ideal Prima 221
16.5 Penerapan pada Perancangan Perangkat Lunak 224
16.6 Pertanyaan Bacaan 227
16.7 Latihan 227
16.8 Latihan Pemrograman 232
16.9 Referensi dan Bacaan yang Disarankan 232

17 Polinomial **234**

17.1 Gelanggang Polinomial 234
17.2 Algoritma Pembagian 237
17.3 Polinomial Tak Tereduksi 241
17.4 Pertanyaan Bacaan 246
17.5 Latihan 246
17.6 Latihan Tambahan: Menyelesaikan Persamaan Kubik dan Kuartik 249

18 Daerah Integral **252**

18.1 Lapangan Pecahan 252
18.2 Faktorisasi dalam Daerah Integral 255
18.3 Pertanyaan Bacaan 263
18.4 Latihan 263
18.5 Referensi dan Bacaan yang Disarankan 266

19 Latis dan Aljabar Boolean **267**

19.1 Latis 267
19.2 Aljabar Boolean 271
19.3 Aljabar Rangkaian Listrik 276
19.4 Pertanyaan Bacaan 278
19.5 Latihan 279
19.6 Latihan Pemrograman 282
19.7 Referensi dan Bacaan yang Disarankan 282

20 Ruang Vektor **283**

20.1 Definisi dan Contoh 283
20.2 Subruang 284
20.3 Kebebasan Linear 286
20.4 Pertanyaan Bacaan 288
20.5 Latihan 288
20.6 Referensi dan Bacaan yang Disarankan 291

21 Lapangan **292**

21.1 Perluasan Lapangan 292
21.2 Lapangan Pemisah 301
21.3 Konstruksi Geometris 303
21.4 Pertanyaan Bacaan 308
21.5 Latihan 309
21.6 Referensi dan Bacaan yang Disarankan 311

22 Lapangan Hingga **312**

22.1 Struktur Lapangan Hingga 312
22.2 Kode Polinomial 316
22.3 Pertanyaan Bacaan 323
22.4 Latihan 324
22.5 Latihan Tambahan: Koreksi Galat untuk Kode BCH 326
22.6 Referensi dan Bacaan yang Disarankan 327

23 Teori Galois **328**

23.1 Automorfisme Lapangan 328
23.2 Teorema Fundamental 333
23.3 Penerapan 340
23.4 Pertanyaan Bacaan 345
23.5 Latihan 345
23.6 Referensi dan Bacaan yang Disarankan 348

Lampiran

A GNU Free Documentation License **349**

B Petunjuk dan Jawaban **356**

C Notasi **370**

Bagian Akhir

Indeks **373**

1

Pendahuluan

Kematangan matematis pada taraf tertentu diperlukan untuk menemukan dan mempelajari penerapan aljabar abstrak. Pengetahuan dasar tentang teori himpunan, induksi matematika, relasi ekuivalensi, dan matriks merupakan suatu keharusan. Yang lebih penting lagi adalah kemampuan membaca dan memahami bukti matematis. Dalam bab ini kita akan menguraikan latar belakang yang diperlukan untuk mengikuti mata kuliah aljabar abstrak.

1.1 Catatan Singkat tentang Pembuktian

Matematika abstrak berbeda dari ilmu-ilmu lain. Dalam ilmu laboratorium seperti kimia dan fisika, para ilmuwan melakukan eksperimen untuk menemukan prinsip-prinsip baru dan menguji teori. Walaupun matematika sering dimotivasi oleh eksperimen fisik atau simulasi komputer, ketelitiannya ditegakkan melalui penggunaan argumen logis. Dalam mempelajari matematika abstrak, kita menggunakan apa yang disebut pendekatan aksiomatik; artinya, kita mengambil suatu koleksi objek $\mathcal{S}$ dan mengasumsikan beberapa aturan mengenai strukturnya. Aturan-aturan ini disebut **aksioma**. Dengan menggunakan aksioma-aksioma untuk $\mathcal{S}$, kita ingin menurunkan informasi lain tentang $\mathcal{S}$ melalui argumen logis. Kita mensyaratkan agar aksioma-aksioma kita konsisten; artinya, aksioma-aksioma itu tidak boleh saling bertentangan. Kita juga menuntut agar jumlah aksioma tidak terlalu banyak. Jika suatu sistem aksioma terlalu membatasi, hanya akan ada sedikit contoh struktur matematis tersebut.

Suatu **pernyataan** dalam logika atau matematika adalah penegasan yang bernilai benar atau salah. Perhatikan contoh-contoh berikut:

- $3 + 56 - 13 + 8/2$.
- Semua kucing berwarna hitam.
- $2 + 3 = 5$.
- $2x = 6$ tepat ketika $x = 4$.
- Jika $ax^2 + bx + c = 0$ dan $a \neq 0$, maka
$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$
- $x^3 - 4x^2 + 5x - 6$.

Semua contoh, kecuali contoh pertama dan terakhir, merupakan pernyataan, dan harus bernilai benar atau salah.

Suatu **bukti matematis** tidak lain adalah argumen yang meyakinkan mengenai kebenaran suatu pernyataan. Argumen semacam itu harus memuat cukup banyak perincian untuk meyakinkan pembacanya; misalnya, kita dapat melihat bahwa pernyataan "$2x = 6$ tepat ketika $x = 4$" salah dengan menghitung $2 \cdot 4$ dan memperhatikan bahwa $6 \neq 8$, suatu argumen yang akan meyakinkan siapa pun. Tentu saja, kalangan pembaca dapat sangat beragam: bukti dapat ditujukan kepada mahasiswa lain, kepada dosen, atau kepada pembaca suatu buku. Jika bukti menyajikan perincian melebihi yang diperlukan, penjelasannya akan bertele-tele atau ditulis dengan buruk. Jika terlalu banyak perincian dihilangkan, bukti itu mungkin tidak meyakinkan. Sekali lagi, penting untuk selalu mempertimbangkan pembacanya. Siswa sekolah menengah memerlukan jauh lebih banyak perincian daripada mahasiswa pascasarjana. Pedoman yang baik untuk suatu argumen dalam mata kuliah pengantar aljabar abstrak ialah menuliskannya sedemikian rupa sehingga meyakinkan rekan sejawat, baik rekan tersebut mahasiswa lain maupun pembaca lain buku ini.

Mari kita telaah berbagai jenis pernyataan. Suatu pernyataan dapat sesederhana "$10/5 = 2$;" namun, matematikawan biasanya tertarik pada pernyataan yang lebih kompleks seperti "Jika p, maka q," dengan p dan q keduanya merupakan pernyataan. Jika pernyataan-pernyataan tertentu diketahui atau diasumsikan benar, kita ingin mengetahui apa yang dapat kita katakan mengenai pernyataan-pernyataan lain. Di sini p disebut **hipotesis** dan q disebut **kesimpulan**. Perhatikan pernyataan berikut: Jika $ax^2+bx+c = 0$ dan $a \neq 0$, maka

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Hipotesisnya adalah $ax^2 + bx + c = 0$ dan $a \neq 0$; kesimpulannya adalah

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Perhatikan bahwa pernyataan tersebut sama sekali tidak mengatakan apakah hipotesisnya benar atau tidak. Namun, jika keseluruhan pernyataan ini benar dan kita dapat menunjukkan bahwa $ax^2 + bx + c = 0$ dengan $a \neq 0$ benar, maka kesimpulannya *harus* benar. Bukti pernyataan ini mungkin hanya berupa serangkaian persamaan:

$$\begin{aligned}
ax^2 + bx + c &= 0 \\
x^2 + \frac{b}{a}x &= -\frac{c}{a} \\
x^2 + \frac{b}{a}x + \left(\frac{b}{2a}\right)^2 &= \left(\frac{b}{2a}\right)^2 - \frac{c}{a} \\
\left(x + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2} \\
x + \frac{b}{2a} &= \frac{\pm\sqrt{b^2 - 4ac}}{2a} \\
x &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.
\end{aligned}$$

Jika kita dapat membuktikan bahwa suatu pernyataan benar, pernyataan itu disebut **proposisi**. Proposisi yang sangat penting disebut **teorema**. Kadang-kadang, alih-alih membuktikan suatu teorema atau proposisi sekaligus, kita memecah bukti tersebut menjadi beberapa modul; artinya, kita

membuktikan beberapa proposisi pendukung, yang disebut **lema**, lalu menggunakan hasil proposisi-proposisi itu untuk membuktikan hasil utama. Jika kita dapat membuktikan suatu proposisi atau teorema, sering kali, dengan upaya yang sangat sedikit, kita dapat menurunkan proposisi terkait lainnya yang disebut **korolari**.

1.1.1 Beberapa Peringatan dan Saran

Ada beberapa strategi berbeda untuk membuktikan proposisi. Selain menggunakan berbagai metode pembuktian, mahasiswa sering melakukan sejumlah kesalahan umum ketika baru belajar membuktikan teorema. Untuk membantu mahasiswa yang mempelajari matematika abstrak untuk pertama kalinya, di sini kami mencantumkan beberapa kesulitan yang mungkin mereka hadapi dan beberapa strategi pembuktian yang dapat digunakan. Ada baiknya daftar ini dirujuk kembali sebagai pengingat. (Teknik pembuktian lainnya akan tampak sepanjang bab ini dan bagian-bagian selanjutnya dalam buku ini.)

- Teorema tidak dapat dibuktikan dengan contoh; namun, cara baku untuk menunjukkan bahwa suatu pernyataan bukan teorema ialah memberikan contoh penyangkal.
- Kuantor itu penting. Kata dan frasa seperti *hanya*, *untuk semua*, *untuk setiap*, dan *untuk beberapa* memiliki arti yang berbeda.
- Jangan pernah mengasumsikan hipotesis yang tidak dinyatakan secara eksplisit dalam teorema. *Jangan menganggap sesuatu benar begitu saja.*
- Misalkan Anda ingin menunjukkan bahwa suatu objek *ada* dan *tunggal*. Pertama-tama tunjukkan bahwa objek semacam itu memang ada. Untuk menunjukkan ketunggalannya, asumsikan bahwa ada dua objek semacam itu, misalkan r dan s, lalu tunjukkan bahwa $r = s$.
- Kadang-kadang lebih mudah membuktikan kontraposisi suatu pernyataan. Membuktikan pernyataan "Jika p, maka q" tepat sama dengan membuktikan pernyataan "Jika bukan q, maka bukan p."
- Walaupun biasanya lebih baik menemukan bukti langsung bagi suatu teorema, tugas ini kadang-kadang sulit. Mungkin lebih mudah mengasumsikan bahwa teorema yang sedang Anda coba buktikan itu salah, lalu berharap bahwa dalam rangkaian argumen tersebut Anda terpaksa membuat suatu pernyataan yang mustahil benar.

Ingatlah bahwa salah satu tujuan utama matematika tingkat lanjut adalah membuktikan teorema. Teorema merupakan alat yang memungkinkan penerapan matematika yang baru dan produktif. Kita menggunakan contoh untuk memberi wawasan tentang teorema yang sudah ada dan menumbuhkan intuisi mengenai teorema baru apa yang mungkin benar. Penerapan, contoh, dan bukti saling terkait erat—jauh lebih erat daripada yang mungkin tampak pada awalnya.

1.2 Himpunan dan Relasi Ekuivalensi

1.2.1 Teori Himpunan

Suatu **himpunan** adalah koleksi objek yang terdefinisi dengan baik; artinya, himpunan itu didefinisikan sedemikian rupa sehingga untuk setiap objek x

yang diberikan kita dapat menentukan apakah x termasuk dalam himpunan tersebut atau tidak. Objek-objek yang termasuk dalam suatu himpunan disebut **elemen** atau **anggota** himpunan itu. Kita akan menyatakan himpunan dengan huruf kapital, seperti A atau X; jika a merupakan elemen himpunan A, kita tulis $a \in A$.

Suatu himpunan biasanya ditentukan dengan mencantumkan semua elemennya di antara sepasang kurung kurawal atau dengan menyatakan sifat yang menentukan apakah suatu objek x termasuk dalam himpunan tersebut atau tidak. Kita dapat menulis

$$X = \{x_1, x_2, \ldots, x_n\}$$

untuk himpunan yang memuat elemen $x_1, x_2, \ldots, x_n$, atau

$$X = \{x : x \text{ memenuhi } \mathcal{P}\}$$

jika setiap x dalam X memenuhi suatu sifat tertentu $\mathcal{P}$. Sebagai contoh, jika E adalah himpunan bilangan bulat positif genap, kita dapat mendeskripsikan E dengan menuliskan salah satu dari

$$E = \{2, 4, 6, \ldots\} \quad \text{atau} \quad E = \{x : x \text{ adalah bilangan bulat genap dan } x > 0\}.$$

Kita tulis $2 \in E$ ketika hendak menyatakan bahwa 2 berada dalam himpunan E, dan $-3 \notin E$ untuk menyatakan bahwa -3 tidak berada dalam himpunan E.

Beberapa himpunan penting yang akan kita bahas adalah sebagai berikut:

$$\begin{gathered}
\mathbb{N} = \{n : n \text{ adalah bilangan asli}\} = \{1, 2, 3, \ldots\}; \\
\mathbb{Z} = \{n : n \text{ adalah bilangan bulat}\} = \{\ldots, -1, 0, 1, 2, \ldots\}; \\
\mathbb{Q} = \{r : r \text{ adalah bilangan rasional}\} = \{p/q : p, q \in \mathbb{Z} \text{ dengan } q \neq 0\}; \\
\mathbb{R} = \{x : x \text{ adalah bilangan real}\}; \\
\mathbb{C} = \{z : z \text{ adalah bilangan kompleks}\}.
\end{gathered}$$

Kita dapat menemukan berbagai relasi di antara himpunan dan juga melakukan operasi pada himpunan. Suatu himpunan A merupakan **himpunan bagian** dari B, ditulis $A \subset B$ atau $B \supset A$, jika setiap elemen A juga merupakan elemen B. Sebagai contoh,

$$\{4, 5, 8\} \subset \{2, 3, 4, 5, 6, 7, 8, 9\}$$

dan

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Secara langsung, setiap himpunan merupakan himpunan bagian dari dirinya sendiri. Suatu himpunan B merupakan **himpunan bagian sejati** dari himpunan A jika $B \subset A$ tetapi $B \neq A$. Jika A bukan himpunan bagian dari B, kita tulis $A \not\subset B$; sebagai contoh, $\{4, 7, 9\} \not\subset \{2, 4, 5, 8, 9\}$. Dua himpunan dikatakan **sama**, ditulis $A = B$, jika kita dapat menunjukkan bahwa $A \subset B$ dan $B \subset A$.

Adanya suatu himpunan yang tidak memiliki elemen sangatlah berguna. Himpunan ini disebut **himpunan kosong** dan dilambangkan dengan $\emptyset$. Perhatikan bahwa himpunan kosong merupakan himpunan bagian dari setiap himpunan.

Untuk membentuk himpunan baru dari himpunan yang sudah ada, kita dapat melakukan operasi tertentu: **gabungan** $A \cup B$ dari dua himpunan A dan B didefinisikan sebagai

$$A \cup B = \{x : x \in A \text{ atau } x \in B\};$$

irisan A dan B didefinisikan oleh

$$A \cap B = \{x : x \in A \text{ dan } x \in B\}.$$

Jika $A = \{1, 3, 5\}$ dan $B = \{1, 2, 3, 9\}$, maka

$$A \cup B = \{1, 2, 3, 5, 9\} \quad \text{dan} \quad A \cap B = \{1, 3\}.$$

Kita dapat meninjau gabungan dan irisan lebih dari dua himpunan. Dalam hal ini kita tulis

$$\bigcup_{i=1}^{n} A_i = A_1 \cup \cdots \cup A_n$$

dan

$$\bigcap_{i=1}^{n} A_i = A_1 \cap \cdots \cap A_n$$

masing-masing untuk gabungan dan irisan himpunan $A_1, \ldots, A_n$.

Jika dua himpunan tidak memiliki satu pun elemen yang sama, keduanya dikatakan **saling lepas**; sebagai contoh, jika E adalah himpunan bilangan bulat genap dan O adalah himpunan bilangan bulat ganjil, maka E dan O saling lepas. Dua himpunan A dan B saling lepas tepat ketika $A \cap B = \emptyset$.

Kadang-kadang kita akan bekerja di dalam satu himpunan tetap U, yang disebut **himpunan semesta**. Untuk setiap himpunan $A \subset U$, kita mendefinisikan **komplemen** dari A, yang dilambangkan dengan A', sebagai himpunan

$$A' = \{x : x \in U \text{ dan } x \notin A\}.$$

Kita mendefinisikan **selisih** dua himpunan A dan B sebagai

$$A \setminus B = A \cap B' = \{x : x \in A \text{ dan } x \notin B\}.$$

Contoh 1.2.1 Misalkan $\mathbb{R}$ adalah himpunan semesta dan andaikan

$$A = \{x \in \mathbb{R} : 0 < x \leq 3\} \quad \text{dan} \quad B = \{x \in \mathbb{R} : 2 \leq x < 4\}.$$

Maka

$$\begin{aligned} A \cap B &= \{x \in \mathbb{R} : 2 \leq x \leq 3\} \\ A \cup B &= \{x \in \mathbb{R} : 0 < x < 4\} \\ A \setminus B &= \{x \in \mathbb{R} : 0 < x < 2\} \\ A' &= \{x \in \mathbb{R} : x \leq 0 \text{ atau } x > 3\}. \end{aligned}$$

▲

Proposisi 1.2.2 *Misalkan A, B, dan C adalah himpunan. Maka*

1. $A \cup A = A$, $A \cap A = A$, *dan* $A \setminus A = \emptyset$;
2. $A \cup \emptyset = A$ *dan* $A \cap \emptyset = \emptyset$;
3. $A \cup (B \cup C) = (A \cup B) \cup C$ *dan* $A \cap (B \cap C) = (A \cap B) \cap C$;
4. $A \cup B = B \cup A$ *dan* $A \cap B = B \cap A$;

5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;

6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

BUKTI. Kita akan membuktikan (1) dan (3), sedangkan hasil-hasil lainnya diserahkan untuk dibuktikan dalam latihan.

(1) Perhatikan bahwa

$$\begin{aligned} A \cup A &= \{x : x \in A \text{ atau } x \in A\} \\ &= \{x : x \in A\} \\ &= A \end{aligned}$$

dan

$$\begin{aligned} A \cap A &= \{x : x \in A \text{ dan } x \in A\} \\ &= \{x : x \in A\} \\ &= A. \end{aligned}$$

Selain itu, $A \setminus A = A \cap A' = \emptyset$.

(3) Untuk himpunan A, B, dan C,

$$\begin{aligned} A \cup (B \cup C) &= A \cup \{x : x \in B \text{ atau } x \in C\} \\ &= \{x : x \in A \text{ atau } x \in B, \text{ atau } x \in C\} \\ &= \{x : x \in A \text{ atau } x \in B\} \cup C \\ &= (A \cup B) \cup C. \end{aligned}$$

Argumen serupa membuktikan bahwa $A \cap (B \cap C) = (A \cap B) \cap C$. ■

Teorema 1.2.3 Hukum De Morgan. *Misalkan A dan B adalah himpunan. Maka*

1. $(A \cup B)' = A' \cap B'$;

2. $(A \cap B)' = A' \cup B'$.

BUKTI. (1) Jika $A \cup B = \emptyset$, teorema tersebut langsung berlaku karena A dan B keduanya merupakan himpunan kosong. Jika tidak, kita harus menunjukkan bahwa $(A \cup B)' \subset A' \cap B'$ dan $(A \cup B)' \supset A' \cap B'$. Misalkan $x \in (A \cup B)'$. Maka $x \notin A \cup B$. Jadi x tidak berada dalam A maupun B, berdasarkan definisi gabungan himpunan. Berdasarkan definisi komplemen, $x \in A'$ dan $x \in B'$. Oleh karena itu, $x \in A' \cap B'$ dan kita peroleh $(A \cup B)' \subset A' \cap B'$.

Untuk menunjukkan inklusi sebaliknya, andaikan $x \in A' \cap B'$. Maka $x \in A'$ dan $x \in B'$, sehingga $x \notin A$ dan $x \notin B$. Jadi $x \notin A \cup B$ dan dengan demikian $x \in (A \cup B)'$. Oleh sebab itu, $(A \cup B)' \supset A' \cap B'$ sehingga $(A \cup B)' = A' \cap B'$.

Bukti untuk (2) diserahkan sebagai latihan. ■

Contoh 1.2.4 Relasi-relasi lain di antara himpunan juga sering berlaku. Sebagai contoh,

$$(A \setminus B) \cap (B \setminus A) = \emptyset.$$

Untuk melihat bahwa hal ini benar, perhatikan bahwa

$$\begin{aligned} (A \setminus B) \cap (B \setminus A) &= (A \cap B') \cap (B \cap A') \\ &= A \cap A' \cap B \cap B' \\ &= \emptyset. \end{aligned}$$

▲

1.2.2 Hasil Kali Kartesius dan Pemetaan

Diberikan himpunan A dan B, kita dapat mendefinisikan suatu himpunan baru $A \times B$, yang disebut **hasil kali Kartesius** dari A dan B, sebagai himpunan pasangan terurut. Artinya,

$$A \times B = \{(a, b) : a \in A \text{ dan } b \in B\}.$$

Contoh 1.2.5 Jika $A = \{x, y\}$, $B = \{1, 2, 3\}$, dan $C = \emptyset$, maka $A \times B$ adalah himpunan

$$\{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$$

dan

$$A \times C = \emptyset.$$

▲

Kita mendefinisikan **hasil kali Kartesius dari** n **himpunan** sebagai

$$A_1 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_i \in A_i \text{ untuk } i = 1, \ldots, n\}.$$

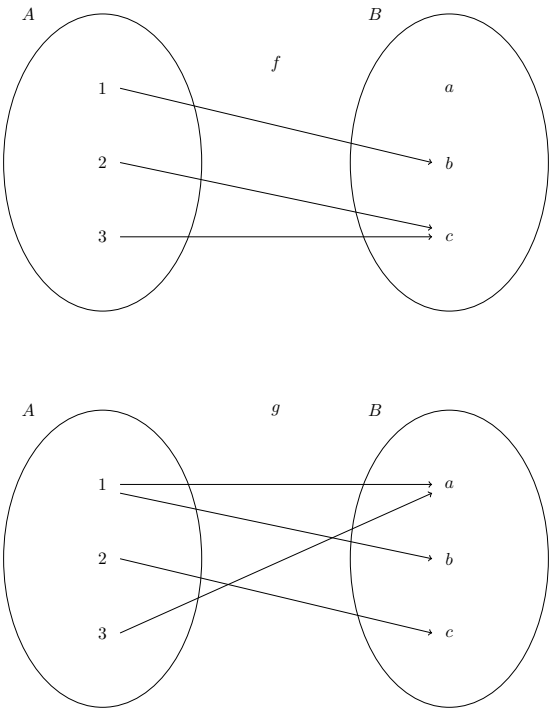
Jika $A = A_1 = A_2 = \cdots = A_n$, kita sering menulis A^n untuk $A \times \cdots \times A$ (dengan A ditulis sebanyak n kali). Sebagai contoh, himpunan $\mathbb{R}^3$ terdiri atas semua tripel bilangan real.

Himpunan bagian dari $A \times B$ disebut **relasi**. Kita mendefinisikan suatu **pemetaan** atau **fungsi** $f \subset A \times B$ dari himpunan A ke himpunan B sebagai jenis relasi khusus, yaitu setiap elemen $a \in A$ memiliki satu elemen tunggal $b \in B$ sedemikian sehingga $(a, b) \in f$. Dengan kata lain, untuk setiap elemen dalam A, f memasangkan satu elemen tunggal dalam B. Kita biasanya menulis $f : A \to B$ atau $A \xrightarrow{f} B$. Alih-alih menuliskan pasangan terurut $(a, b) \in A \times B$, kita menulis $f(a) = b$ atau $f : a \mapsto b$. Himpunan A disebut **domain** dari f, dan

$$f(A) = \{f(a) : a \in A\} \subset B$$

disebut **daerah hasil** atau **citra** dari f. Elemen-elemen dalam domain fungsi dapat dipandang sebagai nilai masukan dan elemen-elemen dalam daerah hasil fungsi sebagai nilai keluaran.

Contoh 1.2.6 Misalkan $A = \{1, 2, 3\}$ dan $B = \{a, b, c\}$. Dalam Gambar 1.2.7 kita mendefinisikan relasi f dan g dari A ke B. Relasi f merupakan pemetaan, tetapi g bukan pemetaan karena $1 \in A$ tidak dipasangkan dengan satu elemen tunggal dalam B; yaitu, $g(1) = a$ dan $g(1) = b$.



Gambar 1.2.7 Pemetaan dan relasi

▲

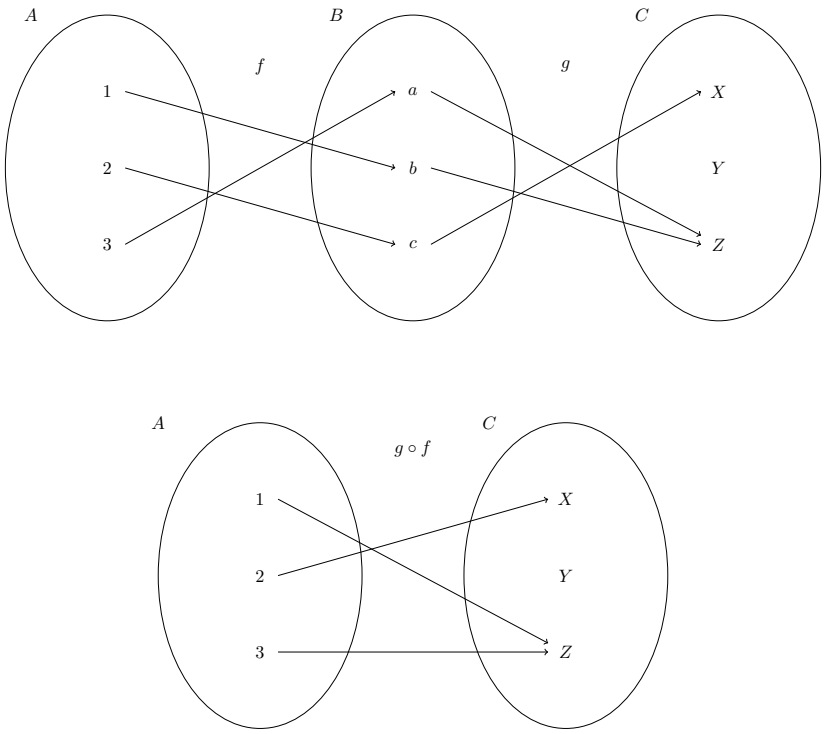
Diberikan suatu fungsi $f : A \to B$, sering kali kita dapat menulis daftar yang mendeskripsikan tindakan fungsi tersebut terhadap setiap elemen tertentu dalam domainnya. Namun, tidak semua fungsi dapat dideskripsikan dengan cara ini. Sebagai contoh, fungsi $f : \mathbb{R} \to \mathbb{R}$ yang membawa setiap bilangan real ke pangkat tiganya merupakan pemetaan yang harus dideskripsikan dengan menulis $f(x) = x^3$ atau $f : x \mapsto x^3$.

Perhatikan relasi $f : \mathbb{Q} \to \mathbb{Z}$ yang diberikan oleh $f(p/q) = p$. Kita mengetahui bahwa $1/2 = 2/4$, tetapi apakah $f(1/2) = 1$ atau 2? Relasi ini tidak mungkin merupakan pemetaan karena tidak terdefinisi dengan baik. Suatu relasi **terdefinisi dengan baik** jika setiap elemen dalam domain dipasangkan dengan satu elemen *tunggal* dalam daerah hasil.

Jika $f : A \to B$ merupakan pemetaan dan citra f adalah B, yaitu $f(A) = B$, maka f disebut **pada (onto)** atau **surjektif**. Dengan kata lain, jika kita dapat memilih suatu $a \in A$ bagi setiap $b \in B$ sedemikian sehingga $f(a) = b$, maka f surjektif. Suatu pemetaan disebut **satu-ke-satu** atau **injektif** jika $a_1 \neq a_2$ mengakibatkan $f(a_1) \neq f(a_2)$. Secara ekuivalen, suatu fungsi injektif jika $f(a_1) = f(a_2)$ mengakibatkan $a_1 = a_2$. Pemetaan yang sekaligus injektif dan surjektif disebut **bijektif**.

Contoh 1.2.8 Misalkan $f : \mathbb{Z} \to \mathbb{Q}$ didefinisikan oleh $f(n) = n/1$. Maka f injektif tetapi tidak surjektif. Definisikan $g : \mathbb{Q} \to \mathbb{Z}$ dengan $g(p/q) = p$, dengan p/q merupakan bilangan rasional yang dinyatakan dalam bentuk paling sederhana dengan penyebut positif. Fungsi g surjektif tetapi tidak injektif. ▲

Diberikan dua fungsi, kita dapat membentuk fungsi baru dengan menggunakan daerah hasil fungsi pertama sebagai domain fungsi kedua. Misalkan $f : A \to B$ dan $g : B \to C$ adalah pemetaan. Definisikan suatu pemetaan baru, yaitu **komposisi** f dan g dari A ke C, dengan $(g \circ f)(x) = g(f(x))$.



Gambar 1.2.9 Komposisi pemetaan

Contoh 1.2.10 Perhatikan fungsi $f : A \to B$ dan $g : B \to C$ yang didefinisikan dalam Gambar 1.2.9 (bagian atas). Komposisi fungsi-fungsi ini, $g \circ f : A \to C$, didefinisikan dalam Gambar 1.2.9 (bagian bawah). ▲

Contoh 1.2.11 Misalkan $f(x) = x^2$ dan $g(x) = 2x + 5$. Maka

$$(f \circ g)(x) = f(g(x)) = (2x + 5)^2 = 4x^2 + 20x + 25$$

dan

$$(g \circ f)(x) = g(f(x)) = 2x^2 + 5.$$

Secara umum, urutan berpengaruh; yaitu, dalam kebanyakan kasus $f \circ g \neq g \circ f$. ▲

Contoh 1.2.12 Kadang-kadang berlaku $f \circ g = g \circ f$. Misalkan $f(x) = x^3$ dan $g(x) = \sqrt[3]{x}$. Maka

$$(f \circ g)(x) = f(g(x)) = f(\sqrt[3]{x}) = (\sqrt[3]{x})^3 = x$$

dan

$$(g \circ f)(x) = g(f(x)) = g(x^3) = \sqrt[3]{x^3} = x.$$

▲

Contoh 1.2.13 Diberikan suatu matriks 2×2

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

kita dapat mendefinisikan pemetaan $T_A : \mathbb{R}^2 \to \mathbb{R}^2$ dengan

$$T_A(x, y) = (ax + by, cx + dy)$$

untuk (x, y) dalam $\mathbb{R}^2$. Ini sesungguhnya merupakan perkalian matriks; yaitu,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Pemetaan dari $\mathbb{R}^n$ ke $\mathbb{R}^m$ yang diberikan oleh matriks disebut **pemetaan linear** atau **transformasi linear**. ▲

Contoh 1.2.14 Misalkan $S = \{1, 2, 3\}$. Definisikan pemetaan $\pi : S \to S$ dengan

$$\pi(1) = 2, \qquad \pi(2) = 1, \qquad \pi(3) = 3.$$

Ini merupakan pemetaan bijektif. Cara lain untuk menulis π adalah

$$\begin{pmatrix} 1 & 2 & 3 \\ \pi(1) & \pi(2) & \pi(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Untuk setiap himpunan S, pemetaan injektif dan surjektif $\pi : S \to S$ disebut **permutasi** dari S. ▲

Teorema 1.2.15 *Misalkan $f : A \to B$, $g : B \to C$, dan $h : C \to D$. Maka*

1. *Komposisi pemetaan bersifat asosiatif; yaitu, $(h \circ g) \circ f = h \circ (g \circ f)$;*
2. *Jika f dan g keduanya injektif, maka pemetaan $g \circ f$ injektif;*
3. *Jika f dan g keduanya surjektif, maka pemetaan $g \circ f$ surjektif;*
4. *Jika f dan g bijektif, maka $g \circ f$ juga bijektif.*

Bukti. Kita akan membuktikan (1) dan (3). Bagian (2) diserahkan sebagai latihan. Bagian (4) langsung mengikuti (2) dan (3).

(1) Kita harus menunjukkan bahwa

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Untuk $a \in A$ kita peroleh

$$\begin{aligned} (h \circ (g \circ f))(a) &= h((g \circ f)(a)) \\ &= h(g(f(a))) \\ &= (h \circ g)(f(a)) \\ &= ((h \circ g) \circ f)(a). \end{aligned}$$

(3) Asumsikan bahwa f dan g keduanya merupakan fungsi surjektif. Diberikan $c \in C$, kita harus menunjukkan bahwa terdapat $a \in A$ sedemikian sehingga $(g \circ f)(a) = g(f(a)) = c$. Karena g surjektif, terdapat elemen $b \in B$ sedemikian sehingga $g(b) = c$. Demikian pula, terdapat $a \in A$ sedemikian sehingga $f(a) = b$. Dengan demikian,

$$(g \circ f)(a) = g(f(a)) = g(b) = c.$$

■

Jika S adalah sembarang himpunan, kita akan menggunakan id_S atau id untuk menyatakan **pemetaan identitas** dari S ke dirinya sendiri. Definisikan pemetaan ini dengan $\mathrm{id}(s) = s$ untuk semua $s \in S$. Suatu pemetaan $g : B \to A$ merupakan **pemetaan invers** dari $f : A \to B$ jika $g \circ f = \mathrm{id}_A$ dan $f \circ g = \mathrm{id}_B$; dengan kata lain, fungsi invers dari suatu fungsi sekadar "membatalkan" kerja fungsi tersebut. Suatu pemetaan disebut **dapat dibalik** jika memiliki invers.

Kita biasanya menulis f^{-1} untuk invers dari f.

Contoh 1.2.16 Fungsi $f(x) = x^3$ memiliki invers $f^{-1}(x) = \sqrt[3]{x}$ berdasarkan Contoh 1.2.12. ▲

Contoh 1.2.17 Fungsi logaritma natural dan fungsi eksponensial, $f(x) = \ln x$ dan $f^{-1}(x) = e^x$, saling invers asalkan kita cermat dalam memilih domain. Perhatikan bahwa

$$f(f^{-1}(x)) = f(e^x) = \ln e^x = x$$

dan

$$f^{-1}(f(x)) = f^{-1}(\ln x) = e^{\ln x} = x$$

bilamana komposisinya terdefinisi. ▲

Contoh 1.2.18 Misalkan

$$A = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}.$$

Maka A mendefinisikan pemetaan dari $\mathbb{R}^2$ ke $\mathbb{R}^2$ dengan

$$T_A(x, y) = (3x + y, 5x + 2y).$$

Kita dapat menemukan pemetaan invers dari T_A hanya dengan membalik matriks A; yaitu, $T_A^{-1} = T_{A^{-1}}$. Dalam contoh ini,

$$A^{-1} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix};$$

sehingga pemetaan inversnya diberikan oleh

$$T_A^{-1}(x, y) = (2x - y, -5x + 3y).$$

Mudah diperiksa bahwa

$$T_A^{-1} \circ T_A(x, y) = T_A \circ T_A^{-1}(x, y) = (x, y).$$

Tidak setiap pemetaan memiliki invers. Jika kita meninjau pemetaan

$$T_B(x, y) = (3x, 0)$$

yang diberikan oleh matriks

$$B = \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix},$$

maka pemetaan inversnya harus berbentuk

$$T_B^{-1}(x, y) = (ax + by, cx + dy)$$

dan

$$(x, y) = T_B \circ T_B^{-1}(x, y) = (3ax + 3by, 0)$$

untuk semua x dan y. Jelas hal ini mustahil karena y belum tentu 0. ▲

Contoh 1.2.19 Diberikan permutasi

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

pada $S = \{1, 2, 3\}$, mudah dilihat bahwa permutasi yang didefinisikan oleh

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

merupakan invers dari π. Sesungguhnya, setiap pemetaan bijektif memiliki invers, sebagaimana akan kita lihat dalam teorema berikut. ▲

Teorema 1.2.20 *Suatu pemetaan dapat dibalik jika dan hanya jika pemetaan tersebut sekaligus injektif dan surjektif.*

BUKTI. Pertama-tama, andaikan $f : A \to B$ dapat dibalik dengan invers $g : B \to A$. Maka $g \circ f = \mathrm{id}_A$ merupakan pemetaan identitas; yaitu, $g(f(a)) = a$. Jika $a_1, a_2 \in A$ dengan $f(a_1) = f(a_2)$, maka $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$. Akibatnya, f injektif. Sekarang andaikan $b \in B$. Untuk menunjukkan bahwa f surjektif, kita perlu menemukan $a \in A$ sedemikian sehingga $f(a) = b$, tetapi $f(g(b)) = b$ dengan $g(b) \in A$. Ambil $a = g(b)$.

Sebaliknya, misalkan f bijektif dan $b \in B$. Karena f surjektif, terdapat $a \in A$ sedemikian sehingga $f(a) = b$. Karena f injektif, a harus tunggal. Definisikan g dengan menetapkan $g(b) = a$. Dengan demikian kita telah membentuk invers dari f. ■

1.2.3 Relasi Ekuivalensi dan Partisi

Salah satu gagasan mendasar dalam matematika adalah kesamaan. Kita dapat memperumum kesamaan dengan relasi ekuivalensi dan kelas ekuivalensi. Suatu **relasi ekuivalensi** pada himpunan X adalah relasi $R \subset X \times X$ sedemikian sehingga

- $(x, x) \in R$ untuk semua $x \in X$ (**sifat refleksif**);
- $(x, y) \in R$ mengakibatkan $(y, x) \in R$ (**sifat simetris**);
- (x, y) dan $(y, z) \in R$ mengakibatkan $(x, z) \in R$ (**sifat transitif**).

Diberikan suatu relasi ekuivalensi R pada himpunan X, kita biasanya menulis $x \sim y$ sebagai pengganti $(x, y) \in R$. Jika relasi ekuivalensi tersebut telah memiliki notasi terkait seperti $=$, $\equiv$, atau $\cong$, kita akan menggunakan notasi tersebut.

Contoh 1.2.21 Misalkan p, q, r, dan s adalah bilangan bulat, dengan q dan s taknol. Definisikan $p/q \sim r/s$ jika $ps = qr$. Jelas bahwa $\sim$ bersifat refleksif dan simetris. Untuk menunjukkan bahwa relasi ini juga transitif, andaikan $p/q \sim r/s$ dan $r/s \sim t/u$, dengan q, s, dan u semuanya taknol. Maka $ps = qr$ dan $ru = st$. Oleh karena itu,

$$psu = qru = qst.$$

Karena $s \neq 0$, maka $pu = qt$. Akibatnya, $p/q \sim t/u$. ▲

Contoh 1.2.22 Misalkan f dan g adalah fungsi yang terdiferensialkan pada $\mathbb{R}$. Kita dapat mendefinisikan relasi ekuivalensi pada fungsi-fungsi semacam itu dengan menetapkan $f(x) \sim g(x)$ jika $f'(x) = g'(x)$. Jelas bahwa $\sim$ bersifat refleksif sekaligus simetris. Untuk menunjukkan transitivitas, andaikan $f(x) \sim g(x)$ dan $g(x) \sim h(x)$. Dari kalkulus kita mengetahui bahwa $f(x) - g(x) = c_1$ dan $g(x) - h(x) = c_2$, dengan c_1 dan c_2 keduanya merupakan konstanta. Jadi,

$$f(x) - h(x) = (f(x) - g(x)) + (g(x) - h(x)) = c_1 + c_2$$

dan $f'(x) - h'(x) = 0$. Oleh karena itu, $f(x) \sim h(x)$. ▲

Contoh 1.2.23 Untuk (x_1, y_1) dan (x_2, y_2) dalam $\mathbb{R}^2$, definisikan $(x_1, y_1) \sim (x_2, y_2)$ jika $x_1^2 + y_1^2 = x_2^2 + y_2^2$. Maka $\sim$ merupakan relasi ekuivalensi pada $\mathbb{R}^2$. ▲

Contoh 1.2.24 Misalkan A dan B adalah matriks 2×2 dengan entri bilangan real. Kita dapat mendefinisikan relasi ekuivalensi pada himpunan matriks 2×2, dengan menyatakan $A \sim B$ jika terdapat matriks P yang dapat dibalik sedemikian sehingga $PAP^{-1} = B$. Sebagai contoh, jika

$$A = \begin{pmatrix} 1 & 2 \\ -1 & 1 \end{pmatrix} \quad \text{dan} \quad B = \begin{pmatrix} -18 & 33 \\ -11 & 20 \end{pmatrix},$$

maka $A \sim B$ karena $PAP^{-1} = B$ untuk

$$P = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}.$$

Misalkan I adalah matriks identitas 2×2; yaitu,

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Maka $IAI^{-1} = IAI = A$; oleh karena itu, relasi tersebut refleksif. Untuk menunjukkan simetri, andaikan $A \sim B$. Maka terdapat matriks P yang dapat dibalik sedemikian sehingga $PAP^{-1} = B$. Jadi

$$A = P^{-1}BP = P^{-1}B(P^{-1})^{-1}.$$

Terakhir, andaikan $A \sim B$ dan $B \sim C$. Maka terdapat matriks P dan Q yang dapat dibalik sedemikian sehingga $PAP^{-1} = B$ dan $QBQ^{-1} = C$. Karena

$$C = QBQ^{-1} = QPAP^{-1}Q^{-1} = (QP)A(QP)^{-1},$$

relasi tersebut transitif. Dua matriks yang ekuivalen dengan cara ini disebut **serupa**. ▲

Suatu **partisi** $\mathcal{P}$ dari himpunan X adalah koleksi himpunan takkosong $X_1, X_2, \ldots$ sedemikian sehingga $X_i \cap X_j = \emptyset$ untuk $i \neq j$ dan $\bigcup_k X_k = X$. Misalkan $\sim$ adalah relasi ekuivalensi pada himpunan X dan $x \in X$. Maka $[x] = \{y \in X : y \sim x\}$ disebut **kelas ekuivalensi** dari x. Kita akan melihat bahwa suatu relasi ekuivalensi menghasilkan partisi melalui kelas-kelas ekuivalensi. Selain itu, bilamana terdapat partisi suatu himpunan, ada suatu relasi ekuivalensi alami yang mendasarinya, seperti ditunjukkan oleh teorema berikut.

Teorema 1.2.25 *Diberikan suatu relasi ekuivalensi $\sim$ pada himpunan X, kelas-kelas ekuivalensi dari X membentuk partisi dari X. Sebaliknya, jika $\mathcal{P} = \{X_i\}$ merupakan partisi dari himpunan X, maka terdapat relasi ekuivalensi pada X dengan kelas-kelas ekuivalensi X_i.*

Bukti. Andaikan terdapat relasi ekuivalensi $\sim$ pada himpunan X. Untuk setiap $x \in X$, sifat refleksif menunjukkan bahwa $x \in [x]$, sehingga $[x]$ takkosong. Jelas bahwa $X = \bigcup_{x \in X} [x]$. Sekarang, misalkan $x, y \in X$. Kita perlu menunjukkan bahwa $[x] = [y]$ atau $[x] \cap [y] = \emptyset$. Andaikan irisan $[x]$ dan $[y]$ tidak kosong serta $z \in [x] \cap [y]$. Maka $z \sim x$ dan $z \sim y$. Berdasarkan simetri dan transitivitas, $x \sim y$; sehingga $[x] \subset [y]$. Demikian pula, $[y] \subset [x]$ sehingga $[x] = [y]$. Oleh karena itu, setiap dua kelas ekuivalensi saling lepas atau tepat sama.

Sebaliknya, andaikan $\mathcal{P} = \{X_i\}$ merupakan partisi dari himpunan X. Nyatakan dua elemen ekuivalen jika keduanya berada dalam partisi yang sama. Jelas bahwa relasi tersebut refleksif. Jika x berada dalam partisi yang sama dengan y, maka y berada dalam partisi yang sama dengan x, sehingga $x \sim y$ mengakibatkan $y \sim x$. Terakhir, jika x berada dalam partisi yang sama dengan y dan y berada dalam partisi yang sama dengan z, maka x harus berada dalam partisi yang sama dengan z, sehingga transitivitas berlaku. ■

Korolari 1.2.26 *Dua kelas ekuivalensi dari suatu relasi ekuivalensi saling lepas atau sama.*

Mari kita telaah beberapa partisi yang diberikan oleh kelas-kelas ekuivalensi dalam rangkaian contoh terakhir.

Contoh 1.2.27 Dalam relasi ekuivalensi pada Contoh 1.2.21, dua pasangan bilangan bulat, (p, q) dan (r, s), berada dalam kelas ekuivalensi yang sama apabila keduanya disederhanakan menjadi pecahan yang sama dalam bentuk paling sederhana. ▲

Contoh 1.2.28 Dalam relasi ekuivalensi pada Contoh 1.2.22, dua fungsi $f(x)$ dan $g(x)$ berada dalam partisi yang sama apabila selisih keduanya merupakan konstanta. ▲

Contoh 1.2.29 Kita mendefinisikan kelas ekuivalensi pada $\mathbb{R}^2$ dengan $(x_1, y_1) \sim (x_2, y_2)$ jika $x_1^2 + y_1^2 = x_2^2 + y_2^2$. Dua pasangan bilangan real berada dalam partisi yang sama apabila keduanya terletak pada lingkaran yang sama berpusat di titik asal. ▲

Contoh 1.2.30 Misalkan r dan s adalah dua bilangan bulat dan andaikan $n \in \mathbb{N}$. Kita katakan bahwa r **kongruen** dengan s **modulo** n, atau r kongruen dengan s mod n, jika $r - s$ habis dibagi n; yaitu, $r - s = nk$ untuk suatu $k \in \mathbb{Z}$. Dalam hal ini kita tulis $r \equiv s \pmod{n}$. Sebagai contoh, $41 \equiv 17 \pmod{8}$ karena $41 - 17 = 24$ habis dibagi 8. Kita menyatakan bahwa kongruensi modulo n membentuk relasi ekuivalensi pada $\mathbb{Z}$. Tentu saja setiap bilangan bulat r ekuivalen dengan dirinya sendiri karena $r - r = 0$ habis dibagi n. Sekarang kita akan menunjukkan bahwa relasi tersebut simetris. Jika $r \equiv s \pmod{n}$, maka $r - s = -(s - r)$ habis dibagi n. Jadi $s - r$ habis dibagi n dan $s \equiv r \pmod{n}$. Sekarang andaikan $r \equiv s \pmod{n}$ dan $s \equiv t \pmod{n}$. Maka terdapat bilangan bulat k dan l sedemikian sehingga $r - s = kn$ dan $s - t = ln$. Untuk menunjukkan transitivitas, kita perlu membuktikan bahwa $r - t$ habis dibagi n. Namun,

$$r - t = r - s + s - t = kn + ln = (k + l)n,$$

sehingga $r - t$ habis dibagi n.

Jika kita meninjau relasi ekuivalensi yang ditentukan oleh bilangan bulat modulo 3, maka

$$\begin{aligned}
[0] &= \{\ldots, -3, 0, 3, 6, \ldots\}, \\
[1] &= \{\ldots, -2, 1, 4, 7, \ldots\}, \\
[2] &= \{\ldots, -1, 2, 5, 8, \ldots\}.
\end{aligned}$$

Perhatikan bahwa $[0] \cup [1] \cup [2] = \mathbb{Z}$ dan bahwa himpunan-himpunan tersebut saling lepas. Himpunan [0], [1], dan [2] membentuk partisi bilangan bulat.

Bilangan bulat modulo n merupakan contoh yang sangat penting dalam kajian aljabar abstrak dan akan sangat berguna dalam penyelidikan kita terhadap berbagai struktur aljabar seperti grup dan gelanggang. Dalam pembahasan bilangan bulat modulo n, sebenarnya kita telah mengasumsikan suatu hasil yang dikenal sebagai algoritma pembagian, yang akan dinyatakan dan dibuktikan dalam Bab 2. ▲

1.3 Pertanyaan Bacaan

1. Apa kesamaan antara relasi dan pemetaan?

2. Apa yang membedakan relasi dan pemetaan?

3. Nyatakan dengan cermat ketiga sifat yang mendefinisikan relasi ekuivalensi. Dengan kata lain, jangan sekadar *menyebutkan nama* sifat-sifat tersebut; berikan definisinya.

4. Mengapa relasi ekuivalensi begitu penting? (Petunjuk: Partisi.)

5. Jelaskan suatu teknik umum untuk membuktikan bahwa dua himpunan sama.

1.4 Latihan

1. Misalkan

$$A = \{x : x \in \mathbb{N} \text{ dan } x \text{ genap}\},$$
$$B = \{x : x \in \mathbb{N} \text{ dan } x \text{ prima}\},$$
$$C = \{x : x \in \mathbb{N} \text{ dan } x \text{ merupakan kelipatan } 5\}.$$

Deskripsikan setiap himpunan berikut.

(a) $A \cap B$ (c) $A \cup B$

(b) $B \cap C$ (d) $A \cap (B \cup C)$

Petunjuk. (a) $A \cap B = \{2\}$; (b) $B \cap C = \{5\}$.

2. Jika $A = \{a, b, c\}$, $B = \{1, 2, 3\}$, $C = \{x\}$, dan $D = \emptyset$, cantumkan semua elemen dalam setiap himpunan berikut.

(a) $A \times B$ (c) $A \times B \times C$

(b) $B \times A$ (d) $A \times D$

Petunjuk. (a) $A \times B = \{(a,1), (a,2), (a,3), (b,1), (b,2), (b,3), (c,1), (c,2), (c,3)\}$; (d) $A \times D = \emptyset$.

3. Temukan contoh dua himpunan takkosong A dan B yang memenuhi $A \times B = B \times A$.

4. Buktikan $A \cup \emptyset = A$ dan $A \cap \emptyset = \emptyset$.

5. Buktikan $A \cup B = B \cup A$ dan $A \cap B = B \cap A$.

6. Buktikan $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Petunjuk. Perhatikan bahwa $x \in A \cup B$ jika dan hanya jika $x \in A$ atau $x \in B$. Secara ekuivalen, $x \in B$ atau $x \in A$, yang sama dengan $x \in B \cup A$. Oleh karena itu, $A \cup B = B \cup A$.

7. Buktikan $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

8. Buktikan $A \subset B$ jika dan hanya jika $A \cap B = A$.

9. Buktikan $(A \cap B)' = A' \cup B'$.

10. Buktikan $A \cup B = (A \cap B) \cup (A \setminus B) \cup (B \setminus A)$.

Petunjuk. $(A \cap B) \cup (A \setminus B) \cup (B \setminus A) = (A \cap B) \cup (A \cap B') \cup (B \cap A') = [A \cap (B \cup B')] \cup (B \cap A') = A \cup (B \cap A') = (A \cup B) \cap (A \cup A') = A \cup B$.

11. Buktikan $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

12. Buktikan $(A \cap B) \setminus B = \emptyset$.

13. Buktikan $(A \cup B) \setminus B = A \setminus B$.

14. Buktikan $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Petunjuk. $A \setminus (B \cup C) = A \cap (B \cup C)' = (A \cap A) \cap (B' \cap C') = (A \cap B') \cap (A \cap C') = (A \setminus B) \cap (A \setminus C)$.

15. Buktikan $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$.

16. Buktikan $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$.

17. Manakah di antara relasi $f : \mathbb{Q} \to \mathbb{Q}$ berikut yang mendefinisikan pemetaan? Untuk setiap kasus, berikan alasan mengapa f merupakan atau bukan merupakan pemetaan.

(a) $f(p/q) = \dfrac{p+1}{p-2}$

(b) $f(p/q) = \dfrac{3p}{3q}$

(c) $f(p/q) = \dfrac{p+q}{q^2}$

(d) $f(p/q) = \dfrac{3p^2}{7q^2} - \dfrac{p}{q}$

Petunjuk. (a) Bukan pemetaan karena $f(2/3)$ tidak terdefinisi; (b) ini merupakan pemetaan; (c) bukan pemetaan, karena $f(1/2) = 3/4$ tetapi $f(2/4) = 3/8$; (d) ini merupakan pemetaan.

18. Tentukan fungsi berikut yang injektif dan yang surjektif. Jika fungsi tersebut tidak surjektif, tentukan daerah hasilnya.

(a) $f : \mathbb{R} \to \mathbb{R}$ yang didefinisikan oleh $f(x) = e^x$

(b) $f : \mathbb{Z} \to \mathbb{Z}$ yang didefinisikan oleh $f(n) = n^2 + 3$

(c) $f : \mathbb{R} \to \mathbb{R}$ yang didefinisikan oleh $f(x) = \sin x$

(d) $f : \mathbb{Z} \to \mathbb{Z}$ yang didefinisikan oleh $f(x) = x^2$

Petunjuk. (a) f injektif tetapi tidak surjektif. $f(\mathbb{R}) = \{x \in \mathbb{R} : x > 0\}$. (c) f tidak injektif maupun surjektif. $f(\mathbb{R}) = \{x : -1 \leq x \leq 1\}$.

19. Misalkan $f : A \to B$ dan $g : B \to C$ adalah pemetaan yang dapat dibalik; yaitu, pemetaan sedemikian sehingga f^{-1} dan g^{-1} ada. Tunjukkan bahwa $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

20.

(a) Definisikan fungsi $f : \mathbb{N} \to \mathbb{N}$ yang injektif tetapi tidak surjektif.

(b) Definisikan fungsi $f : \mathbb{N} \to \mathbb{N}$ yang surjektif tetapi tidak injektif.

Petunjuk. (a) $f(n) = n + 1$.

21. Buktikan bahwa relasi yang didefinisikan pada $\mathbb{R}^2$ oleh $(x_1, y_1) \sim (x_2, y_2)$ jika $x_1^2 + y_1^2 = x_2^2 + y_2^2$ merupakan relasi ekuivalensi.

22. Misalkan $f : A \to B$ dan $g : B \to C$ adalah pemetaan.

(a) Jika f dan g keduanya fungsi injektif, tunjukkan bahwa $g \circ f$ injektif.

(b) Jika $g \circ f$ surjektif, tunjukkan bahwa g surjektif.

(c) Jika $g \circ f$ injektif, tunjukkan bahwa f injektif.

(d) Jika $g \circ f$ injektif dan f surjektif, tunjukkan bahwa g injektif.

(e) Jika $g \circ f$ surjektif dan g injektif, tunjukkan bahwa f surjektif.

Petunjuk. (a) Misalkan $x, y \in A$. Maka $g(f(x)) = (g \circ f)(x) = (g \circ f)(y) = g(f(y))$. Jadi, $f(x) = f(y)$ dan $x = y$, sehingga $g \circ f$ injektif. (b) Misalkan $c \in C$, maka $c = (g \circ f)(x) = g(f(x))$ untuk suatu $x \in A$. Karena $f(x) \in B$, g surjektif.

23. Definisikan suatu fungsi pada bilangan real dengan

$$f(x) = \frac{x+1}{x-1}.$$

Apakah domain dan daerah hasil f? Apakah invers dari f? Hitung $f \circ f^{-1}$ dan $f^{-1} \circ f$.

Petunjuk. $f^{-1}(x) = (x+1)/(x-1)$.

24. Misalkan $f : X \to Y$ merupakan pemetaan dengan $A_1, A_2 \subset X$ dan $B_1, B_2 \subset Y$.

(a) Buktikan $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

(b) Buktikan $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$. Berikan contoh ketika kesamaan tidak berlaku.

(c) Buktikan $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$, dengan

$$f^{-1}(B) = \{x \in X : f(x) \in B\}.$$

(d) Buktikan $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.

(e) Buktikan $f^{-1}(Y \setminus B_1) = X \setminus f^{-1}(B_1)$.

Petunjuk. (a) Misalkan $y \in f(A_1 \cup A_2)$. Maka terdapat $x \in A_1 \cup A_2$ sedemikian sehingga $f(x) = y$. Jadi, $y \in f(A_1)$ atau $f(A_2)$. Oleh karena itu, $y \in f(A_1) \cup f(A_2)$. Akibatnya, $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$. Sebaliknya, jika $y \in f(A_1) \cup f(A_2)$, maka $y \in f(A_1)$ atau $f(A_2)$. Jadi, terdapat x dalam A_1 atau A_2 sedemikian sehingga $f(x) = y$. Dengan demikian, terdapat $x \in A_1 \cup A_2$ sedemikian sehingga $f(x) = y$. Oleh karena itu, $f(A_1) \cup f(A_2) \subset f(A_1 \cup A_2)$, dan $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

25. Tentukan apakah relasi-relasi berikut merupakan relasi ekuivalensi pada himpunan yang diberikan. Jika relasi tersebut merupakan relasi ekuivalensi, deskripsikan partisi yang dihasilkannya. Jika relasi tersebut bukan relasi ekuivalensi, nyatakan mengapa relasi itu gagal menjadi relasi ekuivalensi.

(a) $x \sim y$ dalam $\mathbb{R}$ jika $x \geq y$

(b) $m \sim n$ dalam $\mathbb{Z}$ jika $mn > 0$

(c) $x \sim y$ dalam $\mathbb{R}$ jika $|x-y| \leq 4$

(d) $m \sim n$ dalam $\mathbb{Z}$ jika $m \equiv n \pmod 6$

Petunjuk. (a) Relasi tersebut tidak simetris. (b) Relasi tersebut tidak refleksif, karena 0 tidak ekuivalen dengan dirinya sendiri. (c) Relasi tersebut tidak transitif.

26. Definisikan relasi $\sim$ pada $\mathbb{R}^2$ dengan menyatakan bahwa $(a, b) \sim (c, d)$ jika dan hanya jika $a^2 + b^2 \leq c^2 + d^2$. Tunjukkan bahwa $\sim$ refleksif dan transitif, tetapi tidak simetris.

27. Tunjukkan bahwa suatu matriks $m \times n$ menghasilkan pemetaan yang terdefinisi dengan baik dari $\mathbb{R}^n$ ke $\mathbb{R}^m$.

28. Temukan kesalahan dalam argumen berikut dengan memberikan contoh penyangkal. "Sifat refleksif berlebih dalam aksioma relasi ekuivalensi. Jika $x \sim y$, maka $y \sim x$ berdasarkan sifat simetris. Dengan menggunakan sifat transitif, kita dapat menyimpulkan bahwa $x \sim x$."

Petunjuk. Misalkan $X = \mathbb{N} \cup \{\sqrt{2}\}$ dan definisikan $x \sim y$ jika $x+y \in \mathbb{N}$.

29. Garis Real Proyektif. Definisikan suatu relasi pada $\mathbb{R}^2 \setminus \{(0,0)\}$ dengan menetapkan $(x_1, y_1) \sim (x_2, y_2)$ jika terdapat bilangan real taknol λ sedemikian sehingga $(x_1, y_1) = (\lambda x_2, \lambda y_2)$. Buktikan bahwa $\sim$ mendefinisikan relasi ekuivalensi pada $\mathbb{R}^2 \setminus (0,0)$. Apakah kelas-kelas ekuivalensi yang bersesuaian? Relasi ekuivalensi ini mendefinisikan garis proyektif, yang dilambangkan dengan $\mathbb{P}(\mathbb{R})$, dan sangat penting dalam geometri.

1.5 Referensi dan Bacaan yang Disarankan

[**1**] Artin, M. *Algebra (Classic Version).* 2nd ed. Pearson, Upper Saddle River, NJ, 2018.

[**2**] Childs, L. *A Concrete Introduction to Higher Algebra.* 2nd ed. Springer-Verlag, New York, 1995.

[**3**] Dummit, D. and Foote, R. *Abstract Algebra.* 3rd ed. Wiley, New York, 2003.

[**4**] Ehrlich, G. *Fundamental Concepts of Algebra.* PWS-KENT, Boston, 1991.

[**5**] Fraleigh, J. B. *A First Course in Abstract Algebra.* 7th ed. Pearson, Upper Saddle River, NJ, 2003.

[**6**] Gallian, J. A. *Contemporary Abstract Algebra.* 7th ed. Brooks/Cole, Belmont, CA, 2009.

[**7**] Halmos, P. *Naive Set Theory.* Springer, New York, 1991. Salah satu referensi terbaik untuk teori himpunan.

[**8**] Herstein, I. N. *Abstract Algebra.* 3rd ed. Wiley, New York, 1996.

[**9**] Hungerford, T. W. *Algebra.* Springer, New York, 1974. Salah satu buku teks aljabar baku untuk tingkat pascasarjana.

[**10**] Lang, S. *Algebra.* 3rd ed. Springer, New York, 2002. Buku teks baku lain untuk tingkat pascasarjana.

[**11**] Lidl, R. and Pilz, G. *Applied Abstract Algebra.* 2nd ed. Springer, New York, 1998.

[**12**] Mackiw, G. *Applications of Abstract Algebra.* Wiley, New York, 1985.

[**13**] Nickelson, W. K. *Introduction to Abstract Algebra.* 3rd ed. Wiley, New York, 2006.

[**14**] Solow, D. *How to Read and Do Proofs.* 5th ed. Wiley, New York, 2009.

[**15**] van der Waerden, B. L. *A History of Algebra.* Springer-Verlag, New York, 1985. Uraian mengenai perkembangan historis aljabar.

2

Bilangan Bulat

Bilangan bulat merupakan unsur pembangun matematika. Dalam bab ini kita akan menyelidiki sifat-sifat dasar bilangan bulat, termasuk induksi matematis, algoritma pembagian, dan Teorema Dasar Aritmetika.

2.1 Induksi Matematis

Misalkan kita ingin menunjukkan bahwa

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

untuk setiap bilangan asli n. Rumus ini mudah diperiksa untuk bilangan-bilangan kecil seperti $n = 1$, 2, 3, atau 4, tetapi mustahil memeriksanya satu per satu untuk semua bilangan asli. Untuk membuktikan bahwa rumus tersebut berlaku secara umum, diperlukan metode yang lebih umum.

Misalkan kita telah memeriksa persamaan tersebut untuk n kasus pertama. Kita akan menunjukkan bahwa dari pengetahuan ini kita dapat memperoleh rumus untuk kasus ke-$(n+1)$. Rumus tersebut benar untuk $n = 1$ karena

$$1 = \frac{1(1+1)}{2}.$$

Jika kita telah memeriksa n kasus pertama, maka

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + n + 1 \\ &= \frac{n^2 + 3n + 2}{2} \\ &= \frac{(n+1)[(n+1)+1]}{2}. \end{aligned}$$

Ini tepat merupakan rumus untuk kasus ke-$(n+1)$.

Metode pembuktian ini dikenal sebagai **induksi matematis**. Alih-alih mencoba memeriksa satu per satu suatu pernyataan mengenai himpunan bagian S dari bilangan bulat positif $\mathbb{N}$, suatu tugas yang mustahil jika S merupakan himpunan tak hingga, kita memberikan bukti khusus untuk bilangan bulat terkecil yang sedang dipertimbangkan, diikuti argumen umum yang menunjukkan bahwa jika pernyataan itu berlaku untuk suatu kasus, maka pernyataan tersebut juga harus berlaku untuk kasus berikutnya dalam barisan. Induksi matematis dirangkum dalam aksioma berikut.

Prinsip 2.1.1 Prinsip Pertama Induksi Matematis. *Misalkan $S(n)$ merupakan suatu pernyataan tentang bilangan bulat untuk $n \in \mathbb{N}$, dan misalkan $S(n_0)$ benar untuk suatu bilangan bulat n_0. Jika untuk setiap bilangan bulat k dengan $k \geq n_0$, $S(k)$ mengakibatkan $S(k+1)$ benar, maka $S(n)$ benar untuk setiap bilangan bulat n yang lebih besar daripada atau sama dengan n_0.*

Contoh 2.1.2 Untuk setiap bilangan bulat $n \geq 3$, berlaku $2^n > n+4$. Karena

$$8 = 2^3 > 3 + 4 = 7,$$

pernyataan tersebut benar untuk $n_0 = 3$. Andaikan $2^k > k + 4$ untuk $k \geq 3$. Maka $2^{k+1} = 2 \cdot 2^k > 2(k + 4)$. Namun,

$$2(k + 4) = 2k + 8 > k + 5 = (k + 1) + 4$$

karena k positif. Jadi, berdasarkan induksi, pernyataan tersebut berlaku untuk setiap bilangan bulat $n \geq 3$. ▲

Contoh 2.1.3 Setiap bilangan bulat $10^{n+1} + 3 \cdot 10^n + 5$ habis dibagi 9 untuk $n \in \mathbb{N}$. Untuk $n = 1$,

$$10^{1+1} + 3 \cdot 10 + 5 = 135 = 9 \cdot 15$$

habis dibagi 9. Misalkan $10^{k+1} + 3 \cdot 10^k + 5$ habis dibagi 9 untuk $k \geq 1$. Maka

$$\begin{aligned} 10^{(k+1)+1} + 3 \cdot 10^{k+1} + 5 &= 10^{k+2} + 3 \cdot 10^{k+1} + 50 - 45 \\ &= 10(10^{k+1} + 3 \cdot 10^k + 5) - 45 \end{aligned}$$

habis dibagi 9. ▲

Contoh 2.1.4 Kita akan membuktikan teorema binomial dengan induksi matematis; yaitu,

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k},$$

dengan a dan b bilangan real, $n \in \mathbb{N}$, dan

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

merupakan koefisien binomial. Pertama-tama kita tunjukkan bahwa

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Hasil ini diperoleh dari

$$\begin{aligned} \binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= \frac{(n+1)!}{k!(n+1-k)!} \\ &= \binom{n+1}{k}. \end{aligned}$$

Jika $n = 1$, teorema binomial mudah diperiksa. Sekarang andaikan hasil tersebut benar untuk n yang lebih besar daripada atau sama dengan 1. Maka

$$(a + b)^{n+1} = (a + b)(a + b)^n$$

$$
\begin{aligned}
&= (a+b)\left(\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}\right)\\
&= \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k}\\
&= a^{n+1} + \sum_{k=1}^{n}\binom{n}{k-1}a^k b^{n+1-k} + \sum_{k=1}^{n}\binom{n}{k}a^k b^{n+1-k} + b^{n+1}\\
&= a^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k-1} + \binom{n}{k}\right]a^k b^{n+1-k} + b^{n+1}\\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}.
\end{aligned}
$$

▲

Terdapat bentuk ekuivalen dari Prinsip Induksi Matematis yang sering kali sangat berguna.

Prinsip 2.1.5 Prinsip Kedua Induksi Matematis. *Misalkan $S(n)$ merupakan suatu pernyataan tentang bilangan bulat untuk $n \in \mathbb{N}$, dan misalkan $S(n_0)$ benar untuk suatu bilangan bulat n_0. Jika $S(n_0), S(n_0+1), \ldots, S(k)$ mengakibatkan $S(k+1)$ benar untuk $k \geq n_0$, maka pernyataan $S(n)$ benar untuk setiap bilangan bulat $n \geq n_0$.*

Suatu himpunan bagian tak kosong S dari $\mathbb{Z}$ disebut **terurut baik** jika S memuat suatu elemen terkecil. Perhatikan bahwa himpunan $\mathbb{Z}$ tidak terurut baik karena tidak memuat elemen terkecil. Akan tetapi, bilangan asli terurut baik.

Prinsip 2.1.6 Prinsip Urutan Baik. *Setiap himpunan bagian tak kosong dari bilangan asli terurut baik.*

Prinsip Urutan Baik ekuivalen dengan Prinsip Induksi Matematis.

Lema 2.1.7 *Prinsip Induksi Matematis mengakibatkan bahwa 1 merupakan bilangan asli positif terkecil.*

Bukti. Misalkan $S = \{n \in \mathbb{N} : n \geq 1\}$. Maka $1 \in S$. Andaikan $n \in S$. Karena $0 < 1$, harus berlaku $n = n+0 < n+1$. Oleh karena itu, $1 \leq n < n+1$. Akibatnya, jika $n \in S$, maka $n+1$ juga harus berada dalam S, dan berdasarkan Prinsip Induksi Matematis kita memperoleh $S = \mathbb{N}$. ■

Teorema 2.1.8 *Prinsip Induksi Matematis mengakibatkan Prinsip Urutan Baik. Artinya, setiap himpunan bagian tak kosong dari $\mathbb{N}$ memuat suatu elemen terkecil.*

Bukti. Kita harus menunjukkan bahwa jika S merupakan himpunan bagian tak kosong dari bilangan asli, maka S memuat suatu elemen terkecil. Jika S memuat 1, maka teorema ini benar berdasarkan Lema 2.1.7. Andaikan bahwa jika S memuat suatu bilangan bulat k sedemikian sehingga $1 \leq k \leq n$, maka S memuat suatu elemen terkecil. Kita akan menunjukkan bahwa jika suatu himpunan S memuat bilangan bulat yang lebih kecil daripada atau sama dengan $n+1$, maka S mempunyai suatu elemen terkecil. Jika S tidak memuat bilangan bulat yang lebih kecil daripada $n+1$, maka $n+1$ merupakan bilangan bulat terkecil dalam S. Jika tidak demikian, karena S tak kosong, S harus memuat bilangan bulat yang lebih kecil daripada atau sama dengan n. Dalam hal ini, berdasarkan induksi, S memuat suatu elemen terkecil. ■

Induksi juga dapat sangat berguna dalam merumuskan definisi. Sebagai

contoh, ada dua cara untuk mendefinisikan $n!$, yaitu faktorial dari bilangan bulat positif n.

- Definisi *eksplisit*: $n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$.
- Definisi *induktif* atau *rekursif*: $1! = 1$ dan $n! = n(n-1)!$ untuk $n > 1$.

Setiap matematikawan atau ilmuwan komputer yang baik mengetahui bahwa memandang masalah secara rekursif, alih-alih secara eksplisit, sering kali menghasilkan pemahaman yang lebih baik terhadap persoalan rumit.

2.2 Algoritma Pembagian

Salah satu penerapan Prinsip Urutan Baik yang akan sering kita gunakan adalah algoritma pembagian.

Teorema 2.2.1 Algoritma Pembagian. *Misalkan a dan b bilangan bulat, dengan $b > 0$. Maka terdapat bilangan bulat unik q dan r sedemikian sehingga*

$$a = bq + r$$

dengan $0 \leq r < b$.

Bukti. Ini merupakan contoh sempurna dari jenis bukti keberadaan dan ketunggalan. Pertama-tama kita harus membuktikan bahwa bilangan q dan r benar-benar ada. Kemudian kita harus menunjukkan bahwa jika q' dan r' merupakan dua bilangan lain dengan sifat tersebut, maka $q = q'$ dan $r = r'$.

Keberadaan q dan r. Misalkan

$$S = \{a - bk : k \in \mathbb{Z} \text{ dan } a - bk \geq 0\}.$$

Jika $0 \in S$, maka b membagi a, dan kita dapat mengambil $q = a/b$ dan $r = 0$. Jika $0 \notin S$, kita dapat menggunakan Prinsip Urutan Baik. Pertama-tama kita harus menunjukkan bahwa S tak kosong. Jika $a > 0$, maka $a - b \cdot 0 \in S$. Jika $a < 0$, maka $a - b(2a) = a(1 - 2b) \in S$. Dalam kedua kasus tersebut, $S \neq \emptyset$. Berdasarkan Prinsip Urutan Baik, S harus mempunyai anggota terkecil, misalkan $r = a - bq$. Oleh karena itu, $a = bq + r$, dengan $r \geq 0$. Sekarang kita tunjukkan bahwa $r < b$. Misalkan $r > b$. Maka

$$a - b(q+1) = a - bq - b = r - b > 0.$$

Dalam hal ini, $a - b(q+1)$ akan berada dalam himpunan S. Akan tetapi, $a - b(q+1) < a - bq$, yang bertentangan dengan fakta bahwa $r = a - bq$ merupakan anggota terkecil dari S. Jadi $r \leq b$. Karena $0 \notin S$, berlaku $r \neq b$, sehingga $r < b$.

Ketunggalan q dan r. *Ketunggalan q dan r.* Misalkan terdapat bilangan bulat r, r', q, dan q' sedemikian sehingga

$$a = bq + r, 0 \leq r < b \quad \text{dan} \quad a = bq' + r', 0 \leq r' < b.$$

Maka $bq + r = bq' + r'$. Andaikan $r' \geq r$. Dari persamaan terakhir diperoleh $b(q - q') = r' - r$; oleh karena itu, b harus membagi $r' - r$ dan $0 \leq r' - r \leq r' < b$. Hal ini hanya mungkin jika $r' - r = 0$. Jadi, $r = r'$ dan $q = q'$. ■

Misalkan a dan b bilangan bulat. Jika $b = ak$ untuk suatu bilangan bulat k, kita tulis $a \mid b$. Suatu bilangan bulat d disebut **pembagi bersama** dari a dan b jika $d \mid a$ dan $d \mid b$. **Faktor persekutuan terbesar** (FPB) dari bilangan

bulat a dan b adalah bilangan bulat positif d sedemikian sehingga d merupakan pembagi bersama dari a dan b, dan jika d' adalah pembagi bersama lain dari a dan b, maka $d' \mid d$. Kita tulis $d = \gcd(a, b)$; sebagai contoh, $\gcd(24, 36) = 12$ dan $\gcd(120, 102) = 6$. Dua bilangan bulat a dan b disebut **relatif prima** jika $\gcd(a, b) = 1$.

Teorema 2.2.2 *Misalkan a dan b bilangan bulat tak nol. Maka terdapat bilangan bulat r dan s sedemikian sehingga*

$$\gcd(a, b) = ar + bs.$$

Lebih lanjut, faktor persekutuan terbesar dari a dan b bersifat tunggal.

Bukti. Misalkan

$$S = \{am + bn : m, n \in \mathbb{Z} \text{ dan } am + bn > 0\}.$$

Jelas bahwa himpunan S tak kosong; maka, berdasarkan Prinsip Urutan Baik, S harus mempunyai anggota terkecil, misalkan $d = ar + bs$. Kita menyatakan bahwa $d = \gcd(a, b)$. Tuliskan $a = dq + r'$ dengan $0 \leq r' < d$. Jika $r' > 0$, maka

$$\begin{aligned} r' &= a - dq \\ &= a - (ar + bs)q \\ &= a - arq - bsq \\ &= a(1 - rq) + b(-sq), \end{aligned}$$

yang berada dalam S. Namun, hal ini bertentangan dengan fakta bahwa d merupakan anggota terkecil dari S. Jadi, $r' = 0$ dan d membagi a. Argumen serupa menunjukkan bahwa d membagi b. Oleh karena itu, d merupakan pembagi bersama dari a dan b.

Misalkan d' merupakan pembagi bersama lain dari a dan b, dan kita ingin menunjukkan bahwa $d' \mid d$. Jika kita mengambil $a = d'h$ dan $b = d'k$, maka

$$d = ar + bs = d'hr + d'ks = d'(hr + ks).$$

Jadi d' harus membagi d. Dengan demikian, d harus merupakan satu-satunya faktor persekutuan terbesar dari a dan b. ■

Korolari 2.2.3 *Misalkan a dan b dua bilangan bulat yang relatif prima. Maka terdapat bilangan bulat r dan s sedemikian sehingga $ar + bs = 1$.*

2.2.1 Algoritma Euklides

Salah satu kegunaan Teorema 2.2.2 adalah memungkinkan kita menghitung faktor persekutuan terbesar dari dua bilangan bulat.

Contoh 2.2.4 Mari kita hitung faktor persekutuan terbesar dari 945 dan 2415. Pertama, perhatikan bahwa

$$\begin{aligned} 2415 &= 945 \cdot 2 + 525 \\ 945 &= 525 \cdot 1 + 420 \\ 525 &= 420 \cdot 1 + 105 \\ 420 &= 105 \cdot 4 + 0. \end{aligned}$$

Dengan menelusuri langkah-langkah tersebut secara terbalik, 105 membagi 420, 105 membagi 525, 105 membagi 945, dan 105 membagi 2415. Jadi, 105 memba-

gi baik 945 maupun 2415. Jika d merupakan pembagi bersama lain dari 945 dan 2415, maka d juga harus membagi 105. Oleh karena itu, $\gcd(945, 2415) = 105$.

Jika kita menelusuri barisan persamaan di atas secara terbalik, kita juga dapat memperoleh bilangan r dan s sedemikian sehingga $945r + 2415s = 105$. Perhatikan bahwa

$$\begin{aligned} 105 &= 525 + (-1) \cdot 420 \\ &= 525 + (-1) \cdot [945 + (-1) \cdot 525] \\ &= 2 \cdot 525 + (-1) \cdot 945 \\ &= 2 \cdot [2415 + (-2) \cdot 945] + (-1) \cdot 945 \\ &= 2 \cdot 2415 + (-5) \cdot 945. \end{aligned}$$

Jadi $r = -5$ dan $s = 2$. Perhatikan bahwa r dan s tidak tunggal, karena $r = 41$ dan $s = -16$ juga memenuhi. ▲

Untuk menghitung $\gcd(a, b) = d$, kita menggunakan pembagian berulang untuk memperoleh barisan menurun bilangan bulat positif $r_1 > r_2 > \cdots > r_n = d$; yaitu,

$$\begin{aligned} b &= aq_1 + r_1 \\ a &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_{n+1}. \end{aligned}$$

Untuk mencari r dan s sedemikian sehingga $ar + bs = d$, kita mulai dengan persamaan terakhir ini dan menyubstitusikan hasil yang diperoleh dari persamaan-persamaan sebelumnya:

$$\begin{aligned} d &= r_n \\ &= r_{n-2} - r_{n-1}q_n \\ &= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\ &= -q_nr_{n-3} + (1 + q_nq_{n-1})r_{n-2} \\ &\vdots \\ &= ra + sb. \end{aligned}$$

Algoritma yang baru saja kita gunakan untuk mencari faktor persekutuan terbesar d dari dua bilangan bulat a dan b, serta menuliskan d sebagai kombinasi linear dari a dan b, dikenal sebagai **algoritma Euklides**.

2.2.2 Bilangan Prima

Misalkan p bilangan bulat sedemikian sehingga $p > 1$. Bilangan p disebut **bilangan prima**, atau cukup dikatakan p **prima**, jika satu-satunya bilangan positif yang membagi p adalah 1 dan p itu sendiri. Bilangan bulat $n > 1$ yang tidak prima disebut **komposit**.

Lema 2.2.5 Euclid. *Misalkan a dan b bilangan bulat dan p bilangan prima. Jika $p \mid ab$, maka $p \mid a$ atau $p \mid b$.*

Bukti. Misalkan p tidak membagi a. Kita harus menunjukkan bahwa $p \mid b$. Karena $\gcd(a, p) = 1$, terdapat bilangan bulat r dan s sedemikian sehingga

$ar + ps = 1$. Jadi,

$$b = b(ar + ps) = (ab)r + p(bs).$$

Karena p membagi baik ab maupun dirinya sendiri, p harus membagi $b = (ab)r + p(bs)$. ■

Teorema 2.2.6 Euclid. *Terdapat tak hingga banyaknya bilangan prima.*

BUKTI. Kita akan membuktikan teorema ini dengan kontradiksi. Misalkan hanya terdapat berhingga banyaknya bilangan prima, yaitu $p_1, p_2, \ldots, p_n$. Misalkan $P = p_1 p_2 \cdots p_n + 1$. Maka P harus habis dibagi oleh suatu p_i untuk $1 \leq i \leq n$. Dalam hal ini, p_i harus membagi $P - p_1 p_2 \cdots p_n = 1$, suatu kontradiksi. Jadi, P prima atau terdapat bilangan prima tambahan $p \neq p_i$ yang membagi P. ■

Teorema 2.2.7 Teorema Dasar Aritmetika. *Misalkan n bilangan bulat sedemikian sehingga $n > 1$. Maka*

$$n = p_1 p_2 \cdots p_k,$$

dengan $p_1, \ldots, p_k$ bilangan prima (tidak harus berbeda). Lebih lanjut, faktorisasi ini tunggal; yaitu, jika

$$n = q_1 q_2 \cdots q_l,$$

maka $k = l$ dan q_i hanyalah p_i yang urutannya disusun ulang.

BUKTI.

Ketunggalan. Untuk menunjukkan ketunggalan, kita akan menggunakan induksi pada n. Teorema ini tentu benar untuk $n = 2$ karena dalam hal ini n prima. Sekarang andaikan hasil tersebut berlaku untuk setiap bilangan bulat m sedemikian sehingga $1 \leq m < n$, dan

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l,$$

dengan $p_1 \leq p_2 \leq \cdots \leq p_k$ dan $q_1 \leq q_2 \leq \cdots \leq q_l$. Berdasarkan Lema 2.2.5, berlaku $p_1 \mid q_i$ untuk suatu $i = 1, \ldots, l$ dan $q_1 \mid p_j$ untuk suatu $j = 1, \ldots, k$. Karena semua p_i dan q_i adalah prima, berlaku $p_1 = q_i$ dan $q_1 = p_j$. Jadi, $p_1 = q_1$ karena $p_1 \leq p_j = q_1 \leq q_i = p_1$. Berdasarkan hipotesis induksi,

$$n' = p_2 \cdots p_k = q_2 \cdots q_l$$

mempunyai faktorisasi tunggal. Jadi, $k = l$ dan $q_i = p_i$ untuk $i = 1, \ldots, k$.

Keberadaan. Untuk menunjukkan keberadaan, misalkan terdapat suatu bilangan bulat yang tidak dapat ditulis sebagai hasil kali bilangan-bilangan prima. Misalkan S himpunan semua bilangan tersebut. Berdasarkan Prinsip Urutan Baik, S mempunyai bilangan terkecil, misalkan a. Jika satu-satunya faktor positif dari a adalah a dan 1, maka a prima, suatu kontradiksi. Jadi, $a = a_1 a_2$ dengan $1 < a_1 < a$ dan $1 < a_2 < a$. Tidak berlaku $a_1 \in S$ maupun $a_2 \in S$, karena a merupakan elemen terkecil dalam S. Jadi,

$$a_1 = p_1 \cdots p_r$$
$$a_2 = q_1 \cdots q_s.$$

Oleh karena itu,

$$a = a_1 a_2 = p_1 \cdots p_r q_1 \cdots q_s.$$

Jadi $a \notin S$, suatu kontradiksi. ■

Catatan Sejarah

Bilangan prima pertama kali dipelajari oleh orang Yunani kuno. Dua hasil penting dari zaman kuno adalah bukti Euklides bahwa terdapat tak hingga banyaknya bilangan prima dan Saringan Eratosthenes, suatu metode untuk menghitung semua bilangan prima yang lebih kecil daripada bilangan bulat positif tetap n. Salah satu masalah dalam teori bilangan adalah mencari fungsi f sedemikian sehingga $f(n)$ prima untuk setiap bilangan bulat n. Pierre Fermat (1601?–1665) menduga bahwa $2^{2^n}+1$ prima untuk setiap n, tetapi kemudian Leonhard Euler (1707–1783) menunjukkan bahwa

$$2^{2^5}+1 = 4{,}294{,}967{,}297$$

merupakan bilangan komposit. Salah satu dari banyak dugaan mengenai bilangan prima yang belum terbukti adalah Dugaan Goldbach. Dalam sebuah surat kepada Euler pada tahun 1742, Christian Goldbach mengemukakan dugaan bahwa setiap bilangan bulat genap selain 2 tampaknya merupakan jumlah dua bilangan prima: $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, ... Meskipun dugaan tersebut telah diperiksa untuk bilangan-bilangan hingga 4×10^{18}, dugaan itu masih belum terbukti secara umum. Karena bilangan prima memegang peranan penting dalam kriptografi kunci publik, saat ini terdapat minat yang sangat besar untuk menentukan apakah suatu bilangan besar merupakan bilangan prima.

2.3 Pertanyaan Bacaan

1. Gunakan Sage untuk menyatakan 123456792 sebagai hasil kali bilangan-bilangan prima.

2. Tentukan faktor persekutuan terbesar dari 84 dan 52.

3. Tentukan bilangan bulat r dan s sedemikian sehingga $r(84) + s(52) = \gcd(84, 52)$.

4. Jelaskan penggunaan istilah "hipotesis induksi."

5. Apakah Dugaan Goldbach itu? Mengapa pernyataan tersebut disebut "dugaan"?

2.4 Latihan

1. Buktikan bahwa

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

untuk $n \in \mathbb{N}$.

Petunjuk. Kasus dasar, $S(1) : [1(1+1)(2(1)+1)]/6 = 1 = 1^2$, benar. Andaikan $S(k) : 1^2 + 2^2 + \cdots + k^2 = [k(k+1)(2k+1)]/6$ benar. Maka

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= [k(k+1)(2k+1)]/6 + (k+1)^2 \\ &= [(k+1)((k+1)+1)(2(k+1)+1)]/6, \end{aligned}$$

sehingga $S(k+1)$ benar. Jadi, $S(n)$ benar untuk setiap bilangan bulat positif n.

2. Buktikan bahwa

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$

untuk $n \in \mathbb{N}$.

3. Buktikan bahwa $n! > 2^n$ untuk $n \geq 4$.

Petunjuk. Kasus dasar, $S(4) : 4! = 24 > 16 = 2^4$, benar. Andaikan $S(k) : k! > 2^k$ benar. Maka $(k+1)! = k!(k+1) > 2^k \cdot 2 = 2^{k+1}$, sehingga $S(k+1)$ benar. Jadi, $S(n)$ benar untuk setiap bilangan bulat positif n.

4. Buktikan bahwa

$$x + 4x + 7x + \cdots + (3n-2)x = \frac{n(3n-1)x}{2}$$

untuk $n \in \mathbb{N}$.

5. Buktikan bahwa $10^{n+1} + 10^n + 1$ habis dibagi 3 untuk $n \in \mathbb{N}$.

6. Buktikan bahwa $4 \cdot 10^{2n} + 9 \cdot 10^{2n-1} + 5$ habis dibagi 99 untuk $n \in \mathbb{N}$.

7. Tunjukkan bahwa

$$\sqrt[n]{a_1 a_2 \cdots a_n} \leq \frac{1}{n} \sum_{k=1}^{n} a_k.$$

8. Buktikan aturan Leibniz untuk $f^{(n)}(x)$, dengan $f^{(n)}$ turunan ke-n dari f; yaitu, tunjukkan bahwa

$$(fg)^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}(x) g^{(n-k)}(x).$$

Petunjuk. Ikuti pembuktian dalam Contoh 2.1.4.

9. Gunakan induksi untuk membuktikan bahwa $1+2+2^2+\cdots+2^n = 2^{n+1}-1$ untuk $n \in \mathbb{N}$.

10. Buktikan bahwa

$$\frac{1}{2} + \frac{1}{6} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

untuk $n \in \mathbb{N}$.

11. Jika x merupakan bilangan real tak negatif, tunjukkan bahwa $(1+x)^n - 1 \geq nx$ untuk $n = 0, 1, 2, \ldots$.

Petunjuk. Kasus dasar, $S(0) : (1+x)^0 - 1 = 0 \geq 0 = 0 \cdot x$, benar. Andaikan $S(k) : (1+x)^k - 1 \geq kx$ benar. Maka

$$\begin{aligned}(1+x)^{k+1} - 1 &= (1+x)(1+x)^k - 1 \\ &= (1+x)^k + x(1+x)^k - 1 \\ &\geq kx + x(1+x)^k \\ &\geq kx + x \\ &= (k+1)x,\end{aligned}$$

sehingga $S(k+1)$ benar. Oleh karena itu, $S(n)$ benar untuk setiap bilangan bulat positif n.

12. **Himpunan Kuasa.** Misalkan X suatu himpunan. Definisikan **himpunan kuasa** dari X, yang dinotasikan dengan $\mathcal{P}(X)$, sebagai himpunan semua himpunan bagian dari X. Sebagai contoh,

$$\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}.$$

Untuk setiap bilangan bulat positif n, tunjukkan bahwa suatu himpunan yang mempunyai tepat n elemen memiliki himpunan kuasa dengan tepat

2^n elemen.

13. Buktikan bahwa kedua prinsip induksi matematis yang dinyatakan dalam Bagian 2.1 ekuivalen.

14. Tunjukkan bahwa Prinsip Urutan Baik untuk bilangan asli mengakibatkan bahwa 1 merupakan bilangan asli terkecil. Gunakan hasil ini untuk menunjukkan bahwa Prinsip Urutan Baik mengakibatkan Prinsip Induksi Matematis; yaitu, tunjukkan bahwa jika $S \subset \mathbb{N}$ sedemikian sehingga $1 \in S$ dan $n+1 \in S$ setiap kali $n \in S$, maka $S = \mathbb{N}$.

15. Untuk setiap pasangan bilangan a dan b berikut, hitung $\gcd(a,b)$ dan tentukan bilangan bulat r dan s sedemikian sehingga $\gcd(a,b) = ra + sb$.

(a) 14 dan 39

(b) 234 dan 165

(c) 1739 dan 9923

(d) 471 dan 562

(e) 23771 dan 19945

(f) -4357 dan 3754

16. Misalkan a dan b bilangan bulat tak nol. Jika terdapat bilangan bulat r dan s sedemikian sehingga $ar + bs = 1$, tunjukkan bahwa a dan b relatif prima.

17. **Bilangan Fibonacci.** Bilangan Fibonacci adalah

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots.$$

Kita dapat mendefinisikannya secara induktif dengan $f_1 = 1$, $f_2 = 1$, dan $f_{n+2} = f_{n+1} + f_n$ untuk $n \in \mathbb{N}$.

(a) Buktikan bahwa $f_n < 2^n$.

(b) Buktikan bahwa $f_{n+1}f_{n-1} = f_n^2 + (-1)^n$, $n \geq 2$.

(c) Buktikan bahwa $f_n = [(1+\sqrt{5}\,)^n - (1-\sqrt{5}\,)^n]/2^n\sqrt{5}$.

(d) Tunjukkan bahwa $\phi = \lim_{n\to\infty} f_{n+1}/f_n = (\sqrt{5}+1)/2$. Konstanta ϕ dikenal sebagai **nisbah emas**.

(e) Buktikan bahwa f_n dan f_{n+1} relatif prima.

Petunjuk. Untuk (a) dan (b), gunakan induksi matematis. (c) Tunjukkan bahwa $f_1 = 1$, $f_2 = 1$, dan $f_{n+2} = f_{n+1} + f_n$. (e) Gunakan bagian (b) dan Latihan 2.4.16.

18. Misalkan a dan b bilangan bulat sedemikian sehingga $\gcd(a,b) = 1$. Misalkan r dan s bilangan bulat sedemikian sehingga $ar + bs = 1$. Buktikan bahwa

$$\gcd(a,s) = \gcd(r,b) = \gcd(r,s) = 1.$$

19. Misalkan $x, y \in \mathbb{N}$ relatif prima. Jika xy merupakan kuadrat sempurna, buktikan bahwa x dan y keduanya harus merupakan kuadrat sempurna.

Petunjuk. Gunakan Teorema Dasar Aritmetika.

20. Dengan menggunakan algoritma pembagian, tunjukkan bahwa setiap kuadrat sempurna berbentuk $4k$ atau $4k+1$ untuk suatu bilangan bulat tak negatif k.

21. Misalkan a, b, r, s relatif prima secara berpasangan dan

$$a^2 + b^2 = r^2$$
$$a^2 - b^2 = s^2.$$

Buktikan bahwa a, r, dan s ganjil, sedangkan b genap.

22. Misalkan $n \in \mathbb{N}$. Gunakan algoritma pembagian untuk membuktikan bahwa setiap bilangan bulat kongruen modulo n dengan tepat salah satu dari bilangan bulat $0, 1, \ldots, n-1$. Simpulkan bahwa jika r bilangan bulat, maka terdapat tepat satu s dalam $\mathbb{Z}$ sedemikian sehingga $0 \leq s < n$ dan $[r] = [s]$. Jadi, bilangan bulat memang terpartisi oleh kekongruenan modulo n.

23. Definisikan **kelipatan persekutuan terkecil** dari dua bilangan bulat tak nol a dan b, yang dinotasikan dengan $\text{lcm}(a, b)$, sebagai bilangan bulat tak negatif m sedemikian sehingga a dan b keduanya membagi m, dan jika a dan b membagi suatu bilangan bulat lain n, maka m juga membagi n. Buktikan bahwa terdapat kelipatan persekutuan terkecil yang tunggal untuk sebarang dua bilangan bulat a dan b.

Petunjuk. Gunakan Prinsip Urutan Baik dan algoritma pembagian.

24. Jika $d = \text{gcd}(a, b)$ dan $m = \text{lcm}(a, b)$, buktikan bahwa $dm = |ab|$.

25. Tunjukkan bahwa $\text{lcm}(a, b) = ab$ jika dan hanya jika $\text{gcd}(a, b) = 1$.

26. Buktikan bahwa $\text{gcd}(a, c) = \text{gcd}(b, c) = 1$ jika dan hanya jika $\text{gcd}(ab, c) = 1$ untuk bilangan bulat a, b, dan c.

27. Misalkan $a, b, c \in \mathbb{Z}$. Buktikan bahwa jika $\text{gcd}(a, b) = 1$ dan $a \mid bc$, maka $a \mid c$.

Petunjuk. Karena $\text{gcd}(a, b) = 1$, terdapat bilangan bulat r dan s sedemikian sehingga $ar + bs = 1$. Jadi, $acr + bcs = c$.

28. Misalkan $p \geq 2$. Buktikan bahwa jika $2^p - 1$ prima, maka p juga harus prima.

29. Buktikan bahwa terdapat tak hingga banyaknya bilangan prima berbentuk $6n + 5$.

Petunjuk. Setiap bilangan prima harus berbentuk 2, 3, $6n + 1$, atau $6n + 5$. Misalkan hanya terdapat berhingga banyaknya bilangan prima berbentuk $6k + 5$.

30. Buktikan bahwa terdapat tak hingga banyaknya bilangan prima berbentuk $4n - 1$.

31. Dengan menggunakan fakta bahwa 2 prima, tunjukkan bahwa tidak terdapat bilangan bulat p dan q sedemikian sehingga $p^2 = 2q^2$. Tunjukkan bahwa oleh karena itu $\sqrt{2}$ tidak mungkin merupakan bilangan rasional.

2.5 Latihan Pemrograman

1. **Saringan Eratosthenes.** Salah satu metode untuk menghitung semua bilangan prima yang lebih kecil daripada bilangan bulat positif tetap N adalah mencantumkan semua bilangan n sedemikian sehingga $1 < n < N$. Mulailah dengan mencoret semua kelipatan 2. Selanjutnya, coret semua kelipatan 3. Kemudian coret semua kelipatan 5. Perhatikan bahwa 4 sudah dicoret. Lanjutkan dengan cara ini, dengan memperhatikan bahwa kita tidak perlu meneruskannya hingga N; cukup berhenti pada $\sqrt{N}$. Dengan menggunakan metode ini, hitung semua bilangan prima yang lebih kecil daripada $N = 250$. Kita juga dapat menggunakan metode ini untuk mencari semua bilangan bulat yang relatif prima terhadap suatu bilangan bulat N. Cukup coret faktor-faktor prima dari N beserta semua kelipatannya. Dengan menggunakan metode ini, tentukan semua bilangan yang relatif prima terhadap $N = 120$. Dengan menggunakan Saringan

Eratosthenes, tulislah program yang menghitung semua bilangan prima yang lebih kecil daripada suatu bilangan bulat N.

2. Misalkan $\mathbb{N}^0 = \mathbb{N} \cup \{0\}$. Fungsi Ackermann adalah fungsi $A : \mathbb{N}^0 \times \mathbb{N}^0 \to \mathbb{N}^0$ yang didefinisikan oleh persamaan-persamaan

$$\begin{aligned} A(0, y) &= y + 1, \\ A(x + 1, 0) &= A(x, 1), \\ A(x + 1, y + 1) &= A(x, A(x + 1, y)). \end{aligned}$$

Gunakan definisi ini untuk menghitung $A(3, 1)$. Tulislah program untuk mengevaluasi fungsi Ackermann. Ubah program tersebut agar menghitung banyaknya pernyataan yang dijalankan ketika fungsi Ackermann dievaluasi. Berapa banyak pernyataan yang dijalankan dalam evaluasi $A(4, 1)$? Bagaimana dengan $A(5, 1)$?

3. Tulislah program komputer yang mengimplementasikan algoritma Euklides. Program tersebut harus menerima dua bilangan bulat positif a dan b sebagai masukan serta menghasilkan $\gcd(a, b)$ beserta bilangan bulat r dan s sedemikian sehingga

$$\gcd(a, b) = ra + sb.$$

2.6 Referensi dan Bacaan yang Disarankan

[1] Brookshear, J. G. *Theory of Computation: Formal Languages, Automata, and Complexity*. Benjamin/Cummings, Redwood City, CA, 1989. Menunjukkan hubungan antara aspek-aspek teoretis ilmu komputer dengan teori himpunan dan bilangan bulat.

[2] Hardy, G. H. dan Wright, E. M. *An Introduction to the Theory of Numbers*. Edisi ke-6. Oxford University Press, New York, 2008.

[3] Niven, I. dan Zuckerman, H. S. *An Introduction to the Theory of Numbers*. Edisi ke-5. Wiley, New York, 1991.

[4] Vanden Eynden, C. *Elementary Number Theory*. Edisi ke-2. Waveland Press, Long Grove IL, 2001.

3

Grup

Kita memulai kajian tentang struktur aljabar dengan menyelidiki himpunan yang dilengkapi satu operasi dan memenuhi aksioma-aksioma tertentu yang wajar; dengan kata lain, kita ingin mendefinisikan sebuah operasi pada suatu himpunan dengan cara yang memperumum struktur-struktur yang sudah dikenal, seperti bilangan bulat $\mathbb{Z}$ bersama operasi tunggal berupa penjumlahan, atau matriks 2×2 yang dapat dibalik bersama operasi tunggal berupa perkalian matriks. Bilangan bulat dan matriks 2×2 tersebut, beserta operasi tunggalnya masing-masing, merupakan contoh struktur aljabar yang dikenal sebagai grup.

Teori grup menempati kedudukan sentral dalam matematika. Teori grup modern muncul dari upaya mencari akar-akar polinomial berdasarkan koefisiennya. Kini grup memainkan peran sentral dalam bidang-bidang seperti teori pengodean, pencacahan, dan kajian simetri; banyak bidang biologi, kimia, dan fisika telah memperoleh manfaat dari teori grup.

3.1 Kelas Ekuivalensi Bilangan Bulat dan Simetri

Sekarang mari kita selidiki beberapa struktur matematika yang dapat dipandang sebagai himpunan dengan satu operasi.

3.1.1 Bilangan Bulat modulo n

Bilangan bulat modulo n telah menjadi bagian yang tak terpisahkan dari teori dan penerapan aljabar. Dalam matematika, bilangan-bilangan ini digunakan dalam kriptografi, teori pengodean, dan pendeteksian kesalahan pada kode identifikasi.

Kita telah melihat bahwa dua bilangan bulat a dan b ekuivalen modulo n jika n membagi $a - b$. Bilangan bulat modulo n juga mempartisi $\mathbb{Z}$ menjadi n kelas ekuivalensi yang berbeda; himpunan kelas-kelas ekuivalensi ini akan kita lambangkan dengan $\mathbb{Z}_n$. Perhatikan bilangan bulat modulo 12 dan partisi bilangan bulat yang bersesuaian:

$$\begin{aligned}
[0] &= \{\ldots, -12, 0, 12, 24, \ldots\}, \\
[1] &= \{\ldots, -11, 1, 13, 25, \ldots\}, \\
&\vdots
\end{aligned}$$

$$[11] = \{\ldots, -1, 11, 23, 35, \ldots\}.$$

Jika tidak menimbulkan kerancuan, kita akan menggunakan $0, 1, \ldots, 11$ untuk menyatakan kelas ekuivalensi $[0], [1], \ldots, [11]$ secara berurutan. Kita dapat melakukan aritmetika pada $\mathbb{Z}_n$. Untuk dua bilangan bulat a dan b, penjumlahan modulo n didefinisikan sebagai $(a + b) \pmod{n}$; yaitu, sisa pembagian $a + b$ oleh n. Demikian pula, perkalian modulo n didefinisikan sebagai $(ab) \pmod{n}$, yaitu sisa pembagian ab oleh n.

Contoh 3.1.1 Contoh-contoh berikut menggambarkan aritmetika bilangan bulat modulo n:

$$\begin{aligned} 7 + 4 &\equiv 1 \pmod 5 & \qquad 7 \cdot 3 &\equiv 1 \pmod 5 \\ 3 + 5 &\equiv 0 \pmod 8 & \qquad 3 \cdot 5 &\equiv 7 \pmod 8 \\ 3 + 4 &\equiv 7 \pmod{12} & \qquad 3 \cdot 4 &\equiv 0 \pmod{12}. \end{aligned}$$

Secara khusus, perhatikan bahwa hasil kali dua bilangan tak nol modulo n mungkin ekuivalen dengan 0 modulo n. ▲

Contoh 3.1.2 Sebagian besar, tetapi tidak semua, hukum aritmetika yang lazim berlaku untuk penjumlahan dan perkalian dalam $\mathbb{Z}_n$. Sebagai contoh, invers perkalian belum tentu ada. Perhatikan tabel perkalian untuk $\mathbb{Z}_8$ dalam Gambar 3.1.3. Perhatikan bahwa 2, 4, dan 6 tidak mempunyai invers perkalian; yaitu, untuk $n = 2$, 4, atau 6, tidak ada bilangan bulat k sedemikian sehingga $kn \equiv 1 \pmod 8$.

·	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Gambar 3.1.3 Tabel perkalian untuk $\mathbb{Z}_8$

▲

Proposisi 3.1.4 *Misalkan $\mathbb{Z}_n$ adalah himpunan kelas ekuivalensi bilangan bulat modulo n dan $a, b, c \in \mathbb{Z}_n$.*

1. *Penjumlahan dan perkalian bersifat komutatif:*

$$\begin{aligned} a + b &\equiv b + a \pmod n \\ ab &\equiv ba \pmod n. \end{aligned}$$

2. *Penjumlahan dan perkalian bersifat asosiatif:*

$$\begin{aligned} (a + b) + c &\equiv a + (b + c) \pmod n \\ (ab)c &\equiv a(bc) \pmod n. \end{aligned}$$

3. *Terdapat identitas penjumlahan dan identitas perkalian:*

$$\begin{aligned} a + 0 &\equiv a \pmod n \\ a \cdot 1 &\equiv a \pmod n. \end{aligned}$$

4. *Perkalian bersifat distributif terhadap penjumlahan:*

$$a(b+c) \equiv ab + ac \pmod{n}.$$

5. *Untuk setiap bilangan bulat a, terdapat invers penjumlahan $-a$:*

$$a + (-a) \equiv 0 \pmod{n}.$$

6. *Misalkan a adalah bilangan bulat tak nol. Maka $\gcd(a, n) = 1$ jika dan hanya jika terdapat invers perkalian b untuk $a \pmod{n}$; yaitu, bilangan bulat tak nol b sedemikian sehingga*

$$ab \equiv 1 \pmod{n}.$$

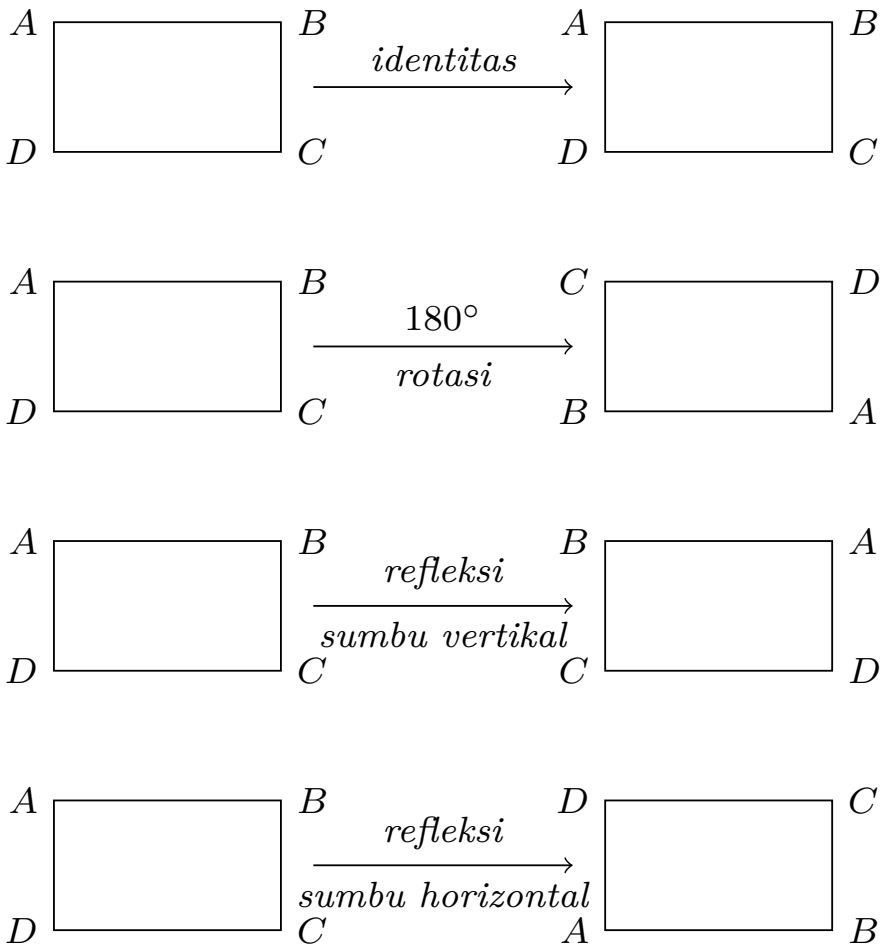
BUKTI. Kita akan membuktikan (1) dan (6), sedangkan pembuktian sifat-sifat lainnya diserahkan sebagai latihan.

(1) Penjumlahan dan perkalian bersifat komutatif modulo n karena sisa pembagian $a + b$ oleh n sama dengan sisa pembagian $b + a$ oleh n.

(6) Andaikan $\gcd(a, n) = 1$. Maka terdapat bilangan bulat r dan s sedemikian sehingga $ar + ns = 1$. Karena $ns = 1 - ar$, haruslah $ar \equiv 1 \pmod{n}$. Dengan mengambil b sebagai kelas ekuivalensi dari r, $ab \equiv 1 \pmod{n}$.

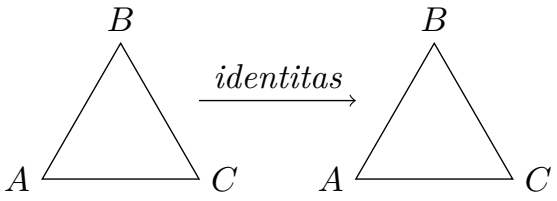
Sebaliknya, andaikan terdapat bilangan bulat b sedemikian sehingga $ab \equiv 1 \pmod{n}$. Maka n membagi $ab - 1$, sehingga terdapat bilangan bulat k sedemikian sehingga $ab - nk = 1$. Misalkan $d = \gcd(a, n)$. Karena d membagi $ab - nk$, d juga harus membagi 1; dengan demikian, $d = 1$. ■

3.1.2 Simetri

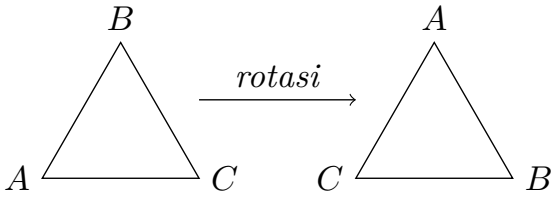


Gambar 3.1.5 Gerak kaku suatu persegi panjang

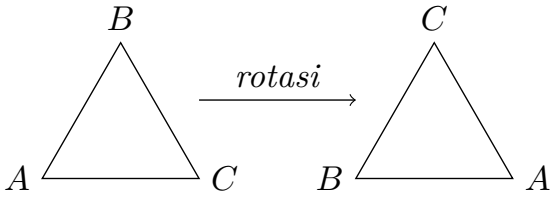
Simetri suatu bangun geometris adalah penataan ulang bangun tersebut yang mempertahankan susunan sisi dan titik sudutnya, serta jarak dan sudutnya. Pemetaan dari bidang ke dirinya sendiri yang mempertahankan simetri suatu objek disebut **gerak kaku**. Sebagai contoh, jika kita mengamati persegi panjang dalam Gambar 3.1.5, mudah dilihat bahwa rotasi sebesar 180° atau 360° menghasilkan kembali persegi panjang pada bidang dengan orientasi yang sama seperti persegi panjang semula dan hubungan antartitik sudut yang sama. Pencerminan persegi panjang terhadap sumbu vertikal maupun sumbu horizontal juga merupakan simetri. Namun, rotasi sebesar 90° ke arah mana pun tidak dapat menjadi simetri, kecuali jika persegi panjang tersebut adalah persegi.



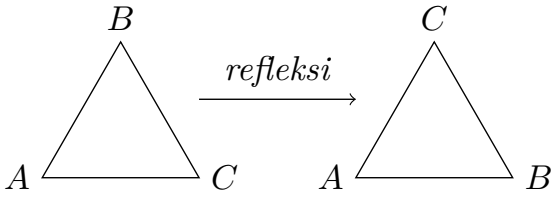
$$id = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$



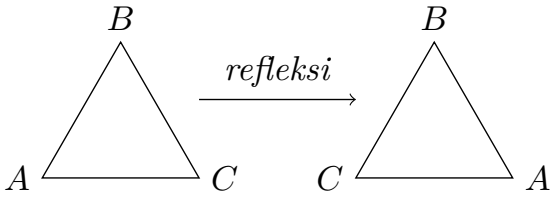
$$\rho_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$



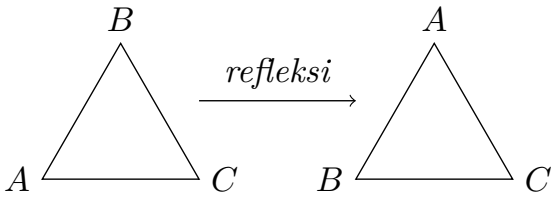
$$\rho_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$



$$\mu_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$



$$\mu_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$



$$\mu_3 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

Gambar 3.1.6 Simetri suatu segitiga

Mari kita tentukan simetri segitiga sama sisi $\triangle ABC$. Untuk menentukan suatu simetri dari $\triangle ABC$, mula-mula kita harus memeriksa permutasi titik-titik sudut A, B, dan C, lalu menanyakan apakah suatu permutasi meluas menjadi simetri segitiga tersebut. Ingat bahwa **permutasi** suatu himpunan S adalah pemetaan satu-ke-satu dan pada $\pi : S \to S$. Ketiga titik sudut itu mempunyai $3! = 6$ permutasi, sehingga segitiga tersebut mempunyai paling banyak enam simetri. Untuk melihat bahwa terdapat enam permutasi, perhatikan bahwa ada tiga kemungkinan berbeda untuk titik sudut pertama, dua untuk titik sudut kedua, dan titik sudut yang tersisa ditentukan oleh penem-

patan dua titik pertama. Jadi, kita memperoleh $3 \cdot 2 \cdot 1 = 3! = 6$ susunan yang berbeda. Untuk menyatakan permutasi titik-titik sudut suatu segitiga sama sisi yang memetakan A ke B, B ke C, dan C ke A, kita menuliskan larik

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}.$$

Perhatikan bahwa permutasi khusus ini bersesuaian dengan gerak kaku yang merotasi segitiga sebesar 120° searah jarum jam. Bahkan, setiap permutasi menghasilkan suatu simetri segitiga. Semua simetri ini ditampilkan dalam Gambar 3.1.6.

Pertanyaan yang wajar adalah apa yang terjadi jika satu gerak segitiga $\triangle ABC$ diikuti oleh gerak lainnya. Simetri manakah $\mu_1\rho_1$ itu? Dengan kata lain, apa yang terjadi ketika kita melakukan permutasi ρ_1, lalu permutasi μ_1? *Ingat bahwa di sini kita sedang mengomposisikan fungsi. Meskipun biasanya kita mengalikan dari kiri ke kanan, kita mengomposisikan fungsi dari kanan ke kiri.* Kita memperoleh

$$\begin{aligned}(\mu_1\rho_1)(A) &= \mu_1(\rho_1(A)) = \mu_1(B) = C \\ (\mu_1\rho_1)(B) &= \mu_1(\rho_1(B)) = \mu_1(C) = B \\ (\mu_1\rho_1)(C) &= \mu_1(\rho_1(C)) = \mu_1(A) = A.\end{aligned}$$

Ini adalah simetri yang sama dengan μ_2. Andaikan gerak-gerak tersebut kita lakukan dalam urutan sebaliknya, μ_1 kemudian ρ_1. Mudah ditentukan bahwa hasilnya sama dengan simetri μ_3; oleh karena itu, $\rho_1\mu_1 \neq \mu_1\rho_1$. Tabel perkalian untuk simetri-simetri segitiga sama sisi $\triangle ABC$ diberikan dalam Gambar 3.1.7.

Perhatikan bahwa dalam tabel perkalian simetri-simetri segitiga sama sisi, untuk setiap gerak segitiga α terdapat gerak lain β sedemikian sehingga $\alpha\beta =$ id; yaitu, untuk setiap gerak terdapat gerak lain yang mengembalikan segitiga ke orientasi semula.

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

Gambar 3.1.7 Simetri segitiga sama sisi

3.2 Definisi dan Contoh

Bilangan bulat modulo n dan simetri suatu segitiga atau persegi panjang merupakan contoh grup. **Operasi biner** atau **hukum komposisi** pada suatu himpunan G adalah fungsi $G \times G \to G$ yang memasangkan setiap pasangan $(a, b) \in G \times G$ dengan satu unsur tunggal $a \circ b$, atau ab dalam G, yang disebut komposisi dari a dan b. Suatu **grup** $(G, \circ)$ adalah himpunan G bersama suatu hukum komposisi $(a, b) \mapsto a \circ b$ yang memenuhi aksioma-aksioma berikut.

- Hukum komposisi tersebut bersifat **asosiatif**. Artinya,

  $$(a \circ b) \circ c = a \circ (b \circ c)$$

  untuk $a, b, c \in G$.

- Terdapat suatu unsur $e \in G$, yang disebut **unsur identitas**, sedemikian sehingga untuk setiap unsur $a \in G$

$$e \circ a = a \circ e = a.$$

- Untuk setiap unsur $a \in G$, terdapat **unsur invers** dalam G, yang dilambangkan dengan a^{-1}, sedemikian sehingga

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

Grup G yang mempunyai sifat $a \circ b = b \circ a$ untuk semua $a, b \in G$ disebut **abelian** atau **komutatif**. Grup yang tidak memenuhi sifat ini disebut **nonabelian** atau **nonkomutatif**.

Contoh 3.2.1 Bilangan bulat $\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$ membentuk grup terhadap operasi penjumlahan. Operasi biner pada dua bilangan bulat $m, n \in \mathbb{Z}$ tidak lain adalah jumlah keduanya. Karena bilangan bulat terhadap penjumlahan telah mempunyai notasi yang mapan, kita akan menggunakan operator $+$ sebagai pengganti $\circ$; yaitu, kita akan menuliskan $m + n$ sebagai pengganti $m \circ n$. Identitasnya adalah 0, dan invers dari $n \in \mathbb{Z}$ ditulis sebagai $-n$, bukan n^{-1}. Perhatikan bahwa himpunan bilangan bulat terhadap penjumlahan mempunyai sifat tambahan $m + n = n + m$ sehingga membentuk grup abelian. ▲

Pada umumnya kita akan menulis ab sebagai pengganti $a \circ b$; namun, jika grup tersebut telah mempunyai operasi alami seperti penjumlahan pada bilangan bulat, kita akan menggunakan operasi itu. Artinya, jika kita menjumlahkan dua bilangan bulat, kita tetap menulis $m+n$, $-n$ untuk invers, dan 0 untuk identitas seperti biasa. Kita juga menulis $m - n$ sebagai pengganti $m + (-n)$.

Sering kali lebih mudah mendeskripsikan suatu grup melalui tabel penjumlahan atau perkalian. Tabel semacam ini disebut **tabel Cayley**.

Contoh 3.2.2 Bilangan bulat modulo n membentuk grup terhadap penjumlahan modulo n. Perhatikan $\mathbb{Z}_5$, yang terdiri atas kelas ekuivalensi bilangan bulat 0, 1, 2, 3, dan 4. Operasi grup pada $\mathbb{Z}_5$ kita definisikan sebagai penjumlahan modular. Operasi biner pada grup tersebut kita tulis secara aditif; yaitu, kita menulis $m + n$. Unsur 0 adalah identitas grup dan setiap unsur dalam $\mathbb{Z}_5$ mempunyai invers. Sebagai contoh, $2 + 3 = 3 + 2 = 0$. Gambar 3.2.3 adalah tabel Cayley untuk $\mathbb{Z}_5$. Berdasarkan Proposisi 3.1.4, $\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$ adalah grup terhadap operasi biner penjumlahan modulo n.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Gambar 3.2.3 Tabel Cayley untuk $(\mathbb{Z}_5, +)$

▲

Contoh 3.2.4 Tidak setiap himpunan dengan operasi biner merupakan grup. Sebagai contoh, jika perkalian modular kita jadikan operasi biner pada $\mathbb{Z}_n$, maka $\mathbb{Z}_n$ bukan grup. Unsur 1 bertindak sebagai identitas grup karena $1 \cdot k = k \cdot 1 = k$ untuk setiap $k \in \mathbb{Z}_n$; namun, invers perkalian untuk 0 tidak ada karena $0 \cdot k = k \cdot 0 = 0$ untuk setiap k dalam $\mathbb{Z}_n$. Bahkan jika kita mempertimbangkan

himpunan $\mathbb{Z}_n \setminus \{0\}$, kita masih belum tentu memperoleh grup. Sebagai contoh, misalkan $2 \in \mathbb{Z}_6$. Maka 2 tidak mempunyai invers perkalian karena

$$\begin{aligned} 0 \cdot 2 &= 0 & 1 \cdot 2 &= 2 \\ 2 \cdot 2 &= 4 & 3 \cdot 2 &= 0 \\ 4 \cdot 2 &= 2 & 5 \cdot 2 &= 4. \end{aligned}$$

Berdasarkan Proposisi 3.1.4, setiap k tak nol mempunyai invers dalam $\mathbb{Z}_n$ jika k relatif prima terhadap n. Lambangkan himpunan semua unsur tak nol semacam itu dalam $\mathbb{Z}_n$ dengan $U(n)$. Maka $U(n)$ adalah grup yang disebut **grup satuan** dari $\mathbb{Z}_n$. Gambar 3.2.5 adalah tabel Cayley untuk grup $U(8)$.

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Gambar 3.2.5 Tabel perkalian untuk $U(8)$

▲

Contoh 3.2.6 Simetri-simetri segitiga sama sisi yang dijelaskan dalam Bagian 3.1 membentuk grup nonabelian. Seperti telah kita amati, belum tentu berlaku $\alpha\beta = \beta\alpha$ untuk dua simetri α dan β. Dengan menggunakan Gambar 3.1.7, yang merupakan tabel Cayley untuk grup ini, kita dapat memeriksa dengan mudah bahwa simetri-simetri segitiga sama sisi memang membentuk grup. Grup ini akan kita lambangkan dengan S_3 atau D_3, untuk alasan yang akan dijelaskan kemudian. ▲

Contoh 3.2.7 Kita menggunakan $\mathbb{M}_2(\mathbb{R})$ untuk melambangkan himpunan semua matriks 2×2. Misalkan $GL_2(\mathbb{R})$ adalah himpunan bagian dari $\mathbb{M}_2(\mathbb{R})$ yang terdiri atas matriks-matriks yang dapat dibalik; yaitu, suatu matriks

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

berada dalam $GL_2(\mathbb{R})$ jika terdapat matriks A^{-1} sedemikian sehingga $AA^{-1} = A^{-1}A = I$, dengan I adalah matriks identitas 2×2. Syarat bahwa A mempunyai invers ekuivalen dengan syarat bahwa determinan A tak nol; yaitu, $\det A = ad - bc \neq 0$. Himpunan matriks yang dapat dibalik membentuk grup yang disebut **grup linear umum**. Identitas grup tersebut adalah matriks identitas

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Invers dari $A \in GL_2(\mathbb{R})$ adalah

$$A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Hasil kali dua matriks yang dapat dibalik juga dapat dibalik. Perkalian matriks bersifat asosiatif, sehingga memenuhi aksioma grup yang tersisa. Untuk matriks, secara umum tidak berlaku $AB = BA$; oleh karena itu, $GL_2(\mathbb{R})$ merupakan contoh lain grup nonabelian. ▲

Contoh 3.2.8 Misalkan

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
$$J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \qquad K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

dengan $i^2 = -1$. Maka berlaku hubungan $I^2 = J^2 = K^2 = -1$, $IJ = K$, $JK = I$, $KI = J$, $JI = -K$, $KJ = -I$, dan $IK = -J$. Himpunan $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$ adalah grup yang disebut **grup kuaternion**. Perhatikan bahwa Q_8 bersifat nonkomutatif. ▲

Contoh 3.2.9 Misalkan $\mathbb{C}^*$ adalah himpunan bilangan kompleks tak nol. Terhadap operasi perkalian, $\mathbb{C}^*$ membentuk grup. Identitasnya adalah 1. Jika $z = a + bi$ adalah bilangan kompleks tak nol, maka

$$z^{-1} = \frac{a - bi}{a^2 + b^2}$$

adalah invers dari z. Mudah dilihat bahwa aksioma grup lainnya terpenuhi. ▲

Suatu grup disebut **berhingga**, atau mempunyai **orde berhingga**, jika grup tersebut memuat sejumlah berhingga unsur; jika tidak, grup tersebut disebut **tak berhingga** atau mempunyai **orde tak berhingga**. **Orde** suatu grup berhingga adalah banyaknya unsur yang dimuatnya. Jika G adalah grup yang memuat n unsur, kita menulis $|G| = n$. Grup $\mathbb{Z}_5$ adalah grup berhingga berorde 5; bilangan bulat $\mathbb{Z}$ membentuk grup tak berhingga terhadap penjumlahan, dan terkadang kita menulis $|\mathbb{Z}| = \infty$.

3.2.1 Sifat Dasar Grup

Proposisi 3.2.10 *Unsur identitas dalam suatu grup G bersifat tunggal; yaitu, hanya ada satu unsur $e \in G$ sedemikian sehingga $eg = ge = g$ untuk semua $g \in G$.*

Bukti. Andaikan e dan e' keduanya merupakan identitas dalam G. Maka $eg = ge = g$ dan $e'g = ge' = g$ untuk semua $g \in G$. Kita perlu menunjukkan bahwa $e = e'$. Jika kita memandang e sebagai identitas, maka $ee' = e'$; tetapi jika e' adalah identitas, maka $ee' = e$. Dengan menggabungkan kedua persamaan ini, kita memperoleh $e = ee' = e'$. ■

Invers dalam suatu grup juga bersifat tunggal. Jika g' dan g'' keduanya merupakan invers dari suatu unsur g dalam grup G, maka $gg' = g'g = e$ dan $gg'' = g''g = e$. Kita ingin menunjukkan bahwa $g' = g''$, dan memang $g' = g'e = g'(gg'') = (g'g)g'' = eg'' = g''$. Fakta ini kita rangkum dalam proposisi berikut.

Proposisi 3.2.11 *Jika g adalah sebarang unsur dalam suatu grup G, maka invers dari g, yang dilambangkan dengan g^{-1}, bersifat tunggal.*

Proposisi 3.2.12 *Misalkan G suatu grup. Jika $a, b \in G$, maka $(ab)^{-1} = b^{-1}a^{-1}$.*

Bukti. Misalkan $a, b \in G$. Maka $abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$. Demikian pula, $b^{-1}a^{-1}ab = e$. Namun, berdasarkan proposisi sebelumnya, invers bersifat tunggal; dengan demikian, $(ab)^{-1} = b^{-1}a^{-1}$. ■

Proposisi 3.2.13 *Misalkan G suatu grup. Untuk setiap $a \in G$, berlaku $(a^{-1})^{-1} = a$.*

BUKTI. Perhatikan bahwa $a^{-1}(a^{-1})^{-1} = e$. Akibatnya, dengan mengalikan kedua ruas persamaan ini dengan a, kita memperoleh

$$(a^{-1})^{-1} = e(a^{-1})^{-1} = aa^{-1}(a^{-1})^{-1} = ae = a.$$

■

Kita dapat menuliskan persamaan yang melibatkan unsur dan operasi grup. Jika a dan b adalah dua unsur dalam suatu grup G, apakah terdapat unsur $x \in G$ sedemikian sehingga $ax = b$? Jika x semacam itu ada, apakah ia tunggal? Proposisi berikut menjawab kedua pertanyaan ini secara afirmatif.

Proposisi 3.2.14 *Misalkan G suatu grup dan a serta b sebarang dua unsur dalam G. Maka persamaan $ax = b$ dan $xa = b$ mempunyai penyelesaian tunggal dalam G.*

BUKTI. Andaikan $ax = b$. Kita harus menunjukkan bahwa x semacam itu ada. Kita dapat mengalikan kedua ruas $ax = b$ dengan a^{-1} untuk memperoleh $x = ex = a^{-1}ax = a^{-1}b$.

Untuk menunjukkan ketunggalan, andaikan x_1 dan x_2 keduanya merupakan penyelesaian $ax = b$; maka $ax_1 = b = ax_2$. Jadi, $x_1 = a^{-1}ax_1 = a^{-1}ax_2 = x_2$. Pembuktian keberadaan dan ketunggalan penyelesaian $xa = b$ serupa. ■

Proposisi 3.2.15 *Jika G suatu grup dan $a, b, c \in G$, maka $ba = ca$ mengakibatkan $b = c$ dan $ab = ac$ mengakibatkan $b = c$.*

Proposisi ini menyatakan bahwa **hukum pencoretan kanan dan kiri** berlaku dalam grup. Pembuktiannya diserahkan sebagai latihan.

Kita dapat menggunakan notasi perpangkatan untuk grup seperti dalam aljabar biasa. Jika G suatu grup dan $g \in G$, kita mendefinisikan $g^0 = e$. Untuk $n \in \mathbb{N}$, kita mendefinisikan

$$g^n = \underbrace{g \cdot g \cdots g}_{n \text{ kali}}$$

dan

$$g^{-n} = \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ kali}}.$$

Teorema 3.2.16 *Dalam suatu grup, hukum-hukum perpangkatan yang lazim berlaku; yaitu, untuk semua $g, h \in G$,*

1. *$g^m g^n = g^{m+n}$ untuk semua $m, n \in \mathbb{Z}$;*
2. *$(g^m)^n = g^{mn}$ untuk semua $m, n \in \mathbb{Z}$;*
3. *$(gh)^n = (h^{-1}g^{-1})^{-n}$ untuk semua $n \in \mathbb{Z}$. Selanjutnya, jika G abelian, maka $(gh)^n = g^n h^n$.*

Pembuktian teorema ini diserahkan sebagai latihan. Perhatikan bahwa secara umum $(gh)^n \neq g^n h^n$, sebab grup tersebut belum tentu abelian. Jika grupnya adalah $\mathbb{Z}$ atau $\mathbb{Z}_n$, kita menulis operasi grup secara aditif dan operasi perpangkatan secara multiplikatif; yaitu, kita menulis ng sebagai pengganti g^n. Hukum-hukum perpangkatan kini menjadi

1. $mg + ng = (m + n)g$ untuk semua $m, n \in \mathbb{Z}$;
2. $m(ng) = (mn)g$ untuk semua $m, n \in \mathbb{Z}$;
3. $m(g + h) = mg + mh$ untuk semua $n \in \mathbb{Z}$.

Penting disadari bahwa pernyataan terakhir hanya dapat dibuat karena $\mathbb{Z}$ dan $\mathbb{Z}_n$ merupakan grup komutatif.

Catatan Sejarah

Meskipun definisi aksiomatik pertama yang jelas tentang grup baru diberikan pada akhir abad ke-19, metode teori grup telah digunakan sebelumnya dalam pengembangan banyak bidang matematika, termasuk geometri dan teori persamaan aljabar.
Joseph-Louis Lagrange menggunakan metode teori grup dalam sebuah memoar tahun 1770–1771 untuk mengkaji metode penyelesaian persamaan polinomial. Kemudian, Évariste Galois (1811–1832) berhasil mengembangkan matematika yang diperlukan untuk menentukan secara tepat persamaan polinomial mana yang dapat diselesaikan berdasarkan koefisien polinomial tersebut. Alat utama Galois adalah teori grup.
Kajian geometri mengalami revolusi pada tahun 1872 ketika Felix Klein mengusulkan agar ruang geometris dikaji dengan menelaah sifat-sifat yang invarian terhadap transformasi ruang tersebut. Sophus Lie, yang sezaman dengan Klein, menggunakan teori grup untuk mengkaji penyelesaian persamaan diferensial parsial. Salah satu pembahasan modern pertama tentang teori grup terdapat dalam karya William Burnside *The Theory of Groups of Finite Order* [1], yang pertama kali diterbitkan pada tahun 1897.

3.3 Subgrup

3.3.1 Definisi dan Contoh

Terkadang kita ingin menyelidiki grup-grup yang lebih kecil di dalam suatu grup yang lebih besar. Himpunan bilangan bulat genap $2\mathbb{Z} = \{\ldots, -2, 0, 2, 4, \ldots\}$ merupakan grup terhadap operasi penjumlahan. Grup yang lebih kecil ini secara alami berada di dalam grup bilangan bulat terhadap penjumlahan. Kita mendefinisikan **subgrup** H dari suatu grup G sebagai himpunan bagian H dari G sedemikian sehingga ketika operasi grup pada G dibatasi pada H, H sendiri merupakan suatu grup. Perhatikan bahwa setiap grup G dengan sekurang-kurangnya dua unsur selalu mempunyai sedikitnya dua subgrup, yaitu subgrup yang hanya terdiri atas unsur identitas dan seluruh grup itu sendiri. Subgrup $H = \{e\}$ dari suatu grup G disebut **subgrup trivial**. Subgrup yang merupakan himpunan bagian sejati dari G disebut **subgrup sejati**. Dalam banyak contoh yang telah kita selidiki hingga titik ini, terdapat subgrup lain selain subgrup trivial dan subgrup tak sejati.

Contoh 3.3.1 Perhatikan himpunan bilangan real tak nol, $\mathbb{R}^*$, dengan operasi grup berupa perkalian. Identitas grup ini adalah 1 dan invers dari setiap unsur $a \in \mathbb{R}^*$ adalah $1/a$. Kita akan menunjukkan bahwa

$$\mathbb{Q}^* = \{p/q : p \,\text{dan}\, q \,\text{adalah bilangan bulat taknol}\}$$

merupakan subgrup dari $\mathbb{R}^*$. Identitas dari $\mathbb{R}^*$ adalah 1; dan $1 = 1/1$ merupakan hasil bagi dua bilangan bulat tak nol. Dengan demikian, identitas dari $\mathbb{R}^*$ berada dalam $\mathbb{Q}^*$. Diberikan dua unsur dalam $\mathbb{Q}^*$, misalnya p/q dan r/s, hasil kalinya pr/qs juga berada dalam $\mathbb{Q}^*$. Invers dari setiap unsur $p/q \in \mathbb{Q}^*$ juga berada dalam $\mathbb{Q}^*$ karena $(p/q)^{-1} = q/p$. Karena perkalian dalam $\mathbb{R}^*$ bersifat asosiatif, perkalian dalam $\mathbb{Q}^*$ juga bersifat asosiatif. ▲

Contoh 3.3.2 Ingat bahwa $\mathbb{C}^*$ adalah grup perkalian bilangan kompleks tak nol. Misalkan $H = \{1, -1, i, -i\}$. Maka H merupakan subgrup dari $\mathbb{C}^*$. Cukup mudah untuk memverifikasi bahwa H adalah grup terhadap perkalian dan bahwa $H \subset \mathbb{C}^*$. ▲

Contoh 3.3.3 Misalkan $SL_2(\mathbb{R})$ adalah himpunan bagian dari $GL_2(\mathbb{R})$ yang terdiri atas matriks-matriks berdeterminan satu; yaitu, suatu matriks

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

berada dalam $SL_2(\mathbb{R})$ tepat ketika $ad - bc = 1$. Untuk menunjukkan bahwa $SL_2(\mathbb{R})$ adalah subgrup dari grup linear umum, kita harus menunjukkan bahwa himpunan tersebut merupakan grup terhadap perkalian matriks. Matriks identitas 2×2 berada dalam $SL_2(\mathbb{R})$, demikian pula invers matriks A:

$$A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Tinggal ditunjukkan bahwa operasi perkalian bersifat tertutup; yaitu, hasil kali dua matriks berdeterminan satu juga berdeterminan satu. Tugas ini diserahkan sebagai latihan. Grup $SL_2(\mathbb{R})$ disebut **grup linear khusus**. ▲

Contoh 3.3.4 Penting disadari bahwa suatu himpunan bagian H dari grup G dapat merupakan grup tanpa menjadi subgrup dari G. Agar H menjadi subgrup dari G, ia harus mewarisi operasi biner pada G. Himpunan semua matriks 2×2, $\mathbb{M}_2(\mathbb{R})$, membentuk grup terhadap operasi penjumlahan. Grup linear umum 2×2 merupakan himpunan bagian dari $\mathbb{M}_2(\mathbb{R})$ dan merupakan grup terhadap perkalian matriks, tetapi bukan subgrup dari $\mathbb{M}_2(\mathbb{R})$. Jika kita menjumlahkan dua matriks yang dapat dibalik, hasilnya belum tentu merupakan matriks yang dapat dibalik. Perhatikan bahwa

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

tetapi matriks nol tidak berada dalam $GL_2(\mathbb{R})$. ▲

Contoh 3.3.5 Salah satu cara menentukan apakah dua grup sama adalah dengan memeriksa subgrup-subgrupnya. Selain subgrup trivial dan grup itu sendiri, grup $\mathbb{Z}_4$ mempunyai satu subgrup yang terdiri atas unsur 0 dan 2. Dari grup $\mathbb{Z}_2$, kita dapat membentuk grup lain dengan empat unsur sebagai berikut. Sebagai himpunan, grup ini adalah $\mathbb{Z}_2 \times \mathbb{Z}_2$. Operasi grup dilakukan menurut koordinat; yaitu, $(a, b) + (c, d) = (a + c, b + d)$. Gambar 3.3.6 adalah tabel penjumlahan untuk $\mathbb{Z}_2 \times \mathbb{Z}_2$. Karena terdapat tiga subgrup sejati nontrivial dari $\mathbb{Z}_2 \times \mathbb{Z}_2$, $H_1 = \{(0,0), (0,1)\}$, $H_2 = \{(0,0), (1,0)\}$, dan $H_3 = \{(0,0), (1,1)\}$, $\mathbb{Z}_4$ dan $\mathbb{Z}_2 \times \mathbb{Z}_2$ pastilah merupakan grup yang berbeda.

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Gambar 3.3.6 Tabel penjumlahan untuk $\mathbb{Z}_2 \times \mathbb{Z}_2$

▲

3.3.2 Beberapa Teorema Subgrup

Mari kita periksa beberapa kriteria untuk menentukan secara tepat kapan suatu himpunan bagian dari sebuah grup merupakan subgrup.

Proposisi 3.3.7 *Himpunan bagian H dari G merupakan subgrup jika dan hanya jika memenuhi syarat-syarat berikut.*

1. *Identitas e dari G berada dalam H.*
2. *Jika $h_1, h_2 \in H$, maka $h_1 h_2 \in H$.*
3. *Jika $h \in H$, maka $h^{-1} \in H$.*

Bukti. Mula-mula andaikan H merupakan subgrup dari G. Kita harus menunjukkan bahwa ketiga syarat tersebut berlaku. Karena H suatu grup, ia harus mempunyai identitas e_H. Kita harus menunjukkan bahwa $e_H = e$, dengan e adalah identitas dari G. Kita mengetahui bahwa $e_H e_H = e_H$ dan $ee_H = e_H e = e_H$; dengan demikian, $ee_H = e_H e_H$. Berdasarkan pencoretan kanan, $e = e_H$. Syarat kedua berlaku karena subgrup H merupakan grup. Untuk membuktikan syarat ketiga, misalkan $h \in H$. Karena H suatu grup, terdapat unsur $h' \in H$ sedemikian sehingga $hh' = h'h = e$. Berdasarkan ketunggalan invers dalam G, $h' = h^{-1}$.

Sebaliknya, jika ketiga syarat tersebut berlaku, kita harus menunjukkan bahwa H merupakan grup terhadap operasi yang sama dengan G; tetapi syarat-syarat ini, bersama sifat asosiatif operasi biner, tepat merupakan aksioma-aksioma yang dinyatakan dalam definisi grup. ■

Proposisi 3.3.8 *Misalkan H suatu himpunan bagian dari grup G. Maka H merupakan subgrup dari G jika dan hanya jika $H \neq \emptyset$, dan setiap kali $g, h \in H$, berlaku gh^{-1} berada dalam H.*

Bukti. Mula-mula andaikan H merupakan subgrup dari G. Kita ingin menunjukkan bahwa $gh^{-1} \in H$ setiap kali g dan h berada dalam H. Karena h berada dalam H, inversnya h^{-1} juga harus berada dalam H. Karena operasi grup bersifat tertutup, $gh^{-1} \in H$.

Sebaliknya, andaikan $H \subset G$ sedemikian sehingga $H \neq \emptyset$ dan $gh^{-1} \in H$ setiap kali $g, h \in H$. Jika $g \in H$, maka $gg^{-1} = e$ berada dalam H. Jika $g \in H$, maka $eg^{-1} = g^{-1}$ juga berada dalam H. Sekarang misalkan $h_1, h_2 \in H$. Kita harus menunjukkan bahwa hasil kali keduanya juga berada dalam H. Namun, $h_1(h_2^{-1})^{-1} = h_1 h_2 \in H$. Dengan demikian, H merupakan subgrup dari G. ■

3.4 Pertanyaan Bacaan

1. Dalam grup $\mathbb{Z}_8$, hitunglah (a) $6 + 7$, dan (b) 2^{-1}.

2. Dalam grup $U(16)$, hitunglah (a) $5 \cdot 7$, dan (b) 3^{-1}.

3. Nyatakan definisi grup.

4. Jelaskan satu metode untuk menentukan apakah suatu himpunan bagian dari grup merupakan subgrup.

5. Jelaskan asal-usul istilah "abelian" untuk grup komutatif.

6. Berikan contoh grup yang pernah Anda jumpai dalam pengalaman matematika sebelumnya, tetapi tidak digunakan sebagai contoh dalam bab ini.

3.5 Latihan

1. Tentukan semua $x \in \mathbb{Z}$ yang memenuhi setiap persamaan berikut.

(a) $3x \equiv 2 \pmod 7$

(b) $5x + 1 \equiv 13 \pmod{23}$

(c) $5x + 1 \equiv 13 \pmod{26}$

(d) $9x \equiv 3 \pmod 5$

(e) $5x \equiv 1 \pmod 6$

(f) $3x \equiv 1 \pmod 6$

Petunjuk. (a) $3 + 7\mathbb{Z} = \{\ldots, -4, 3, 10, \ldots\}$; (c) $18 + 26\mathbb{Z}$; (e) $5 + 6\mathbb{Z}$.

2. Manakah di antara tabel perkalian berikut, yang didefinisikan pada himpunan $G = \{a, b, c, d\}$, yang membentuk grup? Berikan alasan untuk jawaban Anda dalam setiap kasus.

(a)

$\circ$	a	b	c	d
a	a	c	d	a
b	b	b	c	d
c	c	d	a	b
d	d	a	b	c

(b)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

(c)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

(d)

$\circ$	a	b	c	d
a	a	b	c	d
b	b	a	c	d
c	c	b	a	d
d	d	d	b	c

Petunjuk. (a) Bukan grup; (c) grup.

3. Tuliskan tabel Cayley untuk grup yang dibentuk oleh simetri suatu persegi panjang dan untuk $(\mathbb{Z}_4, +)$. Berapa banyak unsur dalam setiap grup? Apakah kedua grup tersebut sama? Mengapa demikian atau mengapa tidak?

4. Deskripsikan simetri suatu belah ketupat dan buktikan bahwa himpunan simetrinya membentuk grup. Berikan tabel Cayley untuk simetri persegi panjang dan simetri belah ketupat. Apakah simetri persegi panjang dan simetri belah ketupat tersebut sama?

5. Deskripsikan simetri suatu persegi dan buktikan bahwa himpunan simetrinya merupakan grup. Berikan tabel Cayley untuk simetri-simetri tersebut. Ada berapa cara untuk mempermutasikan titik-titik sudut persegi? Apakah setiap permutasi pasti merupakan simetri persegi tersebut? Grup simetri persegi dilambangkan dengan D_4.

6. Berikan tabel perkalian untuk grup $U(12)$.

Petunjuk.

$\cdot$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

7. Misalkan $S = \mathbb{R} \setminus \{-1\}$ dan definisikan operasi biner pada S dengan $a * b = a + b + ab$. Buktikan bahwa $(S, *)$ merupakan grup abelian.

8. Berikan contoh dua unsur A dan B dalam $GL_2(\mathbb{R})$ dengan $AB \neq BA$.

Petunjuk. Pilih dua matriks. Hampir setiap pasangan akan memenuhi.

9. Buktikan bahwa hasil kali dua matriks dalam $SL_2(\mathbb{R})$ mempunyai determinan satu.

10. Buktikan bahwa himpunan matriks berbentuk

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

merupakan grup terhadap perkalian matriks. Grup ini, yang dikenal sebagai **grup Heisenberg**, penting dalam fisika kuantum. Perkalian matriks dalam grup Heisenberg didefinisikan oleh

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & y' \\ 0 & 1 & z' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x + x' & y + y' + xz' \\ 0 & 1 & z + z' \\ 0 & 0 & 1 \end{pmatrix}.$$

11. Buktikan bahwa $\det(AB) = \det(A)\det(B)$ dalam $GL_2(\mathbb{R})$. Gunakan hasil ini untuk menunjukkan bahwa operasi biner dalam grup $GL_2(\mathbb{R})$ bersifat tertutup; yaitu, jika A dan B berada dalam $GL_2(\mathbb{R})$, maka $AB \in GL_2(\mathbb{R})$.

12. Misalkan $\mathbb{Z}_2^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{Z}_2\}$. Definisikan operasi biner pada $\mathbb{Z}_2^n$ dengan

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

Buktikan bahwa $\mathbb{Z}_2^n$ merupakan grup terhadap operasi ini. Grup ini penting dalam teori pengodean aljabar.

13. Tunjukkan bahwa $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ merupakan grup terhadap operasi perkalian.

14. Diberikan grup $\mathbb{R}^*$ dan $\mathbb{Z}$, misalkan $G = \mathbb{R}^* \times \mathbb{Z}$. Definisikan operasi biner $\circ$ pada G dengan $(a, m) \circ (b, n) = (ab, m + n)$. Tunjukkan bahwa G merupakan grup terhadap operasi ini.

15. Buktikan atau berikan sangkalan bahwa setiap grup yang memuat enam unsur bersifat abelian.

Petunjuk. Terdapat grup nonabelian yang memuat enam unsur.

16. Berikan contoh khusus suatu grup G dan unsur-unsur $g, h \in G$ yang memenuhi $(gh)^n \neq g^n h^n$.

Petunjuk. Perhatikan grup simetri segitiga sama sisi atau persegi.

17. Berikan contoh tiga grup berbeda yang masing-masing mempunyai delapan unsur. Mengapa grup-grup tersebut berbeda?

Petunjuk. Terdapat lima grup berbeda yang berorde 8.

18. Tunjukkan bahwa terdapat $n!$ permutasi dari suatu himpunan yang memuat n objek.

Petunjuk. Misalkan

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

berada dalam S_n. Semua a_i harus berbeda. Terdapat n cara memilih a_1, $n - 1$ cara memilih a_2, ..., dua cara memilih a_{n-1}, dan hanya satu cara

memilih a_n. Oleh karena itu, kita dapat membentuk σ dengan $n(n-1)\cdots 2\cdot 1 = n!$ cara.

19. Tunjukkan bahwa

$$0 + a \equiv a + 0 \equiv a \pmod{n}$$

untuk semua $a \in \mathbb{Z}_n$.

20. Buktikan bahwa terdapat identitas perkalian untuk bilangan bulat modulo n:

$$a \cdot 1 \equiv a \pmod{n}.$$

21. Untuk setiap $a \in \mathbb{Z}_n$, tentukan unsur $b \in \mathbb{Z}_n$ sedemikian sehingga

$$a + b \equiv b + a \equiv 0 \pmod{n}.$$

22. Tunjukkan bahwa penjumlahan dan perkalian modulo n merupakan operasi yang terdefinisi dengan baik. Artinya, tunjukkan bahwa operasi tersebut tidak bergantung pada pemilihan wakil kelas ekuivalensi modulo n.

23. Tunjukkan bahwa penjumlahan dan perkalian modulo n merupakan operasi asosiatif.

24. Tunjukkan bahwa perkalian bersifat distributif terhadap penjumlahan modulo n:

$$a(b + c) \equiv ab + ac \pmod{n}.$$

25. Misalkan a dan b adalah unsur dalam suatu grup G. Buktikan bahwa $ab^n a^{-1} = (aba^{-1})^n$ untuk $n \in \mathbb{Z}$.

Petunjuk.

$$\begin{aligned}(aba^{-1})^n &= (aba^{-1})(aba^{-1})\cdots(aba^{-1}) \\ &= ab(aa^{-1})b(aa^{-1})b\cdots b(aa^{-1})ba^{-1} \\ &= ab^n a^{-1}.\end{aligned}$$

26. Misalkan $U(n)$ adalah grup satuan dalam $\mathbb{Z}_n$. Jika $n > 2$, buktikan bahwa terdapat unsur $k \in U(n)$ sedemikian sehingga $k^2 = 1$ dan $k \neq 1$.

27. Buktikan bahwa invers dari $g_1 g_2 \cdots g_n$ adalah $g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}$.

28. Buktikan bagian yang tersisa dari Proposisi 3.2.14: jika G suatu grup dan $a, b \in G$, maka persamaan $xa = b$ mempunyai penyelesaian tunggal dalam G.

29. Buktikan Teorema 3.2.16.

30. Buktikan hukum pencoretan kanan dan kiri untuk suatu grup G; yaitu, tunjukkan bahwa dalam grup G, $ba = ca$ mengakibatkan $b = c$ dan $ab = ac$ mengakibatkan $b = c$ untuk unsur-unsur $a, b, c \in G$.

31. Tunjukkan bahwa jika $a^2 = e$ untuk semua unsur a dalam suatu grup G, maka G harus abelian.

Petunjuk. Karena $abab = (ab)^2 = e = a^2b^2 = aabb$, kita mengetahui bahwa $ba = ab$.

32. Tunjukkan bahwa jika G merupakan grup berhingga berorde genap, maka terdapat $a \in G$ sedemikian sehingga a bukan identitas dan $a^2 = e$.

33. Misalkan G suatu grup dan andaikan bahwa $(ab)^2 = a^2b^2$ untuk semua a dan b dalam G. Buktikan bahwa G merupakan grup abelian.

34. Tentukan semua subgrup dari $\mathbb{Z}_3 \times \mathbb{Z}_3$. Gunakan informasi ini untuk menunjukkan bahwa $\mathbb{Z}_3 \times \mathbb{Z}_3$ bukan grup yang sama dengan $\mathbb{Z}_9$. (Lihat Contoh 3.3.5 untuk deskripsi singkat hasil kali grup.)

35. Tentukan semua subgrup dari grup simetri segitiga sama sisi.

Petunjuk. $H_1 = \{\mathrm{id}\}$, $H_2 = \{\mathrm{id}, \rho_1, \rho_2\}$, $H_3 = \{\mathrm{id}, \mu_1\}$, $H_4 = \{\mathrm{id}, \mu_2\}$, $H_5 = \{\mathrm{id}, \mu_3\}$, S_3.

36. Tentukan subgrup-subgrup dari grup simetri persegi.

37. Misalkan $H = \{2^k : k \in \mathbb{Z}\}$. Tunjukkan bahwa H merupakan subgrup dari $\mathbb{Q}^*$.

38. Misalkan $n = 0, 1, 2, \ldots$ dan $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. Buktikan bahwa $n\mathbb{Z}$ merupakan subgrup dari $\mathbb{Z}$. Tunjukkan bahwa subgrup-subgrup ini adalah satu-satunya subgrup dari $\mathbb{Z}$.

39. Misalkan $\mathbb{T} = \{z \in \mathbb{C}^* : |z| = 1\}$. Buktikan bahwa $\mathbb{T}$ merupakan subgrup dari $\mathbb{C}^*$.

40. Misalkan G terdiri atas matriks 2×2 berbentuk

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},$$

dengan $\theta \in \mathbb{R}$. Buktikan bahwa G merupakan subgrup dari $SL_2(\mathbb{R})$.

41. Buktikan bahwa

$$G = \{a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ dan } a \text{ dan } b \text{ tidak keduanya nol}\}$$

merupakan subgrup dari $\mathbb{R}^*$ terhadap operasi grup berupa perkalian.

Petunjuk. Identitas dari G adalah $1 = 1 + 0\sqrt{2}$. Karena $(a + b\sqrt{2}\,)(c + d\sqrt{2}\,) = (ac+2bd)+(ad+bc)\sqrt{2}$, G tertutup terhadap perkalian. Terakhir, $(a + b\sqrt{2}\,)^{-1} = a/(a^2 - 2b^2) - b\sqrt{2}/(a^2 - 2b^2)$.

42. Misalkan G adalah grup matriks 2×2 terhadap penjumlahan dan

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}.$$

Buktikan bahwa H merupakan subgrup dari G.

43. Buktikan atau berikan sangkalan: $SL_2(\mathbb{Z})$, yaitu himpunan matriks 2×2 dengan entri bilangan bulat dan determinan satu, merupakan subgrup dari $SL_2(\mathbb{R})$.

44. Daftarkan subgrup-subgrup dari grup kuaternion Q_8.

45. Buktikan bahwa irisan dua subgrup dari suatu grup G juga merupakan subgrup dari G.

46. Buktikan atau berikan sangkalan: Jika H dan K merupakan subgrup dari suatu grup G, maka $H \cup K$ merupakan subgrup dari G.

Petunjuk. Perhatikan S_3.

47. Buktikan atau berikan sangkalan: Jika H dan K merupakan subgrup dari suatu grup G, maka $HK = \{hk : h \in H \text{ dan } k \in K\}$ merupakan subgrup dari G. Bagaimana jika G abelian?

48. Misalkan G suatu grup dan $g \in G$. Tunjukkan bahwa

$$Z(G) = \{x \in G : gx = xg \text{ untuk semua } g \in G\}$$

merupakan subgrup dari G. Subgrup ini disebut **pusat** dari G.

49. Misalkan a dan b adalah unsur-unsur dari suatu grup G. Jika $a^4b = ba$ dan $a^3 = e$, buktikan bahwa $ab = ba$.

Petunjuk. $ba = a^4b = a^3ab = ab$

50. Berikan contoh grup tak berhingga yang setiap subgrup nontrivialnya tak berhingga.

51. Jika $xy = x^{-1}y^{-1}$ untuk semua x dan y dalam G, buktikan bahwa G harus abelian.

52. Buktikan atau berikan sangkalan: Setiap subgrup sejati dari grup nonabelian bersifat nonabelian.

53. Misalkan H suatu subgrup dari G dan

$$C(H) = \{g \in G : gh = hg \text{ untuk semua } h \in H\}.$$

Buktikan bahwa $C(H)$ merupakan subgrup dari G. Subgrup ini disebut **sentralisator** dari H dalam G.

54. Misalkan H suatu subgrup dari G. Jika $g \in G$, tunjukkan bahwa $gHg^{-1} = \{ghg^{-1} : h \in H\}$ juga merupakan subgrup dari G.

3.6 Latihan Tambahan: Mendeteksi Kesalahan

1. **Simbol UPC.** Simbol Universal Product Code (UPC) terdapat pada sebagian besar produk di toko bahan pangan dan toko ritel. Simbol UPC merupakan kode 12 digit yang mengidentifikasi produsen suatu produk dan produk itu sendiri (Gambar 3.6.1). Sebelas digit pertama memuat informasi tentang produk; digit kedua belas digunakan untuk mendeteksi kesalahan. Jika $d_1 d_2 \cdots d_{12}$ merupakan nomor UPC yang valid, maka

$$3 \cdot d_1 + 1 \cdot d_2 + 3 \cdot d_3 + \cdots + 3 \cdot d_{11} + 1 \cdot d_{12} \equiv 0 \pmod{10}.$$

(a) Tunjukkan bahwa nomor UPC 0-50000-30042-6, yang ditampilkan dalam Gambar 3.6.1, merupakan nomor UPC yang valid.

(b) Tunjukkan bahwa nomor 0-50000-30043-6 bukan nomor UPC yang valid.

(c) Tuliskan rumus untuk menghitung digit pemeriksa, d_{12}, dalam nomor UPC.

(d) Skema pendeteksian kesalahan UPC dapat mendeteksi sebagian besar kesalahan transposisi; artinya, skema tersebut dapat menentukan apakah dua digit telah saling dipertukarkan. Tunjukkan bahwa kesalahan transposisi 0-05000-30042-6 tidak terdeteksi. Temukan suatu kesalahan transposisi yang terdeteksi. Dapatkah Anda menemukan aturan umum untuk jenis kesalahan transposisi yang dapat dideteksi?

(e) Tulislah program yang menentukan apakah suatu nomor UPC valid.



Gambar 3.6.1 Kode UPC

2. Notasi hasil kali dalam sering berguna untuk skema pendeteksian kesalahan jenis ini; oleh karena itu, kita akan menggunakan notasi

$$(d_1, d_2, \ldots, d_k) \cdot (w_1, w_2, \ldots, w_k) \equiv 0 \pmod{n}$$

untuk menyatakan

$$d_1w_1 + d_2w_2 + \cdots + d_kw_k \equiv 0 \pmod{n}.$$

Andaikan bahwa $(d_1, d_2, \ldots, d_k) \cdot (w_1, w_2, \ldots, w_k) \equiv 0 \pmod{n}$ merupakan skema pendeteksian kesalahan untuk nomor identifikasi k digit $d_1d_2\cdots d_k$, dengan $0 \leq d_i < n$. Buktikan bahwa semua kesalahan satu digit terdeteksi jika dan hanya jika $\gcd(w_i, n) = 1$ untuk $1 \leq i \leq k$.

3. Misalkan $(d_1, d_2, \ldots, d_k) \cdot (w_1, w_2, \ldots, w_k) \equiv 0 \pmod{n}$ merupakan skema pendeteksian kesalahan untuk nomor identifikasi k digit $d_1d_2\cdots d_k$, dengan $0 \leq d_i < n$. Buktikan bahwa semua kesalahan transposisi dua digit d_i dan d_j terdeteksi jika dan hanya jika $\gcd(w_i - w_j, n) = 1$ untuk i dan j di antara 1 dan k.

4. **Kode ISBN.** Setiap buku mempunyai kode International Standard Book Number (ISBN). Kode 10 digit ini menunjukkan penerbit dan judul buku. Digit kesepuluh merupakan digit pemeriksa yang memenuhi

$$(d_1, d_2, \ldots, d_{10}) \cdot (10, 9, \ldots, 1) \equiv 0 \pmod{11}.$$

Salah satu masalahnya adalah bahwa d_{10} mungkin harus bernilai 10 agar hasil kali dalam bernilai nol; dalam hal ini, diperlukan 11 digit agar skema tersebut dapat bekerja. Oleh karena itu, karakter X digunakan untuk digit kesebelas. Jadi, ISBN 3-540-96035-X merupakan kode ISBN yang valid.

(a) Apakah ISBN 0-534-91500-0 merupakan kode ISBN yang valid? Bagaimana dengan ISBN 0-534-91700-0 dan ISBN 0-534-19500-0?

(b) Apakah metode ini mendeteksi semua kesalahan satu digit? Bagaimana dengan semua kesalahan transposisi?

(c) Ada berapa banyak kode ISBN yang berbeda?

(d) Tulislah program komputer yang menghitung digit pemeriksa untuk sembilan digit pertama suatu kode ISBN.

(e) Sebuah penerbit mempunyai cabang di Jerman dan Amerika Serikat. Awalan penerbit tersebut di Jerman adalah 3-540. Jika awalannya di Amerika Serikat akan berupa 0-abc, tentukan abc sedemikian sehingga bagian lain kode ISBN sama untuk buku yang dicetak di Jerman dan di Amerika Serikat. Dalam metode pengodean ISBN, digit pertama mengidentifikasi bahasa; bahasa Jerman adalah 3 dan bahasa Inggris adalah 0. Kelompok angka berikutnya mengidentifikasi penerbit, dan kelompok terakhir mengidentifikasi buku tertentu.

3.7 Referensi dan Bacaan yang Disarankan

[1] Burnside, W. *Theory of Groups of Finite Order*. Edisi ke-2. Cambridge University Press, Cambridge, 1911; Dover, New York, 1953. Sebuah karya klasik. Tersedia pula di books.google.com.

[2] Gallian, J. A. dan Winters, S. "Modular Arithmetic in the Marketplace," *The American Mathematical Monthly* 95 (1988): 548–51.

[3] Gallian, J. A. *Contemporary Abstract Algebra*. Edisi ke-7. Brooks/Cole, Belmont, CA, 2009.

[4] Hall, M. *Theory of Groups*. Edisi ke-2. American Mathematical Society,

Providence, 1959.

[5] Kurosh, A. E. *The Theory of Groups*, jilid I dan II. American Mathematical Society, Providence, 1979.

[6] Rotman, J. J. *An Introduction to the Theory of Groups*. Edisi ke-4. Springer, New York, 1995.

4

Grup Siklik

Grup $\mathbb{Z}$ dan $\mathbb{Z}_n$, yang termasuk grup paling dikenal dan mudah dipahami, keduanya merupakan contoh dari apa yang disebut grup siklik. Dalam bab ini kita akan mempelajari sifat-sifat grup siklik dan subgrup siklik, yang berperan mendasar dalam klasifikasi semua grup abelian.

4.1 Subgrup Siklik

Sering kali suatu subgrup sepenuhnya bergantung pada satu elemen grup; artinya, dengan mengetahui elemen tertentu tersebut, kita dapat menghitung setiap elemen lain dalam subgrup itu.

Contoh 4.1.1 Misalkan kita mempertimbangkan $3 \in \mathbb{Z}$ dan melihat semua kelipatan (baik positif maupun negatif) dari 3. Sebagai himpunan, himpunan ini adalah

$$3\mathbb{Z} = \{\ldots, -3, 0, 3, 6, \ldots\}.$$

Mudah dilihat bahwa $3\mathbb{Z}$ merupakan subgrup dari bilangan bulat. Subgrup ini sepenuhnya ditentukan oleh elemen 3 karena semua elemen lain dalam grup dapat diperoleh dengan mengambil kelipatan 3. Setiap elemen dalam subgrup tersebut "dibangkitkan" oleh 3. ▲

Contoh 4.1.2 Jika $H = \{2^n : n \in \mathbb{Z}\}$, maka H merupakan subgrup dari grup perkalian bilangan rasional tak nol, $\mathbb{Q}^*$. Jika $a = 2^m$ dan $b = 2^n$ berada dalam H, maka $ab^{-1} = 2^m 2^{-n} = 2^{m-n}$ juga berada dalam H. Berdasarkan Proposisi 3.3.8, H merupakan subgrup dari $\mathbb{Q}^*$ yang ditentukan oleh elemen 2. ▲

Teorema 4.1.3 *Misalkan G suatu grup dan a sebarang elemen dalam G. Maka himpunan*

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

merupakan subgrup dari G. Lebih lanjut, $\langle a \rangle$ merupakan subgrup terkecil dari G yang memuat a.

Bukti. Elemen identitas berada dalam $\langle a \rangle$ karena $a^0 = e$. Jika g dan h merupakan sebarang dua elemen dalam $\langle a \rangle$, maka berdasarkan definisi $\langle a \rangle$, kita dapat menuliskan $g = a^m$ dan $h = a^n$ untuk suatu bilangan bulat m dan n. Jadi, $gh = a^m a^n = a^{m+n}$ kembali berada dalam $\langle a \rangle$. Terakhir, jika $g = a^n$ berada dalam $\langle a \rangle$, maka invers $g^{-1} = a^{-n}$ juga berada dalam $\langle a \rangle$. Jelas bahwa sebarang subgrup H dari G yang memuat a harus memuat semua

pangkat a berdasarkan ketertutupan; jadi, H memuat $\langle a \rangle$. Oleh karena itu, $\langle a \rangle$ merupakan subgrup terkecil dari G yang memuat a. ■

Catatan 4.1.4 Jika kita menggunakan notasi "+", seperti pada bilangan bulat dengan operasi penjumlahan, kita tulis $\langle a \rangle = \{na : n \in \mathbb{Z}\}$.

Untuk $a \in G$, $\langle a \rangle$ disebut **subgrup siklik** yang dibangkitkan oleh a. Jika G memuat suatu elemen a sedemikian sehingga $G = \langle a \rangle$, maka G merupakan **grup siklik**. Dalam hal ini, a merupakan **pembangkit** dari G. Jika a merupakan elemen suatu grup G, kita mendefinisikan **orde** dari a sebagai bilangan bulat positif terkecil n sedemikian sehingga $a^n = e$, dan kita tulis $|a| = n$. Jika tidak terdapat bilangan bulat n seperti itu, kita mengatakan bahwa orde a tak hingga dan menuliskan $|a| = \infty$ untuk menyatakan orde a.

Contoh 4.1.5 Perhatikan bahwa suatu grup siklik dapat mempunyai lebih dari satu pembangkit. Baik 1 maupun 5 membangkitkan $\mathbb{Z}_6$; jadi, $\mathbb{Z}_6$ merupakan grup siklik. Tidak setiap elemen dalam grup siklik harus merupakan pembangkit grup tersebut. Orde $2 \in \mathbb{Z}_6$ adalah 3. Subgrup siklik yang dibangkitkan oleh 2 adalah $\langle 2 \rangle = \{0, 2, 4\}$. ▲

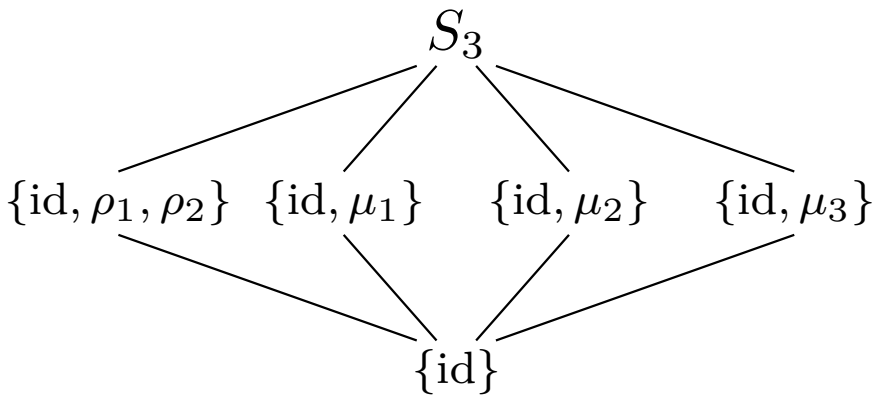
Grup $\mathbb{Z}$ dan $\mathbb{Z}_n$ merupakan grup siklik. Elemen 1 dan -1 merupakan pembangkit bagi $\mathbb{Z}$. Kita tentu dapat membangkitkan $\mathbb{Z}_n$ dengan 1, meskipun mungkin terdapat pembangkit lain dari $\mathbb{Z}_n$, seperti dalam kasus $\mathbb{Z}_6$.

Contoh 4.1.6 Grup unit, $U(9)$, dalam $\mathbb{Z}_9$ merupakan grup siklik. Sebagai himpunan, $U(9)$ adalah $\{1, 2, 4, 5, 7, 8\}$. Elemen 2 merupakan pembangkit bagi $U(9)$ karena

$$\begin{aligned} 2^1 &= 2 & 2^2 &= 4 \\ 2^3 &= 8 & 2^4 &= 7 \\ 2^5 &= 5 & 2^6 &= 1. \end{aligned}$$

▲

Contoh 4.1.7 Tidak setiap grup merupakan grup siklik. Perhatikan grup simetri segitiga sama sisi S_3. Tabel perkalian untuk grup ini diberikan dalam Gambar 3.1.7. Subgrup-subgrup dari S_3 ditunjukkan dalam Gambar 4.1.8. Perhatikan bahwa setiap subgrup bersifat siklik; akan tetapi, tidak ada satu elemen pun yang membangkitkan seluruh grup.



Gambar 4.1.8 Subgrup dari S_3

▲

Teorema 4.1.9 *Setiap grup siklik bersifat abelian.*

BUKTI. Misalkan G grup siklik dan $a \in G$ pembangkit bagi G. Jika g dan h berada dalam G, maka keduanya dapat ditulis sebagai pangkat dari a, misalkan $g = a^r$ dan $h = a^s$. Karena

$$gh = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = hg,$$

G bersifat abelian. ■

4.1.1 Subgrup dari Grup Siklik

Kita dapat mengajukan beberapa pertanyaan menarik mengenai subgrup siklik dari suatu grup dan subgrup dari suatu grup siklik. Jika G suatu grup, subgrup mana dari G yang bersifat siklik? Jika G suatu grup siklik, jenis subgrup apa yang dimiliki G?

Teorema 4.1.10 *Setiap subgrup dari grup siklik bersifat siklik.*

BUKTI. Perangkat utama yang digunakan dalam bukti ini adalah algoritma pembagian dan Prinsip Urutan Baik. Misalkan G grup siklik yang dibangkitkan oleh a, dan misalkan H subgrup dari G. Jika $H = \{e\}$, maka jelas H bersifat siklik. Misalkan H memuat suatu elemen lain g yang berbeda dari identitas. Maka g dapat ditulis sebagai a^n untuk suatu bilangan bulat n. Karena H merupakan subgrup, $g^{-1} = a^{-n}$ juga harus berada dalam H. Karena salah satu dari n atau $-n$ positif, kita dapat mengandaikan bahwa H memuat pangkat positif dari a dan $n > 0$. Misalkan m bilangan asli terkecil sedemikian sehingga $a^m \in H$. Bilangan m seperti itu ada berdasarkan Prinsip Urutan Baik.

Kita menyatakan bahwa $h = a^m$ merupakan pembangkit bagi H. Kita harus menunjukkan bahwa setiap $h' \in H$ dapat ditulis sebagai pangkat dari h. Karena $h' \in H$ dan H merupakan subgrup dari G, berlaku $h' = a^k$ untuk suatu bilangan bulat k. Dengan menggunakan algoritma pembagian, kita dapat mencari bilangan q dan r sedemikian sehingga $k = mq + r$ dengan $0 \leq r < m$; jadi,

$$a^k = a^{mq+r} = (a^m)^q a^r = h^q a^r.$$

Jadi $a^r = a^k h^{-q}$. Karena a^k dan h^{-q} berada dalam H, a^r juga harus berada dalam H. Akan tetapi, m merupakan bilangan positif terkecil sedemikian sehingga a^m berada dalam H; akibatnya, $r = 0$ sehingga $k = mq$. Oleh karena itu,

$$h' = a^k = a^{mq} = h^q$$

dan H dibangkitkan oleh h. ■

Korolari 4.1.11 *Subgrup-subgrup dari $\mathbb{Z}$ tepat merupakan $n\mathbb{Z}$ untuk $n = 0, 1, 2, \ldots$.*

Proposisi 4.1.12 *Misalkan G grup siklik berorde n dan misalkan a pembangkit bagi G. Maka $a^k = e$ jika dan hanya jika n membagi k.*

BUKTI. Pertama, misalkan $a^k = e$. Berdasarkan algoritma pembagian, $k = nq + r$ dengan $0 \leq r < n$; jadi,

$$e = a^k = a^{nq+r} = a^{nq} a^r = e a^r = a^r.$$

Karena bilangan bulat positif terkecil m sedemikian sehingga $a^m = e$ adalah n, $r = 0$.

Sebaliknya, jika n membagi k, maka $k = ns$ untuk suatu bilangan bulat s. Akibatnya,

$$a^k = a^{ns} = (a^n)^s = e^s = e.$$

■

Teorema 4.1.13 *Misalkan G grup siklik berorde n dan misalkan $a \in G$ merupakan pembangkit grup tersebut. Jika $b = a^k$, maka orde b adalah n/d, dengan $d = \gcd(k, n)$.*

BUKTI. Kita ingin mencari bilangan bulat terkecil m sedemikian sehingga $e = b^m = a^{km}$. Berdasarkan Proposisi 4.1.12, bilangan itu adalah bilangan bulat terkecil m sedemikian sehingga n membagi km atau, secara ekuivalen, n/d membagi $m(k/d)$. Karena d merupakan faktor persekutuan terbesar dari n dan k, n/d dan k/d relatif prima. Jadi, agar n/d membagi $m(k/d)$, bilangan tersebut harus membagi m. Bilangan m terkecil seperti itu adalah n/d. ■

Korolari 4.1.14 *Pembangkit-pembangkit dari $\mathbb{Z}_n$ adalah bilangan bulat r sedemikian sehingga $1 \leq r < n$ dan $\gcd(r, n) = 1$.*

Contoh 4.1.15 Mari kita periksa grup $\mathbb{Z}_{16}$. Bilangan 1, 3, 5, 7, 9, 11, 13, dan 15 merupakan elemen-elemen dari $\mathbb{Z}_{16}$ yang relatif prima terhadap 16. Setiap elemen ini membangkitkan $\mathbb{Z}_{16}$. Sebagai contoh,

$$\begin{array}{lll} 1 \cdot 9 = 9 & 2 \cdot 9 = 2 & 3 \cdot 9 = 11 \\ 4 \cdot 9 = 4 & 5 \cdot 9 = 13 & 6 \cdot 9 = 6 \\ 7 \cdot 9 = 15 & 8 \cdot 9 = 8 & 9 \cdot 9 = 1 \\ 10 \cdot 9 = 10 & 11 \cdot 9 = 3 & 12 \cdot 9 = 12 \\ 13 \cdot 9 = 5 & 14 \cdot 9 = 14 & 15 \cdot 9 = 7. \end{array}$$

▲

4.2 Grup Perkalian Bilangan Kompleks

Bilangan kompleks didefinisikan sebagai

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\},$$

dengan $i^2 = -1$. Jika $z = a + bi$, maka a merupakan **bagian real** dari z dan b merupakan **bagian imajiner** dari z.

Untuk menjumlahkan dua bilangan kompleks $z = a + bi$ dan $w = c + di$, kita cukup menjumlahkan bagian real dan imajiner yang bersesuaian:

$$z + w = (a + bi) + (c + di) = (a + c) + (b + d)i.$$

Dengan mengingat bahwa $i^2 = -1$, kita mengalikan bilangan kompleks seperti mengalikan polinomial. Hasil kali z dan w adalah

$$(a + bi)(c + di) = ac + bdi^2 + adi + bci = (ac - bd) + (ad + bc)i.$$

Setiap bilangan kompleks tak nol $z = a + bi$ mempunyai invers perkalian; artinya, terdapat $z^{-1} \in \mathbb{C}^*$ sedemikian sehingga $zz^{-1} = z^{-1}z = 1$. Jika $z = a + bi$, maka

$$z^{-1} = \frac{a - bi}{a^2 + b^2}.$$

Konjugat kompleks dari bilangan kompleks $z = a + bi$ didefinisikan sebagai $\overline{z} = a - bi$. **Nilai mutlak** atau **modulus** dari $z = a + bi$ adalah $|z| = \sqrt{a^2 + b^2}$.

Contoh 4.2.1 Misalkan $z = 2 + 3i$ dan $w = 1 - 2i$. Maka

$$z + w = (2 + 3i) + (1 - 2i) = 3 + i$$

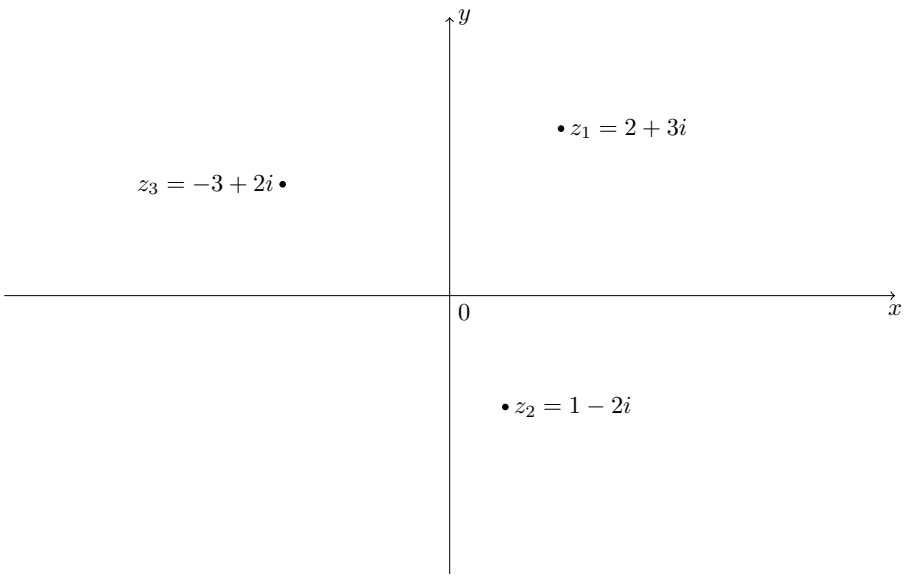
dan

$$zw = (2 + 3i)(1 - 2i) = 8 - i.$$

Selain itu,

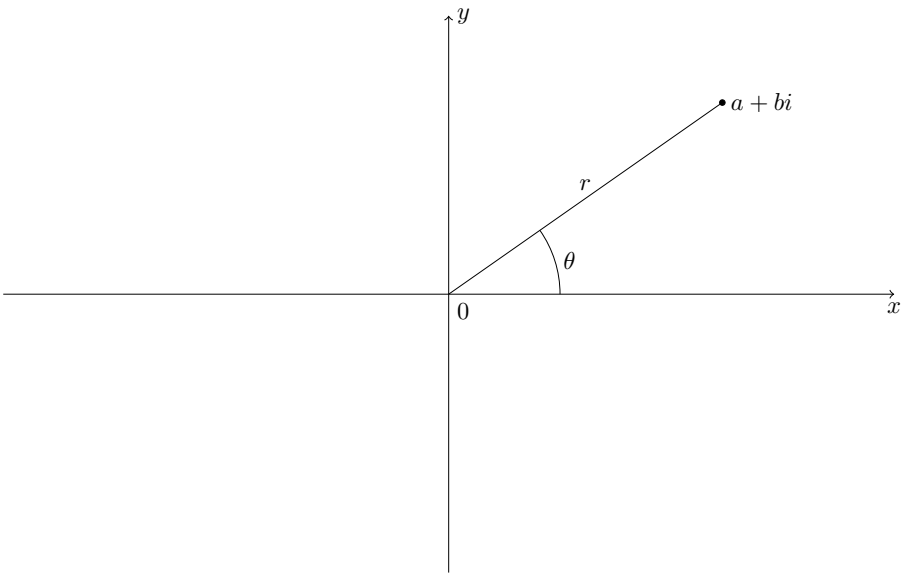
$$\begin{aligned} z^{-1} &= \frac{2}{13} - \frac{3}{13}i \\ |z| &= \sqrt{13} \\ \overline{z} &= 2 - 3i. \end{aligned}$$

▲



Gambar 4.2.2 Koordinat rektangular suatu bilangan kompleks

Terdapat beberapa cara untuk merepresentasikan bilangan kompleks secara grafis. Kita dapat merepresentasikan bilangan kompleks $z = a + bi$ sebagai pasangan terurut pada bidang xy, dengan a sebagai koordinat x (atau real) dan b sebagai koordinat y (atau imajiner). Representasi ini disebut representasi **rektangular** atau **Kartesius**. Representasi rektangular dari $z_1 = 2 + 3i$, $z_2 = 1 - 2i$, dan $z_3 = -3 + 2i$ digambarkan dalam Gambar 4.2.2.



Gambar 4.2.3 Koordinat polar suatu bilangan kompleks

Bilangan kompleks tak nol juga dapat direpresentasikan menggunakan **koordinat polar**. Untuk menentukan sebarang titik tak nol pada bidang, cukup diberikan sudut θ dari sumbu x positif dalam arah berlawanan jarum jam serta jarak r dari titik asal, seperti dalam Gambar 4.2.3. Kita dapat melihat bahwa

$$z = a + bi = r(\cos\theta + i\sin\theta).$$

Jadi,

$$r = |z| = \sqrt{a^2 + b^2}$$

dan

$$\begin{aligned} a &= r\cos\theta \\ b &= r\sin\theta. \end{aligned}$$

Kadang-kadang kita menyingkat $r(\cos\theta + i\sin\theta)$ sebagai $r\,\mathrm{cis}\,\theta$. Untuk memastikan bahwa representasi z terdefinisi dengan baik, kita juga mensyaratkan $0^\circ \le \theta < 360^\circ$. Jika sudut diukur dalam radian, maka $0 \le \theta < 2\pi$.

Contoh 4.2.4 Misalkan $z = 2\,\mathrm{cis}\,60^\circ$. Maka

$$a = 2\cos 60^\circ = 1$$

dan

$$b = 2\sin 60^\circ = \sqrt{3}.$$

Jadi, representasi rektangularnya adalah $z = 1 + \sqrt{3}\,i$.

Sebaliknya, jika diberikan representasi rektangular suatu bilangan kompleks, sering kali berguna untuk mengetahui representasi polar bilangan tersebut. Jika $z = 3\sqrt{2} - 3\sqrt{2}\,i$, maka

$$r = \sqrt{a^2 + b^2} = \sqrt{36} = 6$$

dan

$$\theta = \arctan\left(\frac{b}{a}\right) = \arctan(-1) = 315^\circ,$$

sehingga $3\sqrt{2} - 3\sqrt{2}\,i = 6\,\mathrm{cis}\,315^\circ$. ▲

Representasi polar suatu bilangan kompleks memudahkan pencarian hasil kali dan pangkat bilangan kompleks. Pembuktian proposisi berikut bersifat langsung dan diserahkan sebagai latihan.

Proposisi 4.2.5 *Misalkan* $z = r\,\mathrm{cis}\,\theta$ *dan* $w = s\,\mathrm{cis}\,\phi$ *dua bilangan kompleks tak nol. Maka*

$$zw = rs\,\mathrm{cis}(\theta + \phi).$$

Contoh 4.2.6 Jika $z = 3\,\mathrm{cis}(\pi/3)$ dan $w = 2\,\mathrm{cis}(\pi/6)$, maka $zw = 6\,\mathrm{cis}(\pi/2) = 6i$. ▲

Teorema 4.2.7 DeMoivre. *Misalkan* $z = r\,\mathrm{cis}\,\theta$ *bilangan kompleks tak nol. Maka*

$$[r\,\mathrm{cis}\,\theta]^n = r^n\,\mathrm{cis}(n\theta)$$

untuk $n = 1, 2, \ldots$.

Bukti. Kita akan menggunakan induksi pada n. Untuk $n = 1$, teorema tersebut langsung benar. Andaikan teorema itu benar untuk setiap k sedemikian sehingga $1 \leq k \leq n$. Maka

$$\begin{aligned} z^{n+1} &= z^n z \\ &= r^n(\cos n\theta + i \sin n\theta) r(\cos\theta + i\sin\theta) \\ &= r^{n+1}[(\cos n\theta\cos\theta - \sin n\theta\sin\theta) + i(\sin n\theta\cos\theta + \cos n\theta\sin\theta)] \\ &= r^{n+1}[\cos(n\theta+\theta) + i\sin(n\theta+\theta)] \\ &= r^{n+1}[\cos(n+1)\theta + i\sin(n+1)\theta]. \end{aligned}$$

■

Contoh 4.2.8 Misalkan $z = 1 + i$ dan kita ingin menghitung z^{10}. Alih-alih menghitung $(1+i)^{10}$ secara langsung, jauh lebih mudah beralih ke koordinat polar dan menghitung z^{10} menggunakan Teorema DeMoivre:

$$\begin{aligned} z^{10} &= (1+i)^{10} \\ &= \left(\sqrt{2}\,\mathrm{cis}\left(\frac{\pi}{4}\right)\right)^{10} \\ &= (\sqrt{2}\,)^{10}\,\mathrm{cis}\left(\frac{5\pi}{2}\right) \\ &= 32\,\mathrm{cis}\left(\frac{\pi}{2}\right) \\ &= 32i. \end{aligned}$$

▲

4.2.1 Grup Lingkaran dan Akar Kesatuan

Grup perkalian bilangan kompleks, $\mathbb{C}^*$, mempunyai beberapa subgrup yang menarik. Sementara $\mathbb{Q}^*$ dan $\mathbb{R}^*$ tidak mempunyai subgrup berorde hingga yang menarik, $\mathbb{C}^*$ mempunyai banyak subgrup seperti itu. Pertama-tama kita mempertimbangkan **grup lingkaran**,

$$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}.$$

Proposisi berikut merupakan akibat langsung dari Proposisi 4.2.5.

Proposisi 4.2.9 *Grup lingkaran merupakan subgrup dari* $\mathbb{C}^*$.

Meskipun grup lingkaran berorde tak hingga, grup tersebut mempunyai banyak subgrup hingga yang menarik. Misalkan $H = \{1, -1, i, -i\}$. Maka H merupakan subgrup dari grup lingkaran. Selain itu, 1, -1, i, dan $-i$ tepat merupakan bilangan-bilangan kompleks yang memenuhi persamaan $z^4 = 1$. Bilangan kompleks yang memenuhi persamaan $z^n = 1$ disebut **akar kesatuan ke-n**.

Teorema 4.2.10 *Jika $z^n = 1$, maka akar kesatuan ke-n adalah*

$$z = \operatorname{cis}\left(\frac{2k\pi}{n}\right),$$

dengan $k = 0, 1, \ldots, n-1$. Lebih lanjut, akar kesatuan ke-n membentuk subgrup siklik dari $\mathbb{T}$ yang berorde n

Bukti. Berdasarkan Teorema DeMoivre,

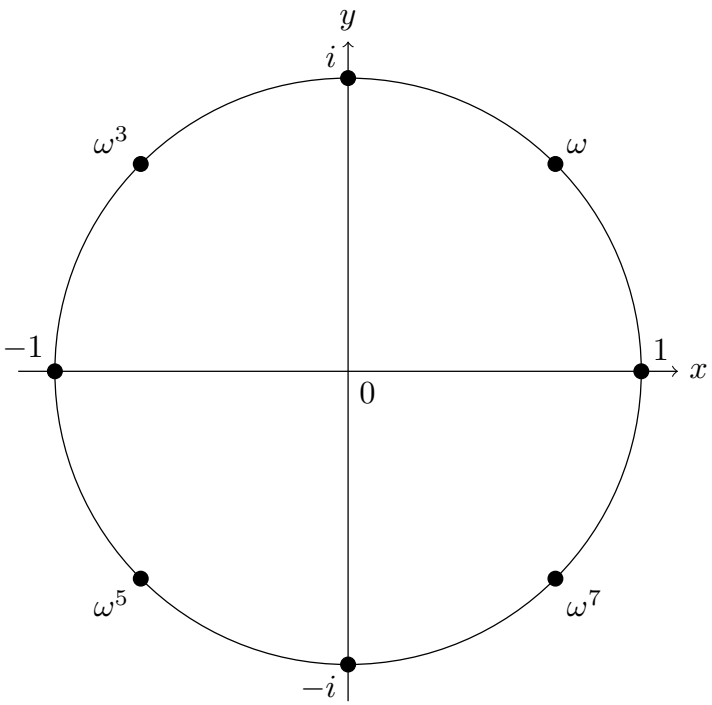
$$z^n = \operatorname{cis}\left(n\frac{2k\pi}{n}\right) = \operatorname{cis}(2k\pi) = 1.$$

Nilai-nilai z tersebut berbeda karena bilangan $2k\pi/n$ semuanya berbeda serta lebih besar daripada atau sama dengan 0, tetapi lebih kecil daripada 2π. Fakta bahwa nilai-nilai tersebut merupakan semua akar persamaan $z^n = 1$ diperoleh dari Korolari 17.2.4, yang menyatakan bahwa polinomial berderajat n mempunyai paling banyak n akar. Pembuktian bahwa akar kesatuan ke-n membentuk subgrup siklik dari $\mathbb{T}$ diserahkan sebagai latihan. ■

Pembangkit bagi grup akar kesatuan ke-n disebut **akar kesatuan ke-n primitif**.

Contoh 4.2.11 Akar kesatuan ke-8 dapat direpresentasikan sebagai delapan titik yang berjarak sama pada lingkaran satuan (Gambar 4.2.12). Akar kesatuan ke-8 primitif adalah

$$\begin{aligned}
\omega &= \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\
\omega^3 &= -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\
\omega^5 &= -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \\
\omega^7 &= \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i.
\end{aligned}$$



Gambar 4.2.12 Akar kesatuan ke-8

▲

4.3 Metode Kuadrat Berulang

Menghitung pangkat besar dapat memakan waktu sangat lama. Sebagaimana siapa pun dapat menghitung 2^2 atau 2^8, semua orang mengetahui cara menghitung

$$2^{2^{1,000,000}}.$$

Akan tetapi, bilangan tersebut begitu besar sehingga kita tidak ingin mencoba melakukan perhitungannya; lebih jauh lagi, setelah titik tertentu komputasi itu tidak mungkin dilakukan sekalipun semua komputer di dunia tersedia bagi kita. Bahkan menuliskan representasi desimal bilangan yang sangat besar mungkin tidak masuk akal. Panjangnya dapat mencapai ribuan atau bahkan jutaan digit. Akan tetapi, jika kita dapat menghitung sesuatu seperti

$$2^{37,398,332} \pmod{46,389},$$

kita dapat menuliskan hasilnya dengan sangat mudah karena hasil tersebut berupa bilangan antara 0 dan 46,388. Jika kita ingin menghitung perpangkatan modulo n dengan cepat dan efisien, kita harus menggunakan cara yang cerdik.[1]

Hal pertama yang perlu diperhatikan adalah bahwa sebarang bilangan a dapat ditulis sebagai jumlah pangkat-pangkat berbeda dari 2; artinya, kita dapat menuliskan

$$a = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_n},$$

dengan $k_1 < k_2 < \cdots < k_n$. Ini tidak lain adalah representasi biner dari a. Sebagai contoh, representasi biner dari 57 adalah 111001, karena kita dapat menuliskan $57 = 2^0 + 2^3 + 2^4 + 2^5$.

[1] Hasil-hasil dalam bagian ini hanya diperlukan dalam Bab 7

Hukum-hukum eksponen tetap berlaku dalam $\mathbb{Z}_n$; artinya, jika $b \equiv a^x \pmod{n}$ dan $c \equiv a^y \pmod{n}$, maka $bc \equiv a^{x+y} \pmod{n}$. Kita dapat menghitung $a^{2^k} \pmod{n}$ dengan k perkalian melalui perhitungan

$$\begin{aligned} &a^{2^0} \pmod{n} \\ &a^{2^1} \pmod{n} \\ &\vdots \\ &a^{2^k} \pmod{n}. \end{aligned}$$

Setiap langkah melibatkan penguadratan jawaban yang diperoleh pada langkah sebelumnya, pembagian dengan n, dan pengambilan sisanya.

Contoh 4.3.1 Kita akan menghitung $271^{321} \pmod{481}$. Perhatikan bahwa

$$321 = 2^0 + 2^6 + 2^8;$$

jadi, menghitung $271^{321} \pmod{481}$ sama dengan menghitung

$$271^{2^0+2^6+2^8} \equiv 271^{2^0} \cdot 271^{2^6} \cdot 271^{2^8} \pmod{481}.$$

Jadi, cukup dihitung $271^{2^i} \pmod{481}$ dengan $i = 0, 6, 8$. Sangat mudah dilihat bahwa

$$271^{2^1} = 73{,}441 \equiv 329 \pmod{481}.$$

Kita dapat menguadratkan hasil ini untuk memperoleh nilai $271^{2^2} \pmod{481}$:

$$\begin{aligned} 271^{2^2} &\equiv (271^{2^1})^2 \pmod{481} \\ &\equiv (329)^2 \pmod{481} \\ &\equiv 108{,}241 \pmod{481} \\ &\equiv 16 \pmod{481}. \end{aligned}$$

Kita menggunakan fakta bahwa $(a^{2^n})^2 \equiv a^{2 \cdot 2^n} \equiv a^{2^{n+1}} \pmod{n}$. Dengan melanjutkan perhitungan, kita memperoleh

$$271^{2^6} \equiv 419 \pmod{481}$$

dan

$$271^{2^8} \equiv 16 \pmod{481}.$$

Oleh karena itu,

$$\begin{aligned} 271^{321} &\equiv 271^{2^0+2^6+2^8} \pmod{481} \\ &\equiv 271^{2^0} \cdot 271^{2^6} \cdot 271^{2^8} \pmod{481} \\ &\equiv 271 \cdot 419 \cdot 16 \pmod{481} \\ &\equiv 1{,}816{,}784 \pmod{481} \\ &\equiv 47 \pmod{481}. \end{aligned}$$

▲

Metode kuadrat berulang akan menjadi perangkat yang sangat berguna ketika kita membahas kriptografi RSA dalam Bab 7. Untuk menyandikan dan menguraikan pesan secara wajar dalam skema ini, kita harus mampu menghitung pangkat besar bilangan bulat modulo n dengan cepat.

4.4 Pertanyaan Bacaan

1. Berapakah orde elemen 3 dalam $U(20)$?

2. Berapakah orde elemen 5 dalam $U(23)$?

3. Tentukan tiga pembangkit dari $\mathbb{Z}_8$.

4. Tentukan tiga pembangkit dari akar kesatuan ke-5.

5. Tunjukkan cara menghitung $15^{40} \pmod{23}$ secara efisien dengan tangan. Periksa jawaban Anda dengan Sage.

4.5 Latihan

1. Buktikan atau sangkal setiap pernyataan berikut.

(a) Semua pembangkit dari $\mathbb{Z}_{60}$ adalah prima.

(b) $U(8)$ bersifat siklik.

(c) $\mathbb{Q}$ bersifat siklik.

(d) Jika setiap subgrup sejati dari suatu grup G bersifat siklik, maka G merupakan grup siklik.

(e) Grup yang mempunyai berhingga banyak subgrup merupakan grup hingga.

Petunjuk. (a) Salah; (c) salah; (e) benar.

2. Tentukan orde setiap elemen berikut.

(a) $5 \in \mathbb{Z}_{12}$

(b) $\sqrt{3} \in \mathbb{R}$

(c) $\sqrt{3} \in \mathbb{R}^*$

(d) $-i \in \mathbb{C}^*$

(e) $72 \in \mathbb{Z}_{240}$

(f) $312 \in \mathbb{Z}_{471}$

Petunjuk. (a) 12; (c) tak hingga; (e) 10.

3. Cantumkan semua elemen dalam setiap subgrup berikut.

(a) Subgrup dari $\mathbb{Z}$ yang dibangkitkan oleh 7

(b) Subgrup dari $\mathbb{Z}_{24}$ yang dibangkitkan oleh 15

(c) Semua subgrup dari $\mathbb{Z}_{12}$

(d) Semua subgrup dari $\mathbb{Z}_{60}$

(e) Semua subgrup dari $\mathbb{Z}_{13}$

(f) Semua subgrup dari $\mathbb{Z}_{48}$

(g) Subgrup yang dibangkitkan oleh 3 dalam $U(20)$

(h) Subgrup yang dibangkitkan oleh 5 dalam $U(18)$

(i) Subgrup dari $\mathbb{R}^*$ yang dibangkitkan oleh 7

(j) Subgrup dari $\mathbb{C}^*$ yang dibangkitkan oleh i dengan $i^2 = -1$

(k) Subgrup dari $\mathbb{C}^*$ yang dibangkitkan oleh $2i$

(l) Subgrup dari $\mathbb{C}^*$ yang dibangkitkan oleh $(1+i)/\sqrt{2}$

(m) Subgrup dari $\mathbb{C}^*$ yang dibangkitkan oleh $(1+\sqrt{3}\,i)/2$

Petunjuk. (a) $7\mathbb{Z} = \{\ldots, -7, 0, 7, 14, \ldots\}$; (b) $\{0, 3, 6, 9, 12, 15, 18, 21\}$; (c) $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, $\{0, 2, 4, 6, 8, 10\}$; (g) $\{1, 3, 7, 9\}$; (j) $\{1, -1, i, -i\}$.

4. Tentukan subgrup dari $GL_2(\mathbb{R})$ yang dibangkitkan oleh setiap matriks berikut.

(a) $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ (e) $\begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}$

(b) $\begin{pmatrix} 0 & 1/3 \\ 3 & 0 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ (f) $\begin{pmatrix} \sqrt{3}/2 & 1/2 \\ -1/2 & \sqrt{3}/2 \end{pmatrix}$

Petunjuk. (a)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(c)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

5. Tentukan orde setiap elemen dalam $\mathbb{Z}_{18}$.

6. Tentukan orde setiap elemen dalam grup simetri persegi, D_4.

7. Tentukan semua subgrup siklik dari grup kuaternion, Q_8?

8. Cantumkan semua subgrup siklik dari $U(30)$.

9. Cantumkan setiap pembangkit dari setiap subgrup berorde 8 dalam $\mathbb{Z}_{32}$.

10. Tentukan semua elemen berorde hingga dalam setiap grup berikut. Di sini "$*$" menunjukkan himpunan yang unsur nolnya dihapus.

(a) $\mathbb{Z}$ (b) $\mathbb{Q}^*$ (c) $\mathbb{R}^*$

Petunjuk. (a) 0; (b) $1, -1$.

11. Jika $a^{24} = e$ dalam suatu grup G, apa saja kemungkinan orde a?

Petunjuk. $1, 2, 3, 4, 6, 8, 12, 24$.

12. Tentukan grup siklik dengan tepat satu pembangkit. Dapatkah Anda menentukan grup siklik dengan tepat dua pembangkit? Empat pembangkit? Bagaimana dengan n pembangkit?

13. Untuk $n \leq 20$, grup $U(n)$ mana yang bersifat siklik? Rumuskan dugaan mengenai hal yang berlaku secara umum. Dapatkah Anda membuktikan dugaan tersebut?

14. Misalkan

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{dan} \quad B = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

merupakan elemen-elemen dalam $GL_2(\mathbb{R})$. Tunjukkan bahwa A dan B berorde hingga, tetapi AB tidak.

15. Hitung setiap bentuk berikut.

(a) $(3-2i)+(5i-6)$
(b) $(4-5i)-\overline{(4i-4)}$
(c) $(5-4i)(7+2i)$
(d) $(9-i)\overline{(9-i)}$
(e) i^{45}
(f) $(1+i)+\overline{(1+i)}$

Petunjuk. (a) $-3+3i$; (c) $43-18i$; (e) i

16. Ubah bilangan-bilangan kompleks berikut ke bentuk $a+bi$.

(a) $2\,\mathrm{cis}(\pi/6)$
(b) $5\,\mathrm{cis}(9\pi/4)$
(c) $3\,\mathrm{cis}(\pi)$
(d) $\mathrm{cis}(7\pi/4)/2$

Petunjuk. (a) $\sqrt{3}+i$; (c) -3.

17. Ubah bilangan-bilangan kompleks berikut ke representasi polar.

(a) $1-i$
(b) -5
(c) $2+2i$
(d) $\sqrt{3}+i$
(e) $-3i$
(f) $2i+2\sqrt{3}$

Petunjuk. (a) $\sqrt{2}\,\mathrm{cis}(7\pi/4)$; (c) $2\sqrt{2}\,\mathrm{cis}(\pi/4)$; (e) $3\,\mathrm{cis}(3\pi/2)$.

18. Hitung setiap bentuk berikut.

(a) $(1+i)^{-1}$
(b) $(1-i)^6$
(c) $(\sqrt{3}+i)^5$
(d) $(-i)^{10}$
(e) $((1-i)/2)^4$
(f) $(-\sqrt{2}-\sqrt{2}\,i)^{12}$
(g) $(-2+2i)^{-5}$

Petunjuk. (a) $(1-i)/2$; (c) $16(i-\sqrt{3}\,)$; (e) $-1/4$.

19. Buktikan setiap pernyataan berikut.

(a) $|z|=|\overline{z}|$
(b) $z\overline{z}=|z|^2$
(c) $z^{-1}=\overline{z}/|z|^2$
(d) $|z+w|\le|z|+|w|$
(e) $|z-w|\ge||z|-|w||$
(f) $|zw|=|z||w|$

20. Cantumkan dan gambarkan akar kesatuan ke-6. Apa saja pembangkit grup ini? Apa saja akar kesatuan ke-6 primitif?

21. Cantumkan dan gambarkan akar kesatuan ke-5. Apa saja pembangkit grup ini? Apa saja akar kesatuan ke-5 primitif?

22. Hitung setiap bentuk berikut.

(a) $292^{3171} \pmod{582}$
(b) $2557^{341} \pmod{5681}$
(c) $2071^{9521} \pmod{4724}$
(d) $971^{321} \pmod{765}$

Petunjuk. (a) 292; (c) 1523.

23. Misalkan $a, b \in G$. Buktikan pernyataan-pernyataan berikut.

(a) Orde a sama dengan orde a^{-1}.

(b) Untuk setiap $g \in G$, berlaku $|a| = |g^{-1}ag|$.

(c) Orde ab sama dengan orde ba.

24. Misalkan p dan q bilangan prima yang berbeda. Berapa banyak pembangkit yang dimiliki $\mathbb{Z}_{pq}$?

25. Misalkan p bilangan prima dan r bilangan bulat positif. Berapa banyak pembangkit yang dimiliki $\mathbb{Z}_{p^r}$?

26. Buktikan bahwa $\mathbb{Z}_p$ tidak mempunyai subgrup nontrivial jika p prima.

27. Jika g dan h masing-masing berorde 15 dan 16 dalam suatu grup G, berapakah orde $\langle g\rangle \cap \langle h\rangle$?

Petunjuk. $|\langle g\rangle \cap \langle h\rangle| = 1$.

28. Misalkan a suatu elemen dalam grup G. Tentukan pembangkit bagi subgrup $\langle a^m\rangle \cap \langle a^n\rangle$.

29. Buktikan bahwa $\mathbb{Z}_n$ mempunyai sejumlah genap pembangkit untuk $n > 2$.

30. Misalkan G suatu grup dan a, $b \in G$. Buktikan bahwa jika $|a| = m$ dan $|b| = n$ dengan $\gcd(m, n) = 1$, maka $\langle a\rangle \cap \langle b\rangle = \{e\}$.

31. Misalkan G grup abelian. Tunjukkan bahwa elemen-elemen berorde hingga dalam G membentuk subgrup. Subgrup ini disebut **subgrup torsi** dari G.

Petunjuk. Elemen identitas dalam sebarang grup berorde hingga. Misalkan $g, h \in G$ masing-masing berorde m dan n. Karena $(g^{-1})^m = e$ dan $(gh)^{mn} = e$, elemen-elemen berorde hingga dalam G membentuk subgrup dari G.

32. Misalkan G grup siklik hingga berorde n yang dibangkitkan oleh x. Tunjukkan bahwa jika $y = x^k$ dengan $\gcd(k, n) = 1$, maka y harus merupakan pembangkit dari G.

33. Jika G grup abelian yang memuat sepasang subgrup siklik berorde 2, tunjukkan bahwa G harus memuat subgrup berorde 4. Apakah subgrup ini harus bersifat siklik?

34. Misalkan G grup abelian berorde pq dengan $\gcd(p, q) = 1$. Jika G memuat elemen a dan b yang masing-masing berorde p dan q, tunjukkan bahwa G bersifat siklik.

35. Buktikan bahwa subgrup-subgrup dari $\mathbb{Z}$ tepat merupakan $n\mathbb{Z}$ untuk $n = 0, 1, 2, \ldots$.

36. Buktikan bahwa pembangkit-pembangkit dari $\mathbb{Z}_n$ adalah bilangan bulat r sedemikian sehingga $1 \leq r < n$ dan $\gcd(r, n) = 1$.

37. Buktikan bahwa jika G tidak mempunyai subgrup sejati nontrivial, maka G merupakan grup siklik.

Petunjuk. Jika g merupakan elemen yang berbeda dari identitas dalam G, g harus membangkitkan G; jika tidak, $\langle g\rangle$ merupakan subgrup sejati nontrivial dari G.

38. Buktikan bahwa orde suatu elemen dalam grup siklik G harus membagi orde grup tersebut.

39. Buktikan bahwa jika G grup siklik berorde m dan $d \mid m$, maka G harus mempunyai subgrup berorde d.

40. Untuk bilangan bulat n manakah -1 merupakan akar kesatuan ke-n?

41. Jika $z = r(\cos\theta + i\sin\theta)$ dan $w = s(\cos\phi + i\sin\phi)$ dua bilangan kompleks tak nol, tunjukkan bahwa

$$zw = rs[\cos(\theta + \phi) + i\sin(\theta + \phi)].$$

42. Buktikan bahwa grup lingkaran merupakan subgrup dari $\mathbb{C}^*$.

43. Buktikan bahwa akar kesatuan ke-n membentuk subgrup siklik dari $\mathbb{T}$ yang berorde n.

44. Misalkan $\alpha \in \mathbb{T}$. Buktikan bahwa $\alpha^m = 1$ dan $\alpha^n = 1$ jika dan hanya jika $\alpha^d = 1$ untuk $d = \gcd(m, n)$.

45. Misalkan $z \in \mathbb{C}^*$. Jika $|z| \neq 1$, buktikan bahwa orde z tak hingga.

46. Misalkan $z = \cos\theta + i \sin\theta$ berada dalam $\mathbb{T}$ dengan $\theta \in \mathbb{Q}$. Buktikan bahwa orde z tak hingga.

4.6 Latihan Pemrograman

1. Tulislah program komputer yang menyatakan sebarang bilangan desimal sebagai jumlah pangkat-pangkat berbeda dari 2. Berapakah bilangan bulat terbesar yang dapat ditangani program Anda?

2. Tulislah program komputer untuk menghitung $a^x \pmod n$ dengan metode kuadrat berulang. Berapakah nilai terbesar n dan x yang dapat diterima program Anda?

4.7 Referensi dan Bacaan yang Disarankan

[1] Koblitz, N. *A Course in Number Theory and Cryptography*. Edisi ke-2. Springer, New York, 1994.

[2] Pomerance, C. "Cryptology and Computational Number Theory—An Introduction," dalam *Cryptology and Computational Number Theory*, Pomerance, C., peny. Proceedings of Symposia in Applied Mathematics, jil. 42, American Mathematical Society, Providence, RI, 1990. Buku ini memberikan uraian yang sangat baik mengenai penggunaan metode kuadrat berulang dalam kriptografi.

5

Grup Permutasi

Grup permutasi menempati posisi sentral dalam kajian simetri geometris dan teori Galois, yaitu kajian untuk menemukan penyelesaian persamaan polinomial. Grup ini juga menyediakan banyak contoh grup nonabelian.

Mari kita ingat kembali simetri segitiga sama sisi $\triangle ABC$ dari Bab 3. Simetri tersebut sebenarnya terdiri atas permutasi ketiga titik sudutnya, dengan suatu **permutasi** dari himpunan $S = \{A, B, C\}$ merupakan pemetaan injektif dan surjektif $\pi : S \to S$. Ketiga titik sudut tersebut memiliki enam permutasi berikut.

$$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$
$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \quad \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

Kita telah menggunakan larik

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

untuk menyatakan permutasi yang membawa A ke B, B ke C, dan C ke A. Yaitu,

$$A \mapsto B$$
$$B \mapsto C$$
$$C \mapsto A.$$

Simetri suatu segitiga membentuk grup. Dalam bab ini kita akan mempelajari grup jenis ini.

5.1 Definisi dan Notasi

Secara umum, permutasi suatu himpunan X membentuk grup S_X. Jika X merupakan himpunan hingga, kita dapat mengasumsikan $X = \{1, 2, \ldots, n\}$. Dalam hal ini kita menulis S_n sebagai pengganti S_X. Teorema berikut menyatakan bahwa S_n merupakan grup. Grup ini kita sebut **grup simetris** pada n huruf.

Teorema 5.1.1 *Grup simetris pada n huruf, S_n, merupakan grup dengan $n!$ elemen, dengan operasi biner berupa komposisi pemetaan.*

BUKTI. Identitas S_n tidak lain adalah pemetaan identitas yang membawa 1 ke 1, 2 ke 2, ..., n ke n. Jika $f : S_n \to S_n$ merupakan permutasi, maka f^{-1} ada, karena f injektif dan surjektif; jadi, setiap permutasi memiliki invers. Komposisi pemetaan bersifat asosiatif, sehingga operasi grup tersebut bersifat asosiatif. Bukti bahwa $|S_n| = n!$ diserahkan sebagai latihan. ■

Subgrup dari S_n disebut **grup permutasi**.

Contoh 5.1.2 Perhatikan subgrup G dari S_5 yang terdiri atas permutasi identitas id dan permutasi

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$
$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

Tabel berikut menunjukkan cara mengalikan elemen-elemen dalam grup permutasi G.

$\circ$	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	id	μ	τ
τ	τ	μ	id	σ
μ	μ	τ	σ	id

▲

Catatan 5.1.3 Walaupun wajar mengalikan elemen suatu grup dari kiri ke kanan, fungsi dikomposisikan dari kanan ke kiri. Misalkan σ dan τ merupakan permutasi pada himpunan X. Untuk mengomposisikan σ dan τ sebagai fungsi, kita menghitung $(\sigma \circ \tau)(x) = \sigma(\tau(x))$. Artinya, kita menerapkan τ terlebih dahulu, kemudian σ. Ada beberapa cara untuk mengatasi ketidakkonsistenan ini. *Kita akan menggunakan konvensi mengalikan permutasi dari kanan ke kiri. Untuk menghitung $\sigma\tau$, terapkan τ terlebih dahulu, kemudian σ.* Artinya, dengan $\sigma\tau(x)$ kita maksudkan $\sigma(\tau(x))$. (Cara lain untuk menyelesaikan masalah ini ialah menulis fungsi di sebelah kanan; yaitu, alih-alih menulis $\sigma(x)$, kita dapat menulis $(x)\sigma$. Kita juga dapat mengalikan permutasi dari kiri ke kanan agar sesuai dengan cara biasa mengalikan elemen dalam grup. Semua metode ini memang pernah digunakan.

Contoh 5.1.4 Perkalian permutasi biasanya tidak komutatif. Misalkan

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Maka

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix},$$

tetapi

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

▲

5.1.1 Notasi Siklus

Notasi yang sejauh ini kita gunakan untuk menyatakan permutasi terasa rumit, kalau tidak ingin disebut sangat merepotkan. Agar dapat bekerja secara efektif dengan grup permutasi, kita memerlukan cara yang lebih ringkas untuk menuliskan dan memanipulasi permutasi.

Suatu permutasi $\sigma \in S_X$ merupakan **siklus dengan panjang** k jika terdapat elemen $a_1, a_2, \ldots, a_k \in X$ sedemikian sehingga

$$\begin{aligned} \sigma(a_1) &= a_2 \\ \sigma(a_2) &= a_3 \\ &\vdots \\ \sigma(a_k) &= a_1 \end{aligned}$$

dan $\sigma(x) = x$ untuk semua elemen lain $x \in X$. Kita akan menulis $(a_1, a_2, \ldots, a_k)$ untuk menyatakan siklus σ. Siklus merupakan unsur pembangun semua permutasi.

Contoh 5.1.5 Permutasi

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (1\,6\,2\,3\,5\,4)$$

merupakan siklus dengan panjang 6, sedangkan

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix} = (2\,4\,3)$$

merupakan siklus dengan panjang 3.

Tidak setiap permutasi merupakan siklus. Perhatikan permutasi

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1\,2\,4\,3)(5\,6).$$

Permutasi ini sebenarnya memuat satu siklus dengan panjang 2 dan satu siklus dengan panjang 4. ▲

Contoh 5.1.6 Hasil kali siklus sangat mudah dihitung. Misalkan

$$\sigma = (1\,3\,5\,2) \quad \text{dan} \quad \tau = (2\,5\,6).$$

Jika kita memandang σ sebagai

$$1 \mapsto 3, \qquad 3 \mapsto 5, \qquad 5 \mapsto 2, \qquad 2 \mapsto 1,$$

dan τ sebagai

$$2 \mapsto 5, \qquad 5 \mapsto 6, \qquad 6 \mapsto 2,$$

maka untuk $\sigma\tau$, dengan mengingat bahwa kita menerapkan τ terlebih dahulu kemudian σ, harus berlaku

$$1 \mapsto 3, \qquad 3 \mapsto 5, \qquad 5 \mapsto 6, \qquad 6 \mapsto 2 \mapsto 1,$$

atau $\sigma\tau = (1\,3\,5\,6)$. Jika $\mu = (1\,6\,3\,4)$, maka $\sigma\mu = (1\,6\,5\,2)(3\,4)$. ▲

Dua siklus dalam S_X, $\sigma = (a_1, a_2, \ldots, a_k)$ dan $\tau = (b_1, b_2, \ldots, b_l)$, dikatakan **saling lepas** jika $a_i \neq b_j$ untuk semua i dan j.

Contoh 5.1.7 Siklus (1 3 5) dan (2 7) saling lepas; namun, siklus (1 3 5) dan (3 4 7) tidak saling lepas. Dengan menghitung hasil kalinya, kita peroleh

$$(1\,3\,5)(2\,7) = (1\,3\,5)(2\,7)$$
$$(1\,3\,5)(3\,4\,7) = (1\,3\,4\,7\,5).$$

Hasil kali dua siklus yang tidak saling lepas mungkin dapat disederhanakan; hasil kali siklus-siklus yang saling lepas tidak dapat disederhanakan. ▲

Proposisi 5.1.8 *Misalkan σ dan τ merupakan dua siklus saling lepas dalam S_X. Maka $\sigma\tau = \tau\sigma$.*

Bukti. Misalkan $\sigma = (a_1, a_2, \ldots, a_k)$ dan $\tau = (b_1, b_2, \ldots, b_l)$. Kita harus menunjukkan bahwa $\sigma\tau(x) = \tau\sigma(x)$ untuk semua $x \in X$. Jika x tidak berada dalam $\{a_1, a_2, \ldots, a_k\}$ maupun $\{b_1, b_2, \ldots, b_l\}$, maka σ dan τ keduanya menetapkan x. Artinya, $\sigma(x) = x$ dan $\tau(x) = x$. Jadi,

$$\sigma\tau(x) = \sigma(\tau(x)) = \sigma(x) = x = \tau(x) = \tau(\sigma(x)) = \tau\sigma(x).$$

Jangan lupa bahwa kita mengalikan permutasi dari kanan ke kiri, berlawanan dengan urutan yang biasanya digunakan untuk mengalikan elemen grup. Sekarang andaikan $x \in \{a_1, a_2, \ldots, a_k\}$. Maka $\sigma(a_i) = a_{(i \bmod k)+1}$; yaitu,

$$\begin{aligned} a_1 &\mapsto a_2 \\ a_2 &\mapsto a_3 \\ &\vdots \\ a_{k-1} &\mapsto a_k \\ a_k &\mapsto a_1. \end{aligned}$$

Namun, $\tau(a_i) = a_i$ karena σ dan τ saling lepas. Oleh karena itu,

$$\begin{aligned} \sigma\tau(a_i) &= \sigma(\tau(a_i)) \\ &= \sigma(a_i) \\ &= a_{(i \bmod k)+1} \\ &= \tau(a_{(i \bmod k)+1}) \\ &= \tau(\sigma(a_i)) \\ &= \tau\sigma(a_i). \end{aligned}$$

Demikian pula, jika $x \in \{b_1, b_2, \ldots, b_l\}$, maka σ dan τ juga komutatif. ■

Teorema 5.1.9 *Setiap permutasi dalam S_n dapat ditulis sebagai hasil kali siklus-siklus saling lepas.*

Bukti. Kita dapat mengasumsikan bahwa $X = \{1, 2, \ldots, n\}$. Jika $\sigma \in S_n$ dan kita mendefinisikan X_1 sebagai $\{\sigma(1), \sigma^2(1), \ldots\}$, maka himpunan X_1 hingga karena X hingga. Sekarang, misalkan i adalah bilangan bulat pertama dalam X yang tidak berada dalam X_1 dan definisikan X_2 dengan $\{\sigma(i), \sigma^2(i), \ldots\}$. Sekali lagi, X_2 merupakan himpunan hingga. Dengan melanjutkan cara ini, kita dapat mendefinisikan himpunan-himpunan hingga yang saling lepas $X_3, X_4, \ldots$. Karena X merupakan himpunan hingga, proses ini pasti berakhir dan hanya akan terdapat sejumlah hingga himpunan semacam itu, misalkan r. Jika σ_i

adalah siklus yang didefinisikan oleh

$$\sigma_i(x) = \begin{cases} \sigma(x) & x \in X_i \\ x & x \notin X_i, \end{cases}$$

maka $\sigma = \sigma_1\sigma_2\cdots\sigma_r$. Karena himpunan $X_1, X_2, \ldots, X_r$ saling lepas, siklus $\sigma_1, \sigma_2, \ldots, \sigma_r$ juga harus saling lepas. ■

Contoh 5.1.10 Misalkan

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 6 & 4 \end{pmatrix}.$$

Dengan menggunakan notasi siklus, kita dapat menulis

$$\sigma = (1\,6\,2\,4)$$
$$\tau = (1\,3)(4\,5\,6)$$
$$\sigma\tau = (1\,3\,6)(2\,4\,5)$$
$$\tau\sigma = (1\,4\,3)(2\,5\,6).$$

▲

Catatan 5.1.11 Mulai saat ini, penggunaan notasi siklus akan memudahkan kita dalam menyatakan permutasi. Ketika menggunakan notasi siklus, kita sering melambangkan permutasi identitas dengan (1).

5.1.2 Transposisi

Permutasi paling sederhana adalah siklus dengan panjang 2. Siklus semacam itu disebut **transposisi**. Karena

$$(a_1, a_2, \ldots, a_n) = (a_1, a_n)(a_1, a_{n-1})\cdots(a_1, a_3)(a_1, a_2),$$

setiap siklus dapat ditulis sebagai hasil kali transposisi, kita memperoleh proposisi berikut.

Proposisi 5.1.12 *Setiap permutasi dari suatu himpunan hingga yang memuat sedikitnya dua elemen dapat ditulis sebagai hasil kali transposisi.*

Contoh 5.1.13 Perhatikan permutasi

$$(1\,6)(2\,5\,3) = (1\,6)(2\,3)(2\,5) = (1\,6)(4\,5)(2\,3)(4\,5)(2\,5).$$

Seperti dapat kita lihat, tidak ada cara tunggal untuk menyatakan suatu permutasi sebagai hasil kali transposisi. Sebagai contoh, kita dapat menulis permutasi identitas sebagai $(1\,2)(1\,2)$, sebagai $(1\,3)(2\,4)(1\,3)(2\,4)$, dan dengan banyak cara lainnya. Namun, ternyata tidak ada permutasi yang dapat ditulis sekaligus sebagai hasil kali sejumlah genap transposisi dan sejumlah ganjil transposisi. Sebagai contoh, kita dapat menyatakan permutasi $(1\,6)$ dengan

$$(2\,3)(1\,6)(2\,3)$$

atau dengan

$$(3\,5)(1\,6)(1\,3)(1\,6)(1\,3)(3\,5)(5\,6),$$

tetapi $(1\,6)$ selalu merupakan hasil kali sejumlah ganjil transposisi. ▲

Lema 5.1.14 *Jika identitas ditulis sebagai hasil kali r transposisi,*

$$\mathrm{id} = \tau_1\tau_2\cdots\tau_r,$$

maka r merupakan bilangan genap.

BUKTI. Kita akan menggunakan induksi pada r. Suatu transposisi tidak mungkin merupakan identitas; jadi, $r > 1$. Jika $r = 2$, pembuktian selesai. Andaikan $r > 2$. Dalam hal ini, hasil kali dua transposisi terakhir, $\tau_{r-1}\tau_r$, harus merupakan salah satu kasus berikut:

$$\begin{aligned}(a,b)(a,b) &= \mathrm{id}\\ (b,c)(a,b) &= (a,c)(b,c)\\ (c,d)(a,b) &= (a,b)(c,d)\\ (a,c)(a,b) &= (a,b)(b,c),\end{aligned}$$

dengan a, b, c, dan d semuanya berbeda.

Persamaan pertama hanya menyatakan bahwa suatu transposisi merupakan invers dirinya sendiri. Jika kasus ini terjadi, hapus $\tau_{r-1}\tau_r$ dari hasil kali untuk memperoleh

$$\mathrm{id} = \tau_1\tau_2\cdots\tau_{r-3}\tau_{r-2}.$$

Berdasarkan induksi, $r-2$ genap; jadi, r harus genap.

Dalam setiap tiga kasus lainnya, kita dapat mengganti $\tau_{r-1}\tau_r$ dengan ruas kanan persamaan yang bersesuaian untuk memperoleh hasil kali baru dari r transposisi bagi identitas. Dalam hasil kali baru ini, kemunculan terakhir a berada pada transposisi kedua dari belakang. Kita dapat melanjutkan proses ini dengan $\tau_{r-2}\tau_{r-1}$ untuk memperoleh hasil kali dari $r-2$ transposisi atau hasil kali baru dari r transposisi dengan kemunculan terakhir a berada dalam τ_{r-2}. Jika identitas merupakan hasil kali dari $r-2$ transposisi, sekali lagi pembuktian selesai berdasarkan hipotesis induksi; jika tidak, kita mengulangi prosedur tersebut dengan $\tau_{r-3}\tau_{r-2}$.

Pada suatu tahap, kita akan memperoleh dua transposisi identik yang berdampingan dan saling menghapus, atau a akan digeser sehingga hanya muncul dalam transposisi pertama. Namun, kasus terakhir tidak mungkin terjadi, karena dalam keadaan ini identitas tidak akan menetapkan a. Oleh karena itu, permutasi identitas harus merupakan hasil kali dari $r-2$ transposisi dan, sekali lagi berdasarkan hipotesis induksi, pembuktian selesai. ■

Teorema 5.1.15 *Jika suatu permutasi σ dapat dinyatakan sebagai hasil kali sejumlah genap transposisi, maka setiap hasil kali transposisi lain yang sama dengan σ juga harus memuat sejumlah genap transposisi. Demikian pula, jika σ dapat dinyatakan sebagai hasil kali sejumlah ganjil transposisi, maka setiap hasil kali transposisi lain yang sama dengan σ juga harus memuat sejumlah ganjil transposisi.*

BUKTI. Andaikan

$$\sigma = \sigma_1\sigma_2\cdots\sigma_m = \tau_1\tau_2\cdots\tau_n,$$

dengan m genap. Kita harus menunjukkan bahwa n juga merupakan bilangan genap. Invers dari σ adalah $\sigma_m\cdots\sigma_1$. Karena

$$\mathrm{id} = \sigma\sigma_m\cdots\sigma_1 = \tau_1\cdots\tau_n\sigma_m\cdots\sigma_1,$$

n harus genap berdasarkan Lema 5.1.14. Bukti untuk kasus ketika σ dapat dinyatakan sebagai sejumlah ganjil transposisi diserahkan sebagai latihan. ■

Berdasarkan Teorema 5.1.15, kita mendefinisikan suatu permutasi sebagai

genap jika dapat dinyatakan sebagai sejumlah genap transposisi, dan sebagai **ganjil** jika dapat dinyatakan sebagai sejumlah ganjil transposisi.

5.1.3 Grup Alternasi

Salah satu subgrup terpenting dari S_n adalah himpunan semua permutasi genap, A_n. Grup A_n disebut **grup alternasi pada** n **huruf**.

Teorema 5.1.16 *Himpunan A_n merupakan subgrup dari S_n.*

BUKTI. Karena hasil kali dua permutasi genap juga harus merupakan permutasi genap, A_n tertutup. Identitas merupakan permutasi genap sehingga berada dalam A_n. Jika σ merupakan permutasi genap, maka

$$\sigma = \sigma_1\sigma_2\cdots\sigma_r,$$

dengan σ_i merupakan transposisi dan r genap. Karena invers setiap transposisi adalah dirinya sendiri,

$$\sigma^{-1} = \sigma_r\sigma_{r-1}\cdots\sigma_1$$

juga berada dalam A_n. ■

Proposisi 5.1.17 *Banyaknya permutasi genap dalam S_n, $n \geq 2$, sama dengan banyaknya permutasi ganjil; jadi, orde A_n adalah $n!/2$.*

BUKTI. Misalkan A_n adalah himpunan permutasi genap dalam S_n dan B_n adalah himpunan permutasi ganjil. Jika kita dapat menunjukkan bahwa terdapat bijeksi di antara kedua himpunan ini, keduanya harus memuat jumlah elemen yang sama. Tetapkan suatu transposisi σ dalam S_n. Karena $n \geq 2$, transposisi σ semacam itu ada. Definisikan

$$\lambda_\sigma : A_n \to B_n$$

dengan

$$\lambda_\sigma(\tau) = \sigma\tau.$$

Andaikan $\lambda_\sigma(\tau) = \lambda_\sigma(\mu)$. Maka $\sigma\tau = \sigma\mu$ sehingga

$$\tau = \sigma^{-1}\sigma\tau = \sigma^{-1}\sigma\mu = \mu.$$

Oleh karena itu, λ_σ injektif. Bukti bahwa λ_σ surjektif diserahkan kepada pembaca. ■

Contoh 5.1.18 Grup A_4 merupakan subgrup dari S_4 yang terdiri atas permutasi genap. Terdapat dua belas elemen dalam A_4:

(1)	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)
(1 2 3)	(1 3 2)	(1 2 4)	(1 4 2)
(1 3 4)	(1 4 3)	(2 3 4)	(2 4 3).

Salah satu latihan akhir bab akan meminta Anda menuliskan semua subgrup A_4. Anda akan menemukan bahwa tidak ada subgrup berorde 6. Apakah hal ini mengejutkan Anda? ▲

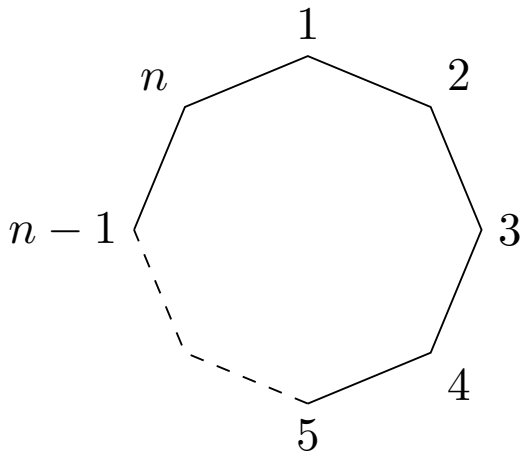
Catatan Sejarah

Lagrange adalah orang pertama yang memandang permutasi sebagai fungsi dari suatu himpunan ke dirinya sendiri, tetapi Cauchy-lah yang mengembangkan teorema dasar dan notasi permutasi. Ia merupakan orang pertama yang meng-

gunakan notasi siklus. Augustin-Louis Cauchy (1789–1857) lahir di Paris pada puncak Revolusi Prancis. Keluarganya segera meninggalkan Paris menuju desa Arcueil untuk menghindari Pemerintahan Teror. Salah satu tetangga keluarganya di sana adalah Pierre-Simon Laplace (1749–1827), yang mendorongnya meniti karier dalam matematika. Cauchy memulai karier sebagai matematikawan dengan menyelesaikan masalah geometri yang diberikan kepadanya oleh Lagrange. Cauchy menulis lebih dari 800 makalah tentang topik yang sangat beragam, seperti persamaan diferensial, grup hingga, matematika terapan, dan analisis kompleks. Ia merupakan salah satu matematikawan yang berperan menjadikan kalkulus rigor. Mungkin lebih banyak teorema dan konsep matematika yang menyandang nama Cauchy daripada nama matematikawan lainnya.

5.2 Grup Dihedral

Jenis khusus grup permutasi lainnya adalah grup dihedral. Ingat kembali grup simetri segitiga sama sisi dalam Bab 3. Grup semacam itu terdiri atas gerak tegar suatu poligon beraturan bersisi n, atau segi-n. Untuk $n = 3, 4, \ldots$, kita mendefinisikan **grup dihedral ke-n** sebagai grup gerak tegar segi-n beraturan. Kita akan melambangkan grup ini dengan D_n. Kita dapat menomori titik-titik sudut segi-n beraturan dengan $1, 2, \ldots, n$ (Gambar 5.2.1). Perhatikan bahwa terdapat tepat n pilihan untuk menggantikan titik sudut pertama. Jika kita menggantikan titik sudut pertama dengan k, maka titik sudut kedua harus digantikan oleh titik sudut $k+1$ atau titik sudut $k-1$; jadi, terdapat $2n$ gerak tegar yang mungkin bagi segi-n tersebut. Hasil ini dirangkum dalam teorema berikut.



Gambar 5.2.1 Segi-n beraturan

Teorema 5.2.2 *Grup dihedral D_n merupakan subgrup dari S_n yang berorde $2n$.*

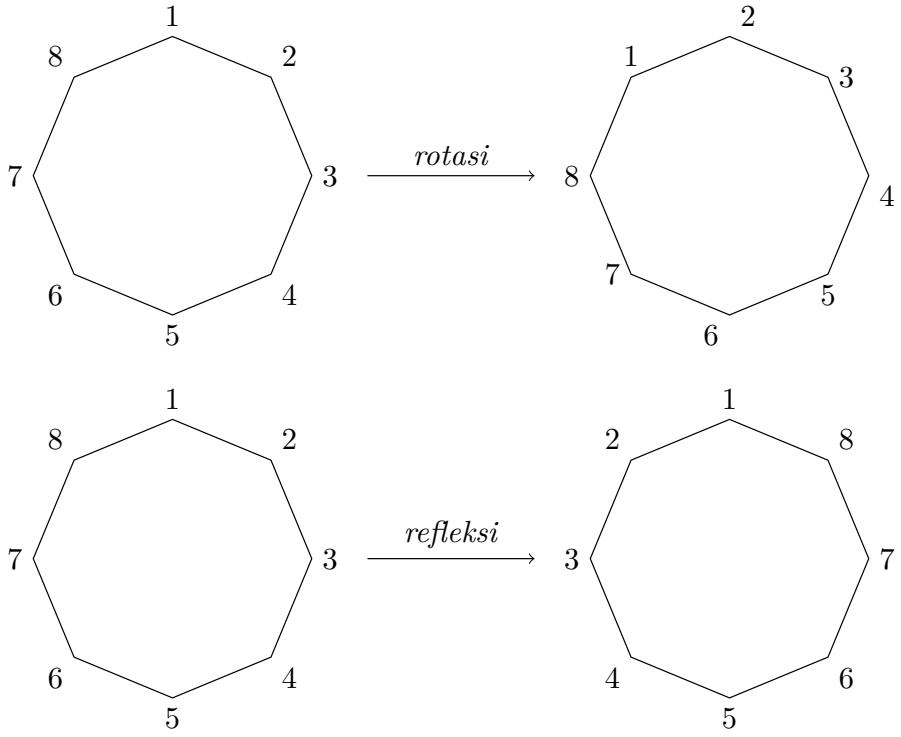
Teorema 5.2.3 *Grup D_n, $n \geq 3$, terdiri atas semua hasil kali dua elemen r dan s, dengan r berorde n dan s berorde 2, serta kedua elemen ini memenuhi relasi $srs = r^{-1}$.*

Bukti. Gerak yang mungkin bagi segi-n beraturan berupa pencerminan atau rotasi (Gambar 5.2.4). Terdapat tepat n rotasi yang mungkin:

$$\text{id}, \frac{360^\circ}{n}, 2 \cdot \frac{360^\circ}{n}, \ldots, (n-1) \cdot \frac{360^\circ}{n}.$$

Kita akan melambangkan rotasi $360°/n$ dengan r. Rotasi r membangkitkan semua rotasi lainnya. Yaitu,

$$r^k = k \cdot \frac{360°}{n}.$$

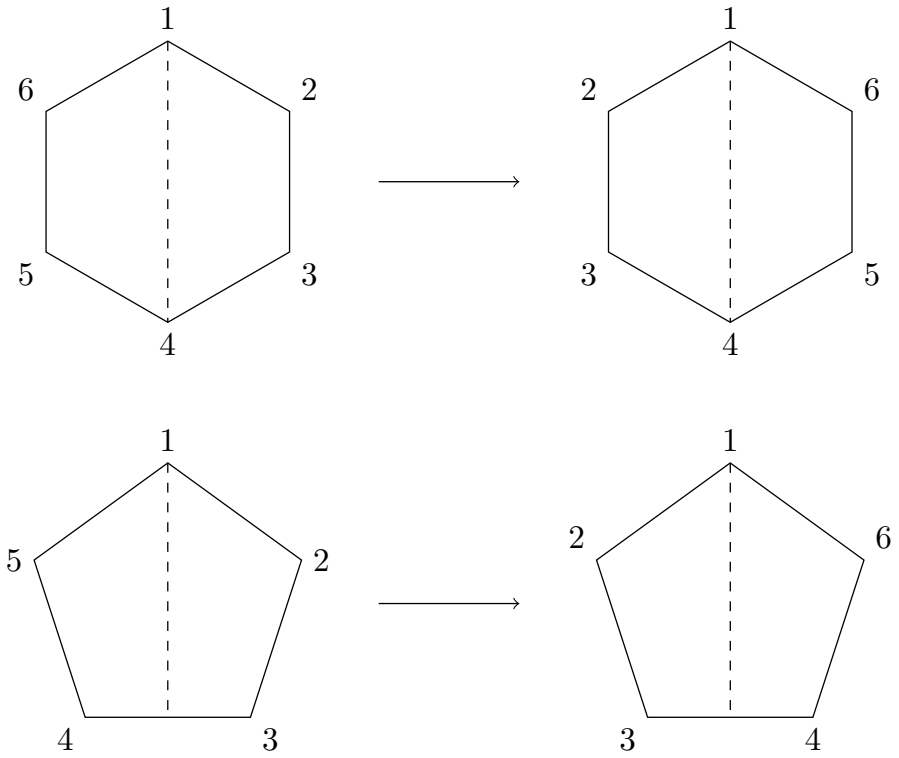


Gambar 5.2.4 Rotasi dan pencerminan segi-n beraturan

Beri label pada n pencerminan sebagai $s_1, s_2, \ldots, s_n$, dengan s_k merupakan pencerminan yang mempertahankan titik sudut k. Terdapat dua kasus pencerminan, bergantung pada apakah n genap atau ganjil. Jika jumlah titik sudut genap, maka dua titik sudut dipertahankan oleh suatu pencerminan, dan $s_1 = s_{n/2+1}, s_2 = s_{n/2+2}, \ldots, s_{n/2} = s_n$. Jika jumlah titik sudut ganjil, maka hanya satu titik sudut yang dipertahankan oleh suatu pencerminan dan $s_1, s_2, \ldots, s_n$ semuanya berbeda (Gambar 5.2.5). Dalam kedua kasus, orde setiap s_k adalah dua. Misalkan $s = s_1$. Maka $s^2 = 1$ dan $r^n = 1$. Karena setiap gerak tegar t dari segi-n menggantikan titik sudut pertama dengan titik sudut k, titik sudut kedua harus digantikan oleh $k+1$ atau $k-1$. Jika titik sudut kedua digantikan oleh $k+1$, maka $t = r^k$. Jika titik sudut kedua digantikan oleh $k-1$, maka $t = r^k s$.[1] Jadi, r dan s membangkitkan D_n. Artinya, D_n terdiri atas semua hasil kali hingga dari r dan s,

$$D_n = \{1, r, r^2, \ldots, r^{n-1}, s, rs, r^2 s, \ldots, r^{n-1}s\}.$$

Bukti bahwa $srs = r^{-1}$ diserahkan sebagai latihan.



Gambar 5.2.5 Jenis pencerminan segi-n beraturan

■

Contoh 5.2.6 Grup gerak tegar persegi, D_4, terdiri atas delapan elemen. Dengan titik-titik sudut bernomor 1, 2, 3, 4 (Gambar 5.2.7), rotasinya adalah

$$\begin{aligned} r &= (1\,2\,3\,4) \\ r^2 &= (1\,3)(2\,4) \\ r^3 &= (1\,4\,3\,2) \\ r^4 &= (1) \end{aligned}$$

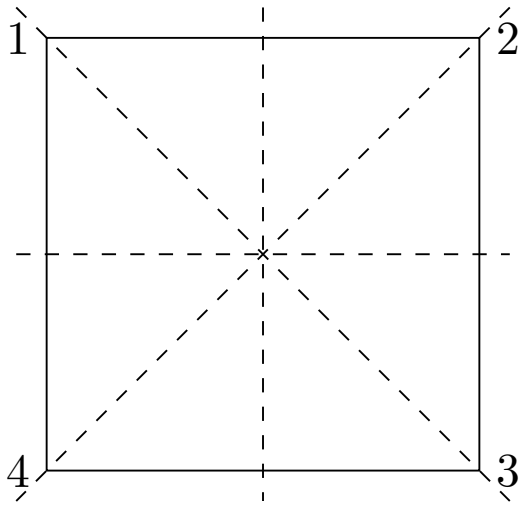
dan pencerminannya adalah

$$\begin{aligned} s_1 &= (2\,4) \\ s_2 &= (1\,3). \end{aligned}$$

Orde D_4 adalah 8. Dua elemen lainnya adalah

$$\begin{aligned} rs_1 &= (1\,2)(3\,4) \\ r^3 s_1 &= (1\,4)(2\,3). \end{aligned}$$

[1]Karena kita berada dalam grup abstrak, kita akan menggunakan konvensi bahwa elemen grup dikalikan dari kiri ke kanan.



Gambar 5.2.7 Grup D_4

▲

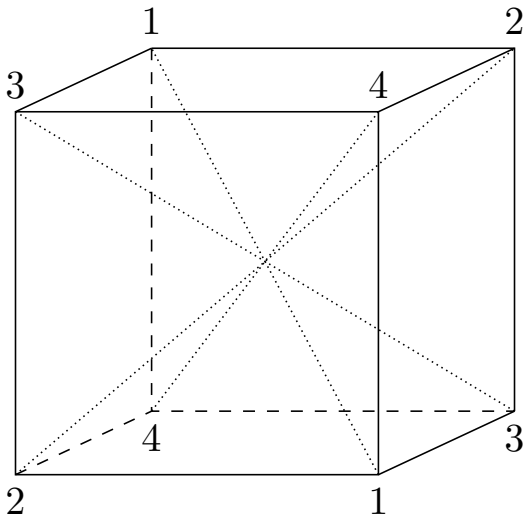
5.2.1 Grup Gerak Kubus

Kita dapat menyelidiki grup gerak tegar objek geometris selain poligon beraturan bersisi n untuk memperoleh contoh grup permutasi yang menarik. Mari kita tinjau grup gerak tegar suatu kubus. Gerak tegar yang dimaksud adalah rotasi dengan sumbu rotasi melalui pasangan sisi, rusuk, atau titik sudut yang berhadapan. Salah satu pertanyaan pertama yang dapat kita ajukan tentang grup ini adalah "berapakah ordenya?" Kubus memiliki 6 sisi. Jika suatu sisi tertentu menghadap ke atas, terdapat empat rotasi kubus yang mungkin dan tetap mempertahankan sisi tersebut menghadap ke atas. Jadi, orde grup ini adalah $6 \cdot 4 = 24$. Kita baru saja membuktikan proposisi berikut.

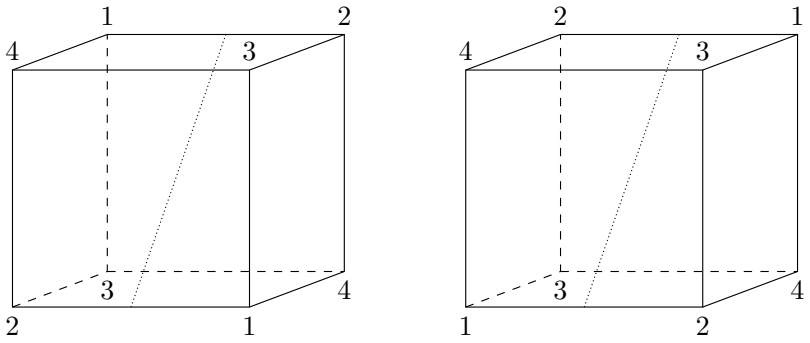
Proposisi 5.2.8 *Grup gerak tegar suatu kubus memuat* 24 *elemen.*

Teorema 5.2.9 *Grup gerak tegar suatu kubus adalah* S_4.

Bukti. Dari Proposisi 5.2.8, kita telah mengetahui bahwa grup gerak kubus memiliki 24 elemen, sama banyaknya dengan elemen dalam S_4. Terdapat tepat empat diagonal ruang dalam kubus. Jika diagonal-diagonal ini kita beri label 1, 2, 3, dan 4, kita harus menunjukkan bahwa grup gerak kubus menghasilkan setiap permutasi diagonal tersebut (Gambar 5.2.10). Jika kita dapat memperoleh semua permutasi ini, maka S_4 dan grup gerak tegar kubus harus sama. Untuk memperoleh suatu transposisi, kita dapat merotasi kubus sebesar 180° terhadap sumbu yang menghubungkan titik tengah rusuk-rusuk berhadapan (Gambar 5.2.11). Terdapat enam sumbu semacam itu, yang menghasilkan semua transposisi dalam S_4. Karena setiap elemen dalam S_4 merupakan hasil kali sejumlah hingga transposisi, grup gerak kubus haruslah S_4.



Gambar 5.2.10 Grup gerak kubus



Gambar 5.2.11 Transposisi dalam grup gerak kubus

■

5.3 Pertanyaan Bacaan

1. Nyatakan $(1\,3\,4)(3\,5\,4)$ sebagai suatu siklus, atau sebagai hasil kali siklus-siklus saling lepas. (Tafsirkan komposisi fungsi menurut urutan yang digunakan Sage, yang merupakan kebalikan urutan dalam buku ini.)

2. Apakah yang dimaksud dengan transposisi?

3. Apakah arti suatu permutasi bersifat genap atau ganjil?

4. Deskripsikan grup lain yang pada dasarnya sama dengan A_3.

5. Tuliskan elemen-elemen grup simetri segi lima menggunakan permutasi dalam notasi siklus. Kerjakan latihan ini dengan tangan, tanpa bantuan Sage.

5.4 Latihan

1. Tuliskan permutasi berikut dalam notasi siklus.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 1 & 3 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

Petunjuk. (a) $(1\,2\,4\,5\,3)$; (c) $(1\,3)(2\,5)$.

2. Hitung setiap bentuk berikut.

(a) $(1\,3\,4\,5)(2\,3\,4)$

(b) $(1\,2)(1\,2\,5\,3)$

(c) $(1\,4\,3)(2\,3)(2\,4)$

(d) $(1\,4\,2\,3)(3\,4)(5\,6)(1\,3\,2\,4)$

(e) $(1\,2\,5\,4)(1\,3)(2\,5)$

(f) $(1\,2\,5\,4)(1\,3)(2\,5)^2$

(g) $(1\,2\,5\,4)^{-1}(1\,2\,3)(4\,5)(1\,2\,5\,4)$

(h) $(1\,2\,5\,4)^2(1\,2\,3)(4\,5)$

(i) $(1\,2\,3)(4\,5)(1\,2\,5\,4)^{-2}$

(j) $(1\,2\,5\,4)^{100}$

(k) $|(1\,2\,5\,4)|$

(l) $|(1\,2\,5\,4)^2|$

(m) $(1\,2)^{-1}$

(n) $(1\,2\,5\,3\,7)^{-1}$

(o) $[(1\,2)(3\,4)(1\,2)(4\,7)]^{-1}$

(p) $[(1\,2\,3\,5)(4\,6\,7)]^{-1}$

Petunjuk. (a) $(1\,3\,5)(2\,4)$; (c) $(1\,4)(2\,3)$; (e) $(1\,3\,2\,4)$; (g) $(1\,3\,4)(2\,5)$; (n) $(1\,7\,3\,5\,2)$.

3. Nyatakan permutasi berikut sebagai hasil kali transposisi dan tentukan apakah masing-masing genap atau ganjil.

(a) $(1\,4\,3\,5\,6)$

(b) $(1\,5\,6)(2\,3\,4)$

(c) $(1\,4\,2\,6)(1\,4\,2)$

(d) $(1\,7\,2\,5\,4)(1\,4\,2\,3)(1\,5\,4\,6\,3\,2)$

(e) $(1\,4\,2\,6\,3\,7)$

Petunjuk. (a) $(1\,6)(1\,5)(1\,3)(1\,4)$; (c) $(1\,6)(1\,4)(1\,2)$.

4. Tentukan $(a_1, a_2, \ldots, a_n)^{-1}$.

Petunjuk. $(a_1, a_2, \ldots, a_n)^{-1} = (a_1, a_n, a_{n-1}, \ldots, a_2)$

5. Cantumkan semua subgrup S_4. Tentukan setiap himpunan berikut:

(a) $\{\sigma \in S_4 : \sigma(1) = 3\}$

(b) $\{\sigma \in S_4 : \sigma(2) = 2\}$

(c) $\{\sigma \in S_4 : \sigma(1) = 3 \text{ dan } \sigma(2) = 2\}$.

Apakah ada di antara himpunan-himpunan ini yang merupakan subgrup S_4?

Petunjuk. (a) $\{(1\,3), (1\,3)(2\,4), (1\,3\,2), (1\,3\,4), (1\,3\,2\,4), (1\,3\,4\,2)\}$ bukan subgrup.

6. Tentukan semua subgrup dalam A_4. Berapakah orde setiap subgrup?

7. Tentukan semua orde elemen yang mungkin dalam S_7 dan A_7.

8. Tunjukkan bahwa A_{10} memuat suatu elemen berorde 15.

Petunjuk. $(1\,2\,3\,4\,5)(6\,7\,8)$.

9. Apakah A_8 memuat elemen berorde 26?

10. Tentukan elemen dengan orde terbesar dalam S_n untuk $n = 3, \ldots, 10$.

11. Apa saja struktur siklus yang mungkin bagi elemen A_5? Bagaimana dengan A_6?

Petunjuk. Permutasi berbentuk

$$(1), (a_1, a_2)(a_3, a_4), (a_1, a_2, a_3), (a_1, a_2, a_3, a_4, a_5)$$

mungkin terdapat dalam A_5.

12. Misalkan $\sigma \in S_n$ berorde n. Tunjukkan bahwa untuk semua bilangan bulat i dan j, $\sigma^i = \sigma^j$ jika dan hanya jika $i \equiv j \pmod{n}$.

13. Misalkan $\sigma = \sigma_1 \cdots \sigma_m \in S_n$ merupakan hasil kali siklus-siklus saling lepas. Buktikan bahwa orde σ adalah kelipatan persekutuan terkecil dari panjang siklus $\sigma_1, \ldots, \sigma_m$.

14. Dengan menggunakan notasi siklus, cantumkan elemen-elemen dalam D_5. Apakah r dan s? Tuliskan setiap elemen sebagai hasil kali r dan s.

15. Jika diagonal-diagonal kubus diberi label seperti dalam Gambar 5.2.10, gerak kubus manakah yang bersesuaian dengan permutasi (12)(34)? Bagaimana dengan permutasi diagonal lainnya?

16. Tentukan grup gerak tegar suatu tetrahedron. Tunjukkan bahwa grup ini sama dengan A_4.

17. Buktikan bahwa S_n nonabelian untuk $n \geq 3$.

Petunjuk. Hitung $(1\,2\,3)(1\,2)$ dan $(1\,2)(1\,2\,3)$.

18. Tunjukkan bahwa A_n nonabelian untuk $n \geq 4$.

19. Buktikan bahwa D_n nonabelian untuk $n \geq 3$.

20. Misalkan $\sigma \in S_n$ merupakan siklus. Buktikan bahwa σ dapat ditulis sebagai hasil kali paling banyak $n - 1$ transposisi.

21. Misalkan $\sigma \in S_n$. Jika σ bukan siklus, buktikan bahwa σ dapat ditulis sebagai hasil kali paling banyak $n - 2$ transposisi.

22. Jika σ dapat dinyatakan sebagai sejumlah ganjil transposisi, tunjukkan bahwa setiap hasil kali transposisi lain yang sama dengan σ juga harus ganjil.

23. Jika σ merupakan siklus dengan panjang ganjil, buktikan bahwa σ^2 juga merupakan siklus.

24. Tunjukkan bahwa siklus-3 merupakan permutasi genap.

25. Buktikan bahwa dalam A_n dengan $n \geq 3$, setiap permutasi merupakan hasil kali siklus-siklus dengan panjang 3.

Petunjuk. Perhatikan kasus $(a, b)(b, c)$ dan $(a, b)(c, d)$.

26. Buktikan bahwa setiap elemen dalam S_n dapat ditulis sebagai hasil kali hingga dari permutasi berikut.

(a) $(1\,2), (1\,3), \ldots, (1\,n)$

(b) $(1\,2), (2\,3), \ldots, (n-1, n)$

(c) $(1\,2), (1\,2\ldots n)$

27. Misalkan G adalah grup dan definisikan pemetaan $\lambda_g : G \to G$ dengan $\lambda_g(a) = ga$. Buktikan bahwa λ_g merupakan permutasi dari G.

28. Buktikan bahwa terdapat $n!$ permutasi dari suatu himpunan yang memuat n elemen.

29. Ingat bahwa **pusat** suatu grup G adalah

$$Z(G) = \{g \in G : gx = xg \text{ untuk semua } x \in G\}.$$

Tentukan pusat D_8. Bagaimana dengan pusat D_{10}? Apakah pusat D_n?

Petunjuk. Tunjukkan bahwa pusat D_n hanya terdiri atas identitas jika n ganjil, serta terdiri atas identitas dan rotasi 180° jika n genap.

30. Misalkan $\tau = (a_1, a_2, \ldots, a_k)$ merupakan siklus dengan panjang k.

(a) Buktikan bahwa jika σ merupakan sembarang permutasi, maka

$$\sigma\tau\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k))$$

merupakan siklus dengan panjang k.

(b) Misalkan μ merupakan siklus dengan panjang k. Buktikan bahwa terdapat permutasi σ sedemikian sehingga $\sigma\tau\sigma^{-1} = \mu$.

Petunjuk. Untuk (a), tunjukkan bahwa $\sigma\tau\sigma^{-1}(\sigma(a_i)) = \sigma(a_{i+1})$.

31. Untuk α dan β dalam S_n, definisikan $\alpha \sim \beta$ jika terdapat $\sigma \in S_n$ sedemikian sehingga $\sigma\alpha\sigma^{-1} = \beta$. Tunjukkan bahwa $\sim$ merupakan relasi ekuivalensi pada S_n.

32. Misalkan $\sigma \in S_X$. Jika $\sigma^n(x) = y$ untuk suatu $n \in \mathbb{Z}$, kita katakan bahwa $x \sim y$.

(a) Tunjukkan bahwa $\sim$ merupakan relasi ekuivalensi pada X.

(b) Definisikan **orbit** dari $x \in X$ di bawah $\sigma \in S_X$ sebagai himpunan

$$\mathcal{O}_{x,\sigma} = \{y : x \sim y\}.$$

Hitung orbit setiap elemen dalam $\{1, 2, 3, 4, 5\}$ di bawah setiap elemen S_5 berikut:

$$\alpha = (1\,2\,5\,4)$$
$$\beta = (1\,2\,3)(4\,5)$$
$$\gamma = (1\,3)(2\,5).$$

(c) Jika $\mathcal{O}_{x,\sigma} \cap \mathcal{O}_{y,\sigma} \neq \emptyset$, buktikan bahwa $\mathcal{O}_{x,\sigma} = \mathcal{O}_{y,\sigma}$. Orbit-orbit di bawah suatu permutasi σ merupakan kelas ekuivalensi yang bersesuaian dengan relasi ekuivalensi $\sim$.

(d) Suatu subgrup H dari S_X disebut **transitif** jika untuk setiap $x, y \in X$, terdapat $\sigma \in H$ sedemikian sehingga $\sigma(x) = y$. Buktikan bahwa $\langle\sigma\rangle$ transitif jika dan hanya jika $\mathcal{O}_{x,\sigma} = X$ untuk suatu $x \in X$.

33. Misalkan $\alpha \in S_n$ untuk $n \geq 3$. Jika $\alpha\beta = \beta\alpha$ untuk semua $\beta \in S_n$, buktikan bahwa α harus merupakan permutasi identitas; jadi, pusat S_n adalah subgrup trivial.

34. Jika α genap, buktikan bahwa α^{-1} juga genap. Apakah hasil yang bersesuaian berlaku jika α ganjil?

35. Jika $\sigma \in A_n$ dan $\tau \in S_n$, tunjukkan bahwa $\tau^{-1}\sigma\tau \in A_n$.

36. Tunjukkan bahwa $\alpha^{-1}\beta^{-1}\alpha\beta$ genap untuk $\alpha, \beta \in S_n$.

37. Misalkan r dan s merupakan elemen dalam D_n yang dideskripsikan dalam Teorema 5.2.3

(a) Tunjukkan bahwa $srs = r^{-1}$.

(b) Tunjukkan bahwa $r^k s = sr^{-k}$ dalam D_n.

(c) Buktikan bahwa orde $r^k \in D_n$ adalah $n/\gcd(k, n)$.

6

Koset dan Teorema Lagrange

Teorema Lagrange, salah satu hasil terpenting dalam teori grup hingga, menyatakan bahwa orde suatu subgrup harus membagi orde grup tersebut. Teorema ini menyediakan perangkat ampuh untuk menganalisis grup hingga; teorema tersebut memberi kita gambaran tepat mengenai jenis subgrup yang mungkin dimiliki suatu grup hingga. Gagasan koset merupakan inti untuk memahami Teorema Lagrange.

6.1 Koset

Misalkan G suatu grup dan H subgrup dari G. Definisikan **koset kiri** dari H dengan **wakil** $g \in G$ sebagai himpunan

$$gH = \{gh : h \in H\}.$$

Koset kanan dapat didefinisikan secara serupa dengan

$$Hg = \{hg : h \in H\}.$$

Jika koset kiri dan kanan berimpit, atau jika jenis koset yang dimaksud sudah jelas dari konteks, kita akan menggunakan kata *koset* tanpa menentukan kiri atau kanan.

Contoh 6.1.1 Misalkan H subgrup dari $\mathbb{Z}_6$ yang terdiri atas elemen 0 dan 3. Koset-kosetnya adalah

$$\begin{aligned} 0 + H = 3 + H &= \{0, 3\} \\ 1 + H = 4 + H &= \{1, 4\} \\ 2 + H = 5 + H &= \{2, 5\}. \end{aligned}$$

Kita akan selalu menuliskan koset subgrup dari $\mathbb{Z}$ dan $\mathbb{Z}_n$ dengan notasi aditif yang digunakan untuk koset di sini. Dalam grup komutatif, koset kiri dan kanan selalu identik. ▲

Contoh 6.1.2 Misalkan H subgrup dari S_3 yang didefinisikan oleh permutasi $\{(1), (1\,2\,3), (1\,3\,2)\}$. Koset kiri dari H adalah

$$\begin{aligned} (1)H = (1\,2\,3)H = (1\,3\,2)H &= \{(1), (1\,2\,3), (1\,3\,2)\} \\ (1\,2)H = (1\,3)H = (2\,3)H &= \{(1\,2), (1\,3), (2\,3)\}. \end{aligned}$$

Koset kanan dari H tepat sama dengan koset kirinya:

$$H(1) = H(1\,2\,3) = H(1\,3\,2) = \{(1), (1\,2\,3), (1\,3\,2)\}$$
$$H(1\,2) = H(1\,3) = H(2\,3) = \{(1\,2), (1\,3), (2\,3)\}.$$

Koset kiri tidak selalu sama dengan koset kanan. Misalkan K subgrup dari S_3 yang didefinisikan oleh permutasi $\{(1), (1\,2)\}$. Maka koset kiri dari K adalah

$$(1)K = (1\,2)K = \{(1), (1\,2)\}$$
$$(1\,3)K = (1\,2\,3)K = \{(1\,3), (1\,2\,3)\}$$
$$(2\,3)K = (1\,3\,2)K = \{(2\,3), (1\,3\,2)\};$$

sedangkan koset kanan dari K adalah

$$K(1) = K(1\,2) = \{(1), (1\,2)\}$$
$$K(1\,3) = K(1\,3\,2) = \{(1\,3), (1\,3\,2)\}$$
$$K(2\,3) = K(1\,2\,3) = \{(2\,3), (1\,2\,3)\}.$$

▲

Lema berikut sangat berguna ketika membahas koset. (Pembuktiannya diserahkan sebagai latihan.)

Lema 6.1.3 *Misalkan H subgrup dari suatu grup G dan misalkan $g_1, g_2 \in G$. Syarat-syarat berikut ekuivalen.*

1. $g_1H = g_2H$;
2. $Hg_1^{-1} = Hg_2^{-1}$;
3. $g_1H \subset g_2H$;
4. $g_2 \in g_1H$;
5. $g_1^{-1}g_2 \in H$.

Dalam semua contoh kita, koset dari suatu subgrup H mempartisi grup yang lebih besar G. Teorema berikut menyatakan bahwa hal ini selalu berlaku.

Teorema 6.1.4 *Misalkan H subgrup dari suatu grup G. Maka koset kiri dari H dalam G mempartisi G. Artinya, grup G merupakan gabungan saling lepas dari koset kiri H dalam G.*

Bukti. Misalkan g_1H dan g_2H dua koset dari H dalam G. Kita harus menunjukkan bahwa $g_1H \cap g_2H = \emptyset$ atau $g_1H = g_2H$. Misalkan $g_1H \cap g_2H \neq \emptyset$ dan $a \in g_1H \cap g_2H$. Maka berdasarkan definisi koset kiri, berlaku $a = g_1h_1 = g_2h_2$ untuk suatu elemen h_1 dan h_2 dalam H. Jadi, $g_1 = g_2h_2h_1^{-1}$ atau $g_1 \in g_2H$. Berdasarkan Lema 6.1.3, berlaku $g_1H = g_2H$. ■

Catatan 6.1.5 Koset kiri tidak mempunyai keistimewaan khusus dalam teorema ini. Koset kanan juga mempartisi G; pembuktian fakta ini tepat sama dengan pembuktian untuk koset kiri, kecuali bahwa semua perkalian grup dilakukan pada sisi lain dari H.

Misalkan G suatu grup dan H subgrup dari G. Definisikan **indeks** dari H dalam G sebagai banyaknya koset kiri dari H dalam G. Indeks tersebut dinotasikan dengan $[G : H]$.

Contoh 6.1.6 Misalkan $G = \mathbb{Z}_6$ dan $H = \{0, 3\}$. Maka $[G : H] = 3$. ▲

Contoh 6.1.7 Misalkan $G = S_3$, $H = \{(1), (1\,2\,3), (1\,3\,2)\}$, dan $K = \{(1), (1\,2)\}$. Maka $[G : H] = 2$ dan $[G : K] = 3$. ▲

Teorema 6.1.8 *Misalkan H subgrup dari suatu grup G. Banyaknya koset kiri dari H dalam G sama dengan banyaknya koset kanan dari H dalam G.*

BUKTI. Misalkan $\mathcal{L}_H$ dan $\mathcal{R}_H$ masing-masing menyatakan himpunan koset kiri dan kanan dari H dalam G. Jika kita dapat mendefinisikan pemetaan bijektif $\phi : \mathcal{L}_H \to \mathcal{R}_H$, maka teorema tersebut terbukti. Jika $gH \in \mathcal{L}_H$, definisikan $\phi(gH) = Hg^{-1}$. Berdasarkan Lema 6.1.3, pemetaan ϕ terdefinisi dengan baik; artinya, jika $g_1H = g_2H$, maka $Hg_1^{-1} = Hg_2^{-1}$. Untuk menunjukkan bahwa ϕ satu-ke-satu, misalkan

$$Hg_1^{-1} = \phi(g_1H) = \phi(g_2H) = Hg_2^{-1}.$$

Sekali lagi berdasarkan Lema 6.1.3, berlaku $g_1H = g_2H$. Pemetaan ϕ surjektif karena $\phi(g^{-1}H) = Hg$. ■

6.2 Teorema Lagrange

Proposisi 6.2.1 *Misalkan H subgrup dari G dengan $g \in G$, dan definisikan pemetaan $\phi : H \to gH$ dengan $\phi(h) = gh$. Pemetaan ϕ bersifat bijektif; jadi, banyaknya elemen dalam H sama dengan banyaknya elemen dalam gH.*

BUKTI. Pertama-tama kita tunjukkan bahwa pemetaan ϕ satu-ke-satu. Misalkan $\phi(h_1) = \phi(h_2)$ untuk elemen $h_1, h_2 \in H$. Kita harus menunjukkan bahwa $h_1 = h_2$, sedangkan $\phi(h_1) = gh_1$ dan $\phi(h_2) = gh_2$. Jadi $gh_1 = gh_2$, dan berdasarkan hukum pencoretan kiri, $h_1 = h_2$. Mudah ditunjukkan bahwa ϕ surjektif. Berdasarkan definisi, setiap elemen dari gH berbentuk gh untuk suatu $h \in H$ dan $\phi(h) = gh$. ■

Teorema 6.2.2 Lagrange. *Misalkan G grup hingga dan H subgrup dari G. Maka $|G|/|H| = [G : H]$ merupakan banyaknya koset kiri berbeda dari H dalam G. Secara khusus, banyaknya elemen dalam H harus membagi banyaknya elemen dalam G.*

BUKTI. Grup G terpartisi menjadi $[G : H]$ koset kiri yang berbeda. Setiap koset kiri mempunyai $|H|$ elemen; oleh karena itu, $|G| = [G : H]|H|$. ■

Korolari 6.2.3 *Misalkan G grup hingga dan $g \in G$. Maka orde g harus membagi banyaknya elemen dalam G.*

Korolari 6.2.4 *Misalkan $|G| = p$ dengan p bilangan prima. Maka G bersifat siklik dan sebarang $g \in G$ sedemikian sehingga $g \neq e$ merupakan pembangkit.*

BUKTI. Misalkan g berada dalam G sedemikian sehingga $g \neq e$. Berdasarkan Korolari 6.2.3, orde g harus membagi orde grup. Karena $|\langle g \rangle| > 1$, nilainya harus p. Jadi, g membangkitkan G. ■

Korolari 6.2.4 menunjukkan bahwa grup berorde prima p dalam suatu arti harus menyerupai $\mathbb{Z}_p$.

Korolari 6.2.5 *Misalkan H dan K subgrup dari grup hingga G sedemikian sehingga $G \supset H \supset K$. Maka*

$$[G : K] = [G : H][H : K].$$

BUKTI. Perhatikan bahwa

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G : H][H : K].$$

■

Catatan 6.2.6 Kebalikan Teorema Lagrange Salah. Grup A_4 berorde 12; akan tetapi, dapat ditunjukkan bahwa grup tersebut tidak mempunyai subgrup berorde 6. Menurut Teorema Lagrange, subgrup dari grup berorde 12 dapat berorde 1, 2, 3, 4, atau 6. Akan tetapi, tidak ada jaminan bahwa subgrup dari setiap orde yang mungkin benar-benar ada. Untuk membuktikan bahwa A_4 tidak mempunyai subgrup berorde 6, kita akan mengandaikan bahwa grup tersebut mempunyai subgrup H seperti itu dan menunjukkan bahwa kontradiksi harus terjadi. Karena A_4 memuat delapan siklus-3, kita mengetahui bahwa H harus memuat suatu siklus-3. Kita akan menunjukkan bahwa jika H memuat satu siklus-3, maka subgrup tersebut harus memuat lebih dari 6 elemen.

Proposisi 6.2.7 *Grup A_4 tidak mempunyai subgrup berorde* 6.

BUKTI. Karena $[A_4 : H] = 2$, hanya terdapat dua koset dari H dalam A_4. Karena salah satu koset tersebut adalah H sendiri, koset kanan dan kiri harus berimpit; oleh karena itu, $gH = Hg$ atau $gHg^{-1} = H$ untuk setiap $g \in A_4$. Karena terdapat delapan siklus-3 dalam A_4, paling sedikit satu siklus-3 harus berada dalam H. Tanpa mengurangi keumuman, andaikan $(1\,2\,3)$ berada dalam H. Maka $(1\,2\,3)^{-1} = (1\,3\,2)$ juga harus berada dalam H. Karena $ghg^{-1} \in H$ untuk setiap $g \in A_4$ dan setiap $h \in H$ serta

$$(1\,2\,4)(1\,2\,3)(1\,2\,4)^{-1} = (1\,2\,4)(1\,2\,3)(1\,4\,2) = (2\,4\,3)$$
$$(2\,4\,3)(1\,2\,3)(2\,4\,3)^{-1} = (2\,4\,3)(1\,2\,3)(2\,3\,4) = (1\,4\,2)$$

kita dapat menyimpulkan bahwa H harus mempunyai paling sedikit tujuh elemen

$$(1), (1\,2\,3), (1\,3\,2), (2\,4\,3), (2\,4\,3)^{-1} = (2\,3\,4), (1\,4\,2), (1\,4\,2)^{-1} = (1\,2\,4).$$

Oleh karena itu, A_4 tidak mempunyai subgrup berorde 6. ■

Bahkan, kita dapat mengatakan lebih banyak mengenai kapan dua siklus mempunyai panjang yang sama.

Teorema 6.2.8 *Dua siklus τ dan μ dalam S_n mempunyai panjang yang sama jika dan hanya jika terdapat $\sigma \in S_n$ sedemikian sehingga $\mu = \sigma\tau\sigma^{-1}$.*

BUKTI. Misalkan

$$\tau = (a_1, a_2, \ldots, a_k)$$
$$\mu = (b_1, b_2, \ldots, b_k).$$

Definisikan σ sebagai permutasi

$$\sigma(a_1) = b_1$$
$$\sigma(a_2) = b_2$$
$$\vdots$$
$$\sigma(a_k) = b_k.$$

Maka $\mu = \sigma\tau\sigma^{-1}$.

Sebaliknya, misalkan $\tau = (a_1, a_2, \ldots, a_k)$ suatu siklus-k dan $\sigma \in S_n$. Jika $\sigma(a_i) = b$ dan $\sigma(a_{(i \bmod k)+1}) = b'$, maka $\mu(b) = b'$. Jadi,

$$\mu = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_k)).$$

Karena σ satu-ke-satu dan surjektif, μ merupakan siklus yang panjangnya sama dengan τ. ■

6.3 Teorema Fermat dan Euler

Fungsi ϕ Euler adalah pemetaan $\phi : \mathbb{N} \to \mathbb{N}$ yang didefinisikan oleh $\phi(n) = 1$ untuk $n = 1$, dan untuk $n > 1$, $\phi(n)$ merupakan banyaknya bilangan bulat positif m dengan $1 \leq m < n$ dan $\gcd(m, n) = 1$.

Berdasarkan Proposisi 3.1.4, kita mengetahui bahwa orde $U(n)$, yaitu grup unit dalam $\mathbb{Z}_n$, adalah $\phi(n)$. Sebagai contoh, $|U(12)| = \phi(12) = 4$ karena bilangan yang relatif prima terhadap 12 adalah 1, 5, 7, dan 11. Untuk sebarang bilangan prima p, berlaku $\phi(p) = p - 1$. Hasil-hasil ini dinyatakan dalam teorema berikut.

Teorema 6.3.1 *Misalkan $U(n)$ grup unit dalam $\mathbb{Z}_n$. Maka $|U(n)| = \phi(n)$.*

Teorema berikut merupakan hasil penting dalam teori bilangan yang ditemukan oleh Leonhard Euler.

Teorema 6.3.2 Teorema Euler. *Misalkan a dan n bilangan bulat sedemikian sehingga $n > 0$ dan $\gcd(a, n) = 1$. Maka $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Bukti. Berdasarkan Teorema 6.3.1, orde $U(n)$ adalah $\phi(n)$. Akibatnya, $a^{\phi(n)} = 1$ untuk setiap $a \in U(n)$; atau $a^{\phi(n)} - 1$ habis dibagi n. Oleh karena itu, $a^{\phi(n)} \equiv 1 \pmod{n}$. ■

Jika kita mempertimbangkan kasus khusus Teorema Euler ketika $n = p$ prima dan mengingat bahwa $\phi(p) = p - 1$, kita memperoleh hasil berikut, yang ditemukan oleh Pierre de Fermat.

Teorema 6.3.3 Teorema Kecil Fermat. *Misalkan p sebarang bilangan prima dan misalkan $p \nmid a$ (p tidak membagi a). Maka*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Lebih lanjut, untuk sebarang bilangan bulat b, $b^p \equiv b \pmod{p}$.

Catatan Sejarah

Joseph-Louis Lagrange (1736–1813), yang lahir di Turin, Italia, merupakan keturunan Prancis dan Italia. Bakat matematikanya tampak sejak usia dini. Leonhard Euler mengenali kemampuan Lagrange ketika Lagrange, yang saat itu baru berusia 19 tahun, menyampaikan kepada Euler beberapa karya yang telah dikerjakannya dalam kalkulus variasi. Pada tahun itu ia juga diangkat menjadi profesor di Sekolah Artileri Kerajaan di Turin. Pada usia 23 tahun ia bergabung dengan Akademi Berlin. Frederick Agung menulis kepada Lagrange dengan menyatakan bahwa "raja terbesar di Eropa" seharusnya mempunyai "matematikawan terbesar di Eropa" di istananya. Selama 20 tahun Lagrange menduduki jabatan yang ditinggalkan mentornya, Euler. Karyanya mencakup sumbangsih pada teori bilangan, teori grup, fisika dan mekanika, kalkulus variasi, teori persamaan, serta persamaan diferensial. Bersama Laplace dan Lavoisier, Lagrange merupakan salah satu tokoh yang bertanggung jawab merancang sistem metrik. Sepanjang hidupnya Lagrange sangat me-

mengaruhi perkembangan matematika, dan mewariskan banyak hal kepada generasi matematikawan berikutnya dalam bentuk contoh serta masalah baru untuk dipecahkan.

6.4 Pertanyaan Bacaan

1. Nyatakan Teorema Lagrange dengan kata-kata Anda sendiri.

2. Tentukan koset kiri dari $\langle 3 \rangle$ dalam $\mathbb{Z}_9$.

3. Himpunan $\{(), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ merupakan subgrup dari S_4. Berapakah indeksnya dalam S_4?

4. Misalkan G grup berorde 29. Deskripsikan G.

5. Bilangan $p = 137909$ prima. Jelaskan cara menghitung $57^{137909} \pmod{137909}$ tanpa kalkulator.

6.5 Latihan

1. Misalkan G grup hingga dengan suatu elemen g berorde 5 dan suatu elemen h berorde 7. Mengapa harus berlaku $|G| \geq 35$?

Petunjuk. Orde g dan orde h keduanya harus membagi orde G.

2. Misalkan G grup hingga dengan 60 elemen. Apa saja kemungkinan orde subgrup dari G?

Petunjuk. Orde yang mungkin harus membagi 60.

3. Buktikan atau sangkal: Setiap subgrup dari bilangan bulat mempunyai indeks hingga.

Petunjuk. Pernyataan ini benar untuk setiap subgrup sejati nontrivial.

4. Buktikan atau sangkal: Setiap subgrup dari bilangan bulat berorde hingga.

Petunjuk. Salah.

5. Cantumkan koset kiri dan kanan dari subgrup dalam setiap kasus berikut.

(a) $\langle 8 \rangle$ dalam $\mathbb{Z}_{24}$

(b) $\langle 3 \rangle$ dalam $U(8)$

(c) $3\mathbb{Z}$ dalam $\mathbb{Z}$

(d) A_4 dalam S_4

(e) A_n dalam S_n

(f) D_4 dalam S_4

(g) $\mathbb{T}$ dalam $\mathbb{C}^*$

(h) $H = \{(1), (1\,2\,3), (1\,3\,2)\}$ dalam S_4

Petunjuk. (a) $\langle 8 \rangle$, $1 + \langle 8 \rangle$, $2 + \langle 8 \rangle$, $3 + \langle 8 \rangle$, $4 + \langle 8 \rangle$, $5 + \langle 8 \rangle$, $6 + \langle 8 \rangle$, dan $7 + \langle 8 \rangle$; (c) $3\mathbb{Z}$, $1 + 3\mathbb{Z}$, dan $2 + 3\mathbb{Z}$.

6. Deskripsikan koset kiri dari $SL_2(\mathbb{R})$ dalam $GL_2(\mathbb{R})$. Berapakah indeks $SL_2(\mathbb{R})$ dalam $GL_2(\mathbb{R})$?

7. Periksa Teorema Euler untuk $n = 15$ dan $a = 4$.

Petunjuk. $4^{\phi(15)} \equiv 4^8 \equiv 1 \pmod{15}$.

8. Gunakan Teorema Kecil Fermat untuk menunjukkan bahwa jika $p = 4n + 3$ prima, maka tidak terdapat penyelesaian bagi persamaan $x^2 \equiv -1 \pmod{p}$.

9. Tunjukkan bahwa bilangan bulat mempunyai indeks tak hingga dalam grup aditif bilangan rasional.

10. Tunjukkan bahwa grup aditif bilangan real mempunyai indeks tak hingga dalam grup aditif bilangan kompleks.

11. Misalkan H subgrup dari suatu grup G dan misalkan $g_1, g_2 \in G$. Buktikan bahwa syarat-syarat berikut ekuivalen.

(a) $g_1H = g_2H$

(b) $Hg_1^{-1} = Hg_2^{-1}$

(c) $g_1H \subset g_2H$

(d) $g_2 \in g_1H$

(e) $g_1^{-1}g_2 \in H$

12. Jika $ghg^{-1} \in H$ untuk setiap $g \in G$ dan $h \in H$, tunjukkan bahwa koset kanan identik dengan koset kiri. Artinya, tunjukkan bahwa $gH = Hg$ untuk setiap $g \in G$.

Petunjuk. Misalkan $g_1 \in gH$. Tunjukkan bahwa $g_1 \in Hg$, sehingga $gH \subset Hg$.

13. Bagian mana dari pembuktian Teorema 6.1.8 yang gagal jika $\phi : \mathcal{L}_H \to \mathcal{R}_H$ didefinisikan dengan $\phi(gH) = Hg$?

14. Misalkan $g^n = e$. Tunjukkan bahwa orde g membagi n.

15. **Struktur siklus** suatu permutasi σ didefinisikan sebagai daftar tak terurut ukuran siklus-siklus dalam dekomposisi siklus σ. Sebagai contoh, permutasi $\sigma = (1\,2)(3\,4\,5)(7\,8)(9)$ mempunyai struktur siklus $(2, 3, 2, 1)$, yang juga dapat ditulis sebagai $(1, 2, 2, 3)$.

Tunjukkan bahwa sebarang dua permutasi $\alpha, \beta \in S_n$ mempunyai struktur siklus yang sama jika dan hanya jika terdapat permutasi γ sedemikian sehingga $\beta = \gamma\alpha\gamma^{-1}$. Jika $\beta = \gamma\alpha\gamma^{-1}$ untuk suatu $\gamma \in S_n$, maka α dan β disebut **konjugat**.

16. Jika $|G| = 2n$, buktikan bahwa banyaknya elemen berorde 2 ganjil. Gunakan hasil ini untuk menunjukkan bahwa G harus memuat subgrup berorde 2.

17. Misalkan $[G : H] = 2$. Jika a dan b tidak berada dalam H, tunjukkan bahwa $ab \in H$.

18. Jika $[G : H] = 2$, buktikan bahwa $gH = Hg$ untuk setiap $g \in G$.

19. Misalkan H dan K subgrup dari suatu grup G. Buktikan bahwa $gH \cap gK$ merupakan koset dari $H \cap K$ dalam G.

Petunjuk. Tunjukkan bahwa $g(H \cap K) = gH \cap gK$.

20. Misalkan H dan K subgrup dari suatu grup G. Definisikan relasi $\sim$ pada G dengan $a \sim b$ jika terdapat $h \in H$ dan $k \in K$ sedemikian sehingga $hak = b$. Tunjukkan bahwa relasi ini merupakan relasi ekuivalensi. Kelas ekuivalensi yang bersesuaian disebut **koset ganda**. Hitung koset ganda dari $H = \{(1), (1\,2\,3), (1\,3\,2)\}$ dalam A_4.

21. Misalkan G grup siklik berorde n. Tunjukkan bahwa terdapat tepat $\phi(n)$ pembangkit bagi G.

22. Misalkan $n = p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$, dengan $p_1, p_2, \ldots, p_k$ bilangan-bilangan prima

yang berbeda. Buktikan bahwa

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Petunjuk. Jika $\gcd(m, n) = 1$, maka $\phi(mn) = \phi(m)\phi(n)$ (Latihan 2.4.26 dalam Bab 2).

23. Tunjukkan bahwa

$$n = \sum_{d|n} \phi(d)$$

untuk setiap bilangan bulat positif n.

7

Pengantar Kriptografi

Kriptografi adalah ilmu tentang pengiriman dan penerimaan pesan rahasia. Tujuan kriptografi adalah mengirimkan pesan melalui suatu saluran sedemikian rupa sehingga hanya penerima yang dituju yang dapat membacanya. Selain itu, ketika menerima sebuah pesan, penerima biasanya memerlukan kepastian bahwa pesan tersebut autentik; artinya, pesan itu bukan dikirim oleh seseorang yang berusaha menipu penerima. Kriptografi modern sangat bergantung pada aljabar abstrak dan teori bilangan.

Pesan yang akan dikirim disebut pesan **teks terang**. Pesan yang telah disamarkan disebut **teks tersandi**. Teks terang maupun teks tersandi ditulis menggunakan sebuah **alfabet**, yang terdiri atas **huruf** atau **karakter**. Karakter tidak hanya dapat berupa karakter alfabet A, . . ., Z dan a, . . ., z yang sudah dikenal, tetapi juga angka, tanda baca, dan spasi. Sebuah **sistem kriptografi**, atau **sandi**, memiliki dua bagian: **enkripsi**, yaitu proses mengubah pesan teks terang menjadi pesan teks tersandi, dan **dekripsi**, yaitu transformasi sebaliknya yang mengubah pesan teks tersandi menjadi pesan teks terang.

Ada banyak keluarga sistem kriptografi yang berbeda, dan masing-masing dibedakan oleh algoritma enkripsi tertentu. Sistem-sistem kriptografi dalam satu keluarga tertentu dibedakan satu sama lain oleh parameter pada fungsi enkripsinya yang disebut **kunci**. Sistem kriptografi klasik memiliki satu kunci yang harus dirahasiakan dan hanya diketahui oleh pengirim serta penerima pesan. Jika orang A ingin mengirimkan pesan rahasia kepada dua orang berbeda, B dan C, dan tidak ingin B memahami pesan untuk C ataupun sebaliknya, A harus menggunakan dua kunci terpisah, sehingga satu sistem kriptografi digunakan untuk bertukar pesan dengan B, dan sistem yang lain digunakan untuk bertukar pesan dengan C.

Sistem yang menggunakan dua kunci terpisah, satu untuk enkripsi dan satu lagi untuk dekripsi, disebut **sistem kriptografi kunci publik**. Karena mengetahui kunci enkripsi tidak memungkinkan seseorang menebak kunci dekripsi, kunci enkripsi dapat diumumkan kepada publik. Sistem kriptografi kunci publik memungkinkan A dan B mengirimkan pesan kepada C dengan menggunakan kunci enkripsi yang sama. Siapa pun dapat mengenkripsi pesan yang hendak dikirimkan kepada C, tetapi hanya C yang mengetahui cara mendekripsi pesan tersebut.

7.1 Kriptografi Kunci Privat

Dalam **sistem kriptografi berkunci tunggal** atau **sistem kriptografi kunci privat**, kunci yang sama digunakan untuk mengenkripsi maupun mendekripsi pesan. Untuk mengenkripsi pesan teks terang, kita menerapkan suatu fungsi yang dirahasiakan pada pesan tersebut, misalkan f. Fungsi ini menghasilkan pesan terenkripsi. Jika bentuk terenkripsi dari pesan diketahui, kita dapat memperoleh kembali pesan semula dengan menerapkan transformasi invers f^{-1}. Transformasi f harus relatif mudah dihitung, demikian pula f^{-1}; namun, f harus sangat sulit ditebak dari contoh-contoh pesan tersandi yang tersedia.

Contoh 7.1.1 Salah satu sistem kriptografi kunci privat yang paling awal dan terkenal adalah sandi geser yang digunakan oleh Julius Caesar. Mula-mula kita nyatakan alfabet dengan angka melalui $\mathrm{A} = 00, \mathrm{B} = 01, \ldots, \mathrm{Z} = 25$. Fungsi enkripsinya adalah

$$f(p) = p + 3 \bmod 26;$$

yaitu, $A \mapsto D, B \mapsto E, \ldots, Z \mapsto C$. Dengan demikian, fungsi dekripsinya adalah

$$f^{-1}(p) = p - 3 \bmod 26 = p + 23 \bmod 26.$$

Misalkan kita menerima pesan terenkripsi `DOJHEUD`. Untuk mendekripsi pesan ini, mula-mula kita nyatakan pesan tersebut dengan angka:

$$3, 14, 9, 7, 4, 20, 3.$$

Selanjutnya, kita terapkan transformasi invers untuk memperoleh

$$0, 11, 6, 4, 1, 17, 0,$$

atau `ALGEBRA`. Perhatikan bahwa tidak ada sesuatu yang istimewa pada bilangan 3 maupun 26. Kita dapat saja menggunakan alfabet yang lebih besar atau pergeseran yang berbeda. ▲

Kriptanalisis membahas penguraian pesan yang diterima atau disadap. Metode dari peluang dan statistika sangat membantu dalam menguraikan pesan yang disadap; misalnya, analisis frekuensi karakter yang muncul dalam pesan tersebut sering memungkinkan pesan itu didekripsi.

Contoh 7.1.2 Misalkan kita menerima pesan yang diketahui telah dienkripsi dengan transformasi geser pada huruf tunggal dari alfabet 26 huruf. Untuk mengetahui secara tepat transformasi geser yang digunakan, kita harus menghitung b dalam persamaan $f(p) = p + b \bmod 26$. Hal ini dapat dilakukan dengan analisis frekuensi. Huruf $\mathrm{E} = 04$ adalah huruf yang paling sering muncul dalam bahasa Inggris. Misalkan $\mathrm{S} = 18$ adalah huruf yang paling sering muncul dalam teks tersandi. Maka kita memiliki alasan kuat untuk menduga bahwa $18 = 4 + b \bmod 26$, atau $b = 14$. Oleh karena itu, fungsi enkripsi yang paling mungkin adalah

$$f(p) = p + 14 \bmod 26.$$

Fungsi dekripsi yang bersesuaian adalah

$$f^{-1}(p) = p + 12 \bmod 26.$$

Sekarang mudah untuk menentukan apakah dugaan kita benar. ▲

Sandi geser sederhana merupakan contoh **sistem kriptografi monoalfabetik**. Dalam sandi semacam ini, satu karakter pada pesan tersandi mewakili

tepat satu karakter pada pesan asli. Sistem kriptografi seperti ini tidak terlalu canggih dan cukup mudah dipecahkan. Bahkan, pada pergeseran sederhana seperti yang dijelaskan dalam Contoh 7.1.1, hanya ada 26 kemungkinan kunci. Mencoba semuanya akan cukup mudah dibandingkan menggunakan analisis frekuensi.

Mari kita selidiki sistem kriptografi yang sedikit lebih canggih. Misalkan fungsi enkripsinya diberikan oleh

$$f(p) = ap + b \bmod 26.$$

Pertama-tama, kita perlu menentukan kapan fungsi dekripsi f^{-1} ada. Fungsi dekripsi tersebut ada apabila kita dapat menyelesaikan persamaan

$$c = ap + b \bmod 26$$

terhadap p. Berdasarkan Proposisi 3.1.4, hal ini dapat dilakukan tepat ketika a memiliki invers atau, secara ekuivalen, ketika $\gcd(a, 26) = 1$. Dalam hal ini,

$$f^{-1}(p) = a^{-1}p - a^{-1}b \bmod 26.$$

Sistem kriptografi seperti ini disebut **sistem kriptografi afin**.

Contoh 7.1.3 Perhatikan sistem kriptografi afin $f(p) = ap + b \bmod 26$. Agar sistem ini bekerja, kita harus memilih $a \in \mathbb{Z}_{26}$ yang memiliki invers. Hal ini hanya mungkin jika $\gcd(a, 26) = 1$. Dengan memperhatikan fakta tersebut, kita ambil $a = 5$ karena $\gcd(5, 26) = 1$. Mudah dilihat bahwa $a^{-1} = 21$. Oleh karena itu, kita dapat mengambil fungsi enkripsi $f(p) = 5p + 3 \bmod 26$. Dengan demikian, `ALGEBRA` dienkripsi menjadi $3, 6, 7, 23, 8, 10, 3$, atau `DGHXIKD`. Fungsi dekripsinya adalah

$$f^{-1}(p) = 21p - 21 \cdot 3 \bmod 26 = 21p + 15 \bmod 26.$$

▲

Sistem kriptografi akan lebih aman jika sebuah huruf teks tersandi dapat mewakili lebih dari satu huruf teks terang. Sebagai contoh sistem kriptografi jenis ini, yang disebut **sistem kriptografi polialfabetik**, kita akan memperumum sandi afin dengan menggunakan matriks. Gagasannya bekerja kurang lebih seperti sebelumnya; namun, alih-alih mengenkripsi satu huruf pada satu waktu, kita akan mengenkripsi pasangan huruf. Kita dapat menyimpan pasangan huruf p_1 dan p_2 dalam sebuah vektor

$$\mathbf{p} = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}.$$

Misalkan A adalah matriks 2×2 yang memiliki invers dan entri-entrinya berada dalam $\mathbb{Z}_{26}$. Kita dapat mendefinisikan fungsi enkripsi dengan

$$f(\mathbf{p}) = A\mathbf{p} + \mathbf{b},$$

dengan $\mathbf{b}$ sebagai vektor kolom tetap dan operasi matriks dilakukan dalam $\mathbb{Z}_{26}$. Fungsi dekripsinya haruslah

$$f^{-1}(\mathbf{p}) = A^{-1}\mathbf{p} - A^{-1}\mathbf{b}.$$

Contoh 7.1.4 Misalkan kita ingin mengenkripsi kata `HELP`. Untai angka yang

bersesuaian adalah $7, 4, 11, 15$. Jika

$$A = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix},$$

maka

$$A^{-1} = \begin{pmatrix} 2 & 21 \\ 25 & 3 \end{pmatrix}.$$

Jika $\mathbf{b} = (2, 2)^{\mathrm{t}}$, maka pesan kita dienkripsi menjadi `RRGR`. Huruf R yang terenkripsi mewakili lebih dari satu huruf teks terang. ▲

Analisis frekuensi masih dapat dilakukan pada sistem kriptografi polialfabetik, karena kita memahami dengan baik bagaimana pasangan huruf muncul dalam bahasa Inggris. Pasangan *th* cukup sering muncul; sedangkan pasangan *qz* tidak pernah muncul. Untuk mencegah dekripsi oleh pihak ketiga, kita harus menggunakan matriks yang lebih besar daripada matriks dalam Contoh 7.1.4.

7.2 Kriptografi Kunci Publik

Jika sistem kriptografi tradisional digunakan, siapa pun yang cukup memahami cara mengenkripsi pesan juga akan cukup memahami cara mendekripsi pesan yang disadap. Pada tahun 1976, W. Diffie dan M. Hellman mengusulkan kriptografi kunci publik, yang didasarkan pada pengamatan bahwa prosedur enkripsi dan dekripsi tidak harus menggunakan kunci yang sama. Hal ini menghilangkan keharusan untuk merahasiakan kunci enkripsi. Fungsi enkripsi f harus relatif mudah dihitung, tetapi f^{-1} harus sangat sulit dihitung tanpa informasi tambahan, sehingga orang yang hanya mengetahui kunci enkripsi tidak dapat menemukan kunci dekripsi tanpa komputasi yang terlampau berat. Menarik untuk dicatat bahwa hingga kini, belum ada sistem yang terbukti "satu arah;" artinya, untuk setiap sistem kriptografi kunci publik yang ada, belum pernah dibuktikan bahwa mendekripsi pesan hanya dengan mengetahui kunci enkripsinya memerlukan komputasi yang terlampau berat.

7.2.1 Sistem Kriptografi RSA

Sistem kriptografi RSA yang diperkenalkan oleh R. Rivest, A. Shamir, dan L. Adleman pada tahun 1978 didasarkan pada sulitnya memfaktorkan bilangan besar. Walaupun mencari dua bilangan prima besar secara acak lalu mengalikannya bukan tugas yang sulit, dengan algoritma tercepat yang tersedia pada awal 1990-an, memfaktorkan bilangan 150 digit yang merupakan hasil kali dua bilangan prima besar akan memerlukan sekitar 50 juta tahun jika dikerjakan oleh 100 juta komputer yang masing-masing menjalankan 10 juta instruksi per detik. Meskipun algoritmanya telah berkembang, memfaktorkan bilangan yang merupakan hasil kali dua bilangan prima besar tetap memerlukan komputasi yang terlampau berat.

Sistem kriptografi RSA bekerja sebagai berikut. Misalkan kita memilih dua bilangan prima acak berukuran 150 digit, p dan q. Selanjutnya, kita hitung hasil kali $n = pq$ dan juga $\phi(n) = m = (p-1)(q-1)$, dengan ϕ sebagai fungsi ϕ Euler. Kemudian kita memilih bilangan bulat acak E sampai menemukan satu yang relatif prima terhadap m; yaitu, kita pilih E sedemikian sehingga $\gcd(E, m) = 1$. Dengan algoritma Euklides, kita dapat menemukan bilangan D sedemikian sehingga $DE \equiv 1 \pmod{m}$. Bilangan n dan E kemudian diumumkan kepada publik.

Sekarang, misalkan orang B (Bob) ingin mengirimkan pesan kepada orang A (Alice) melalui saluran publik. Karena E dan n diketahui oleh semua orang, siapa pun dapat mengenkripsi pesan. Mula-mula Bob menyatakan pesan dengan angka menurut suatu skema, misalnya $\mathrm{A} = 00, \mathrm{B} = 02, \ldots, \mathrm{Z} = 25$. Jika perlu, ia memecah pesan menjadi bagian-bagian sehingga setiap bagian merupakan bilangan bulat positif yang lebih kecil daripada n. Misalkan x adalah salah satu bagian tersebut. Bob membentuk bilangan $y = x^E \mod n$ dan mengirimkan y kepada Alice. Untuk memperoleh kembali x, Alice cukup menghitung $x = y^D \mod n$. Hanya Alice yang mengetahui D.

Contoh 7.2.1 Sebelum menyelidiki teori di balik sistem kriptografi RSA atau mencoba menggunakan bilangan bulat besar, kita akan menggunakan beberapa bilangan bulat kecil untuk melihat bahwa sistem tersebut memang bekerja. Misalkan kita ingin mengirim suatu pesan yang setelah dinyatakan dengan angka menjadi 25. Ambil $p = 23$ dan $q = 29$. Maka

$$n = pq = 667$$

dan

$$\phi(n) = m = (p-1)(q-1) = 616.$$

Kita dapat mengambil $E = 487$, karena $\gcd(616, 487) = 1$. Pesan terenkripsi dihitung sebagai

$$25^{487} \mod 667 = 169.$$

Perhitungan ini dapat dilakukan secara wajar dengan metode kuadrat berulang seperti yang dijelaskan dalam Bab 4. Dengan algoritma Euklides, kita memperoleh $191E = 1 + 151m$; oleh karena itu, kunci dekripsinya adalah $(n, D) = (667, 191)$. Kita dapat memperoleh kembali pesan asli dengan menghitung

$$169^{191} \mod 667 = 25.$$

▲

Sekarang mari kita periksa mengapa sistem kriptografi RSA bekerja. Kita mengetahui bahwa $DE \equiv 1 \pmod{m}$; maka terdapat k sedemikian sehingga

$$DE = km + 1 = k\phi(n) + 1.$$

Ada dua kasus yang perlu dipertimbangkan. Pada kasus pertama, anggap bahwa $\gcd(x, n) = 1$. Berdasarkan Teorema 6.3.2,

$$y^D = (x^E)^D = x^{DE} = x^{km+1} = (x^{\phi(n)})^k x = (1)^k x = x \mod n.$$

Jadi, kita melihat bahwa Alice memperoleh kembali pesan asli x ketika menghitung $y^D \mod n$.

Untuk kasus lainnya, anggap bahwa $\gcd(x, n) \neq 1$. Karena $n = pq$ dan $x < n$, kita mengetahui bahwa x merupakan kelipatan p atau kelipatan q, tetapi bukan keduanya. Kita hanya akan menjelaskan kemungkinan pertama, karena kemungkinan kedua sepenuhnya serupa. Maka terdapat bilangan bulat r dengan $r < q$ dan $x = rp$. Perhatikan bahwa $\gcd(x, q) = 1$ dan $m = \phi(n) = (p-1)(q-1) = \phi(p)\phi(q)$. Kemudian, dengan menggunakan Teorema 6.3.2, tetapi sekarang modulo q,

$$x^{km} = x^{k\phi(p)\phi(q)} = (x^{\phi(q)})^{k\phi(p)} = (1)^{k\phi(p)} = 1 \mod q.$$

Jadi terdapat bilangan bulat t sedemikian sehingga $x^{km} = 1 + tq$. Dengan demikian, Alice juga memperoleh kembali pesan pada kasus ini,

$$y^D = x^{km+1} = x^{km}x = (1 + tq)x = x + tq(rp) = x + trn = x \mod n.$$

Sekarang kita dapat menanyakan bagaimana cara memecahkan sistem kriptografi RSA. Untuk menemukan D jika n dan E diketahui, kita hanya perlu memfaktorkan n dan mencari D dengan menggunakan algoritma Euklides. Jika kita mengetahui bahwa $667 = 23 \cdot 29$ dalam Contoh 7.2.1, kita dapat memperoleh D.

7.2.2 Verifikasi Pesan

Sistem kriptografi kunci publik menghadapi masalah verifikasi pesan. Karena kunci enkripsi diketahui publik, siapa pun dapat mengirimkan pesan terenkripsi. Jika Alice menerima pesan dari Bob, ia ingin dapat memverifikasi bahwa Bob benar-benar mengirim pesan tersebut. Misalkan kunci enkripsi Bob adalah (n', E') dan kunci dekripsinya adalah (n', D'). Misalkan pula kunci enkripsi Alice adalah (n, E) dan kunci dekripsinya adalah (n, D). Karena kunci enkripsi merupakan informasi publik, mereka dapat bertukar pesan tersandi kapan pun diperlukan. Bob ingin meyakinkan Alice bahwa pesan yang dikirimnya autentik. Sebelum mengirimkan pesan x kepada Alice, Bob mendekripsi x dengan kuncinya sendiri:

$$x' = x^{D'} \bmod n'.$$

Siapa pun dapat mengubah x' kembali menjadi x hanya dengan enkripsi, tetapi hanya Bob yang dapat membentuk x'. Sekarang Bob mengenkripsi x' dengan kunci enkripsi Alice untuk membentuk

$$y' = {x'}^{E} \bmod n,$$

yaitu pesan yang hanya dapat didekripsi oleh Alice. Alice mendekripsi pesan tersebut, kemudian mengenkripsi hasilnya dengan kunci Bob untuk membaca pesan asli, yaitu pesan yang hanya mungkin dikirim oleh Bob.

Catatan Sejarah

Enkripsi pesan rahasia telah dilakukan sejak zaman Yunani dan Romawi kuno. Seperti yang telah kita ketahui, Julius Caesar menggunakan sandi geser sederhana untuk mengirim dan menerima pesan. Namun, kajian formal mengenai enkripsi dan dekripsi pesan kemungkinan dimulai oleh bangsa Arab pada abad ke-15. Pada abad ke-15 dan ke-16, matematikawan seperti Alberti dan Viete menemukan bahwa sistem kriptografi monoalfabetik tidak memberikan keamanan yang nyata. Pada abad ke-19, F. W. Kasiski menyusun metode untuk memecahkan sandi yang memungkinkan satu huruf teks tersandi mewakili lebih dari satu huruf teks terang, apabila kunci yang sama digunakan beberapa kali. Penemuan ini mendorong penggunaan sistem kriptografi dengan kunci yang hanya dipakai satu kali. Pada awal abad ke-20, tokoh seperti W. Friedman dan L. Hill meletakkan kriptografi di atas landasan matematika yang kukuh.

Setelah Perang Dunia I, dikembangkan mesin-mesin khusus untuk mengenkripsi dan mendekripsi pesan, dan para matematikawan sangat aktif dalam kriptografi selama Perang Dunia II. Upaya menembus sistem kriptografi negara-negara Poros diselenggarakan di Inggris dan Amerika Serikat oleh matematikawan terkemuka seperti Alan Turing dan A. A. Albert. Pihak Sekutu memperoleh keuntungan besar dalam Perang Dunia II dengan memecahkan sandi yang dihasilkan oleh mesin Enigma Jerman dan sandi Purple Jepang.

Menjelang 1970-an, minat terhadap kriptografi komersial mulai berkembang. Kebutuhan untuk melindungi transaksi perbankan, data komputer, dan surat elektronik terus meningkat. Pada awal 1970-an, IBM mengembangkan dan menerapkan LUZIFER, pendahulu Data Encryption Standard (DES) milik Na-

tional Bureau of Standards.
Konsep sistem kriptografi kunci publik yang dikemukakan oleh Diffie dan Hellman masih sangat baru (1976). Konsep ini dikembangkan lebih lanjut oleh Rivest, Shamir, dan Adleman melalui sistem kriptografi RSA (1978). Belum diketahui seberapa aman sistem-sistem tersebut. Sistem kriptografi ransel berpintu jebak yang dikembangkan oleh Merkle dan Hellman telah berhasil dipecahkan. Apakah sistem RSA dapat dipecahkan masih merupakan pertanyaan terbuka. Pada tahun 1991, RSA Laboratories menerbitkan daftar bilangan semiprima (bilangan yang memiliki tepat dua faktor prima) dengan hadiah uang bagi siapa pun yang mampu memberikan faktorisasi (http://www.emc.com/emc-plus/rsa-labs/historical/the-rsa-challenge-numbers.htm). Meskipun tantangan tersebut berakhir pada tahun 2007, banyak di antara bilangan-bilangan ini belum berhasil difaktorkan.
Penelitian kriptografi dan kriptografi itu sendiri telah menimbulkan banyak kontroversi. Pada tahun 1929, Henry Stimson, Menteri Luar Negeri di bawah Herbert Hoover, membubarkan Black Chamber (divisi kriptografi Departemen Luar Negeri) atas dasar etika bahwa "pria terhormat tidak membaca surat milik satu sama lain." Selama dua dasawarsa terakhir abad ke-20, National Security Agency ingin merahasiakan informasi tentang kriptografi, sedangkan komunitas akademik memperjuangkan hak untuk menerbitkan penelitian dasar. Saat ini, penelitian dalam kriptografi matematika dan teori bilangan komputasional sangat aktif, dan para matematikawan bebas menerbitkan hasil mereka dalam bidang-bidang tersebut.

7.3 Pertanyaan Bacaan

1. Gunakan fungsi `euler_phi()` dalam Sage untuk menghitung $\phi(893\,456\,123)$.

2. Gunakan fungsi `power_mod()` dalam Sage untuk menghitung $7^{324} \pmod{895}$.

3. Jelaskan dasar matematika dari pernyataan berikut: mengenkripsi pesan dengan kunci publik RSA sangat mudah secara komputasional, sedangkan mendekripsi komunikasi tanpa kunci privat sangat sulit secara komputasional.

4. Jelaskan perbedaan antara enkripsi pesan dan verifikasi pesan dalam RSA.

5. Jelaskan alasan yang membenarkan penyebutan usulan Diffie dan Hellman pada tahun 1976 sebagai sesuatu yang "revolusioner."

7.4 Latihan

1. Enkripsikan `IXLOVEXMATH` menggunakan sistem kriptografi dalam Contoh 7.1.1.

Petunjuk. `LAORYHAPDWK`

2. Dekripsikan `ZLOOA WKLVA EHARQ WKHA ILQDO`, yang dienkripsi menggunakan sistem kriptografi dalam Contoh 7.1.1.

3. Dengan menganggap bahwa sandi monoalfabetik digunakan untuk mengenkripsi pesan rahasia berikut, apakah pesan aslinya?

```
APHUO EGEHP PEXOV FKEUH CKVUE CHKVE APHUO
EGEHU EXOVL EXDKT VGEFT EHFKE UHCKF TZEXO
VEZDT TVKUE XOVKV ENOHK ZFTEH TEHKQ LEROF
PVEHP PEXOV ERYKP GERYT GVKEG XDRTE RGAGA
```

Apa arti penting pesan ini dalam sejarah kriptografi?

Petunjuk. Petunjuk: `V = E`, `E = X` (juga digunakan untuk spasi dan tanda baca), `K = R`.

4. Berapa banyak keseluruhan sistem kriptografi monoalfabetik yang mungkin? Seberapa aman sistem-sistem tersebut?

Petunjuk. $26! - 1$

5. Buktikan bahwa matriks 2×2 A dengan entri dalam $\mathbb{Z}_{26}$ memiliki invers jika dan hanya jika $\gcd(\det(A), 26) = 1$.

6. Diberikan matriks

$$A = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix},$$

gunakan fungsi enkripsi $f(\mathbf{p}) = A\mathbf{p} + \mathbf{b}$ untuk mengenkripsi pesan `CRYPTOLOGY`, dengan $\mathbf{b} = (2, 5)^{\mathrm{t}}$. Apakah fungsi dekripsinya?

7. Enkripsikan setiap pesan RSA x berikut dengan membagi x menjadi blok-blok bilangan bulat sepanjang 2; yaitu, jika $x = 142528$, enkripsikan 14, 25, dan 28 secara terpisah.

(a) $n = 3551, E = 629, x = 31$

(b) $n = 2257, E = 47, x = 23$

(c) $n = 120979, E = 13251, x = 142371$

(d) $n = 45629, E = 781, x = 231561$

Petunjuk. (a) 2791; (c) 11213525032442.

8. Hitung kunci dekripsi D untuk setiap kunci enkripsi dalam Latihan 7.4.7.

9. Dekripsikan setiap pesan RSA y berikut.

(a) $n = 3551, D = 1997, y = 2791$

(b) $n = 5893, D = 81, y = 34$

(c) $n = 120979, D = 27331, y = 112135$

(d) $n = 79403, D = 671, y = 129381$

Petunjuk. (a) 31 (c) 14.

10. Untuk setiap kunci enkripsi (n, E) berikut dalam sistem kriptografi RSA, hitung D.

(a) $(n, E) = (451, 231)$

(b) $(n, E) = (3053, 1921)$

(c) $(n, E) = (37986733, 12371)$

(d) $(n, E) = (16394854313, 34578451)$

Petunjuk. (a) $n = 11 \cdot 41$; (c) $n = 8779 \cdot 4327$.

11. Pesan terenkripsi sering dibagi menjadi blok-blok yang masing-masing terdiri atas n huruf. Pesan seperti `THE WORLD WONDERS WHY` dapat dienkripsi menjadi `JIW OCFRJ LPOEVYQ IOC`, tetapi dikirim sebagai `JIW OCF RJL POE VYQ IOC`. Apa keuntungan menggunakan blok yang terdiri atas n huruf?

12. Carilah bilangan bulat n, E, dan X sedemikian sehingga

$$X^E \equiv X \pmod{n}.$$

Apakah hal ini merupakan potensi masalah dalam sistem kriptografi RSA?

13. Setiap orang di kelas harus menyusun sistem kriptografi RSA menggunakan bilangan prima yang panjangnya 10 sampai 15 digit. Kumpulkan (n, E) dan sebuah pesan terenkripsi. Rahasiakan D. Cobalah memecahkan sandi milik satu sama lain.

7.5 Latihan Tambahan: Keprimaan dan Faktorisasi

Dalam sistem kriptografi RSA, kemampuan menemukan bilangan prima besar dengan mudah sangatlah penting. Selain itu, sistem ini tidak aman jika kita dapat memfaktorkan bilangan komposit yang merupakan hasil kali dua bilangan prima besar. Pendekatan dasar untuk kedua masalah ini cukup sederhana. Untuk menentukan apakah bilangan n prima atau untuk memfaktorkan n, kita dapat menggunakan pembagian percobaan. Kita cukup membagi n dengan $d = 2, 3, \ldots, \sqrt{n}$. Kita akan memperoleh suatu faktorisasi, atau n prima jika tidak ada d yang membagi n. Masalahnya, komputasi semacam ini memerlukan waktu yang terlampau lama jika n sangat besar.

1. Algoritma yang lebih baik untuk memfaktorkan bilangan bulat positif ganjil adalah **algoritma faktorisasi Fermat**.

(a) Misalkan $n = ab$ adalah bilangan komposit ganjil. Buktikan bahwa n dapat ditulis sebagai selisih dua kuadrat sempurna:

$$n = x^2 - y^2 = (x - y)(x + y).$$

Akibatnya, bilangan bulat positif ganjil dapat difaktorkan tepat ketika kita dapat menemukan bilangan bulat x dan y sedemikian sehingga $n = x^2 - y^2$.

(b) Tulislah program yang menerapkan algoritma faktorisasi berikut berdasarkan pengamatan pada bagian (a). Ekspresi `ceiling(sqrt(n))` berarti bilangan bulat terkecil yang lebih besar daripada atau sama dengan akar kuadrat n. Tulislah program lain untuk melakukan faktorisasi dengan pembagian percobaan, lalu bandingkan kecepatan kedua algoritma. Algoritma mana yang lebih cepat, dan mengapa?

```
x := ceiling(sqrt(n))
y := 1

1 : while x^2 - y^2 > n do
    y := y + 1

if x^2 - y^2 < n then
    x := x + 1
    y := 1
    goto 1
else if x^2 - y^2 = 0 then
    a := x - y
    b := x + y
    write n = a * b
```

2. **Uji Keprimaan.** Ingat kembali Teorema Kecil Fermat dari Bab 6. Misalkan p prima dengan $\gcd(a, p) = 1$. Maka $a^{p-1} \equiv 1 \pmod{p}$. Kita dapat menggunakan Teorema Kecil Fermat sebagai uji penyaring untuk bilangan prima. Sebagai contoh, 15 tidak mungkin prima karena

$$2^{15-1} \equiv 2^{14} \equiv 4 \pmod{15}.$$

Namun, 17 berpotensi prima karena

$$2^{17-1} \equiv 2^{16} \equiv 1 \pmod{17}.$$

Bilangan komposit ganjil n disebut **pseudoprima** jika

$$2^{n-1} \equiv 1 \pmod{n}.$$

Manakah di antara bilangan berikut yang prima dan manakah yang pseudoprima?

(a) 342 (c) 601 (e) 771

(b) 811 (d) 561 (f) 631

3. Misalkan n adalah bilangan komposit ganjil dan b adalah bilangan bulat positif sedemikian sehingga $\gcd(b, n) = 1$. Jika $b^{n-1} \equiv 1 \pmod{n}$, maka n disebut **pseudoprima terhadap basis** b. Tunjukkan bahwa 341 merupakan pseudoprima terhadap basis 2, tetapi bukan terhadap basis 3.

4. Tulislah program untuk menentukan semua bilangan prima yang kurang dari 2000 dengan pembagian percobaan. Tulislah program kedua yang menentukan semua bilangan kurang dari 2000 yang merupakan bilangan prima atau pseudoprima. Bandingkan kecepatan kedua program tersebut. Berapa banyak pseudoprima di bawah 2000?

Terdapat bilangan komposit yang merupakan pseudoprima untuk setiap basis yang relatif prima terhadap bilangan tersebut. Bilangan-bilangan ini disebut **bilangan Carmichael**. Bilangan Carmichael pertama adalah $561 = 3 \cdot 11 \cdot 17$. Pada tahun 1992, Alford, Granville, dan Pomerance membuktikan bahwa terdapat tak berhingga banyak bilangan Carmichael [4]. Namun, bilangan Carmichael sangat jarang. Hanya ada 2163 bilangan Carmichael yang kurang dari 25×10^9. Untuk uji keprimaan yang lebih canggih, lihat [1], [6], atau [7].

7.6 Referensi dan Bacaan yang Disarankan

[1] Bressoud, D. M. *Factorization and Primality Testing.* Springer-Verlag, New York, 1989.

[2] Diffie, W. and Hellman, M. E. "New Directions in Cryptography," *IEEE Trans. Inform. Theory* 22 (1976), 644–54.

[3] Gardner, M. "Mathematical games: A new kind of cipher that would take millions of years to break," *Scientific American* 237 (1977), 120–24.

[4] Granville, A. "Primality Testing and Carmichael Numbers," *Notices of the American Mathematical Society* 39 (1992), 696–700.

[5] Hellman, M. E. "The Mathematics of Public Key Cryptography," *Scientific American* 241 (1979), 130–39.

[6] Koblitz, N. *A Course in Number Theory and Cryptography.* 2nd ed. Springer, New York, 1994.

[7] Pomerance, C., ed. "Cryptology and Computational Number Theory", *Proceedings of Symposia in Applied Mathematics* 42 (1990) American Mathematical Society, Providence, RI.

[8] Rivest, R. L., Shamir, A., and Adleman, L., "A Method for Obtaining Signatures and Public-key Cryptosystems," *Comm. ACM* 21 (1978), 120–26.

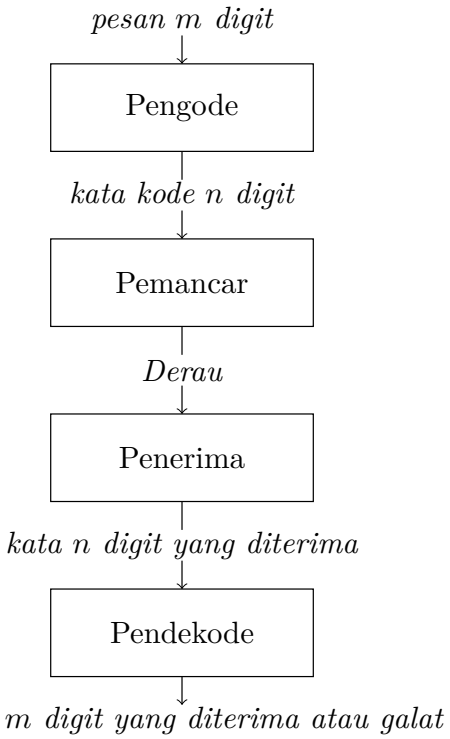
8

Teori Pengodean Aljabar

Teori pengodean merupakan penerapan aljabar yang menjadi semakin penting selama beberapa dasawarsa terakhir. Ketika mentransmisikan data, kita berkepentingan mengirimkan pesan melalui saluran yang dapat dipengaruhi oleh "derau." Kita ingin dapat mengodekan dan mendekode informasi dengan cara yang memungkinkan pendeteksian, dan jika mungkin pengoreksian, kesalahan yang disebabkan oleh derau. Situasi ini muncul dalam banyak bidang komunikasi, termasuk radio, telepon, televisi, komunikasi komputer, dan teknologi media digital. Probabilitas, kombinatorika, teori grup, aljabar linear, serta gelanggang polinomial atas lapangan berhingga semuanya memainkan peran penting dalam teori pengodean.

8.1 Kode Pendeteksi dan Pengoreksi Kesalahan

Mari kita periksa model sederhana sistem komunikasi untuk mentransmisikan dan menerima pesan berkode (Gambar 8.1.1).



Gambar 8.1.1 Mengodekan dan mendekode pesan

Pesan yang belum dikodekan dapat tersusun atas huruf atau karakter, tetapi biasanya terdiri atas tupel-m biner. Pesan-pesan ini dikodekan menjadi kata kode, yang terdiri atas tupel-n biner, oleh perangkat yang disebut **pengode**. Pesan tersebut ditransmisikan, lalu didekode. Kita akan mempertimbangkan terjadinya kesalahan selama transmisi. **Kesalahan** terjadi jika terdapat perubahan pada satu atau lebih bit dalam kata kode. **Skema pendekodean** adalah metode yang mengubah sebarang tupel-n yang diterima menjadi pesan bermakna yang telah didekode atau memberikan pesan kesalahan untuk tupel-n tersebut. Jika pesan yang diterima merupakan kata kode (salah satu tupel-n khusus yang diizinkan untuk ditransmisikan), maka pesan yang didekode harus merupakan pesan tunggal yang dikodekan menjadi kata kode tersebut. Untuk kata bukan-kode yang diterima, skema pendekodean akan memberikan tanda kesalahan, atau, jika dirancang dengan lebih cermat, benar-benar mencoba mengoreksi kesalahan dan merekonstruksi pesan semula. Tujuan kita adalah mentransmisikan pesan bebas kesalahan semurah dan secepat mungkin.

Contoh 8.1.2 Salah satu skema pengodean yang mungkin adalah mengirimkan pesan beberapa kali dan membandingkan salinan-salinan yang diterima. Andaikan pesan yang hendak dikodekan adalah tupel-n biner $(x_1, x_2, \ldots, x_n)$. Pesan tersebut dikodekan menjadi tupel-$3n$ biner dengan mengulang pesan itu tiga kali:

$$(x_1, x_2, \ldots, x_n) \mapsto (x_1, x_2, \ldots, x_n, x_1, x_2, \ldots, x_n, x_1, x_2, \ldots, x_n).$$

Untuk mendekode pesan, sebagai digit ke-i kita memilih digit yang muncul pada posisi ke-i dalam sedikitnya dua dari tiga transmisi. Sebagai contoh, jika pesan semula adalah (0110), maka pesan yang ditransmisikan adalah (0110 0110 0110). Jika terjadi kesalahan transmisi pada digit kelima, kata kode yang diterima adalah (0110 1110 0110), yang akan didekode dengan benar sebagai (0110).[1] Metode pengulangan tiga kali ini secara otomatis mendeteksi

dan mengoreksi semua kesalahan tunggal, tetapi metode tersebut lambat dan tidak efisien: untuk mengirimkan pesan yang terdiri atas n bit, diperlukan $2n$ bit tambahan, dan kita hanya dapat mendeteksi serta mengoreksi kesalahan tunggal. Kita akan melihat bahwa dapat ditemukan skema pengodean yang mengodekan pesan n bit menjadi m bit dengan m jauh lebih kecil daripada $3n$. ▲

Contoh 8.1.3 Paritas genap, suatu skema pengodean yang umum digunakan, jauh lebih efisien daripada skema pengulangan sederhana. Sistem pengodean ASCII (American Standard Code for Information Interchange) menggunakan tupel-8 biner, yang menghasilkan $2^8 = 256$ kemungkinan tupel-8. Namun, hanya diperlukan tujuh bit karena hanya terdapat $2^7 = 128$ karakter ASCII. Apa yang dapat atau seharusnya dilakukan dengan bit tambahan tersebut? Dengan menggunakan kedelapan bit sepenuhnya, kita dapat mendeteksi kesalahan transmisi tunggal. Sebagai contoh, kode ASCII untuk A, B, dan C adalah

$$\begin{aligned} \text{A} &= 65_{10} = 01000001_2, \\ \text{B} &= 66_{10} = 01000010_2, \\ \text{C} &= 67_{10} = 01000011_2. \end{aligned}$$

Perhatikan bahwa bit paling kiri selalu ditetapkan sebagai 0; yaitu, 128 karakter ASCII mempunyai kode

$$\begin{aligned} 00000000_2 &= 0_{10}, \\ &\vdots \\ 01111111_2 &= 127_{10}. \end{aligned}$$

Bit tersebut dapat digunakan untuk memeriksa kesalahan pada tujuh bit lainnya. Bit itu ditetapkan sebagai 0 atau 1 agar jumlah keseluruhan bit 1 dalam representasi suatu karakter genap. Dengan menggunakan paritas genap, kode untuk A, B, dan C kini menjadi

$$\begin{aligned} \text{A} &= 01000001_2, \\ \text{B} &= 01000010_2, \\ \text{C} &= 11000011_2. \end{aligned}$$

Andaikan A dikirimkan dan derau pada saluran komunikasi menyebabkan kesalahan transmisi pada bit keenam sehingga (0100 0101) diterima. Kita mengetahui bahwa telah terjadi kesalahan karena kata yang diterima mempunyai jumlah bit 1 yang ganjil, dan kini kita dapat meminta agar kata kode ditransmisikan kembali. Ketika digunakan untuk memeriksa kesalahan, bit paling kiri disebut **bit pemeriksa paritas**.

Kode pendeteksi kesalahan yang paling umum digunakan dalam komputer sejauh ini didasarkan pada penambahan bit paritas. Biasanya, komputer menyimpan informasi dalam tupel-m yang disebut **kata**. Panjang kata yang umum adalah 8, 16, dan 32 bit. Satu bit dalam kata dicadangkan sebagai bit pemeriksa paritas dan tidak digunakan untuk menyimpan informasi. Bit ini ditetapkan sebagai 0 atau 1, bergantung pada banyaknya bit 1 dalam kata tersebut.

Penambahan bit pemeriksa paritas memungkinkan pendeteksian semua kesalahan tunggal karena perubahan satu bit akan menambah atau mengurangi

[1]Kita akan menggunakan konvensi bahwa bit dalam tupel-n biner dinomori dari kiri ke kanan.

banyaknya bit 1 sebanyak satu, dan dalam kedua kasus paritas berubah dari genap menjadi ganjil, sehingga kata baru tersebut bukan kata kode. (Kita juga dapat menyusun skema pendeteksian kesalahan berdasarkan **paritas ganjil**; yaitu, kita dapat menetapkan bit pemeriksa paritas sedemikian sehingga kata kode selalu mempunyai jumlah bit 1 yang ganjil.) ▲

Sistem paritas genap mudah diimplementasikan, tetapi mempunyai dua kelemahan. Pertama, kesalahan jamak tidak dapat dideteksi. Andaikan A dikirimkan dan bit pertama serta ketujuh diubah dari 0 menjadi 1. Kata yang diterima merupakan kata kode, tetapi akan didekode menjadi C, bukan A. Kedua, kita tidak mempunyai kemampuan untuk mengoreksi kesalahan. Jika tupel-8 (1001 1000) diterima, kita mengetahui bahwa telah terjadi kesalahan, tetapi tidak mengetahui bit mana yang telah berubah. Sekarang kita akan menyelidiki skema pengodean yang tidak hanya memungkinkan pendeteksian kesalahan transmisi, tetapi benar-benar mengoreksinya.

Contoh 8.1.4 Andaikan pesan semula adalah 0 atau 1, dan 0 dikodekan menjadi (000), sedangkan 1 dikodekan menjadi (111). Jika hanya terjadi satu kesalahan selama transmisi, kita dapat mendeteksi dan mengoreksi kesalahan tersebut. Sebagai contoh, jika (101) diterima, bit kedua pastilah telah berubah dari 1 menjadi 0. Kata kode yang semula ditransmisikan pastilah (111). Metode ini akan mendeteksi dan mengoreksi semua kesalahan tunggal.

Tabel 8.1.5 Kode pengulangan

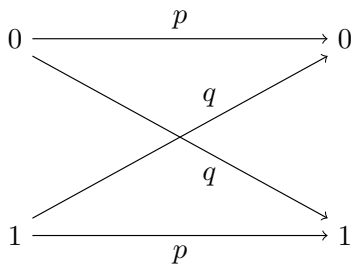
Ditransmisikan	Kata yang Diterima							
Kata Kode	000	001	010	011	100	101	110	111
000	0	1	1	2	1	2	2	3
111	3	2	2	1	2	1	1	0

Dalam Tabel 8.1.5, kita menyajikan semua kemungkinan kata yang dapat diterima untuk kata kode (000) dan (111) yang ditransmisikan. Tabel 8.1.5 juga menunjukkan banyaknya bit yang membedakan setiap tupel-3 yang diterima dari setiap kata kode semula. ▲

8.1.1 Pendekodean Kemungkinan Maksimum

Skema pengodean yang disajikan dalam Contoh 8.1.4 belum merupakan penyelesaian lengkap karena tidak memperhitungkan kemungkinan terjadinya kesalahan jamak. Sebagai contoh, (000) ataupun (111) dapat dikirimkan dan (001) diterima. Dari kata yang diterima, kita tidak dapat menentukan apakah terjadi satu kesalahan pada bit ketiga atau dua kesalahan, masing-masing pada bit pertama dan kedua. Apa pun skema pengodean yang digunakan, pesan yang salah dapat diterima. Kita dapat mentransmisikan (000), mengalami kesalahan pada ketiga bit, lalu menerima kata kode (111). Penting untuk menyatakan secara eksplisit asumsi tentang kemungkinan dan distribusi kesalahan transmisi agar, dalam penerapan tertentu, dapat diketahui apakah suatu skema pendeteksian kesalahan sesuai. Kita akan mengasumsikan bahwa kesalahan transmisi jarang terjadi dan, ketika terjadi, kesalahan pada setiap bit saling bebas; yaitu, jika p adalah probabilitas kesalahan pada satu bit dan q adalah probabilitas kesalahan pada bit lain, maka probabilitas terjadinya kesalahan pada kedua bit tersebut secara bersamaan adalah pq. Kita juga akan mengasumsikan bahwa tupel-n yang diterima didekode menjadi kata kode yang paling dekat dengannya; yaitu, kita mengasumsikan bahwa penerima

menggunakan **pendekodean kemungkinan maksimum**.[2]



Gambar 8.1.6 Saluran simetris biner

Saluran simetris biner adalah model yang terdiri atas pemancar yang mampu mengirimkan sinyal biner, yakni 0 atau 1, bersama sebuah penerima. Misalkan p adalah probabilitas bahwa sinyal diterima dengan benar. Maka $q = 1 - p$ adalah probabilitas penerimaan yang salah. Jika 1 dikirimkan, probabilitas diterimanya 1 adalah p dan probabilitas diterimanya 0 adalah q (Gambar 8.1.6). Probabilitas tidak terjadinya kesalahan selama transmisi kata kode biner dengan panjang n adalah p^n. Sebagai contoh, jika $p = 0.999$ dan pesan yang terdiri atas 10.000 bit dikirimkan, probabilitas transmisi sempurna adalah

$$(0.999)^{10,000} \approx 0.00005.$$

Teorema 8.1.7 *Jika tupel-n biner* $(x_1, \ldots, x_n)$ *ditransmisikan melalui saluran simetris biner dengan probabilitas p bahwa tidak terjadi kesalahan pada setiap koordinat, maka probabilitas terjadinya kesalahan pada tepat k koordinat adalah*

$$\binom{n}{k} q^k p^{n-k}.$$

BUKTI. Tetapkan k koordinat yang berbeda. Mula-mula kita menghitung probabilitas terjadinya kesalahan pada himpunan koordinat tetap ini. Probabilitas terjadinya kesalahan pada salah satu koordinat tertentu dari k koordinat tersebut adalah q; probabilitas tidak terjadinya kesalahan pada setiap koordinat dari $n - k$ koordinat yang tersisa adalah p. Probabilitas masing-masing dari n kejadian saling bebas ini adalah $q^k p^{n-k}$. Banyaknya pola kesalahan yang mungkin dengan tepat k kesalahan adalah

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

yaitu banyaknya kombinasi n objek yang diambil k sekaligus. Setiap pola kesalahan ini mempunyai probabilitas $q^k p^{n-k}$ untuk terjadi; dengan demikian, probabilitas seluruh pola kesalahan tersebut adalah

$$\binom{n}{k} q^k p^{n-k}.$$

■

Contoh 8.1.8 Andaikan $p = 0.995$ dan pesan 500 bit dikirimkan. Probabilitas bahwa pesan tersebut dikirim tanpa kesalahan adalah

$$p^n = (0.995)^{500} \approx 0.082.$$

[2]Bagian ini memerlukan pengetahuan tentang probabilitas, tetapi dapat dilewati tanpa mengganggu kesinambungan pembahasan.

Probabilitas terjadinya tepat satu kesalahan adalah

$$\binom{n}{1} qp^{n-1} = 500(0.005)(0.995)^{499} \approx 0.204.$$

Probabilitas terjadinya tepat dua kesalahan adalah

$$\binom{n}{2} q^2 p^{n-2} = \frac{500 \cdot 499}{2}(0.005)^2(0.995)^{498} \approx 0.257.$$

Probabilitas terjadinya lebih dari dua kesalahan kira-kira

$$1 - 0.082 - 0.204 - 0.257 = 0.457.$$

▲

8.1.2 Kode Blok

Untuk mengembangkan kode pendeteksi dan pengoreksi kesalahan yang efisien, kita memerlukan perangkat matematika yang lebih canggih. Teori grup memungkinkan metode pengodean dan pendekodean pesan yang lebih cepat. Suatu kode adalah (n, m)-**kode blok** jika informasi yang hendak dikodekan dapat dibagi menjadi blok-blok berisi m digit biner, yang masing-masing dapat dikodekan menjadi n digit biner. Secara lebih khusus, kode blok-(n, m) terdiri atas **fungsi pengodean**

$$E : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$$

dan **fungsi pendekodean**

$$D : \mathbb{Z}_2^n \to \mathbb{Z}_2^m.$$

Kata kode adalah sebarang unsur dalam citra E. Kita juga mensyaratkan agar E bersifat satu-ke-satu sehingga dua blok informasi tidak dikodekan menjadi kata kode yang sama. Jika kode kita hendak mengoreksi kesalahan, maka D harus bersifat pada.

Contoh 8.1.9 Sistem pengodean paritas genap yang dikembangkan untuk mendeteksi kesalahan tunggal pada karakter ASCII merupakan kode blok-$(8, 7)$. Fungsi pengodeannya adalah

$$E(x_7, x_6, \ldots, x_1) = (x_8, x_7, \ldots, x_1),$$

dengan $x_8 = x_7 + x_6 + \cdots + x_1$, menggunakan penjumlahan dalam $\mathbb{Z}_2$. ▲

Misalkan $\mathbf{x} = (x_1, \ldots, x_n)$ dan $\mathbf{y} = (y_1, \ldots, y_n)$ adalah tupel-n biner. **Jarak Hamming** atau **jarak**, $d(\mathbf{x}, \mathbf{y})$, antara $\mathbf{x}$ dan $\mathbf{y}$ adalah banyaknya bit tempat $\mathbf{x}$ dan $\mathbf{y}$ berbeda. Jarak antara dua kata kode adalah jumlah minimum kesalahan transmisi yang diperlukan untuk mengubah satu kata kode menjadi kata kode lainnya. **Jarak minimum** suatu kode, $d_{\min}$, adalah nilai minimum dari semua jarak $d(\mathbf{x}, \mathbf{y})$, dengan $\mathbf{x}$ dan $\mathbf{y}$ merupakan kata kode yang berbeda. **Bobot**, $w(\mathbf{x})$, dari suatu kata kode biner $\mathbf{x}$ adalah banyaknya bit 1 dalam $\mathbf{x}$. Jelas bahwa $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$, dengan $\mathbf{0} = (00 \cdots 0)$.

Contoh 8.1.10 Misalkan $\mathbf{x} = (10101)$, $\mathbf{y} = (11010)$, dan $\mathbf{z} = (00011)$ merupakan semua kata kode dalam suatu kode C. Maka kita memperoleh jarak Hamming berikut:

$$d(\mathbf{x}, \mathbf{y}) = 4, \qquad d(\mathbf{x}, \mathbf{z}) = 3, \qquad d(\mathbf{y}, \mathbf{z}) = 3.$$

Jarak minimum kode ini adalah 3. Kita juga memperoleh bobot berikut:

$$w(\mathbf{x}) = 3, \qquad w(\mathbf{y}) = 3, \qquad w(\mathbf{z}) = 2.$$

▲

Proposisi berikut mencantumkan beberapa sifat dasar bobot suatu kata kode dan jarak antara dua kata kode. Pembuktiannya diserahkan sebagai latihan.

Proposisi 8.1.11 *Misalkan* $\mathbf{x}$, $\mathbf{y}$, *dan* $\mathbf{z}$ *merupakan tupel-n biner. Maka*

1. $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$;
2. $d(\mathbf{x}, \mathbf{y}) \geq 0$;
3. $d(\mathbf{x}, \mathbf{y}) = 0$ *tepat ketika* $\mathbf{x} = \mathbf{y}$;
4. $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$;
5. $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$.

Bobot dalam suatu kode biasanya jauh lebih mudah dihitung daripada jarak Hamming antara semua kata kode dalam kode tersebut. Jika kode disusun dengan cermat, fakta ini dapat kita manfaatkan.

Andaikan $\mathbf{x} = (1101)$ dan $\mathbf{y} = (1100)$ merupakan kata kode dalam suatu kode. Jika kita mentransmisikan (1101) dan terjadi kesalahan pada bit paling kanan, maka (1100) akan diterima. Karena (1100) merupakan kata kode, pendekode akan mendekode (1100) sebagai pesan yang ditransmisikan. Kode ini jelas kurang sesuai untuk mendeteksi kesalahan. Masalahnya adalah $d(\mathbf{x}, \mathbf{y}) = 1$. Jika $\mathbf{x} = (1100)$ dan $\mathbf{y} = (1010)$ merupakan kata kode, maka $d(\mathbf{x}, \mathbf{y}) = 2$. Jika $\mathbf{x}$ ditransmisikan dan terjadi satu kesalahan, maka $\mathbf{y}$ tidak mungkin diterima. Tabel 8.1.12 memberikan jarak antara semua kata kode 4 bit dengan tiga bit pertama membawa informasi dan bit keempat merupakan bit pemeriksa paritas genap. Kita dapat melihat bahwa jarak minimum di sini adalah 2; oleh karena itu, kode tersebut sesuai sebagai kode pendeteksi kesalahan tunggal.

Tabel 8.1.12 Jarak antara kata kode 4 bit

	0000	0011	0101	0110	1001	1010	1100	1111
0000	0	2	2	2	2	2	2	4
0011	2	0	2	2	2	2	4	2
0101	2	2	0	2	2	4	2	2
0110	2	2	2	0	4	2	2	2
1001	2	2	2	4	0	2	2	2
1010	2	2	4	2	2	0	2	2
1100	2	4	2	2	2	2	0	2
1111	4	2	2	2	2	2	2	0

Untuk menentukan secara tepat kemampuan suatu kode dalam mendeteksi dan mengoreksi kesalahan, kita perlu menganalisis jarak minimum kode tersebut. Misalkan $\mathbf{x}$ dan $\mathbf{y}$ merupakan kata kode. Jika $d(\mathbf{x}, \mathbf{y}) = 1$ dan terjadi kesalahan pada posisi tempat $\mathbf{x}$ dan $\mathbf{y}$ berbeda, maka $\mathbf{x}$ berubah menjadi $\mathbf{y}$. Kata kode yang diterima adalah $\mathbf{y}$ dan tidak diberikan pesan kesalahan. Sekarang andaikan $d(\mathbf{x}, \mathbf{y}) = 2$. Maka satu kesalahan tidak dapat mengubah $\mathbf{x}$ menjadi $\mathbf{y}$. Oleh karena itu, jika $d_{\min} = 2$, kita mampu mendeteksi kesalahan tunggal. Namun, andaikan $d(\mathbf{x}, \mathbf{y}) = 2$, $\mathbf{y}$ dikirimkan, dan suatu kata bukan-kode $\mathbf{z}$ diterima sedemikian sehingga

$$d(\mathbf{x}, \mathbf{z}) = d(\mathbf{y}, \mathbf{z}) = 1.$$

Maka pendekode tidak dapat memilih antara $\mathbf{x}$ dan $\mathbf{y}$. Meskipun mengetahui bahwa telah terjadi kesalahan, kita tidak mengetahui kesalahan tersebut.

Andaikan $d_{\min} \geq 3$. Maka skema pendekodean kemungkinan maksimum mengoreksi semua kesalahan tunggal. Berawal dari kata kode $\mathbf{x}$, kesalahan dalam transmisi satu bit menghasilkan $\mathbf{y}$ dengan $d(\mathbf{x}, \mathbf{y}) = 1$, tetapi $d(\mathbf{z}, \mathbf{y}) \geq 2$ untuk setiap kata kode lain $\mathbf{z} \neq \mathbf{x}$. Jika kita tidak mensyaratkan pengoreksian kesalahan, kita dapat mendeteksi kesalahan jamak ketika kode mempunyai jarak minimum yang lebih besar dari atau sama dengan 3.

Teorema 8.1.13 *Misalkan C suatu kode dengan $d_{\min} = 2n + 1$. Maka C dapat mengoreksi sebarang n kesalahan atau kurang. Selanjutnya, sebarang $2n$ kesalahan atau kurang dapat dideteksi dalam C.*

BUKTI. Andaikan kata kode $\mathbf{x}$ dikirimkan dan kata $\mathbf{y}$ diterima dengan paling banyak n kesalahan. Maka $d(\mathbf{x}, \mathbf{y}) \leq n$. Jika $\mathbf{z}$ adalah sebarang kata kode selain $\mathbf{x}$, maka

$$2n + 1 \leq d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \leq n + d(\mathbf{y}, \mathbf{z}).$$

Dengan demikian, $d(\mathbf{y}, \mathbf{z}) \geq n+1$ dan $\mathbf{y}$ akan didekode dengan benar sebagai $\mathbf{x}$. Sekarang andaikan $\mathbf{x}$ ditransmisikan dan $\mathbf{y}$ diterima serta sedikitnya satu kesalahan telah terjadi, tetapi tidak lebih dari $2n$ kesalahan. Maka $1 \leq d(\mathbf{x}, \mathbf{y}) \leq 2n$. Karena jarak minimum antara kata kode adalah $2n + 1$, $\mathbf{y}$ tidak mungkin merupakan kata kode. Akibatnya, kode tersebut dapat mendeteksi antara 1 dan $2n$ kesalahan. ■

Contoh 8.1.14 Dalam Tabel 8.1.15, kata-kata kode $\mathbf{c}_1 = (00000)$, $\mathbf{c}_2 = (00111)$, $\mathbf{c}_3 = (11100)$, dan $\mathbf{c}_4 = (11011)$ menentukan kode pengoreksi kesalahan tunggal.

Tabel 8.1.15 Jarak Hamming untuk kode pengoreksi kesalahan

	00000	00111	11100	11011
00000	0	3	3	4
00111	3	0	4	3
11100	3	4	0	3
11011	4	3	3	0

▲

Catatan Sejarah

Teori pengodean modern dimulai pada tahun 1948 melalui makalah C. Shannon, "A Mathematical Theory of Information" [7]. Makalah ini memberikan contoh kode aljabar, dan Teorema Shannon menyatakan secara tepat seberapa baik kode yang dapat diharapkan. Richard Hamming mulai meneliti kode linear di Bell Labs pada akhir 1940-an dan awal 1950-an setelah merasa frustrasi karena program yang dijalankannya tidak dapat pulih dari kesalahan sederhana yang ditimbulkan oleh derau. Teori pengodean telah berkembang pesat selama beberapa dasawarsa terakhir. *The Theory of Error-Correcting Codes*, karya MacWilliams dan Sloane [5], yang diterbitkan pada tahun 1977, telah memuat lebih dari 1.500 referensi. Kode linear (kode blok Reed-Muller $(32, 6)$) digunakan pada wahana antariksa Mariner milik NASA. Wahana antariksa yang lebih baru, seperti Voyager, menggunakan apa yang disebut kode konvolusi. Saat ini, penelitian yang sangat aktif dilakukan terhadap kode Goppa, yang sangat bergantung pada geometri aljabar.

8.2 Kode Linear

Untuk memperoleh pemahaman lebih mendalam tentang suatu kode dan mengembangkan teknik pengodean, pendekodean, dan pendeteksian kesalahan yang lebih efisien, kita perlu menambahkan struktur pada kode tersebut. Salah satu caranya adalah mensyaratkan agar kode tersebut juga merupakan grup. **Kode grup** adalah kode yang juga merupakan subgrup dari $\mathbb{Z}_2^n$.

Untuk memeriksa bahwa suatu kode merupakan kode grup, kita hanya perlu memverifikasi satu hal. Jika sebarang dua unsur dalam kode dijumlahkan, hasilnya harus merupakan tupel-n yang kembali berada dalam kode. Tidak perlu diperiksa bahwa invers tupel-n tersebut berada dalam kode, sebab setiap kata kode merupakan invers dirinya sendiri, dan juga tidak perlu diperiksa bahwa $\mathbf{0}$ merupakan kata kode. Sebagai contoh,

$$(11000101) + (11000101) = (00000000).$$

Contoh 8.2.1 Andaikan kita mempunyai kode yang terdiri atas tupel-7 berikut:

(0000000)	(0001111)	(0010101)	(0011010)
(0100110)	(0101001)	(0110011)	(0111100)
(1000011)	(1001100)	(1010110)	(1011001)
(1100101)	(1101010)	(1110000)	(1111111).

Memverifikasi bahwa kode ini juga merupakan subgrup dari $\mathbb{Z}_2^7$, dan oleh karena itu merupakan kode grup, merupakan tugas langsung meskipun melelahkan. Kode ini merupakan kode pendeteksi dan pengoreksi kesalahan tunggal, tetapi menghitung semua jarak antara pasangan kata kode untuk menentukan bahwa $d_{\min} = 3$ merupakan proses yang panjang dan melelahkan. Jauh lebih mudah melihat bahwa bobot minimum semua kata kode tak nol adalah 3. Seperti akan segera kita lihat, hal ini bukan kebetulan. Namun, hubungan antara bobot dan jarak dalam suatu kode sangat bergantung pada fakta bahwa kode tersebut merupakan grup. ▲

Lema 8.2.2 *Misalkan* $\mathbf{x}$ *dan* $\mathbf{y}$ *merupakan tupel-n biner. Maka* $w(\mathbf{x} + \mathbf{y}) = d(\mathbf{x}, \mathbf{y})$.

Bukti. Andaikan $\mathbf{x}$ dan $\mathbf{y}$ merupakan tupel-n biner. Maka jarak antara $\mathbf{x}$ dan $\mathbf{y}$ tepat sama dengan banyaknya posisi tempat $\mathbf{x}$ dan $\mathbf{y}$ berbeda. Namun, $\mathbf{x}$ dan $\mathbf{y}$ berbeda pada suatu koordinat tepat ketika jumlah pada koordinat tersebut adalah 1, sebab

$$\begin{aligned} 1 + 1 &= 0 \\ 0 + 0 &= 0 \\ 1 + 0 &= 1 \\ 0 + 1 &= 1. \end{aligned}$$

Akibatnya, bobot jumlah tersebut harus sama dengan jarak antara kedua kata kode. ■

Teorema 8.2.3 *Misalkan* $d_{\min}$ *adalah jarak minimum suatu kode grup* C. *Maka* $d_{\min}$ *adalah bobot minimum dari semua kata kode tak nol dalam* C. *Artinya,*

$$d_{\min} = \min\{w(\mathbf{x}) : \mathbf{x} \neq \mathbf{0}\}.$$

BUKTI. Perhatikan bahwa

$$\begin{aligned} d_{\min} &= \min\{d(\mathbf{x},\mathbf{y}) : \mathbf{x} \neq \mathbf{y}\} \\ &= \min\{d(\mathbf{x},\mathbf{y}) : \mathbf{x}+\mathbf{y} \neq \mathbf{0}\} \\ &= \min\{w(\mathbf{x}+\mathbf{y}) : \mathbf{x}+\mathbf{y} \neq \mathbf{0}\} \\ &= \min\{w(\mathbf{z}) : \mathbf{z} \neq \mathbf{0}\}. \end{aligned}$$

■

8.2.1 Kode Linear

Dari Contoh 8.2.1, kini mudah diperiksa bahwa bobot tak nol minimum adalah 3; dengan demikian, kode tersebut memang mendeteksi dan mengoreksi semua kesalahan tunggal. Kini kita telah mereduksi masalah pencarian kode yang "baik" menjadi masalah membangkitkan kode grup. Salah satu cara mudah membangkitkan kode grup adalah menggunakan sedikit teori matriks.

Definisikan **hasil kali dalam** dari dua tupel-n biner sebagai

$$\mathbf{x} \cdot \mathbf{y} = x_1y_1 + \cdots + x_ny_n,$$

dengan $\mathbf{x} = (x_1, x_2, \ldots, x_n)^{\mathrm{t}}$ dan $\mathbf{y} = (y_1, y_2, \ldots, y_n)^{\mathrm{t}}$ merupakan vektor kolom.[1] Sebagai contoh, jika $\mathbf{x} = (011001)^{\mathrm{t}}$ dan $\mathbf{y} = (110101)^{\mathrm{t}}$, maka $\mathbf{x} \cdot \mathbf{y} = 0$. Kita juga dapat memandang hasil kali dalam sebagai hasil kali matriks baris dengan matriks kolom; yaitu,

$$\begin{aligned} \mathbf{x} \cdot \mathbf{y} &= \mathbf{x}^{\mathrm{t}}\mathbf{y} \\ &= \begin{pmatrix} x_1 & x_2 & \cdots & x_n \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \\ &= x_1y_1 + x_2y_2 + \cdots + x_ny_n. \end{aligned}$$

Contoh 8.2.4 Andaikan kata-kata yang hendak dikodekan terdiri atas semua tupel-3 biner dan skema pengodean kita menggunakan paritas genap. Untuk mengodekan sebarang tupel-3, kita menambahkan bit keempat agar diperoleh jumlah bit 1 yang genap. Perhatikan bahwa sebarang tupel-n $\mathbf{x} = (x_1, x_2, \ldots, x_n)^{\mathrm{t}}$ mempunyai jumlah bit 1 yang genap tepat ketika $x_1+x_2+\cdots+x_n = 0$; dengan demikian, tupel-4 $\mathbf{x} = (x_1, x_2, x_3, x_4)^{\mathrm{t}}$ mempunyai jumlah bit 1 yang genap jika $x_1 + x_2 + x_3 + x_4 = 0$, atau

$$\mathbf{x} \cdot \mathbf{1} = \mathbf{x}^{\mathrm{t}}\mathbf{1} = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 0.$$

Contoh ini memberi petunjuk bahwa terdapat hubungan antara matriks dan teori pengodean. ▲

Misalkan $\mathbb{M}_{m\times n}(\mathbb{Z}_2)$ melambangkan himpunan semua matriks $m \times n$ dengan entri dalam $\mathbb{Z}_2$. Kita melakukan operasi matriks seperti biasa, kecuali bahwa semua operasi penjumlahan dan perkalian berlangsung dalam $\mathbb{Z}_2$. Definisikan **ruang nol** dari suatu matriks $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$ sebagai himpunan

[1] Karena kita akan bekerja dengan matriks, dalam sisa bab ini kita akan menulis tupel-n biner sebagai vektor kolom.

semua tupel-n biner $\mathbf{x}$ sedemikian sehingga $H\mathbf{x} = \mathbf{0}$. Kita melambangkan ruang nol matriks H dengan Null(H).

Contoh 8.2.5 Andaikan

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Agar tupel-5 $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5)^{\mathrm{t}}$ berada dalam ruang nol H, $H\mathbf{x} = \mathbf{0}$. Secara ekuivalen, sistem persamaan berikut harus dipenuhi:

$$\begin{aligned} x_2 + x_4 &= 0 \\ x_1 + x_2 + x_3 + x_4 &= 0 \\ x_3 + x_4 + x_5 &= 0. \end{aligned}$$

Himpunan tupel-5 biner yang memenuhi persamaan-persamaan ini adalah

$$(00000) \qquad (11110) \qquad (10101) \qquad (01011).$$

Mudah ditentukan bahwa kode ini merupakan kode grup. ▲

Teorema 8.2.6 *Misalkan H berada dalam $\mathbb{M}_{m\times n}(\mathbb{Z}_2)$. Maka ruang nol H merupakan kode grup.*

Bukti. Karena setiap unsur $\mathbb{Z}_2^n$ merupakan invers dirinya sendiri, satu-satunya hal yang benar-benar perlu diperiksa di sini adalah ketertutupan. Misalkan $\mathbf{x}, \mathbf{y} \in \mathrm{Null}(H)$ untuk suatu matriks H dalam $\mathbb{M}_{m\times n}(\mathbb{Z}_2)$. Maka $H\mathbf{x} = \mathbf{0}$ dan $H\mathbf{y} = \mathbf{0}$. Jadi,

$$H(\mathbf{x} + \mathbf{y}) = H\mathbf{x} + H\mathbf{y} = \mathbf{0} + \mathbf{0} = \mathbf{0}.$$

Dengan demikian, $\mathbf{x} + \mathbf{y}$ berada dalam ruang nol H dan karenanya harus merupakan kata kode. ■

Suatu kode disebut **kode linear** jika ditentukan oleh ruang nol suatu matriks $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$.

Contoh 8.2.7 Misalkan C adalah kode yang diberikan oleh matriks

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Andaikan tupel-6 $\mathbf{x} = (010011)^{\mathrm{t}}$ diterima. Menentukan apakah $\mathbf{x}$ merupakan kata kode cukup dilakukan melalui perkalian matriks sederhana. Karena

$$H\mathbf{x} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},$$

kata yang diterima bukan kata kode. Kita harus mencoba mengoreksi kata tersebut atau meminta agar kata itu ditransmisikan kembali. ▲

8.3 Matriks Pemeriksa Paritas dan Matriks Pembangkit

Kita perlu menemukan cara sistematis untuk membangkitkan kode linear serta metode pendekodean yang cepat. Dengan memeriksa sifat-sifat matriks H dan memilih H dengan cermat, kita dapat mengembangkan metode pengodean dan pendekodean pesan yang sangat efisien. Untuk tujuan ini, kita akan memperkenalkan matriks pembangkit standar dan matriks pemeriksa paritas kanonik.

Andaikan H adalah matriks $m \times n$ dengan entri dalam $\mathbb{Z}_2$ dan $n > m$. Jika m kolom terakhir matriks tersebut membentuk matriks identitas $m \times m$, I_m, maka matriks tersebut merupakan **matriks pemeriksa paritas kanonik**. Secara lebih khusus, $H = (A \mid I_m)$, dengan A adalah matriks $m \times (n-m)$

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,n-m} \\ a_{21} & a_{22} & \cdots & a_{2,n-m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{m,n-m} \end{pmatrix}$$

dan I_m adalah matriks identitas $m \times m$

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Dengan setiap matriks pemeriksa paritas kanonik, kita dapat mengaitkan sebuah $n \times (n-m)$ **matriks pembangkit standar**

$$G = \begin{pmatrix} I_{n-m} \\ \hline A \end{pmatrix}.$$

Tujuan kita adalah menunjukkan bahwa terdapat $\mathbf{x}$ yang memenuhi $G\mathbf{x} = \mathbf{y}$ jika dan hanya jika $H\mathbf{y} = \mathbf{0}$. Diberikan blok pesan $\mathbf{x}$ yang hendak dikodekan, matriks G memungkinkan kita mengodekannya dengan cepat menjadi kata kode linear $\mathbf{y}$.

Contoh 8.3.1 Andaikan kita mempunyai delapan kata berikut untuk dikodekan:

$$(000), (001), (010), \ldots, (111).$$

Untuk

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

matriks pembangkit standar dan matriks pemeriksa paritas kanonik yang terkait adalah

$$G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

dan

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

secara berurutan.

Perhatikan bahwa baris-baris dalam H merepresentasikan pemeriksaan paritas pada posisi bit tertentu dalam tupel-6. Bit-bit 1 dalam matriks identitas berfungsi sebagai pemeriksa paritas untuk bit-bit 1 pada baris yang sama. Jika $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5, x_6)$, maka

$$\mathbf{0} = H\mathbf{x} = \begin{pmatrix} x_2 + x_3 + x_4 \\ x_1 + x_2 + x_5 \\ x_1 + x_3 + x_6 \end{pmatrix},$$

yang menghasilkan sistem persamaan:

$$\begin{aligned} x_2 + x_3 + x_4 &= 0 \\ x_1 + x_2 + x_5 &= 0 \\ x_1 + x_3 + x_6 &= 0. \end{aligned}$$

Di sini x_4 berfungsi sebagai bit pemeriksa untuk x_2 dan x_3; x_5 adalah bit pemeriksa untuk x_1 dan x_2; dan x_6 adalah bit pemeriksa untuk x_1 dan x_3. Matriks identitas mencegah x_4, x_5, dan x_6 harus saling memeriksa. Dengan demikian, x_1, x_2, dan x_3 dapat dipilih sebarang, tetapi x_4, x_5, dan x_6 harus dipilih untuk menjamin paritas. Ruang nol H mudah dihitung sebagai

$$\begin{array}{llll} (000000) & (001101) & (010110) & (011011) \\ (100011) & (101110) & (110101) & (111000). \end{array}$$

Cara yang lebih mudah lagi untuk menghitung ruang nol adalah menggunakan matriks pembangkit G (Tabel 8.3.2). ▲

Tabel 8.3.2 Kode yang dibangkitkan oleh matriks

Kata Pesan $\mathbf{x}$	Kata Kode $G\mathbf{x}$
000	000000
001	001101
010	010110
011	011011
100	100011
101	101110
110	110101
111	111000

Teorema 8.3.3 *Jika $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$ merupakan matriks pemeriksa paritas kanonik, maka* $\text{Null}(H)$ *terdiri atas semua $\mathbf{x} \in \mathbb{Z}_2^n$ yang $n - m$ bit pertamanya sebarang, sedangkan m bit terakhirnya ditentukan oleh $H\mathbf{x} = \mathbf{0}$. Setiap bit di antara m bit terakhir berfungsi sebagai bit pemeriksa paritas genap bagi sebagian dari $n - m$ bit pertama. Jadi, H menghasilkan kode blok $(n, n - m)$.*

Pembuktian teorema ini kami serahkan sebagai latihan. Berdasarkan teorema tersebut, $n - m$ bit pertama dalam $\mathbf{x}$ disebut **bit informasi**, sedangkan m bit terakhir disebut **bit pemeriksa**. Dalam Contoh 8.3.1, tiga bit pertama merupakan bit informasi dan tiga bit terakhir merupakan bit pemeriksa.

Teorema 8.3.4 *Misalkan G adalah matriks pembangkit standar $n \times k$. Maka $C = \{\mathbf{y} : G\mathbf{x} = \mathbf{y}$ untuk $\mathbf{x} \in \mathbb{Z}_2^k\}$ merupakan kode blok (n, k). Secara lebih khusus, C merupakan kode grup.*

BUKTI. Misalkan $G\mathbf{x}_1 = \mathbf{y}_1$ dan $G\mathbf{x}_2 = \mathbf{y}_2$ adalah dua kata kode. Maka $\mathbf{y}_1 + \mathbf{y}_2$ berada dalam C karena

$$G(\mathbf{x}_1 + \mathbf{x}_2) = G\mathbf{x}_1 + G\mathbf{x}_2 = \mathbf{y}_1 + \mathbf{y}_2.$$

Kita juga harus menunjukkan bahwa dua blok pesan tidak dapat dikodekan menjadi kata kode yang sama. Artinya, kita harus menunjukkan bahwa jika $G\mathbf{x} = G\mathbf{y}$, maka $\mathbf{x} = \mathbf{y}$. Misalkan $G\mathbf{x} = G\mathbf{y}$. Maka

$$G\mathbf{x} - G\mathbf{y} = G(\mathbf{x} - \mathbf{y}) = \mathbf{0}.$$

Namun, k koordinat pertama dalam $G(\mathbf{x} - \mathbf{y})$ tepat sama dengan $x_1 - y_1, \ldots, x_k - y_k$, karena koordinat-koordinat tersebut ditentukan oleh matriks identitas I_k, yang merupakan bagian dari G. Jadi, $G(\mathbf{x} - \mathbf{y}) = \mathbf{0}$ tepat ketika $\mathbf{x} = \mathbf{y}$. ■

Sebelum kita dapat membuktikan hubungan antara matriks pemeriksa paritas kanonik dan matriks pembangkit standar, kita perlu membuktikan sebuah lema.

Lema 8.3.5 *Misalkan $H = (A \mid I_m)$ adalah matriks pemeriksa paritas kanonik $m \times n$ dan $G = \begin{pmatrix} I_{n-m} \\ A \end{pmatrix}$ adalah matriks pembangkit standar $n \times (n - m)$ yang bersesuaian. Maka $HG = \mathbf{0}$.*

BUKTI. Misalkan $C = HG$. Entri ke-ij dalam C adalah

$$\begin{aligned} c_{ij} &= \sum_{k=1}^{n} h_{ik} g_{kj} \\ &= \sum_{k=1}^{n-m} h_{ik} g_{kj} + \sum_{k=n-m+1}^{n} h_{ik} g_{kj} \\ &= \sum_{k=1}^{n-m} a_{ik} \delta_{kj} + \sum_{k=n-m+1}^{n} \delta_{i-(m-n),k} a_{kj} \\ &= a_{ij} + a_{ij} \\ &= 0, \end{aligned}$$

dengan

$$\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

adalah delta Kronecker. ■

Teorema 8.3.6 *Misalkan $H = (A \mid I_m)$ adalah matriks pemeriksa paritas kanonik $m \times n$ dan $G = \begin{pmatrix} I_{n-m} \\ A \end{pmatrix}$ adalah matriks pembangkit standar $n \times (n-m)$ yang terkait dengan H. Misalkan C adalah kode yang dibangkitkan oleh G. Maka $\mathbf{y}$ berada dalam C jika dan hanya jika $H\mathbf{y} = \mathbf{0}$. Secara khusus, C merupakan kode linear dengan matriks pemeriksa paritas kanonik H.*

BUKTI. Pertama, misalkan $\mathbf{y} \in C$. Maka $G\mathbf{x} = \mathbf{y}$ untuk suatu $\mathbf{x} \in \mathbb{Z}_2^m$. Berdasarkan Lema 8.3.5, $H\mathbf{y} = HG\mathbf{x} = \mathbf{0}$.

Sebaliknya, misalkan $\mathbf{y} = (y_1, \ldots, y_n)^{\mathrm{t}}$ berada dalam ruang nol H. Kita perlu mencari suatu $\mathbf{x}$ dalam $\mathbb{Z}_2^{n-m}$ sedemikian sehingga $G\mathbf{x}^{\mathrm{t}} = \mathbf{y}$. Karena

$H\mathbf{y} = \mathbf{0}$, sistem persamaan berikut harus dipenuhi:

$$\begin{aligned} a_{11}y_1 + a_{12}y_2 + \cdots + a_{1,n-m}y_{n-m} + y_{n-m+1} &= 0 \\ a_{21}y_1 + a_{22}y_2 + \cdots + a_{2,n-m}y_{n-m} + y_{n-m+2} &= 0 \\ &\vdots \\ a_{m1}y_1 + a_{m2}y_2 + \cdots + a_{m,n-m}y_{n-m} + y_{n-m+m} &= 0. \end{aligned}$$

Secara ekuivalen, $y_{n-m+1}, \ldots, y_n$ ditentukan oleh $y_1, \ldots, y_{n-m}$:

$$\begin{aligned} y_{n-m+1} &= a_{11}y_1 + a_{12}y_2 + \cdots + a_{1,n-m}y_{n-m} \\ y_{n-m+2} &= a_{21}y_1 + a_{22}y_2 + \cdots + a_{2,n-m}y_{n-m} \\ &\vdots \\ y_n &= a_{m1}y_1 + a_{m2}y_2 + \cdots + a_{m,n-m}y_{n-m}. \end{aligned}$$

Akibatnya, kita dapat menetapkan $x_i = y_i$ untuk $i = 1, \ldots, n-m$. ■

Akan sangat membantu apabila kita dapat menghitung jarak minimum suatu kode linear secara langsung dari matriks H-nya untuk menentukan kemampuan kode tersebut dalam mendeteksi dan mengoreksi kesalahan. Misalkan

$$\begin{aligned} \mathbf{e}_1 &= (100\cdots00)^{\mathrm{t}} \\ \mathbf{e}_2 &= (010\cdots00)^{\mathrm{t}} \\ &\vdots \\ \mathbf{e}_n &= (000\cdots01)^{\mathrm{t}} \end{aligned}$$

adalah tupel-n dalam $\mathbb{Z}_2^n$ yang berbobot 1. Untuk matriks biner $m \times n$ H, $H\mathbf{e}_i$ tepat merupakan kolom ke-i dari matriks H.

Contoh 8.3.7 Perhatikan bahwa

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

▲

Hasil ini kita nyatakan dalam proposisi berikut dan pembuktiannya kita serahkan sebagai latihan.

Proposisi 8.3.8 *Misalkan $\mathbf{e}_i$ adalah tupel-n biner yang memiliki 1 pada koordinat ke-i dan 0 di tempat lainnya, dan misalkan $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$. Maka $H\mathbf{e}_i$ merupakan kolom ke-i dari matriks H.*

Teorema 8.3.9 *Misalkan H adalah matriks biner $m \times n$. Maka ruang nol H merupakan kode pendeteksi kesalahan tunggal jika dan hanya jika tidak ada kolom H yang seluruhnya terdiri atas nol.*

Bukti. Misalkan $\mathrm{Null}(H)$ merupakan kode pendeteksi kesalahan tunggal. Maka jarak minimum kode tersebut harus sekurang-kurangnya 2. Karena ruang nol tersebut merupakan kode grup, cukup disyaratkan bahwa kode itu tidak memuat kata kode berbobot kurang dari 2, selain kata kode nol. Artinya, $\mathbf{e}_i$ tidak boleh menjadi kata kode untuk $i = 1, \ldots, n$. Karena $H\mathbf{e}_i$ merupakan kolom ke-i dari H, satu-satunya cara $\mathbf{e}_i$ dapat berada dalam ruang nol H adalah jika kolom ke-i seluruhnya nol, yang mustahil; jadi, kode tersebut setidaknya

harus memiliki kemampuan untuk mendeteksi kesalahan tunggal.

Sebaliknya, misalkan tidak ada kolom H yang merupakan kolom nol. Berdasarkan Proposisi 8.3.8, $H\mathbf{e}_i \neq \mathbf{0}$. ■

Contoh 8.3.10 Jika kita meninjau matriks-matriks

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

dan

$$H_2 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix},$$

maka ruang nol H_1 merupakan kode pendeteksi kesalahan tunggal, sedangkan ruang nol H_2 bukan. ▲

Kita bahkan dapat memperoleh hasil yang lebih kuat daripada Teorema 8.3.9. Teorema ini memberikan syarat-syarat pada suatu matriks H yang menunjukkan kapan bobot minimum kode yang dibentuk oleh ruang nol H adalah 2. Kita juga dapat menentukan kapan jarak minimum suatu kode linear adalah 3 dengan memeriksa matriks yang bersesuaian.

Contoh 8.3.11 Jika kita menetapkan

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

dan ingin menentukan apakah H merupakan matriks pemeriksa paritas kanonik bagi suatu kode pengoreksi kesalahan, kita perlu memastikan bahwa Null(H) tidak memuat tupel-4 berbobot 2. Artinya, (1100), (1010), (1001), (0110), (0101), dan (0011) tidak boleh berada dalam Null(H). Teorema berikut menyatakan bahwa kita memang dapat menentukan bahwa kode yang dibangkitkan oleh H mengoreksi kesalahan dengan memeriksa kolom-kolom H. Perhatikan dalam contoh ini bahwa H bukan hanya tidak memiliki kolom nol, melainkan juga tidak memiliki dua kolom yang sama. ▲

Teorema 8.3.12 *Misalkan H adalah suatu matriks biner. Ruang nol H merupakan kode pengoreksi kesalahan tunggal jika dan hanya jika H tidak memiliki kolom nol dan tidak ada dua kolom H yang identik.*

BUKTI. Tupel-n $\mathbf{e}_i + \mathbf{e}_j$ memiliki 1 pada entri ke-i dan ke-j, serta 0 di tempat lainnya, dan $w(\mathbf{e}_i + \mathbf{e}_j) = 2$ untuk $i \neq j$. Karena

$$\mathbf{0} = H(\mathbf{e}_i + \mathbf{e}_j) = H\mathbf{e}_i + H\mathbf{e}_j$$

hanya dapat terjadi jika kolom ke-i dan ke-j identik, ruang nol H merupakan kode pengoreksi kesalahan tunggal. ■

Sekarang, misalkan kita memiliki matriks pemeriksa paritas kanonik H dengan tiga baris. Kita dapat menanyakan berapa banyak kolom lagi yang dapat ditambahkan ke matriks tersebut sambil tetap memperoleh ruang nol yang merupakan kode pendeteksi dan pengoreksi kesalahan tunggal. Karena setiap kolom memiliki tiga entri, terdapat $2^3 = 8$ kemungkinan kolom yang

berbeda. Kita tidak dapat menambahkan kolom-kolom

$$\begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix}.$$

Jadi, kita dapat menambahkan hingga empat kolom dan tetap mempertahankan jarak minimum 3.

Secara umum, jika H adalah matriks pemeriksa paritas kanonik $m \times n$, maka terdapat $n - m$ posisi informasi dalam setiap kata kode. Setiap kolom memiliki m bit, sehingga terdapat 2^m kemungkinan kolom yang berbeda. Kolom-kolom $\mathbf{0}, \mathbf{e}_1, \ldots, \mathbf{e}_m$ harus dikecualikan, sehingga tersisa $2^m - (1+m)$ kolom bagi informasi jika kita ingin tetap mempertahankan kemampuan bukan hanya untuk mendeteksi, melainkan juga untuk mengoreksi kesalahan tunggal.

8.4 Pendekodean Efisien

Sekarang kita telah sampai pada tahap ketika kita dapat membangkitkan kode linear yang mendeteksi dan mengoreksi kesalahan dengan cukup mudah, tetapi mendekode tupel-n yang diterima dan menentukan kata kode terdekat masih merupakan proses yang memakan waktu, sebab tupel-n yang diterima harus dibandingkan dengan setiap kata kode yang mungkin untuk menentukan pendekodean yang tepat. Hal ini dapat menjadi kendala serius jika kodenya sangat besar.

Contoh 8.4.1 Diberikan matriks biner

$$H = \begin{pmatrix}1 & 1 & 1 & 0 & 0\\ 0 & 1 & 0 & 1 & 0\\ 1 & 0 & 0 & 0 & 1\end{pmatrix}$$

serta tupel-5 $\mathbf{x} = (11011)^{\mathrm{t}}$ dan $\mathbf{y} = (01011)^{\mathrm{t}}$, kita dapat menghitung

$$H\mathbf{x} = \begin{pmatrix}0\\0\\0\end{pmatrix} \qquad \text{dan} \qquad H\mathbf{y} = \begin{pmatrix}1\\0\\1\end{pmatrix}.$$

Jadi, $\mathbf{x}$ merupakan kata kode, sedangkan $\mathbf{y}$ bukan, sebab $\mathbf{x}$ berada dalam ruang nol, sedangkan $\mathbf{y}$ tidak. Perhatikan bahwa $H\mathbf{y}$ identik dengan kolom pertama H. Sesungguhnya, pada posisi inilah kesalahan terjadi. Jika kita membalik bit pertama dalam $\mathbf{y}$ dari 0 menjadi 1, kita memperoleh $\mathbf{x}$. ▲

Jika H merupakan matriks $m \times n$ dan $\mathbf{x} \in \mathbb{Z}_2^n$, maka kita mengatakan bahwa **sindrom** dari $\mathbf{x}$ adalah $H\mathbf{x}$. Proposisi berikut memungkinkan pendeteksian dan pengoreksian kesalahan secara cepat.

Proposisi 8.4.2 *Misalkan matriks biner $m \times n$ H menentukan suatu kode linear dan misalkan $\mathbf{x}$ adalah tupel-n yang diterima. Tuliskan $\mathbf{x}$ sebagai $\mathbf{x} = \mathbf{c} + \mathbf{e}$, dengan $\mathbf{c}$ sebagai kata kode yang ditransmisikan dan $\mathbf{e}$ sebagai kesalahan transmisi. Maka sindrom $H\mathbf{x}$ dari kata kode yang diterima $\mathbf{x}$ juga merupakan sindrom dari kesalahan $\mathbf{e}$.*

Bukti. Pembuktian ini diperoleh dari fakta bahwa

$$H\mathbf{x} = H(\mathbf{c} + \mathbf{e}) = H\mathbf{c} + H\mathbf{e} = \mathbf{0} + H\mathbf{e} = H\mathbf{e}.$$

■

Proposisi ini menunjukkan bahwa sindrom suatu kata yang diterima hanya bergantung pada kesalahannya, bukan pada kata kode yang ditransmisikan. Pembuktian teorema berikut langsung diperoleh dari Proposisi 8.4.2 dan dari fakta bahwa $H\mathbf{e}$ merupakan kolom ke-i dari matriks H.

Teorema 8.4.3 *Misalkan $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$ dan misalkan kode linear yang bersesuaian dengan H mengoreksi kesalahan tunggal. Misalkan $\mathbf{r}$ adalah tupel-n yang diterima setelah ditransmisikan dengan paling banyak satu kesalahan. Jika sindrom $\mathbf{r}$ adalah $\mathbf{0}$, maka tidak terjadi kesalahan; jika tidak, apabila sindrom $\mathbf{r}$ sama dengan suatu kolom H, misalnya kolom ke-i, maka kesalahan terjadi pada bit ke-i.*

Contoh 8.4.4 Tinjau matriks

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

dan misalkan tupel-6 $\mathbf{x} = (111110)^{\mathrm{t}}$, $\mathbf{y} = (111111)^{\mathrm{t}}$, dan $\mathbf{z} = (010111)^{\mathrm{t}}$ telah diterima. Maka

$$H\mathbf{x} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, H\mathbf{y} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, H\mathbf{z} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Jadi, $\mathbf{x}$ memiliki kesalahan pada bit ketiga dan $\mathbf{z}$ memiliki kesalahan pada bit keempat. Kata kode yang ditransmisikan untuk $\mathbf{x}$ dan $\mathbf{z}$ masing-masing pasti adalah (110110) dan (010011). Sindrom $\mathbf{y}$ tidak muncul pada kolom mana pun dari matriks H, sehingga pasti terjadi beberapa kesalahan yang menghasilkan $\mathbf{y}$. ▲

8.4.1 Pendekodean Koset

Kita dapat menggunakan teori grup untuk memperoleh cara lain dalam mendekode pesan. Suatu kode linear C merupakan subgrup dari $\mathbb{Z}_2^n$. **Pendekodean koset** atau **pendekodean standar** menggunakan koset-koset C dalam $\mathbb{Z}_2^n$ untuk menerapkan pendekodean kemungkinan maksimum. Misalkan C adalah kode linear (n, m). Suatu koset C dalam $\mathbb{Z}_2^n$ dituliskan dalam bentuk $\mathbf{x} + C$, dengan $\mathbf{x} \in \mathbb{Z}_2^n$. Berdasarkan Teorema Lagrange (Teorema 6.2.2), terdapat $2^{n-(n-m)} = 2^m$ koset berbeda dari C dalam $\mathbb{Z}_2^n$.

Contoh 8.4.5 Misalkan C adalah kode linear $(5, 3)$ yang diberikan oleh matriks pemeriksa paritas

$$H = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Kode tersebut terdiri atas kata-kata kode

$$(00000) \quad (01101) \quad (10011) \quad (11110).$$

Terdapat $2^{5-2} = 2^3$ koset C dalam $\mathbb{Z}_2^5$, masing-masing berorde $2^2 = 4$. Koset-koset ini tercantum dalam Tabel 8.4.6. ▲

Tabel 8.4.6 Koset-koset C

Koset Wakil	Koset
C	(00000)(01101)(10011)(11110)
$(10000)+C$	(10000)(11101)(00011)(01110)
$(01000)+C$	(01000)(00101)(11011)(10110)
$(00100)+C$	(00100)(01001)(10111)(11010)
$(00010)+C$	(00010)(01111)(10001)(11100)
$(00001)+C$	(00001)(01100)(10010)(11111)
$(10100)+C$	(00111)(01010)(10100)(11001)
$(00110)+C$	(00110)(01011)(10101)(11000)

Tugas kita adalah mencari tahu bagaimana pengetahuan tentang koset dapat membantu kita mendekode suatu pesan. Misalkan $\mathbf{x}$ adalah kata kode asli yang dikirim dan $\mathbf{r}$ adalah tupel-n yang diterima. Jika $\mathbf{e}$ adalah kesalahan transmisi, maka $\mathbf{r}=\mathbf{e}+\mathbf{x}$ atau, secara ekuivalen, $\mathbf{x}=\mathbf{e}+\mathbf{r}$. Namun, ini tepat merupakan pernyataan bahwa $\mathbf{r}$ adalah suatu unsur dalam koset $\mathbf{e}+C$. Dalam pendekodean kemungkinan maksimum, kita mengharapkan kesalahan $\mathbf{e}$ sekecil mungkin; artinya, $\mathbf{e}$ memiliki bobot terkecil. Tupel-n berbobot terkecil dalam suatu koset disebut **pemimpin koset**. Setelah kita menentukan pemimpin koset bagi setiap koset, proses pendekodean menjadi tugas menghitung $\mathbf{r}+\mathbf{e}$ untuk memperoleh $\mathbf{x}$.

Contoh 8.4.7 Dalam Tabel 8.4.6, perhatikan bahwa kita telah memilih wakil dengan bobot sekecil mungkin bagi setiap koset. Wakil-wakil ini merupakan pemimpin koset. Sekarang, misalkan $\mathbf{r}=(01111)$ adalah kata yang diterima. Untuk mendekode $\mathbf{r}$, kita mendapati bahwa kata tersebut berada dalam koset $(00010)+C$; jadi, kata kode yang mula-mula ditransmisikan pasti adalah $(01101)=(01111)+(00010)$. ▲

Potensi masalah dengan metode pendekodean ini adalah bahwa kita mungkin harus memeriksa setiap koset untuk mencari kata kode yang diterima. Proposisi berikut memberikan metode untuk menerapkan pendekodean koset. Proposisi itu menyatakan bahwa kita dapat mengaitkan suatu sindrom dengan setiap koset; jadi, kita dapat membuat tabel yang menetapkan pemimpin koset yang bersesuaian dengan setiap sindrom. Daftar semacam itu disebut **tabel pendekodean**.

Tabel 8.4.8 Sindrom untuk setiap koset

Sindrom	Pemimpin Koset
(000)	(00000)
(001)	(00001)
(010)	(00010)
(011)	(10000)
(100)	(00100)
(101)	(01000)
(110)	(00110)
(111)	(10100)

Proposisi 8.4.9 *Misalkan C adalah kode linear (n,k) yang diberikan oleh matriks H, dan misalkan $\mathbf{x}$ serta $\mathbf{y}$ berada dalam $\mathbb{Z}_2^n$. Maka $\mathbf{x}$ dan $\mathbf{y}$ berada dalam koset C yang sama jika dan hanya jika $H\mathbf{x}=H\mathbf{y}$. Artinya, dua tupel-n berada dalam koset yang sama jika dan hanya jika sindrom keduanya sama.*

BUKTI. Dua tupel-n $\mathbf{x}$ dan $\mathbf{y}$ berada dalam koset C yang sama tepat ketika $\mathbf{x} - \mathbf{y} \in C$; namun, hal ini ekuivalen dengan $H(\mathbf{x} - \mathbf{y}) = 0$ atau $H\mathbf{x} = H\mathbf{y}$. ■

Contoh 8.4.10 Tabel 8.4.8 merupakan tabel pendekodean bagi kode C yang diberikan dalam Contoh 8.4.5. Jika $\mathbf{x} = (01111)$ diterima, maka sindromnya dapat dihitung sebagai

$$H\mathbf{x} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

Dengan memeriksa tabel pendekodean, kita menentukan bahwa pemimpin kosetnya adalah (00010). Sekarang, kata kode yang diterima dapat didekode dengan mudah. ▲

Untuk suatu kode blok (n, k), timbul pertanyaan apakah pendekodean koset merupakan skema yang dapat dikelola. Suatu tabel pendekodean memerlukan daftar koset dan sindrom, masing-masing satu untuk setiap 2^{n-k} koset C. Misalkan kita memiliki kode blok $(32, 24)$. Kita memiliki kata kode dalam jumlah yang sangat besar, yaitu 2^{24}, tetapi hanya terdapat $2^{32-24} = 2^8 = 256$ koset.

8.5 Pertanyaan Bacaan

1. Misalkan suatu kode biner memiliki jarak minimum $d = 6$. Berapa banyak kesalahan yang dapat dideteksi? Berapa banyak kesalahan yang dapat dikoreksi?

2. Jelaskan mengapa untai 8 bit dengan nilai desimal 56_{10} tidak mungkin menjadi kode ASCII untuk suatu karakter. Asumsikan bahwa bit paling kiri dari untai tersebut digunakan sebagai bit pemeriksa paritas.

3. Misalkan kita menerima untai 8 bit dengan nilai desimal 56_{10} ketika kita mengharapkan karakter ASCII dengan bit pemeriksa paritas pada bit pertama (paling kiri). Kita mengetahui bahwa suatu kesalahan telah terjadi dalam transmisi. Berikan salah satu dugaan yang masuk akal tentang karakter yang sebenarnya dikirim (selain '8'), dengan asumsi bahwa kesalahan pada suatu bit tunggal jarang terjadi dalam pengiriman. Jelaskan penalaran yang mendasari jawaban Anda. (Anda mungkin perlu melihat tabel nilai ASCII daring.)

4. Misalkan suatu kode linear C dibentuk sebagai ruang nol dari matriks pemeriksa paritas

$$H = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Maka $x = 11100$ bukan kata kode. Uraikan suatu perhitungan, dan berikan hasil perhitungan tersebut, yang memverifikasi bahwa x bukan kata kode dari kode C.

5. Untuk H dan x seperti dalam pertanyaan sebelumnya, misalkan x diterima sebagai suatu pesan. Berikan pendekodean kemungkinan maksimum untuk pesan yang diterima tersebut.

8.6 Latihan

1. Mengapa skema pengodean berikut tidak dapat diterima?

Informasi	0	1	2	3	4	5	6	7	8
Kata kode	000	001	010	011	101	110	111	000	001

2. Tanpa melakukan penjumlahan apa pun, jelaskan mengapa himpunan tupel-4 berikut dalam $\mathbb{Z}_2^4$ tidak dapat menjadi kode grup.

$$(0110) \quad (1001) \quad (1010) \quad (1100)$$

Petunjuk. Ini tidak dapat menjadi kode grup karena $(0000) \notin C$.

3. Hitung jarak Hamming antara pasangan-pasangan tupel-n berikut.

(a) $(011010), (011100)$

(b) $(11110101), (01010100)$

(c) $(00110), (01111)$

(d) $(1001), (0111)$

Petunjuk. (a) 2; (c) 2.

4. Hitung bobot tupel-tupel-n berikut.

(a) (011010)

(b) (11110101)

(c) (01111)

(d) (1011)

Petunjuk. (a) 3; (c) 4.

5. Misalkan suatu kode linear C memiliki bobot minimum 7. Apa kemampuan C dalam mendeteksi dan mengoreksi kesalahan?

6. Untuk setiap kode berikut, berapakah jarak minimum kode tersebut? Apa hasil terbaik yang dapat kita harapkan sehubungan dengan pendeteksian dan pengoreksian kesalahan?

(a) (011010) (011100) (110111) (110000)

(b) (011100) (011011) (111011) (100011)
(000000) (010101) (110100) (110011)

(c) (000000) (011100) (110101) (110001)

(d) (0110110) (0111100) (1110000) (1111111)
(1001001) (1000011) (0001111) (0000000)

Petunjuk. (a) $d_{\min} = 2$; (c) $d_{\min} = 1$.

7. Hitung ruang nol dari setiap matriks berikut. Ruang-ruang nol tersebut merupakan kode blok (n, k) jenis apa? Dapatkah Anda menemukan suatu matriks (tidak harus berupa matriks pembangkit standar) yang membangkitkan setiap kode? Apakah matriks-matriks pembangkit Anda unik?

(a)
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

(c)
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(d)
$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Petunjuk.

(a) $(00000), (00101), (10011), (10110)$

$$G = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$$

(b) $(000000), (010111), (101101), (111010)$

$$G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$$

8. Konstruksikan suatu kode blok $(5, 2)$. Bahas kemampuan kode Anda dalam mendeteksi maupun mengoreksi kesalahan.

9. Misalkan C adalah kode yang diperoleh dari ruang nol matriks

$$H = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Dekodekan pesan

$$01111 \quad 10101 \quad 01110 \quad 00011$$

jika memungkinkan.

Petunjuk. Beberapa kesalahan terjadi dalam salah satu kata yang diterima.

10. Misalkan suatu pesan biner sepanjang 1000 bit ditransmisikan. Asumsikan bahwa probabilitas kesalahan pada satu bit adalah p dan bahwa kesalahan yang terjadi pada bit-bit berbeda saling bebas. Jika $p = 0.01$, berapakah probabilitas terjadinya lebih dari satu kesalahan? Berapakah probabilitas terjadinya tepat dua kesalahan? Ulangi soal ini untuk $p = 0.0001$.

11. Matriks manakah yang merupakan matriks pemeriksa paritas kanonik? Untuk matriks-matriks yang merupakan matriks pemeriksa paritas kanonik, apa matriks pembangkit standar yang bersesuaian? Apa kemampuan kode yang dihasilkan oleh setiap matriks tersebut dalam mendeteksi dan mengoreksi kesalahan?

(a)
$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(c)
$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

(d)
$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Petunjuk. (a) Matriks pemeriksa paritas kanonik dengan matriks pembangkit standar
$$G = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

(c) Matriks pemeriksa paritas kanonik dengan matriks pembangkit standar
$$G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

12. Cantumkan semua sindrom yang mungkin bagi kode-kode yang dihasilkan oleh setiap matriks dalam Latihan 8.6.11.

Petunjuk. (a) Semua sindrom yang mungkin muncul.

13. Misalkan
$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Hitung sindrom yang disebabkan oleh setiap kesalahan transmisi berikut.

(a) Kesalahan pada bit pertama.

(b) Kesalahan pada bit ketiga.

(c) Kesalahan pada bit terakhir.

(d) Kesalahan pada bit ketiga dan keempat.

14. Misalkan C adalah kode grup dalam $\mathbb{Z}_2^3$ yang didefinisikan oleh kata-kata kode (000) dan (111). Hitung koset-koset C dalam $\mathbb{Z}_2^3$. Mengapa koset kanan atau kiri tidak perlu ditentukan? Berikan kesalahan transmisi tunggal, jika ada, yang bersesuaian dengan setiap koset.

15. Untuk setiap matriks berikut, carilah koset-koset dari kode C yang bersesuaian. Berikan tabel pendekodean bagi setiap kode jika memungkinkan.

(a)
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(c)
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(d)
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Petunjuk. (a) C, $(10000) + C$, $(01000) + C$, $(00100) + C$, $(00010) + C$, $(11000) + C$, $(01100) + C$, $(01010) + C$. Tabel pendekodean tidak ada untuk C karena kode ini hanya mendeteksi kesalahan tunggal.

16. Misalkan $\mathbf{x}$, $\mathbf{y}$, dan $\mathbf{z}$ adalah tupel-n biner. Buktikan setiap pernyataan berikut.

(a) $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$

(b) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x} + \mathbf{z}, \mathbf{y} + \mathbf{z})$

(c) $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$

17. Suatu **metrik** pada himpunan X adalah pemetaan $d : X \times X \to \mathbb{R}$ yang memenuhi syarat-syarat berikut.

(a) $d(\mathbf{x}, \mathbf{y}) \geq 0$ untuk semua $\mathbf{x}, \mathbf{y} \in X$;

(b) $d(\mathbf{x}, \mathbf{y}) = 0$ tepat ketika $\mathbf{x} = \mathbf{y}$;

(c) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$;

(d) $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$.

Dengan kata lain, metrik hanyalah suatu perumuman dari gagasan jarak. Buktikan bahwa jarak Hamming merupakan metrik pada $\mathbb{Z}_2^n$. Mendekode suatu pesan sesungguhnya dapat direduksi menjadi penentuan kata kode yang terdekat dalam hal jarak.

18. Misalkan C adalah suatu kode linear. Tunjukkan bahwa semua koordinat ke-i dalam kata-kata kode C bernilai nol, atau tepat separuh di antaranya bernilai nol.

19. Misalkan C adalah suatu kode linear. Tunjukkan bahwa setiap kata kode berbobot genap, atau tepat separuh kata kode berbobot genap.

Petunjuk. Misalkan $\mathbf{x} \in C$ berbobot ganjil dan definisikan suatu pemetaan dari himpunan kata kode berbobot ganjil ke himpunan kata kode berbobot genap dengan $\mathbf{y} \mapsto \mathbf{x} + \mathbf{y}$. Tunjukkan bahwa pemetaan ini merupakan bijeksi.

20. Tunjukkan bahwa kata-kata kode berbobot genap dalam suatu kode linear C juga membentuk kode linear.

21. Jika kita hendak menggunakan kode linear pengoreksi kesalahan untuk mentransmisikan 128 karakter ASCII, matriks berukuran berapa yang harus digunakan? Matriks berukuran berapa yang harus digunakan untuk mentransmisikan himpunan karakter ASCII perluasan yang terdiri atas

256 karakter? Bagaimana jika dalam kedua kasus kita hanya memerlukan pendeteksian kesalahan?

22. Carilah matriks pemeriksa paritas kanonik yang menghasilkan kode bit pemeriksa paritas genap dengan tiga posisi informasi. Bagaimanakah matriksnya untuk tujuh posisi informasi? Apa matriks pembangkit standar yang bersesuaian?

23. Berapa banyak posisi pemeriksa yang diperlukan bagi kode pengoreksi kesalahan tunggal dengan 20 posisi informasi? Bagaimana dengan 32 posisi informasi?

Petunjuk. Untuk 20 posisi informasi, diperlukan sekurang-kurangnya 6 bit pemeriksa untuk menjamin diperolehnya kode pengoreksi kesalahan.

24. Misalkan $\mathbf{e}_i$ adalah tupel-n biner yang memiliki 1 pada koordinat ke-i dan 0 di tempat lainnya, dan misalkan $H \in \mathbb{M}_{m\times n}(\mathbb{Z}_2)$. Tunjukkan bahwa $H\mathbf{e}_i$ merupakan kolom ke-i dari matriks H.

25. Misalkan C adalah suatu kode linear (n, k). Definisikan **kode dual** atau **kode ortogonal** dari C sebagai

$$C^{\perp} = \{\mathbf{x} \in \mathbb{Z}_2^n : \mathbf{x} \cdot \mathbf{y} = 0 \text{ untuk semua } \mathbf{y} \in C\}.$$

(a) Carilah kode dual dari kode linear C, dengan C diberikan oleh matriks

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

(b) Tunjukkan bahwa $C^{\perp}$ merupakan kode linear $(n, n-k)$.

(c) Carilah matriks pembangkit standar dan matriks pemeriksa paritas dari C dan $C^{\perp}$. Apa yang terjadi secara umum? Buktikan konjektur Anda.

26. Misalkan H adalah matriks $m \times n$ atas $\mathbb{Z}_2$, dengan kolom ke-i berupa bilangan i yang ditulis dalam bentuk biner dengan m bit. Ruang nol dari matriks semacam itu disebut **kode Hamming**.

(a) Tunjukkan bahwa matriks

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

menghasilkan suatu kode Hamming. Apa sifat pengoreksi kesalahan dari kode Hamming?

(b) Kolom yang bersesuaian dengan sindrom juga menunjukkan bit yang salah; artinya, kolom ke-i dari matriks merupakan i yang ditulis sebagai bilangan biner, dan sindrom langsung menunjukkan bit mana yang salah. Jika kata yang diterima adalah (101011), hitung sindromnya. Pada bit manakah kesalahan terjadi dalam kasus ini, dan kata kode apa yang mula-mula ditransmisikan?

(c) Berikan matriks biner H bagi kode Hamming dengan enam posisi informasi dan empat posisi pemeriksa. Manakah posisi pemeriksa dan manakah posisi informasi? Kodekan pesan (101101) dan (001001). Dekodekan kata yang diterima (0010000101) dan (0000101100). Apa saja sindrom yang mungkin bagi kode ini?

(d) Berapakah banyaknya bit pemeriksa dan bit informasi dalam kode Hamming blok (m, n)? Berikan batas atas maupun batas bawah bagi banyaknya bit informasi dalam hubungannya dengan banyaknya bit pemeriksa. Kode Hamming yang memiliki sebanyak mungkin bit informasi dengan k bit pemeriksa disebut **sempurna**. Setiap sindrom yang mungkin selain **0** muncul sebagai suatu kolom. Jika banyaknya bit informasi kurang dari maksimum, maka kode tersebut disebut **dipendekkan**. Dalam kasus ini, berikan contoh yang menunjukkan bahwa beberapa sindrom dapat merepresentasikan lebih dari satu kesalahan.

8.7 Latihan Pemrograman

1. Tulislah program untuk mengimplementasikan kode linear $(16, 12)$. Program Anda harus dapat mengodekan dan mendekode pesan menggunakan pendekodean koset. Setelah program tersebut selesai ditulis, tulislah program untuk menyimulasikan saluran simetris biner dengan derau transmisi. Bandingkan hasil simulasi Anda dengan probabilitas kesalahan yang diprediksi secara teoretis.

8.8 Referensi dan Bacaan yang Disarankan

[**1**] Blake, I. F. "Codes and Designs," *Mathematics Magazine* 52 (1979), 81–95.

[**2**] Hill, R. *A First Course in Coding Theory.* Oxford University Press, Oxford, 1990.

[**3**] Levinson, N. "Coding Theory: A Counterexample to G. H. Hardy's Conception of Applied Mathematics," *American Mathematical Monthly* 77 (1970), 249–58.

[**4**] Lidl, R. and Pilz, G. *Applied Abstract Algebra.* 2nd ed. Springer, New York, 1998.

[**5**] MacWilliams, F. J. and Sloane, N. J. A. *The Theory of Error-Correcting Codes.* North-Holland Mathematical Library, 16, Elsevier, Amsterdam, 1983.

[**6**] Roman, S. *Coding and Information Theory.* Springer-Verlag, New York, 1992.

[**7**] Shannon, C. E. "A Mathematical Theory of Communication," *Bell System Technical Journal* 27 (1948), 379–423, 623–56.

[**8**] Thompson, T. M. *From Error-Correcting Codes through Sphere Packing to Simple Groups.* Carus Monograph Series, No. 21. Mathematical Association of America, Washington, DC, 1983.

[**9**] van Lint, J. H. *Introduction to Coding Theory.* Springer, New York, 1999.

9

Isomorfisma

Banyak grup mungkin tampak berbeda pada pandangan pertama, tetapi dapat ditunjukkan sama hanya dengan mengganti nama elemen-elemen grup tersebut. Sebagai contoh, $\mathbb{Z}_4$ dan subgrup dari grup lingkaran $\mathbb{T}$ yang dibangkitkan oleh i dapat ditunjukkan sama dengan memperlihatkan korespondensi satu-satu antara elemen-elemen kedua grup dan antara operasi-operasi grupnya. Dalam kasus seperti ini, kita mengatakan bahwa kedua grup tersebut isomorfik.

9.1 Definisi dan Contoh

Dua grup $(G, \cdot)$ dan $(H, \circ)$ disebut **isomorfik** jika terdapat pemetaan injektif dan surjektif $\phi : G \to H$ yang mempertahankan operasi grup; yaitu,

$$\phi(a \cdot b) = \phi(a) \circ \phi(b)$$

untuk semua a dan b di G. Jika G isomorfik dengan H, kita tuliskan $G \cong H$. Pemetaan ϕ disebut **isomorfisma**.

Contoh 9.1.1 Untuk menunjukkan bahwa $\mathbb{Z}_4 \cong \langle i \rangle$, definisikan pemetaan $\phi : \mathbb{Z}_4 \to \langle i \rangle$ dengan $\phi(n) = i^n$. Kita harus menunjukkan bahwa ϕ bijektif dan mempertahankan operasi grup. Pemetaan ϕ injektif dan surjektif karena

$$\begin{aligned} \phi(0) &= 1 \\ \phi(1) &= i \\ \phi(2) &= -1 \\ \phi(3) &= -i. \end{aligned}$$

Karena

$$\phi(m+n) = i^{m+n} = i^m i^n = \phi(m)\phi(n),$$

operasi grup dipertahankan. ▲

Contoh 9.1.2 Kita dapat mendefinisikan isomorfisma ϕ dari grup aditif bilangan real $(\mathbb{R}, +)$ ke grup multiplikatif bilangan real positif $(\mathbb{R}^+, \cdot)$ dengan pemetaan eksponensial; yaitu,

$$\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y).$$

Tentu saja, kita masih harus menunjukkan bahwa ϕ injektif dan surjektif, tetapi hal ini dapat ditentukan menggunakan kalkulus. ▲

Contoh 9.1.3 Bilangan bulat isomorfik dengan subgrup dari $\mathbb{Q}^*$ yang terdiri atas elemen berbentuk 2^n. Definisikan pemetaan $\phi : \mathbb{Z} \to \mathbb{Q}^*$ dengan $\phi(n) = 2^n$. Maka

$$\phi(m+n) = 2^{m+n} = 2^m 2^n = \phi(m)\phi(n).$$

Berdasarkan definisi, pemetaan ϕ bersifat surjektif ke himpunan bagian $\{2^n : n \in \mathbb{Z}\}$ dari $\mathbb{Q}^*$. Untuk menunjukkan bahwa pemetaan tersebut injektif, andaikan $m \neq n$. Jika kita dapat menunjukkan bahwa $\phi(m) \neq \phi(n)$, selesailah pembuktian. Misalkan $m > n$ dan andaikan $\phi(m) = \phi(n)$. Maka $2^m = 2^n$ atau $2^{m-n} = 1$, yang mustahil karena $m - n > 0$. ▲

Contoh 9.1.4 Grup $\mathbb{Z}_8$ dan $\mathbb{Z}_{12}$ tidak mungkin isomorfik karena memiliki orde yang berbeda; namun, memang benar bahwa $U(8) \cong U(12)$. Kita mengetahui bahwa

$$U(8) = \{1, 3, 5, 7\}$$
$$U(12) = \{1, 5, 7, 11\}.$$

Isomorfisma $\phi : U(8) \to U(12)$ kemudian diberikan oleh

$$1 \mapsto 1$$
$$3 \mapsto 5$$
$$5 \mapsto 7$$
$$7 \mapsto 11.$$

Pemetaan ϕ bukan satu-satunya isomorfisma yang mungkin antara kedua grup ini. Kita dapat mendefinisikan isomorfisma lain ψ dengan $\psi(1) = 1$, $\psi(3) = 11$, $\psi(5) = 5$, $\psi(7) = 7$. Bahkan, kedua grup ini isomorfik dengan $\mathbb{Z}_2 \times \mathbb{Z}_2$ (lihat Contoh 3.3.5 dalam Bab 3). ▲

Contoh 9.1.5 Meskipun S_3 dan $\mathbb{Z}_6$ memiliki jumlah elemen yang sama, kita menduga bahwa keduanya tidak isomorfik, karena $\mathbb{Z}_6$ abelian sedangkan S_3 nonabelian. Untuk menunjukkan bahwa memang demikian, andaikan $\phi : \mathbb{Z}_6 \to S_3$ adalah suatu isomorfisma. Misalkan $a, b \in S_3$ merupakan dua elemen sedemikian sehingga $ab \neq ba$. Karena ϕ adalah isomorfisma, terdapat elemen m dan n di $\mathbb{Z}_6$ sedemikian sehingga

$$\phi(m) = a \quad \text{dan} \quad \phi(n) = b.$$

Namun,

$$ab = \phi(m)\phi(n) = \phi(m+n) = \phi(n+m) = \phi(n)\phi(m) = ba,$$

yang bertentangan dengan fakta bahwa a dan b tidak komutatif. ▲

Teorema 9.1.6 *Misalkan $\phi : G \to H$ merupakan isomorfisma antara dua grup. Maka pernyataan-pernyataan berikut benar.*

1. *$\phi^{-1} : H \to G$ adalah suatu isomorfisma.*
2. *$|G| = |H|$.*
3. *Jika G abelian, maka H abelian.*
4. *Jika G siklik, maka H siklik.*
5. *Jika G memiliki subgrup berorde n, maka H memiliki subgrup berorde n.*

BUKTI. Pernyataan (1) dan (2) mengikuti fakta bahwa ϕ merupakan suatu bijeksi. Di sini kita akan membuktikan (3) dan menyerahkan pembuktian bagian teorema lainnya sebagai latihan.

(3) Misalkan h_1 dan h_2 merupakan elemen-elemen H. Karena ϕ surjektif, terdapat elemen $g_1, g_2 \in G$ sedemikian sehingga $\phi(g_1) = h_1$ dan $\phi(g_2) = h_2$. Oleh karena itu,

$$h_1h_2 = \phi(g_1)\phi(g_2) = \phi(g_1g_2) = \phi(g_2g_1) = \phi(g_2)\phi(g_1) = h_2h_1.$$

■

Sekarang kita dapat mengarakterisasi semua grup siklik.

Teorema 9.1.7 *Semua grup siklik berorde tak hingga isomorfik dengan $\mathbb{Z}$.*

BUKTI. Misalkan G grup siklik berorde tak hingga dan andaikan a adalah pembangkit G. Definisikan pemetaan $\phi : \mathbb{Z} \to G$ dengan $\phi : n \mapsto a^n$. Maka

$$\phi(m + n) = a^{m+n} = a^m a^n = \phi(m)\phi(n).$$

Untuk menunjukkan bahwa ϕ injektif, misalkan m dan n merupakan dua elemen dalam $\mathbb{Z}$, dengan $m \neq n$. Kita dapat mengandaikan bahwa $m > n$. Kita harus menunjukkan bahwa $a^m \neq a^n$. Andaikan sebaliknya; yaitu, $a^m = a^n$. Dalam hal ini $a^{m-n} = e$, dengan $m - n > 0$, yang bertentangan dengan fakta bahwa a memiliki orde tak hingga. Pemetaan kita surjektif karena setiap elemen dalam G dapat ditulis sebagai a^n untuk suatu bilangan bulat n dan $\phi(n) = a^n$. ■

Teorema 9.1.8 *Jika G adalah grup siklik berorde n, maka G isomorfik dengan $\mathbb{Z}_n$.*

BUKTI. Misalkan G grup siklik berorde n yang dibangkitkan oleh a, dan definisikan pemetaan $\phi : \mathbb{Z}_n \to G$ dengan $\phi : k \mapsto a^k$, dengan $0 \leq k < n$. Pembuktian bahwa ϕ merupakan isomorfisma menjadi salah satu latihan akhir bab. ■

Korolari 9.1.9 *Jika G adalah grup berorde p, dengan p suatu bilangan prima, maka G isomorfik dengan $\mathbb{Z}_p$.*

BUKTI. Pembuktian ini merupakan akibat langsung dari Korolari 6.2.4. ■

Tujuan utama dalam teori grup adalah mengklasifikasikan semua grup; namun, wajar untuk menganggap dua grup sama jika keduanya isomorfik. Kita nyatakan hasil ini dalam teorema berikut, yang pembuktiannya diserahkan sebagai latihan.

Teorema 9.1.10 *Keisomorfikan grup menentukan suatu relasi ekuivalensi pada kelas semua grup.*

Dengan demikian, kita dapat mengubah tujuan kita dari mengklasifikasikan semua grup menjadi mengklasifikasikan semua grup **hingga isomorfisma**; yaitu, kita akan menganggap dua grup sama jika keduanya isomorfik.

9.1.1 Teorema Cayley

Cayley membuktikan bahwa jika G adalah suatu grup, maka grup tersebut isomorfik dengan grup permutasi pada suatu himpunan; dengan demikian, setiap grup merupakan grup permutasi. Teorema Cayley adalah apa yang disebut teorema representasi. Tujuan teori representasi adalah menemukan isomorfisma dari suatu grup G yang ingin kita pelajari ke grup yang telah banyak kita ketahui, seperti grup permutasi atau matriks.

Contoh 9.1.11 Tinjau grup $\mathbb{Z}_3$. Tabel Cayley untuk $\mathbb{Z}_3$ adalah sebagai berikut.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabel penjumlahan $\mathbb{Z}_3$ menunjukkan bahwa grup ini sama dengan grup permutasi $G = \{(0), (012), (021)\}$. Isomorfisma dalam hal ini adalah

$$0 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} = (0)$$
$$1 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} = (0\,1\,2)$$
$$2 \mapsto \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} = (0\,2\,1).$$

▲

Teorema 9.1.12 Cayley. *Setiap grup isomorfik dengan suatu grup permutasi.*

Bukti. Misalkan G suatu grup. Kita harus menemukan suatu grup permutasi $\overline{G}$ yang isomorfik dengan G. Untuk setiap $g \in G$, definisikan fungsi $\lambda_g : G \to G$ dengan $\lambda_g(a) = ga$. Kita menyatakan bahwa λ_g adalah permutasi dari G. Untuk menunjukkan bahwa λ_g injektif, andaikan $\lambda_g(a) = \lambda_g(b)$. Maka

$$ga = \lambda_g(a) = \lambda_g(b) = gb.$$

Dengan demikian, $a = b$. Untuk menunjukkan bahwa λ_g surjektif, kita harus membuktikan bahwa untuk setiap $a \in G$, terdapat b sedemikian sehingga $\lambda_g(b) = a$. Ambil $b = g^{-1}a$.

Sekarang kita siap mendefinisikan grup $\overline{G}$. Misalkan

$$\overline{G} = \{\lambda_g : g \in G\}.$$

Kita harus menunjukkan bahwa $\overline{G}$ merupakan grup terhadap komposisi fungsi dan menemukan isomorfisma antara G dan $\overline{G}$. Kita memperoleh ketertutupan terhadap komposisi fungsi karena

$$(\lambda_g \circ \lambda_h)(a) = \lambda_g(ha) = gha = \lambda_{gh}(a).$$

Selain itu,

$$\lambda_e(a) = ea = a$$

dan

$$(\lambda_{g^{-1}} \circ \lambda_g)(a) = \lambda_{g^{-1}}(ga) = g^{-1}ga = a = \lambda_e(a).$$

Kita dapat mendefinisikan isomorfisma dari G ke $\overline{G}$ dengan $\phi : g \mapsto \lambda_g$. Operasi grup dipertahankan karena

$$\phi(gh) = \lambda_{gh} = \lambda_g\lambda_h = \phi(g)\phi(h).$$

Pemetaan ini juga injektif, karena jika $\phi(g)(a) = \phi(h)(a)$, maka

$$ga = \lambda_g a = \lambda_h a = ha.$$

Dengan demikian, $g = h$. Sifat surjektif ϕ mengikuti fakta bahwa $\phi(g) = \lambda_g$ untuk setiap $\lambda_g \in \overline{G}$. ■

Isomorfisma $g \mapsto \lambda_g$ dikenal sebagai **representasi reguler kiri** dari G.

Catatan Sejarah

Arthur Cayley lahir di Inggris pada tahun 1821, meskipun ia menghabiskan sebagian besar masa awal hidupnya di Rusia, tempat ayahnya bekerja sebagai pedagang. Cayley menempuh pendidikan di Cambridge, tempat ia meraih Smith's Prize pertama dalam matematika. Sepanjang sebagian besar masa dewasanya ia bekerja sebagai pengacara; pada awal usia dua puluhan, ia menulis beberapa makalah sebelum memasuki profesi hukum pada usia 25 tahun. Sembari berpraktik sebagai pengacara, ia melanjutkan penelitian matematikanya, dengan menulis lebih dari 300 makalah selama periode tersebut. Di antaranya terdapat beberapa karya terbaiknya. Pada tahun 1863, ia meninggalkan bidang hukum untuk menjadi profesor di Cambridge. Cayley menulis lebih dari 900 makalah dalam bidang-bidang seperti teori grup, geometri, dan aljabar linear. Pengetahuan hukumnya sangat berharga bagi Cambridge; ia turut serta menyusun banyak statuta universitas tersebut. Cayley juga merupakan salah seorang yang berjasa dalam penerimaan perempuan di Cambridge.

9.2 Hasil Kali Langsung

Jika diberikan dua grup G dan H, kita dapat membentuk grup baru dari hasil kali Kartesius G dan H, $G \times H$. Sebaliknya, jika diberikan suatu grup besar, terkadang grup tersebut dapat diuraikan; yaitu, suatu grup terkadang isomorfik dengan hasil kali langsung dua grup yang lebih kecil. Alih-alih mempelajari suatu grup besar G, sering kali lebih mudah mempelajari grup-grup komponen dari G.

9.2.1 Hasil Kali Langsung Eksternal

Jika $(G, \cdot)$ dan $(H, \circ)$ adalah grup, maka kita dapat menjadikan hasil kali Kartesius G dan H sebagai grup baru. Sebagai himpunan, grup kita hanyalah pasangan-pasangan terurut $(g, h) \in G \times H$ dengan $g \in G$ dan $h \in H$. Kita dapat mendefinisikan operasi biner pada $G \times H$ dengan

$$(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2);$$

yaitu, kita mengalikan elemen-elemen pada koordinat pertama seperti dalam G dan elemen-elemen pada koordinat kedua seperti dalam H. Demi kejelasan, di sini kita telah mencantumkan operasi khusus $\cdot$ dan $\circ$ pada masing-masing grup; biasanya kita cukup menuliskan $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$.

Proposisi 9.2.1 *Misalkan G dan H adalah grup. Himpunan $G \times H$ merupakan grup terhadap operasi $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ dengan $g_1, g_2 \in G$ dan $h_1, h_2 \in H$.*

Bukti. Jelas bahwa operasi biner yang didefinisikan di atas bersifat tertutup. Jika e_G dan e_H berturut-turut merupakan identitas grup G dan H, maka (e_G, e_H) adalah identitas dari $G \times H$. Invers dari $(g, h) \in G \times H$ adalah (g^{-1}, h^{-1}). Sifat asosiatif operasi tersebut mengikuti langsung dari sifat asosiatif G dan H. ■

Contoh 9.2.2 Misalkan $\mathbb{R}$ adalah grup bilangan real terhadap penjumlahan. Hasil kali Kartesius $\mathbb{R}$ dengan dirinya sendiri, $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, juga merupakan grup, dengan operasi grup berupa penjumlahan pada setiap koordinat; yaitu, $(a, b) + (c, d) = (a + c, b + d)$. Identitasnya adalah $(0, 0)$ dan invers dari (a, b) adalah $(-a, -b)$. ▲

Contoh 9.2.3 Tinjau

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}.$$

Meskipun $\mathbb{Z}_2 \times \mathbb{Z}_2$ dan $\mathbb{Z}_4$ sama-sama memuat empat elemen, keduanya tidak isomorfik. Setiap elemen (a,b) dalam $\mathbb{Z}_2 \times \mathbb{Z}_2$ selain identitas berorde 2, karena $(a,b)+(a,b)=(0,0)$; namun, $\mathbb{Z}_4$ bersifat siklik. ▲

Grup $G \times H$ disebut **hasil kali langsung eksternal** dari G dan H. Perhatikan bahwa penggunaan hanya dua grup untuk membentuk grup baru tidaklah bersifat khusus. Hasil kali langsung

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n$$

dari grup-grup $G_1, G_2, \ldots, G_n$ didefinisikan dengan cara yang persis sama. Jika $G = G_1 = G_2 = \cdots = G_n$, kita sering menuliskan G^n sebagai pengganti $G_1 \times G_2 \times \cdots \times G_n$.

Contoh 9.2.4 Grup $\mathbb{Z}_2^n$, jika dipandang sebagai himpunan, hanyalah himpunan semua tupel-n biner. Operasi grupnya adalah "atau eksklusif" dari dua tupel-n biner. Sebagai contoh,

$$(01011101) + (01001011) = (00010110).$$

Grup ini penting dalam teori pengodean, kriptografi, dan banyak bidang ilmu komputer. ▲

Teorema 9.2.5 *Misalkan $(g,h) \in G \times H$. Jika g dan h berturut-turut memiliki orde hingga r dan s, maka orde (g,h) dalam $G \times H$ adalah kelipatan persekutuan terkecil dari r dan s.*

Bukti. Misalkan m adalah kelipatan persekutuan terkecil dari r dan s, dan misalkan $n = |(g,h)|$. Maka

$$(g,h)^m = (g^m, h^m) = (e_G, e_H)$$
$$(g^n, h^n) = (g,h)^n = (e_G, e_H).$$

Dengan demikian, n harus membagi m, dan $n \leq m$. Namun, berdasarkan persamaan kedua, r dan s keduanya harus membagi n; oleh karena itu, n merupakan kelipatan persekutuan dari r dan s. Karena m adalah *kelipatan persekutuan terkecil* dari r dan s, $m \leq n$. Akibatnya, m harus sama dengan n. ■

Korolari 9.2.6 *Misalkan $(g_1, \ldots, g_n) \in \prod G_i$. Jika g_i memiliki orde hingga r_i dalam G_i, maka orde $(g_1, \ldots, g_n)$ dalam $\prod G_i$ adalah kelipatan persekutuan terkecil dari $r_1, \ldots, r_n$.*

Contoh 9.2.7 Misalkan $(8,56) \in \mathbb{Z}_{12} \times \mathbb{Z}_{60}$. Karena $\gcd(8,12) = 4$, orde 8 adalah $12/4 = 3$ dalam $\mathbb{Z}_{12}$. Demikian pula, orde 56 dalam $\mathbb{Z}_{60}$ adalah 15. Kelipatan persekutuan terkecil dari 3 dan 15 adalah 15; dengan demikian, $(8,56)$ berorde 15 dalam $\mathbb{Z}_{12} \times \mathbb{Z}_{60}$. ▲

Contoh 9.2.8 Grup $\mathbb{Z}_2 \times \mathbb{Z}_3$ terdiri atas pasangan-pasangan

$$(0,0), \quad (0,1), \quad (0,2), \quad (1,0), \quad (1,1), \quad (1,2).$$

Dalam kasus ini, tidak seperti pada $\mathbb{Z}_2 \times \mathbb{Z}_2$ dan $\mathbb{Z}_4$, berlaku bahwa $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. Kita hanya perlu menunjukkan bahwa $\mathbb{Z}_2 \times \mathbb{Z}_3$ bersifat siklik. Mudah dilihat bahwa $(1,1)$ merupakan pembangkit dari $\mathbb{Z}_2 \times \mathbb{Z}_3$. ▲

Teorema berikut menjelaskan secara tepat kapan hasil kali langsung dua grup siklik bersifat siklik.

Teorema 9.2.9 *Grup $\mathbb{Z}_m \times \mathbb{Z}_n$ isomorfik dengan $\mathbb{Z}_{mn}$ jika dan hanya jika* $\gcd(m,n) = 1$.

BUKTI. Pertama-tama kita akan menunjukkan bahwa jika $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$, maka $\gcd(m,n) = 1$. Kita akan membuktikan kontraposisinya; yaitu, kita akan menunjukkan bahwa jika $\gcd(m,n) = d > 1$, maka $\mathbb{Z}_m \times \mathbb{Z}_n$ tidak mungkin siklik. Perhatikan bahwa mn/d habis dibagi oleh m maupun n; dengan demikian, untuk setiap elemen $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$,

$$\underbrace{(a,b) + (a,b) + \cdots + (a,b)}_{mn/d \text{ kali}} = (0,0).$$

Oleh karena itu, tidak ada (a,b) yang dapat membangkitkan seluruh $\mathbb{Z}_m \times \mathbb{Z}_n$.

Kebalikannya mengikuti langsung dari Teorema 9.2.5 karena $\operatorname{lcm}(m,n) = mn$ jika dan hanya jika $\gcd(m,n) = 1$. ■

Korolari 9.2.10 *Misalkan $n_1, \ldots, n_k$ adalah bilangan bulat positif. Maka*

$$\prod_{i=1}^{k} \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 \cdots n_k}$$

jika dan hanya jika $\gcd(n_i, n_j) = 1$ *untuk* $i \neq j$.

Korolari 9.2.11 *Jika*

$$m = p_1^{e_1} \cdots p_k^{e_k},$$

dengan p_i merupakan bilangan-bilangan prima yang berbeda, maka

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}.$$

BUKTI. Karena faktor persekutuan terbesar dari $p_i^{e_i}$ dan $p_j^{e_j}$ adalah 1 untuk $i \neq j$, pembuktiannya mengikuti Korolari 9.2.10. ■

Dalam Bab 13, kita akan membuktikan bahwa semua grup abelian hingga isomorfik dengan hasil kali langsung berbentuk

$$\mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$$

dengan $p_1, \ldots, p_k$ merupakan bilangan-bilangan prima (yang tidak harus berbeda).

9.2.2 Hasil Kali Langsung Internal

Hasil kali langsung eksternal dua grup membentuk suatu grup besar dari dua grup yang lebih kecil. Kita ingin dapat membalik proses ini dan menguraikan suatu grup menjadi komponen-komponen hasil kali langsungnya dengan mudah; yaitu, kita ingin dapat menentukan kapan suatu grup isomorfik dengan hasil kali langsung dua subgrupnya.

Misalkan G suatu grup dengan subgrup H dan K yang memenuhi syarat-syarat berikut.

- $G = HK = \{hk : h \in H, k \in K\}$;
- $H \cap K = \{e\}$;
- $hk = kh$ untuk semua $k \in K$ dan $h \in H$.

Maka G merupakan **hasil kali langsung internal** dari H dan K.

Contoh 9.2.12 Grup $U(8)$ merupakan hasil kali langsung internal dari

$$H = \{1, 3\} \quad \text{dan} \quad K = \{1, 5\}.$$

▲

Contoh 9.2.13 Grup dihedral D_6 merupakan hasil kali langsung internal dari dua subgrupnya

$$H = \{\mathrm{id}, r^3\} \quad \text{dan} \quad K = \{\mathrm{id}, r^2, r^4, s, r^2s, r^4s\}.$$

Dapat ditunjukkan dengan mudah bahwa $K \cong S_3$; akibatnya, $D_6 \cong \mathbb{Z}_2 \times S_3$.
▲

Contoh 9.2.14 Tidak setiap grup dapat ditulis sebagai hasil kali langsung internal dari dua subgrup sejatinya. Jika grup S_3 merupakan hasil kali langsung internal dari subgrup-subgrup sejatinya H dan K, maka salah satu subgrup, katakanlah H, harus berorde 3. Dalam hal ini H adalah subgrup $\{(1), (123), (132)\}$. Subgrup K harus berorde 2, tetapi subgrup mana pun yang kita pilih sebagai K, syarat $hk = kh$ tidak akan pernah terpenuhi untuk $h \in H$ dan $k \in K$. ▲

Teorema 9.2.15 *Misalkan G merupakan hasil kali langsung internal dari subgrup H dan K. Maka G isomorfik dengan $H \times K$.*

Bukti. Karena G merupakan hasil kali langsung internal, kita dapat menulis setiap elemen $g \in G$ sebagai $g = hk$ untuk suatu $h \in H$ dan suatu $k \in K$. Definisikan pemetaan $\phi : G \to H \times K$ dengan $\phi(g) = (h, k)$.

Masalah pertama yang harus kita hadapi adalah menunjukkan bahwa ϕ merupakan pemetaan yang terdefinisi dengan baik; yaitu, kita harus menunjukkan bahwa h dan k ditentukan secara tunggal oleh g. Andaikan $g = hk = h'k'$. Maka $h^{-1}h' = k(k')^{-1}$ berada dalam H maupun K, sehingga elemen tersebut harus merupakan identitas. Oleh karena itu, $h = h'$ dan $k = k'$, yang membuktikan bahwa ϕ memang terdefinisi dengan baik.

Untuk menunjukkan bahwa ϕ mempertahankan operasi grup, misalkan $g_1 = h_1k_1$ dan $g_2 = h_2k_2$, lalu perhatikan bahwa

$$\begin{aligned}
\phi(g_1g_2) &= \phi(h_1k_1h_2k_2) \\
&= \phi(h_1h_2k_1k_2) \\
&= (h_1h_2, k_1k_2) \\
&= (h_1, k_1)(h_2, k_2) \\
&= \phi(g_1)\phi(g_2).
\end{aligned}$$

Pembuktian bahwa ϕ injektif dan surjektif diserahkan sebagai latihan. ■

Contoh 9.2.16 Grup $\mathbb{Z}_6$ merupakan hasil kali langsung internal yang isomorfik dengan $\{0, 2, 4\} \times \{0, 3\}$. ▲

Kita dapat memperluas definisi hasil kali langsung internal dari G ke suatu koleksi subgrup $H_1, H_2, \ldots, H_n$ dari G, dengan mensyaratkan bahwa

- $G = H_1H_2 \cdots H_n = \{h_1h_2 \cdots h_n : h_i \in H_i\}$;
- $H_i \cap \langle \cup_{j \neq i} H_j \rangle = \{e\}$;
- $h_ih_j = h_jh_i$ untuk semua $h_i \in H_i$ dan $h_j \in H_j$.

Pembuktian teorema berikut diserahkan sebagai latihan.

Teorema 9.2.17 *Misalkan G merupakan hasil kali langsung internal dari subgrup-subgrup H_i, dengan $i = 1, 2, \ldots, n$. Maka G isomorfik dengan $\prod_i H_i$.*

9.3 Pertanyaan Bacaan

1. Tentukan orde $(1, 2)$ dalam $\mathbb{Z}_4 \times \mathbb{Z}_8$.

2. Sebutkan tiga sifat grup yang dipertahankan oleh suatu isomorfisma.

3. Temukan suatu grup yang isomorfik dengan $\mathbb{Z}_{15}$ dan merupakan hasil kali langsung eksternal dari dua grup nontrivial.

4. Jelaskan mengapa sekarang kita dapat mengatakan "*grup siklik tak hingga tersebut*"?

5. Bandingkan persamaan dan perbedaan hasil kali langsung eksternal dan hasil kali langsung internal.

9.4 Latihan

1. Buktikan bahwa $\mathbb{Z} \cong n\mathbb{Z}$ untuk $n \neq 0$.

Petunjuk. Setiap grup siklik tak hingga isomorfik dengan $\mathbb{Z}$ berdasarkan Teorema 9.1.7.

2. Buktikan bahwa $\mathbb{C}^*$ isomorfik dengan subgrup dari $GL_2(\mathbb{R})$ yang terdiri atas matriks-matriks berbentuk

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Petunjuk. Definisikan $\phi : \mathbb{C}^* \to GL_2(\mathbb{R})$ dengan

$$\phi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

3. Buktikan atau bantah: $U(8) \cong \mathbb{Z}_4$.

Petunjuk. Salah.

4. Buktikan bahwa $U(8)$ isomorfik dengan grup matriks

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

5. Tunjukkan bahwa $U(5)$ isomorfik dengan $U(10)$, tetapi tidak isomorfik dengan $U(12)$.

6. Tunjukkan bahwa akar-akar kesatuan ke-n isomorfik dengan $\mathbb{Z}_n$.

Petunjuk. Definisikan pemetaan dari $\mathbb{Z}_n$ ke akar-akar kesatuan ke-n dengan $k \mapsto \text{cis}(2k\pi/n)$.

7. Tunjukkan bahwa setiap grup siklik berorde n isomorfik dengan $\mathbb{Z}_n$.

8. Buktikan bahwa $\mathbb{Q}$ tidak isomorfik dengan $\mathbb{Z}$.

Petunjuk. Andaikan $\mathbb{Q}$ siklik dan cobalah mencari pembangkitnya.

9. Misalkan $G = \mathbb{R} \setminus \{-1\}$ dan definisikan operasi biner pada G dengan

$$a * b = a + b + ab.$$

Buktikan bahwa G merupakan grup terhadap operasi ini. Tunjukkan bahwa $(G, *)$ isomorfik dengan grup multiplikatif bilangan real taknol.

10. Tunjukkan bahwa matriks-matriks

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} \quad \begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix} \quad \begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}$$
$$\begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix} \quad \begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix} \quad \begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}$$

membentuk suatu grup. Temukan isomorfisma dari G dengan grup berorde 6 yang lebih dikenal.

11. Temukan lima grup berorde 8 yang saling takisomorfik.

Petunjuk. Terdapat dua grup nonabelian dan tiga grup abelian yang saling takisomorfik.

12. Buktikan bahwa S_4 tidak isomorfik dengan D_{12}.

13. Misalkan $\omega = \text{cis}(2\pi/n)$ adalah akar kesatuan primitif ke-n. Buktikan bahwa matriks-matriks

$$A = \begin{pmatrix}\omega&0\\0&\omega^{-1}\end{pmatrix} \quad \text{dan} \quad B = \begin{pmatrix}0&1\\1&0\end{pmatrix}$$

membangkitkan grup multiplikatif yang isomorfik dengan D_n.

14. Tunjukkan bahwa himpunan semua matriks berbentuk

$$\begin{pmatrix}\pm 1&k\\0&1\end{pmatrix},$$

merupakan grup yang isomorfik dengan D_n, dengan semua entri matriks berada dalam $\mathbb{Z}_n$.

15. Daftarkan semua elemen $\mathbb{Z}_4 \times \mathbb{Z}_2$.

16. Tentukan orde setiap elemen berikut.

(a) $(3, 4)$ dalam $\mathbb{Z}_4 \times \mathbb{Z}_6$

(b) $(6, 15, 4)$ dalam $\mathbb{Z}_{30} \times \mathbb{Z}_{45} \times \mathbb{Z}_{24}$

(c) $(5, 10, 15)$ dalam $\mathbb{Z}_{25} \times \mathbb{Z}_{25} \times \mathbb{Z}_{25}$

(d) $(8, 8, 8)$ dalam $\mathbb{Z}_{10} \times \mathbb{Z}_{24} \times \mathbb{Z}_{80}$

Petunjuk. (a) 12; (c) 5.

17. Buktikan bahwa D_4 tidak mungkin merupakan hasil kali langsung internal dari dua subgrup sejatinya.

18. Buktikan bahwa subgrup dari $\mathbb{Q}^*$ yang terdiri atas elemen berbentuk $2^m 3^n$ untuk $m, n \in \mathbb{Z}$ merupakan hasil kali langsung internal yang isomorfik dengan $\mathbb{Z} \times \mathbb{Z}$.

19. Buktikan bahwa $S_3 \times \mathbb{Z}_2$ isomorfik dengan D_6. Dapatkah Anda membuat konjektur tentang D_{2n}? Buktikan konjektur Anda.

Petunjuk. Gambarlah diagramnya.

20. Buktikan atau bantah: Setiap grup abelian yang ordenya habis dibagi 3 memuat subgrup berorde 3.

Petunjuk. Benar.

21. Buktikan atau bantah: Setiap grup nonabelian yang ordenya habis dibagi 6 memuat subgrup berorde 6.

22. Misalkan G suatu grup berorde 20. Jika G memiliki subgrup H dan K yang berturut-turut berorde 4 dan 5 sedemikian sehingga $hk = kh$ untuk semua $h \in H$ dan $k \in K$, buktikan bahwa G merupakan hasil kali langsung internal dari H dan K.

23. Buktikan atau bantah pernyataan berikut. Misalkan G, H, dan K adalah grup. Jika $G \times K \cong H \times K$, maka $G \cong H$.

24. Buktikan atau bantah: Terdapat grup abelian taksiklik berorde 51.

25. Buktikan atau bantah: Terdapat grup abelian taksiklik berorde 52.

Petunjuk. Benar.

26. Misalkan $\phi : G \to H$ suatu isomorfisma grup. Tunjukkan bahwa $\phi(x) = e_H$ jika dan hanya jika $x = e_G$, dengan e_G dan e_H berturut-turut merupakan identitas dari G dan H.

27. Misalkan $G \cong H$. Tunjukkan bahwa jika G siklik, maka H juga siklik.

Petunjuk. Misalkan a suatu pembangkit dari G. Jika $\phi : G \to H$ adalah isomorfisma, tunjukkan bahwa $\phi(a)$ merupakan pembangkit dari H.

28. Buktikan bahwa setiap grup G berorde p, dengan p prima, harus isomorfik dengan $\mathbb{Z}_p$.

29. Tunjukkan bahwa S_n isomorfik dengan suatu subgrup dari A_{n+2}.

30. Buktikan bahwa D_n isomorfik dengan suatu subgrup dari S_n.

31. Misalkan $\phi : G_1 \to G_2$ dan $\psi : G_2 \to G_3$ adalah isomorfisma. Tunjukkan bahwa ϕ^{-1} dan $\psi \circ \phi$ keduanya merupakan isomorfisma. Dengan menggunakan hasil-hasil ini, tunjukkan bahwa keisomorfikan grup menentukan suatu relasi ekuivalensi pada kelas semua grup.

32. Buktikan bahwa $U(5) \cong \mathbb{Z}_4$. Dapatkah Anda memperumum hasil ini untuk $U(p)$, dengan p prima?

33. Tuliskan permutasi yang dikaitkan dengan setiap elemen S_3 dalam pembuktian Teorema Cayley.

34. **Automorfisme** dari suatu grup G adalah isomorfisma grup tersebut dengan dirinya sendiri. Buktikan bahwa konjugasi kompleks merupakan automorfisme dari grup aditif bilangan kompleks; yaitu, tunjukkan bahwa pemetaan $\phi(a + bi) = a - bi$ merupakan isomorfisma dari $\mathbb{C}$ ke $\mathbb{C}$.

35. Buktikan bahwa $a + ib \mapsto a - ib$ merupakan automorfisme dari $\mathbb{C}^*$.

36. Buktikan bahwa $A \mapsto B^{-1}AB$ merupakan automorfisme dari $SL_2(\mathbb{R})$ untuk semua B dalam $GL_2(\mathbb{R})$.

37. Kita akan menyatakan himpunan semua automorfisme dari G dengan $\mathrm{Aut}(G)$. Buktikan bahwa $\mathrm{Aut}(G)$ merupakan subgrup dari S_G, yaitu grup permutasi dari G.

38. Tentukan $\mathrm{Aut}(\mathbb{Z}_6)$.

Petunjuk. Setiap automorfisme dari $\mathbb{Z}_6$ harus memetakan 1 ke pembangkit lain dari $\mathbb{Z}_6$.

39. Tentukan $\mathrm{Aut}(\mathbb{Z})$.

40. Temukan dua grup takisomorfik G dan H sedemikian sehingga $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$.

41. Misalkan G suatu grup dan $g \in G$. Definisikan pemetaan $i_g : G \to G$ dengan $i_g(x) = gxg^{-1}$. Buktikan bahwa i_g mendefinisikan suatu automor-

fisme dari G. Automorfisme semacam ini disebut **automorfisme dalam**. Himpunan semua automorfisme dalam dinyatakan dengan $\text{Inn}(G)$.

42. Buktikan bahwa $\text{Inn}(G)$ merupakan subgrup dari $\text{Aut}(G)$.

43. Apa saja automorfisme dalam dari grup kuaternion Q_8? Apakah $\text{Inn}(G) = \text{Aut}(G)$ dalam kasus ini?

44. Misalkan G suatu grup dan $g \in G$. Definisikan pemetaan $\lambda_g : G \to G$ dan $\rho_g : G \to G$ dengan $\lambda_g(x) = gx$ dan $\rho_g(x) = xg^{-1}$. Tunjukkan bahwa $i_g = \rho_g \circ \lambda_g$ merupakan automorfisme dari G. Isomorfisma $g \mapsto \rho_g$ disebut **representasi reguler kanan** dari G.

45. Misalkan G merupakan hasil kali langsung internal dari subgrup H dan K. Tunjukkan bahwa pemetaan $\phi : G \to H \times K$ yang didefinisikan oleh $\phi(g) = (h, k)$ untuk $g = hk$, dengan $h \in H$ dan $k \in K$, bersifat injektif dan surjektif.

Petunjuk. Untuk menunjukkan bahwa ϕ injektif, misalkan $g_1 = h_1k_1$ dan $g_2 = h_2k_2$, lalu tinjau $\phi(g_1) = \phi(g_2)$.

46. Misalkan G dan H adalah grup-grup isomorfik. Jika G memiliki subgrup berorde n, buktikan bahwa H juga harus memiliki subgrup berorde n.

47. Jika $G \cong \overline{G}$ dan $H \cong \overline{H}$, tunjukkan bahwa $G \times H \cong \overline{G} \times \overline{H}$.

48. Buktikan bahwa $G \times H$ isomorfik dengan $H \times G$.

49. Misalkan $n_1, \ldots, n_k$ adalah bilangan bulat positif. Tunjukkan bahwa

$$\prod_{i=1}^{k} \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 \cdots n_k}$$

jika dan hanya jika $\gcd(n_i, n_j) = 1$ untuk $i \neq j$.

50. Buktikan bahwa $A \times B$ abelian jika dan hanya jika A dan B abelian.

51. Jika G merupakan hasil kali langsung internal dari $H_1, H_2, \ldots, H_n$, buktikan bahwa G isomorfik dengan $\prod_i H_i$.

52. Misalkan H_1 dan H_2 berturut-turut merupakan subgrup dari G_1 dan G_2. Buktikan bahwa $H_1 \times H_2$ merupakan subgrup dari $G_1 \times G_2$.

53. Misalkan $m, n \in \mathbb{Z}$. Buktikan bahwa $\langle m, n\rangle = \langle d\rangle$ jika dan hanya jika $d = \gcd(m, n)$.

54. Misalkan $m, n \in \mathbb{Z}$. Buktikan bahwa $\langle m\rangle \cap \langle n\rangle = \langle l\rangle$ jika dan hanya jika $l = \text{lcm}(m, n)$.

55. Grup berorde $2p$. Dalam rangkaian latihan ini, kita akan mengklasifikasikan semua grup berorde $2p$, dengan p suatu bilangan prima ganjil.

(a) Andaikan G merupakan grup berorde $2p$, dengan p suatu bilangan prima ganjil. Jika $a \in G$, tunjukkan bahwa a harus berorde 1, 2, p, atau $2p$.

(b) Misalkan G memiliki elemen berorde $2p$. Buktikan bahwa G isomorfik dengan $\mathbb{Z}_{2p}$. Dengan demikian, G bersifat siklik.

(c) Misalkan G tidak memuat elemen berorde $2p$. Tunjukkan bahwa G harus memuat elemen berorde p. *Petunjuk*: Andaikan G tidak memuat elemen berorde p.

(d) Misalkan G tidak memuat elemen berorde $2p$. Tunjukkan bahwa G harus memuat elemen berorde 2.

(e) Misalkan P merupakan subgrup dari G yang berorde p, dan $y \in G$ berorde 2. Tunjukkan bahwa $yP = Py$.

(f) Misalkan G tidak memuat elemen berorde $2p$ dan $P = \langle z \rangle$ merupakan subgrup berorde p yang dibangkitkan oleh z. Jika y merupakan elemen berorde 2, maka $yz = z^k y$ untuk suatu $2 \leq k < p$.

(g) Misalkan G tidak memuat elemen berorde $2p$. Buktikan bahwa G tidak abelian.

(h) Misalkan G tidak memuat elemen berorde $2p$ dan $P = \langle z \rangle$ merupakan subgrup berorde p yang dibangkitkan oleh z, serta y merupakan elemen berorde 2. Tunjukkan bahwa kita dapat mendaftarkan elemen-elemen G sebagai $\{z^i y^j \mid 0 \leq i < p, 0 \leq j < 2\}$.

(i) Misalkan G tidak memuat elemen berorde $2p$ dan $P = \langle z \rangle$ merupakan subgrup berorde p yang dibangkitkan oleh z, serta y merupakan elemen berorde 2. Buktikan bahwa hasil kali $(z^i y^j)(z^r y^s)$ dapat dinyatakan secara tunggal sebagai $z^m y^n$ untuk suatu bilangan bulat taknegatif m, n. Dengan demikian, simpulkan bahwa hanya ada satu kemungkinan untuk grup nonabelian berorde $2p$, sehingga grup tersebut pastilah grup yang sudah kita jumpai, yaitu grup dihedral.

10

Subgrup Normal dan Grup Hasil Bagi

Jika H merupakan subgrup dari suatu grup G, koset kanan tidak selalu sama dengan koset kiri; yaitu, tidak selalu berlaku $gH = Hg$ untuk semua $g \in G$. Subgrup yang memenuhi sifat ini memainkan peran penting dalam teori grup—subgrup tersebut memungkinkan pembentukan suatu kelas grup baru, yang disebut grup hasil bagi. Grup hasil bagi dapat dipelajari secara langsung ataupun dengan menggunakan homomorfisma, yang merupakan perumuman isomorfisma. Kita akan mempelajari homomorfisma dalam Bab 11.

10.1 Grup Hasil Bagi dan Subgrup Normal

10.1.1 Subgrup Normal

Suatu subgrup H dari grup G disebut **normal** dalam G jika $gH = Hg$ untuk semua $g \in G$. Dengan kata lain, subgrup normal dari suatu grup G adalah subgrup yang koset kanan dan koset kirinya tepat sama.

Contoh 10.1.1 Misalkan G suatu grup abelian. Setiap subgrup H dari G merupakan subgrup normal. Karena $gh = hg$ untuk semua $g \in G$ dan $h \in H$, selalu berlaku $gH = Hg$. ▲

Contoh 10.1.2 Misalkan H merupakan subgrup dari S_3 yang terdiri atas elemen (1) dan (12). Karena

$$(123)H = \{(1\,2\,3), (1\,3)\} \quad \text{dan} \quad H(1\,2\,3) = \{(1\,2\,3), (2\,3)\},$$

H bukan subgrup normal dari S_3. Akan tetapi, subgrup N, yang terdiri atas permutasi (1), (1 2 3), dan (1 3 2), adalah normal karena koset-koset N ialah

$$N = \{(1), (1\,2\,3), (1\,3\,2)\}$$
$$(1\,2)N = N(1\,2) = \{(1\,2), (1\,3), (2\,3)\}.$$

▲

Teorema berikut mendasari pemahaman kita mengenai subgrup normal.

Teorema 10.1.3 *Misalkan G suatu grup dan N suatu subgrup dari G. Pernyataan-pernyataan berikut ekuivalen.*

1. *Subgrup N normal dalam G.*
2. *Untuk semua $g \in G$, $gNg^{-1} \subset N$.*

3. Untuk semua $g \in G$, $gNg^{-1} = N$.

BUKTI. (1) $\Rightarrow$ (2). Karena N normal dalam G, $gN = Ng$ untuk semua $g \in G$. Oleh karena itu, untuk suatu $g \in G$ dan $n \in N$, terdapat n' dalam N sedemikian sehingga $gn = n'g$. Jadi, $gng^{-1} = n' \in N$, atau $gNg^{-1} \subset N$.

(2) $\Rightarrow$ (3). Misalkan $g \in G$. Karena $gNg^{-1} \subset N$, kita hanya perlu menunjukkan $N \subset gNg^{-1}$. Untuk $n \in N$, $g^{-1}ng = g^{-1}n(g^{-1})^{-1} \in N$. Dengan demikian, $g^{-1}ng = n'$ untuk suatu $n' \in N$. Oleh karena itu, $n = gn'g^{-1}$ berada dalam gNg^{-1}.

(3) $\Rightarrow$ (1). Andaikan $gNg^{-1} = N$ untuk semua $g \in G$. Maka, untuk setiap $n \in N$, terdapat $n' \in N$ sedemikian sehingga $gng^{-1} = n'$. Akibatnya, $gn = n'g$, atau $gN \subset Ng$. Demikian pula, $Ng \subset gN$. ■

10.1.2 Grup Hasil Bagi

Jika N merupakan subgrup normal dari suatu grup G, koset-koset N dalam G membentuk grup G/N di bawah operasi $(aN)(bN) = abN$. Grup ini disebut **grup hasil bagi** atau **grup kuosien** dari G oleh N. Tugas pertama kita adalah membuktikan bahwa G/N benar-benar merupakan sebuah grup.

Teorema 10.1.4 *Misalkan N suatu subgrup normal dari grup G. Koset-koset N dalam G membentuk grup G/N yang berorde $[G : N]$.*

BUKTI. Operasi grup pada G/N adalah $(aN)(bN) = abN$. Kita harus menunjukkan bahwa operasi ini terdefinisi dengan baik; yaitu, perkalian grup harus tidak bergantung pada pemilihan wakil koset. Misalkan $aN = bN$ dan $cN = dN$. Kita harus menunjukkan bahwa

$$(aN)(cN) = acN = bdN = (bN)(dN).$$

Maka $a = bn_1$ dan $c = dn_2$ untuk suatu n_1 dan n_2 dalam N. Jadi,

$$\begin{aligned} acN &= bn_1dn_2N \\ &= bn_1dN \\ &= bn_1Nd \\ &= bNd \\ &= bdN. \end{aligned}$$

Bagian lain dari teorema ini mudah: $eN = N$ merupakan identitas dan $g^{-1}N$ merupakan invers dari gN. Orde G/N tentu saja sama dengan banyaknya koset N dalam G. ■

Sangat penting untuk mengingat bahwa elemen-elemen dalam suatu grup hasil bagi merupakan *himpunan elemen* dalam grup asal.

Contoh 10.1.5 Perhatikan subgrup normal dari S_3, $N = \{(1), (1\,2\,3), (1\,3\,2)\}$. Koset-koset N dalam S_3 adalah N dan $(12)N$. Grup hasil bagi S_3/N memiliki tabel perkalian berikut.

	N	$(1\,2)N$
N	N	$(1\,2)N$
$(1\,2)N$	$(1\,2)N$	N

Grup ini isomorfik dengan $\mathbb{Z}_2$. Pada awalnya, perkalian koset tampak rumit sekaligus ganjil; akan tetapi, perhatikan bahwa S_3/N merupakan grup yang lebih kecil. Grup hasil bagi tersebut menampilkan sejumlah informasi mengenai S_3. Sesungguhnya, $N = A_3$ adalah grup permutasi genap, sedangk-

an $(1\,2)N = \{(1\,2), (1\,3), (2\,3)\}$ adalah himpunan permutasi ganjil. Informasi yang ditangkap oleh G/N ialah paritas; yaitu, perkalian dua permutasi genap atau dua permutasi ganjil menghasilkan permutasi genap, sedangkan perkalian permutasi ganjil dengan permutasi genap menghasilkan permutasi ganjil. ▲

Contoh 10.1.6 Perhatikan subgrup normal $3\mathbb{Z}$ dari $\mathbb{Z}$. Koset-koset $3\mathbb{Z}$ dalam $\mathbb{Z}$ adalah

$$\begin{aligned} 0 + 3\mathbb{Z} &= \{\ldots, -3, 0, 3, 6, \ldots\} \\ 1 + 3\mathbb{Z} &= \{\ldots, -2, 1, 4, 7, \ldots\} \\ 2 + 3\mathbb{Z} &= \{\ldots, -1, 2, 5, 8, \ldots\}. \end{aligned}$$

Grup $\mathbb{Z}/3\mathbb{Z}$ diberikan oleh tabel Cayley di bawah ini.

$+$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$0+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$1+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$
$2+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$

Secara umum, subgrup $n\mathbb{Z}$ dari $\mathbb{Z}$ adalah normal. Koset-koset $\mathbb{Z}/n\mathbb{Z}$ adalah

$$\begin{aligned} &n\mathbb{Z} \\ &1 + n\mathbb{Z} \\ &2 + n\mathbb{Z} \\ &\vdots \\ &(n-1) + n\mathbb{Z}. \end{aligned}$$

Jumlah koset $k+n\mathbb{Z}$ dan $l+n\mathbb{Z}$ adalah $k+l+n\mathbb{Z}$. Perhatikan bahwa kita telah menuliskan koset-koset tersebut secara aditif, karena operasi grupnya adalah penjumlahan bilangan bulat. ▲

Contoh 10.1.7 Perhatikan grup dihedral D_n, yang dibangkitkan oleh dua elemen r dan s yang memenuhi relasi

$$\begin{aligned} r^n &= \mathrm{id} \\ s^2 &= \mathrm{id} \\ srs &= r^{-1}. \end{aligned}$$

Elemen r membangkitkan subgrup siklik rotasi, R_n, dari D_n. Karena $srs^{-1} = srs = r^{-1} \in R_n$, grup rotasi merupakan subgrup normal dari D_n; oleh karena itu, D_n/R_n merupakan sebuah grup. Karena grup ini memiliki tepat dua elemen, grup tersebut harus isomorfik dengan $\mathbb{Z}_2$. ▲

10.2 Kesederhanaan Grup Alternasi

Grup yang tidak memiliki subgrup normal taktrivial sangat menarik untuk dikaji. Grup semacam itu disebut **grup sederhana**. Tentu saja, kita sudah mempunyai satu kelas lengkap contoh grup sederhana, yaitu $\mathbb{Z}_p$, dengan p prima. Grup-grup ini secara langsung bersifat sederhana karena tidak memiliki subgrup sejati selain subgrup yang hanya terdiri atas identitas. Contoh lain grup sederhana tidak mudah ditemukan. Akan tetapi, kita dapat menunjukkan bahwa grup alternasi A_n bersifat sederhana untuk $n \geq 5$. Pembuktian hasil ini memerlukan beberapa lema.

Lema 10.2.1 *Grup alternasi A_n dibangkitkan oleh siklus-3 untuk $n \geq 3$.*

BUKTI. Untuk menunjukkan bahwa siklus-3 membangkitkan A_n, kita hanya perlu menunjukkan bahwa setiap pasangan transposisi dapat dituliskan sebagai hasil kali siklus-3. Karena $(a, b) = (b, a)$, setiap pasangan transposisi harus memiliki salah satu bentuk berikut:

$$\begin{aligned}(a, b)(a, b) &= \mathrm{id}\\ (a, b)(c, d) &= (a, c, b)(a, c, d)\\ (a, b)(a, c) &= (a, c, b).\end{aligned}$$

■

Lema 10.2.2 *Misalkan N suatu subgrup normal dari A_n, dengan $n \geq 3$. Jika N memuat suatu siklus-3, maka $N = A_n$.*

BUKTI. Pertama-tama kita akan menunjukkan bahwa A_n dibangkitkan oleh siklus-3 yang berbentuk khusus (i, j, k), dengan i dan j tetap di dalam $\{1, 2, \ldots, n\}$, sedangkan k bervariasi. Setiap siklus-3 merupakan hasil kali siklus-3 berbentuk demikian, sebab

$$\begin{aligned}(i, a, j) &= (i, j, a)^2\\ (i, a, b) &= (i, j, b)(i, j, a)^2\\ (j, a, b) &= (i, j, b)^2(i, j, a)\\ (a, b, c) &= (i, j, a)^2(i, j, c)(i, j, b)^2(i, j, a).\end{aligned}$$

Sekarang andaikan N merupakan subgrup normal taktrivial dari A_n untuk $n \geq 3$ dan N memuat siklus-3 berbentuk (i, j, a). Dengan menggunakan kenormalan N, kita memperoleh bahwa

$$[(i, j)(a, k)](i, j, a)^2[(i, j)(a, k)]^{-1} = (i, j, k)$$

berada dalam N. Jadi, N harus memuat semua siklus-3 (i, j, k) untuk $1 \leq k \leq n$. Berdasarkan Lema 10.2.1, siklus-3 tersebut membangkitkan A_n; oleh karena itu, $N = A_n$. ■

Lema 10.2.3 *Untuk $n \geq 5$, setiap subgrup normal taktrivial N dari A_n memuat suatu siklus-3.*

BUKTI. Misalkan σ suatu elemen sembarang dalam subgrup normal N. Terdapat beberapa kemungkinan struktur siklus bagi σ.

- σ merupakan siklus-3.
- σ merupakan hasil kali siklus-siklus saling lepas, $\sigma = \tau(a_1, a_2, \ldots, a_r) \in N$, dengan $r > 3$.
- σ merupakan hasil kali siklus-siklus saling lepas, $\sigma = \tau(a_1, a_2, a_3)(a_4, a_5, a_6)$.
- $\sigma = \tau(a_1, a_2, a_3)$, dengan τ merupakan hasil kali siklus-2 yang saling lepas.
- $\sigma = \tau(a_1, a_2)(a_3, a_4)$, dengan τ merupakan hasil kali sejumlah genap siklus-2 yang saling lepas.

Jika σ merupakan siklus-3, pembuktian selesai. Jika N memuat suatu hasil kali siklus-siklus saling lepas, σ, dan setidaknya satu siklus tersebut panjangnya

lebih besar daripada 3, misalkan $\sigma = \tau(a_1, a_2, \ldots, a_r)$, maka

$$(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$$

berada dalam N karena N normal; akibatnya,

$$\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$$

juga berada dalam N. Karena

$$\begin{aligned}\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1} &= \sigma^{-1}(a_1, a_2, a_3) \\ &\quad \cdot \sigma(a_1, a_3, a_2) \\ &= (a_1, a_2, \ldots, a_r)^{-1}\tau^{-1}(a_1, a_2, a_3) \\ &\quad \cdot \tau(a_1, a_2, \ldots, a_r)(a_1, a_3, a_2) \\ &= (a_1, a_r, a_{r-1}, \ldots, a_2)(a_1, a_2, a_3) \\ &\quad \cdot (a_1, a_2, \ldots, a_r)(a_1, a_3, a_2) \\ &= (a_1, a_3, a_r),\end{aligned}$$

N harus memuat suatu siklus-3; oleh karena itu, $N = A_n$.

Sekarang andaikan N memuat suatu hasil kali saling lepas berbentuk

$$\sigma = \tau(a_1, a_2, a_3)(a_4, a_5, a_6).$$

Maka

$$\sigma^{-1}(a_1, a_2, a_4)\sigma(a_1, a_2, a_4)^{-1} \in N$$

karena

$$(a_1, a_2, a_4)\sigma(a_1, a_2, a_4)^{-1} \in N.$$

Jadi,

$$\begin{aligned}\sigma^{-1}(a_1, a_2, a_4)\sigma(a_1, a_2, a_4)^{-1} &= [\tau(a_1, a_2, a_3)(a_4, a_5, a_6)]^{-1} \\ &\quad \cdot (a_1, a_2, a_4)\tau(a_1, a_2, a_3) \\ &\quad \cdot (a_4, a_5, a_6)(a_1, a_2, a_4)^{-1} \\ &= (a_4, a_6, a_5)(a_1, a_3, a_2) \\ &\quad \cdot \tau^{-1}(a_1, a_2, a_4)\tau(a_1, a_2, a_3) \\ &\quad \cdot (a_4, a_5, a_6)(a_1, a_4, a_2) \\ &= (a_4, a_6, a_5)(a_1, a_3, a_2)(a_1, a_2, a_4) \\ &\quad \cdot (a_1, a_2, a_3)(a_4, a_5, a_6) \\ &\quad \cdot (a_1, a_4, a_2) \\ &= (a_1, a_4, a_2, a_6, a_3).\end{aligned}$$

Dengan demikian, N memuat siklus saling lepas yang panjangnya lebih besar daripada 3, sehingga kita dapat menerapkan kasus sebelumnya.

Andaikan N memuat suatu hasil kali saling lepas berbentuk $\sigma = \tau(a_1, a_2, a_3)$, dengan τ merupakan hasil kali siklus-2 yang saling lepas. Karena $\sigma \in N$, maka $\sigma^2 \in N$, dan

$$\begin{aligned}\sigma^2 &= \tau(a_1, a_2, a_3)\tau(a_1, a_2, a_3) \\ &= (a_1, a_3, a_2).\end{aligned}$$

Jadi, N memuat suatu siklus-3.

Satu-satunya kemungkinan kasus yang tersisa adalah hasil kali saling lepas berbentuk

$$\sigma = \tau(a_1, a_2)(a_3, a_4),$$

dengan τ merupakan hasil kali sejumlah genap siklus-2 yang saling lepas. Akan tetapi,

$$\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$$

berada dalam N karena $(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$ berada dalam N; sehingga

$$\begin{aligned}\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1} &= \tau^{-1}(a_1, a_2)(a_3, a_4) \\ &\quad \cdot (a_1, a_2, a_3)\tau(a_1, a_2) \\ &\quad \cdot (a_3, a_4)(a_1, a_2, a_3)^{-1} \\ &= (a_1, a_3)(a_2, a_4).\end{aligned}$$

Karena $n \geq 5$, kita dapat menemukan $b \in \{1, 2, \ldots, n\}$ sedemikian sehingga $b \neq a_1, a_2, a_3, a_4$. Misalkan $\mu = (a_1, a_3, b)$. Maka

$$\mu^{-1}(a_1, a_3)(a_2, a_4)\mu(a_1, a_3)(a_2, a_4) \in N$$

dan

$$\begin{aligned}\mu^{-1}(a_1, a_3)(a_2, a_4)\mu(a_1, a_3)(a_2, a_4) &= (a_1, b, a_3) \\ &\quad \cdot (a_1, a_3)(a_2, a_4) \\ &\quad \cdot (a_1, a_3, b)(a_1, a_3)(a_2, a_4) \\ &= (a_1, a_3, b).\end{aligned}$$

Oleh karena itu, N memuat suatu siklus-3. Dengan demikian, pembuktian lema ini selesai. ■

Teorema 10.2.4 *Grup alternasi A_n bersifat sederhana untuk $n \geq 5$.*

BUKTI. Misalkan N suatu subgrup normal dari A_n. Berdasarkan Lema 10.2.3, N memuat suatu siklus-3. Berdasarkan Lema 10.2.2, $N = A_n$; oleh karena itu, A_n tidak memuat subgrup normal sejati yang taktrivial untuk $n \geq 5$. ■

Catatan Sejarah

Salah satu masalah terpenting dalam teori grup ialah mengklasifikasikan semua grup sederhana hingga. Masalah ini telah berusia lebih dari satu abad dan baru diselesaikan dalam beberapa dasawarsa terakhir abad kedua puluh. Dalam suatu pengertian, grup sederhana hingga merupakan blok pembangun semua grup hingga. Grup sederhana nonabelian pertama yang ditemukan adalah grup-grup alternasi. Galois adalah orang pertama yang membuktikan bahwa A_5 sederhana. Kemudian, matematikawan seperti C. Jordan dan L. E. Dickson menemukan beberapa keluarga takhingga grup matriks yang sederhana. Keluarga lain grup sederhana ditemukan pada dasawarsa 1950-an. Pada pergantian abad, William Burnside menduga bahwa semua grup sederhana nonabelian harus berorde genap. Pada tahun 1963, W. Feit dan J. Thompson membuktikan dugaan Burnside dan menerbitkan hasil mereka dalam makalah "Solvability of Groups of Odd Order," yang dimuat dalam *Pacific Journal of Mathematics*. Pembuktian mereka, yang panjangnya lebih dari 250 halaman, mendorong suatu program pada dasawarsa 1960-an dan 1970-an untuk mengklasifikasikan semua grup sederhana hingga. Daniel Gorenstein merupakan pengorganisasi upaya luar biasa ini. Salah satu grup sederhana terakhir adalah "Monster," yang ditemukan oleh R. Greiss. Monster, suatu grup matriks $196{,}833 \times 196{,}833$, merupakan salah satu dari 26 grup sederhana sporadik, atau khusus. Grup sederhana sporadik ini tidak termasuk dalam keluarga takhingga grup sederhana mana pun. Beberapa grup sporadik memainkan peran penting dalam fisika.

10.3 Pertanyaan Bacaan

1. Misalkan G grup simetri suatu segitiga sama sisi, yang dinyatakan sebagai permutasi titik-titik sudut bernomor $1, 2, 3$. Misalkan H subgrup $H = \langle (1\,2) \rangle$. Bentuk koset kiri dan koset kanan H dalam G.

2. Berdasarkan jawaban Anda atas pertanyaan sebelumnya, apakah H normal dalam G? Jelaskan alasannya.

3. Subgrup $8\mathbb{Z}$ normal dalam $\mathbb{Z}$. Dalam grup hasil bagi $\mathbb{Z}/8\mathbb{Z}$, lakukan perhitungan $(3 + 8\mathbb{Z}) + (7 + 8\mathbb{Z})$.

4. Tuliskan dua pernyataan mengenai suatu grup G dan subgrup H yang ekuivalen dengan "H normal dalam G."

5. Dengan kata-kata Anda sendiri, apakah yang dimaksud dengan grup hasil bagi?

10.4 Latihan

1. Untuk setiap grup G berikut, tentukan apakah H merupakan subgrup normal dari G. Jika H merupakan subgrup normal, tuliskan tabel Cayley untuk grup hasil bagi G/H.

(a) $G = S_4$ dan $H = A_4$

(b) $G = A_5$ dan $H = \{(1), (1\,2\,3), (1\,3\,2)\}$

(c) $G = S_4$ dan $H = D_4$

(d) $G = Q_8$ dan $H = \{1, -1, I, -I\}$

(e) $G = \mathbb{Z}$ dan $H = 5\mathbb{Z}$

Petunjuk. (a)

	A_4	$(1\,2)A_4$
A_4	A_4	$(1\,2)A_4$
$(1\,2)A_4$	$(1\,2)A_4$	A_4

(c) D_4 tidak normal dalam S_4.

2. Carilah semua subgrup dari D_4. Subgrup manakah yang normal? Tentukan semua grup hasil bagi dari D_4 hingga isomorfisma.

3. Carilah semua subgrup dari grup kuaternion Q_8. Subgrup manakah yang normal? Tentukan semua grup hasil bagi dari Q_8 hingga isomorfisma.

4. Misalkan T grup matriks segitiga atas nonsingular berukuran 2×2 dengan entri dalam $\mathbb{R}$; yaitu, matriks berbentuk

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix},$$

dengan a, b, $c \in \mathbb{R}$ dan $ac \neq 0$. Misalkan U terdiri atas matriks berbentuk

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

dengan $x \in \mathbb{R}$.

(a) Tunjukkan bahwa U merupakan subgrup dari T.

(b) Buktikan bahwa U abelian.

(c) Buktikan bahwa U normal dalam T.

(d) Tunjukkan bahwa T/U abelian.

(e) Apakah T normal dalam $GL_2(\mathbb{R})$?

5. Tunjukkan bahwa irisan dua subgrup normal merupakan subgrup normal.

6. Jika G abelian, buktikan bahwa G/H juga harus abelian.

7. Buktikan atau bantah: Jika H merupakan subgrup normal dari G sedemikian sehingga H dan G/H abelian, maka G abelian.

8. Jika G siklik, buktikan bahwa G/H juga harus siklik.

Petunjuk. Jika $a \in G$ merupakan pembangkit G, maka aH merupakan pembangkit G/H.

9. Buktikan atau bantah: Jika H dan G/H siklik, maka G siklik.

10. Misalkan H suatu subgrup berindeks 2 dari grup G. Buktikan bahwa H harus merupakan subgrup normal dari G. Simpulkan bahwa S_n tidak sederhana untuk $n \geq 3$.

11. Jika suatu grup G memiliki tepat satu subgrup H berorde k, buktikan bahwa H normal dalam G.

Petunjuk. Untuk setiap $g \in G$, tunjukkan bahwa pemetaan $i_g : G \to G$ yang didefinisikan oleh $i_g : x \mapsto gxg^{-1}$ merupakan isomorfisma dari G ke dirinya sendiri. Kemudian perhatikan $i_g(H)$.

12. Definisikan **sentralisator** suatu elemen g dalam grup G sebagai himpunan

$$C(g) = \{x \in G : xg = gx\}.$$

Tunjukkan bahwa $C(g)$ merupakan subgrup dari G. Jika g membangkitkan subgrup normal dari G, buktikan bahwa $C(g)$ normal dalam G.

Petunjuk. Andaikan $\langle g \rangle$ normal dalam G dan misalkan y suatu elemen sembarang dari G. Jika $x \in C(g)$, kita harus menunjukkan bahwa yxy^{-1} juga berada dalam $C(g)$. Tunjukkan bahwa $(yxy^{-1})g = g(yxy^{-1})$.

13. Ingat bahwa **pusat** suatu grup G adalah himpunan

$$Z(G) = \{x \in G : xg = gx \text{ untuk semua } g \in G\}.$$

(a) Hitung pusat S_3.

(b) Hitung pusat $GL_2(\mathbb{R})$.

(c) Tunjukkan bahwa pusat setiap grup G merupakan subgrup normal dari G.

(d) Jika $G/Z(G)$ siklik, tunjukkan bahwa G abelian.

14. Misalkan G suatu grup dan misalkan $G' = \langle aba^{-1}b^{-1} \rangle$; yaitu, G' merupakan subgrup yang terdiri atas semua hasil kali hingga elemen-elemen dalam G yang berbentuk $aba^{-1}b^{-1}$. Subgrup G' disebut **subgrup komutator** dari G.

(a) Tunjukkan bahwa G' merupakan subgrup normal dari G.

(b) Misalkan N suatu subgrup normal dari G. Buktikan bahwa G/N abelian jika dan hanya jika N memuat subgrup komutator dari G.

Petunjuk. (a) Misalkan $g \in G$ dan $h \in G'$. Jika $h = aba^{-1}b^{-1}$, maka

$$\begin{aligned} ghg^{-1} &= gaba^{-1}b^{-1}g^{-1} \\ &= (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \\ &= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}. \end{aligned}$$

Kita juga perlu menunjukkan bahwa jika $h = h_1 \cdots h_n$ dengan $h_i = a_i b_i a_i^{-1} b_i^{-1}$, maka ghg^{-1} merupakan hasil kali elemen-elemen berjenis sama. Namun, $ghg^{-1} = gh_1 \cdots h_n g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) \cdots (gh_ng^{-1})$.

11

Homomorfisma

Salah satu gagasan dasar dalam aljabar adalah konsep homomorfisma, yaitu perumuman alami dari isomorfisma. Jika syarat bahwa suatu isomorfisma grup harus bijektif dilonggarkan, kita memperoleh homomorfisma.

11.1 Homomorfisma Grup

Sebuah **homomorfisma** antara grup $(G, \cdot)$ dan $(H, \circ)$ adalah pemetaan $\phi : G \to H$ sedemikian sehingga

$$\phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2)$$

untuk $g_1, g_2 \in G$. Daerah hasil ϕ dalam H disebut **citra homomorfik** dari ϕ.

Dua grup memiliki hubungan sekuat mungkin apabila keduanya isomorfik; namun, dua grup juga dapat memiliki hubungan yang lebih lemah. Sebagai contoh, grup simetrik S_n dan grup $\mathbb{Z}_2$ berhubungan karena S_n dapat dibagi menjadi permutasi genap dan ganjil yang memperlihatkan struktur grup seperti $\mathbb{Z}_2$, sebagaimana ditunjukkan oleh tabel perkalian berikut.

	genap	ganjil
genap	genap	ganjil
ganjil	ganjil	genap

Kita menggunakan homomorfisma untuk mempelajari hubungan seperti yang baru saja dijelaskan.

Contoh 11.1.1 Misalkan G adalah grup dan $g \in G$. Definisikan pemetaan $\phi : \mathbb{Z} \to G$ dengan $\phi(n) = g^n$. Maka ϕ merupakan homomorfisma grup, karena

$$\phi(m + n) = g^{m+n} = g^m g^n = \phi(m)\phi(n).$$

Homomorfisma ini memetakan $\mathbb{Z}$ secara surjektif ke subgrup siklik dari G yang dibangkitkan oleh g. ▲

Contoh 11.1.2 Misalkan $G = GL_2(\mathbb{R})$. Jika

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

berada dalam G, maka determinannya tak nol; yaitu, $\det(A) = ad - bc \neq 0$. Selain itu, untuk sembarang dua elemen A dan B dalam G, $\det(AB) = \det(A)\det(B)$. Dengan menggunakan determinan, kita dapat mendefinisikan

homomorfisma $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ melalui $A \mapsto \det(A)$. ▲

Contoh 11.1.3 Ingat bahwa grup lingkaran $\mathbb{T}$ terdiri atas semua bilangan kompleks z sedemikian sehingga $|z| = 1$. Kita dapat mendefinisikan homomorfisma ϕ dari grup aditif bilangan real $\mathbb{R}$ ke $\mathbb{T}$ melalui $\phi : \theta \mapsto \cos\theta + i\sin\theta$. Memang,

$$\begin{aligned}\phi(\alpha+\beta) &= \cos(\alpha+\beta) + i\sin(\alpha+\beta)\\ &= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta + \cos\alpha\sin\beta)\\ &= (\cos\alpha + i\sin\alpha)(\cos\beta + i\sin\beta)\\ &= \phi(\alpha)\phi(\beta).\end{aligned}$$

Secara geometris, kita sekadar melilitkan garis real mengelilingi lingkaran dengan cara yang sesuai dengan teori grup. ▲

Proposisi berikut mencantumkan beberapa sifat dasar homomorfisma grup.

Proposisi 11.1.4 *Misalkan $\phi : G_1 \to G_2$ adalah homomorfisma grup. Maka*

1. *Jika e adalah identitas dalam G_1, maka $\phi(e)$ adalah identitas dalam G_2;*
2. *Untuk setiap elemen $g \in G_1$, $\phi(g^{-1}) = [\phi(g)]^{-1}$;*
3. *Jika H_1 adalah subgrup dari G_1, maka $\phi(H_1)$ adalah subgrup dari G_2;*
4. *Jika H_2 adalah subgrup dari G_2, maka $\phi^{-1}(H_2) = \{g \in G_1 : \phi(g) \in H_2\}$ adalah subgrup dari G_1. Lebih lanjut, jika H_2 normal dalam G_2, maka $\phi^{-1}(H_2)$ normal dalam G_1.*

Bukti. (1) Misalkan e dan e' masing-masing merupakan identitas dalam G_1 dan G_2; maka

$$e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e).$$

Berdasarkan hukum pencoretan, $\phi(e) = e'$.

(2) Pernyataan ini mengikuti fakta bahwa

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(e) = e'.$$

(3) Himpunan $\phi(H_1)$ tidak kosong karena identitas dalam G_2 berada dalam $\phi(H_1)$. Misalkan H_1 adalah subgrup dari G_1, dan ambil x serta y dalam $\phi(H_1)$. Terdapat elemen $a, b \in H_1$ sedemikian sehingga $\phi(a) = x$ dan $\phi(b) = y$. Karena

$$xy^{-1} = \phi(a)[\phi(b)]^{-1} = \phi(ab^{-1}) \in \phi(H_1),$$

$\phi(H_1)$ merupakan subgrup dari G_2 berdasarkan Proposisi 3.3.8.

(4) Misalkan H_2 adalah subgrup dari G_2 dan definisikan H_1 sebagai $\phi^{-1}(H_2)$; yaitu, H_1 merupakan himpunan semua $g \in G_1$ sedemikian sehingga $\phi(g) \in H_2$. Identitas berada dalam H_1 karena $\phi(e) = e'$. Jika a dan b berada dalam H_1, maka $\phi(ab^{-1}) = \phi(a)[\phi(b)]^{-1}$ berada dalam H_2 karena H_2 merupakan subgrup dari G_2. Oleh karena itu, $ab^{-1} \in H_1$ dan H_1 merupakan subgrup dari G_1. Jika H_2 normal dalam G_2, kita harus menunjukkan bahwa $g^{-1}hg \in H_1$ untuk $h \in H_1$ dan $g \in G_1$. Namun,

$$\phi(g^{-1}hg) = [\phi(g)]^{-1}\phi(h)\phi(g) \in H_2,$$

karena H_2 merupakan subgrup normal dari G_2. Oleh karena itu, $g^{-1}hg \in H_1$. ■

Misalkan $\phi : G \to H$ adalah homomorfisma grup dan e merupakan identitas dalam H. Berdasarkan Proposisi 11.1.4, $\phi^{-1}(\{e\})$ adalah subgrup dari G.

Subgrup ini disebut **kernel** dari ϕ dan dinotasikan dengan $\ker\phi$. Bahkan, subgrup ini merupakan subgrup normal dari G karena subgrup trivial normal dalam H. Hasil ini kita nyatakan dalam teorema berikut, yang mengatakan bahwa setiap homomorfisma grup secara alami dapat dikaitkan dengan sebuah subgrup normal.

Teorema 11.1.5 *Misalkan $\phi : G \to H$ adalah homomorfisma grup. Maka kernel ϕ merupakan subgrup normal dari G.*

Contoh 11.1.6 Perhatikan homomorfisma $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ yang didefinisikan oleh $A \mapsto \det(A)$. Karena 1 adalah identitas dalam $\mathbb{R}^*$, kernel homomorfisma ini terdiri atas semua matriks 2×2 yang determinannya satu. Dengan kata lain, $\ker\phi = SL_2(\mathbb{R})$. ▲

Contoh 11.1.7 Kernel homomorfisma grup $\phi : \mathbb{R} \to \mathbb{C}^*$ yang didefinisikan oleh $\phi(\theta) = \cos\theta + i\sin\theta$ adalah $\{2\pi n : n \in \mathbb{Z}\}$. Perhatikan bahwa $\ker\phi \cong \mathbb{Z}$. ▲

Contoh 11.1.8 Misalkan kita ingin menentukan semua kemungkinan homomorfisma ϕ dari $\mathbb{Z}_7$ ke $\mathbb{Z}_{12}$. Karena kernel ϕ harus merupakan subgrup dari $\mathbb{Z}_7$, hanya ada dua kemungkinan kernel, yaitu $\{0\}$ dan seluruh $\mathbb{Z}_7$. Citra suatu subgrup dari $\mathbb{Z}_7$ harus merupakan subgrup dari $\mathbb{Z}_{12}$. Oleh karena itu, tidak ada homomorfisma injektif; jika ada, $\mathbb{Z}_{12}$ akan memiliki subgrup berorde 7, padahal hal ini mustahil. Akibatnya, satu-satunya homomorfisma yang mungkin dari $\mathbb{Z}_7$ ke $\mathbb{Z}_{12}$ adalah homomorfisma yang memetakan semua elemen ke nol. ▲

Contoh 11.1.9 Misalkan G adalah grup. Misalkan $g \in G$ dan ϕ adalah homomorfisma dari $\mathbb{Z}$ ke G yang diberikan oleh $\phi(n) = g^n$. Jika orde g tak berhingga, maka kernel homomorfisma ini adalah $\{0\}$ karena ϕ memetakan $\mathbb{Z}$ secara surjektif ke subgrup siklik dari G yang dibangkitkan oleh g. Namun, jika orde g berhingga, misalkan n, maka kernel ϕ adalah $n\mathbb{Z}$. ▲

11.2 Teorema-Teorema Isomorfisma

Walaupun pada awalnya tidak tampak jelas, grup hasil bagi bersesuaian tepat dengan citra homomorfik, dan kita dapat menggunakan grup hasil bagi untuk mempelajari homomorfisma. Kita telah mengetahui bahwa pada setiap homomorfisma grup $\phi : G \to H$ kita dapat mengaitkan subgrup normal dari G, yaitu $\ker\phi$. Kebalikannya juga benar; yaitu, setiap subgrup normal dari suatu grup G menghasilkan homomorfisma grup.

Misalkan H adalah subgrup normal dari G. Definisikan **homomorfisma alami** atau **homomorfisma kanonik**

$$\phi : G \to G/H$$

melalui

$$\phi(g) = gH.$$

Pemetaan ini memang merupakan homomorfisma, karena

$$\phi(g_1g_2) = g_1g_2H = g_1Hg_2H = \phi(g_1)\phi(g_2).$$

Kernel homomorfisma ini adalah H. Teorema-teorema berikut menjelaskan hubungan antara homomorfisma grup, subgrup normal, dan grup hasil bagi.

Teorema 11.2.1 Teorema Isomorfisma Pertama. *Jika $\psi : G \to H$ adalah homomorfisma grup dengan $K = \ker\psi$, maka K normal dalam G. Misalkan $\phi : G \to G/K$ adalah homomorfisma kanonik. Maka terdapat tepat*

satu isomorfisma $\eta : G/K \to \psi(G)$ sedemikian sehingga $\psi = \eta\phi$.

BUKTI. Kita telah mengetahui bahwa K normal dalam G. Definisikan $\eta : G/K \to \psi(G)$ melalui $\eta(gK) = \psi(g)$. Pertama-tama, kita tunjukkan bahwa η terdefinisi dengan baik. Jika $g_1K = g_2K$, maka untuk suatu $k \in K$, $g_1k = g_2$; akibatnya,

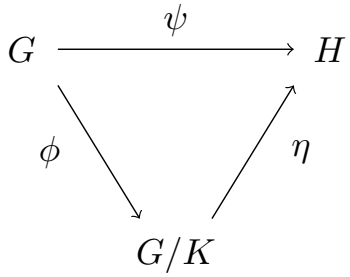
$$\eta(g_1K) = \psi(g_1) = \psi(g_1)\psi(k) = \psi(g_1k) = \psi(g_2) = \eta(g_2K).$$

Jadi, η tidak bergantung pada pemilihan wakil koset, dan pemetaan $\eta : G/K \to \psi(G)$ terdefinisi secara unik karena $\psi = \eta\phi$. Kita juga harus menunjukkan bahwa η merupakan homomorfisma. Memang,

$$\begin{aligned}\eta(g_1Kg_2K) &= \eta(g_1g_2K)\\ &= \psi(g_1g_2)\\ &= \psi(g_1)\psi(g_2)\\ &= \eta(g_1K)\eta(g_2K).\end{aligned}$$

Jelas bahwa η memetakan secara surjektif ke $\psi(G)$. Untuk menunjukkan bahwa η injektif, misalkan $\eta(g_1K) = \eta(g_2K)$. Maka $\psi(g_1) = \psi(g_2)$. Ini menyiratkan $\psi(g_1^{-1}g_2) = e$, atau $g_1^{-1}g_2$ berada dalam kernel ψ; oleh karena itu, $g_1^{-1}g_2K = K$; yaitu, $g_1K = g_2K$. ■

Matematikawan sering menggunakan diagram yang disebut **diagram komutatif** untuk menjelaskan teorema semacam ini. Diagram berikut "komutatif" karena $\psi = \eta\phi$.



Contoh 11.2.2 Misalkan G adalah grup siklik dengan pembangkit g. Definisikan pemetaan $\phi : \mathbb{Z} \to G$ melalui $n \mapsto g^n$. Pemetaan ini merupakan homomorfisma surjektif karena

$$\phi(m+n) = g^{m+n} = g^m g^n = \phi(m)\phi(n).$$

Jelas bahwa ϕ surjektif. Jika $|g| = m$, maka $g^m = e$. Oleh karena itu, $\ker\phi = m\mathbb{Z}$ dan $\mathbb{Z}/\ker\phi = \mathbb{Z}/m\mathbb{Z} \cong G$. Sebaliknya, jika orde g tak berhingga, maka $\ker\phi = 0$ dan ϕ merupakan isomorfisma antara G dan $\mathbb{Z}$. Jadi, dua grup siklik isomorfik tepat ketika keduanya memiliki orde yang sama. Hingga isomorfisma, grup siklik yang ada hanyalah $\mathbb{Z}$ dan $\mathbb{Z}_n$. ▲

Teorema 11.2.3 Teorema Isomorfisma Kedua. *Misalkan H adalah subgrup dari grup G (tidak harus normal dalam G) dan N adalah subgrup normal dari G. Maka HN merupakan subgrup dari G, $H \cap N$ merupakan subgrup normal dari H, dan*

$$H/H \cap N \cong HN/N.$$

BUKTI. Pertama-tama, kita tunjukkan bahwa $HN = \{hn : h \in H, n \in N\}$ merupakan subgrup dari G. Misalkan $h_1n_1, h_2n_2 \in HN$. Karena N normal,

$(h_2)^{-1}n_1h_2 \in N$. Jadi,

$$(h_1n_1)(h_2n_2) = h_1h_2((h_2)^{-1}n_1h_2)n_2$$

berada dalam HN. Invers dari $hn \in HN$ berada dalam HN karena

$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1}).$$

Selanjutnya, kita buktikan bahwa $H \cap N$ normal dalam H. Misalkan $h \in H$ dan $n \in H \cap N$. Maka $h^{-1}nh \in H$ karena setiap elemennya berada dalam H. Selain itu, $h^{-1}nh \in N$ karena N normal dalam G; oleh karena itu, $h^{-1}nh \in H \cap N$.

Sekarang definisikan pemetaan ϕ dari H ke HN/N melalui $h \mapsto hN$. Pemetaan ϕ surjektif, karena setiap koset $hnN = hN$ merupakan citra dari h dalam H. Kita juga mengetahui bahwa ϕ merupakan homomorfisma karena

$$\phi(hh') = hh'N = hNh'N = \phi(h)\phi(h').$$

Berdasarkan Teorema Isomorfisma Pertama, citra ϕ isomorfik dengan $H/\ker\phi$; yaitu,

$$HN/N = \phi(H) \cong H/\ker\phi.$$

Karena

$$\ker\phi = \{h \in H : h \in N\} = H \cap N,$$

$HN/N = \phi(H) \cong H/H \cap N$. ■

Teorema 11.2.4 Teorema Korespondensi. *Misalkan N adalah subgrup normal dari grup G. Maka $H \mapsto H/N$ merupakan korespondensi satu-satu antara himpunan subgrup H dari G yang memuat N dan himpunan subgrup dari G/N. Lebih lanjut, subgrup normal dari G yang memuat N bersesuaian dengan subgrup normal dari G/N.*

Bukti. Misalkan H adalah subgrup dari G yang memuat N. Karena N normal dalam H, maka H/N merupakan grup hasil bagi. Misalkan aN dan bN adalah elemen dari H/N. Maka $(aN)(b^{-1}N) = ab^{-1}N \in H/N$; oleh karena itu, H/N merupakan subgrup dari G/N.

Misalkan S adalah subgrup dari G/N. Subgrup ini merupakan himpunan koset dari N. Jika $H = \{g \in G : gN \in S\}$, maka untuk $h_1, h_2 \in H$, berlaku $(h_1N)(h_2N) = h_1h_2N \in S$ dan $h_1^{-1}N \in S$. Oleh karena itu, H harus merupakan subgrup dari G. Jelas bahwa H memuat N. Jadi, $S = H/N$. Akibatnya, pemetaan $H \mapsto H/N$ bersifat surjektif.

Misalkan H_1 dan H_2 adalah subgrup dari G yang memuat N sedemikian sehingga $H_1/N = H_2/N$. Jika $h_1 \in H_1$, maka $h_1N \in H_1/N$. Jadi, $h_1N = h_2N \subset H_2$ untuk suatu h_2 dalam H_2. Namun, karena N termuat dalam H_2, kita mengetahui bahwa $h_1 \in H_2$ atau $H_1 \subset H_2$. Dengan cara yang sama, $H_2 \subset H_1$. Karena $H_1 = H_2$, pemetaan $H \mapsto H/N$ bersifat injektif.

Misalkan H normal dalam G dan N adalah subgrup dari H. Mudah diverifikasi bahwa pemetaan $G/N \to G/H$ yang didefinisikan oleh $gN \mapsto gH$ merupakan homomorfisma. Kernel homomorfisma ini adalah H/N, yang membuktikan bahwa H/N normal dalam G/N.

Sebaliknya, misalkan H/N normal dalam G/N. Homomorfisma yang diberikan oleh

$$G \to G/N \to \frac{G/N}{H/N}$$

memiliki kernel H. Oleh karena itu, H harus normal dalam G. ■

Perhatikan bahwa selama membuktikan Teorema 11.2.4, kita juga telah

membuktikan teorema berikut.

Teorema 11.2.5 Teorema Isomorfisma Ketiga. *Misalkan G adalah grup dan N serta H adalah subgrup normal dari G dengan $N \subset H$. Maka*

$$G/H \cong \frac{G/N}{H/N}.$$

Contoh 11.2.6 Berdasarkan Teorema Isomorfisma Ketiga,

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/mn\mathbb{Z})/(m\mathbb{Z}/mn\mathbb{Z}).$$

Karena $|\mathbb{Z}/mn\mathbb{Z}| = mn$ dan $|\mathbb{Z}/m\mathbb{Z}| = m$, kita memperoleh $|m\mathbb{Z}/mn\mathbb{Z}| = n$. ▲

11.3 Pertanyaan Bacaan

1. Perhatikan fungsi $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ yang didefinisikan oleh $\phi(x) = x + x$. Buktikan bahwa ϕ merupakan homomorfisma grup.

2. Untuk ϕ yang didefinisikan pada pertanyaan sebelumnya, jelaskan mengapa ϕ bukan isomorfisma grup.

3. Bandingkan persamaan dan perbedaan antara isomorfisma dan homomorfisma.

4. Parafrasekan Teorema Isomorfisma Pertama dengan menggunakan *kata-kata saja. Sama sekali* tidak boleh menggunakan simbol.

5. "Untuk setiap subgrup normal terdapat suatu homomorfisma, dan untuk setiap homomorfisma terdapat suatu subgrup normal." Jelaskan dasar (yang tepat) bagi pernyataan (yang samar) ini.

11.4 Latihan

1. Buktikan bahwa $\det(AB) = \det(A)\det(B)$ untuk $A, B \in GL_2(\mathbb{R})$. Hal ini menunjukkan bahwa determinan merupakan homomorfisma dari $GL_2(\mathbb{R})$ ke $\mathbb{R}^*$.

2. Manakah di antara pemetaan berikut yang merupakan homomorfisma? Jika pemetaannya merupakan homomorfisma, apakah kernelnya?

(a) $\phi : \mathbb{R}^* \to GL_2(\mathbb{R})$ yang didefinisikan oleh

$$\phi(a) = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$$

(b) $\phi : \mathbb{R} \to GL_2(\mathbb{R})$ yang didefinisikan oleh

$$\phi(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$

(c) $\phi : GL_2(\mathbb{R}) \to \mathbb{R}$ yang didefinisikan oleh

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a + d$$

(d) $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ yang didefinisikan oleh

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = ad - bc$$

(e) $\phi : \mathbb{M}_2(\mathbb{R}) \to \mathbb{R}$ yang didefinisikan oleh

$$\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = b,$$

dengan $\mathbb{M}_2(\mathbb{R})$ sebagai grup aditif dari matriks 2×2 yang entri-entrinya berada dalam $\mathbb{R}$.

Petunjuk. (a) merupakan homomorfisma dengan kernel $\{1\}$; (c) bukan homomorfisma.

3. Misalkan A adalah matriks $m \times n$. Tunjukkan bahwa perkalian matriks, $x \mapsto Ax$, mendefinisikan homomorfisma $\phi : \mathbb{R}^n \to \mathbb{R}^m$.

4. Misalkan $\phi : \mathbb{Z} \to \mathbb{Z}$ diberikan oleh $\phi(n) = 7n$. Buktikan bahwa ϕ merupakan homomorfisma grup. Carilah kernel dan citra ϕ.

Petunjuk. Karena $\phi(m+n) = 7(m+n) = 7m + 7n = \phi(m) + \phi(n)$, ϕ merupakan homomorfisma.

5. Jelaskan semua homomorfisma dari $\mathbb{Z}_{24}$ ke $\mathbb{Z}_{18}$.

Petunjuk. Untuk setiap homomorfisma $\phi : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$, kernel ϕ harus merupakan subgrup dari $\mathbb{Z}_{24}$ dan citra ϕ harus merupakan subgrup dari $\mathbb{Z}_{18}$. Sekarang gunakan fakta bahwa suatu pembangkit harus dipetakan ke pembangkit.

6. Jelaskan semua homomorfisma dari $\mathbb{Z}$ ke $\mathbb{Z}_{12}$.

7. Dalam grup $\mathbb{Z}_{24}$, ambil $H = \langle 4 \rangle$ dan $N = \langle 6 \rangle$.

(a) Daftarkan elemen-elemen dalam HN (untuk grup aditif ini, kita biasanya menulis $H + N$) dan $H \cap N$.

(b) Daftarkan koset-koset dalam HN/N, beserta elemen-elemen dalam setiap koset.

(c) Daftarkan koset-koset dalam $H/(H \cap N)$, beserta elemen-elemen dalam setiap koset.

(d) Berikan korespondensi antara HN/N dan $H/(H \cap N)$ yang dijelaskan dalam pembuktian Teorema Isomorfisma Kedua.

8. Jika G adalah grup abelian dan $n \in \mathbb{N}$, tunjukkan bahwa $\phi : G \to G$ yang didefinisikan oleh $g \mapsto g^n$ merupakan homomorfisma grup.

9. Jika $\phi : G \to H$ merupakan homomorfisma grup dan G abelian, buktikan bahwa $\phi(G)$ juga abelian.

Petunjuk. Misalkan $a, b \in G$. Maka $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$.

10. Jika $\phi : G \to H$ merupakan homomorfisma grup dan G siklik, buktikan bahwa $\phi(G)$ juga siklik.

11. Tunjukkan bahwa homomorfisma yang didefinisikan pada grup siklik sepenuhnya ditentukan oleh tindakannya pada pembangkit grup tersebut.

12. Jika grup G memiliki tepat satu subgrup H berorde k, buktikan bahwa H normal dalam G.

13. Buktikan atau sangkal: $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}$.

14. Misalkan G adalah grup berhingga dan N merupakan subgrup normal dari G. Jika H adalah subgrup dari G/N, buktikan bahwa $\phi^{-1}(H)$ merupakan subgrup dalam G yang berorde $|H| \cdot |N|$, dengan $\phi : G \to G/N$ sebagai homomorfisma kanonik.

15. Misalkan G_1 dan G_2 adalah grup, dan H_1 serta H_2 masing-masing merupakan subgrup normal dari G_1 dan G_2. Misalkan $\phi : G_1 \to G_2$ adalah homomorfisma. Tunjukkan bahwa ϕ menginduksi homomorfisma $\overline{\phi} : (G_1/H_1) \to (G_2/H_2)$ jika $\phi(H_1) \subset H_2$.

16. Jika H dan K merupakan subgrup normal dari G dan $H \cap K = \{e\}$, buktikan bahwa G isomorfik dengan suatu subgrup dari $G/H \times G/K$.

17. Misalkan $\phi : G_1 \to G_2$ adalah homomorfisma grup surjektif. Misalkan H_1 merupakan subgrup normal dari G_1 dan anggap bahwa $\phi(H_1) = H_2$. Buktikan atau sangkal bahwa $G_1/H_1 \cong G_2/H_2$.

Petunjuk. Carilah contoh penyangkal.

18. Misalkan $\phi : G \to H$ adalah homomorfisma grup. Tunjukkan bahwa ϕ injektif jika dan hanya jika $\phi^{-1}(e) = \{e\}$.

19. Diberikan homomorfisma $\phi : G \to H$, definisikan relasi $\sim$ pada G melalui $a \sim b$ jika $\phi(a) = \phi(b)$ untuk $a, b \in G$. Tunjukkan bahwa relasi ini merupakan relasi ekuivalensi dan jelaskan kelas-kelas ekuivalensinya.

11.5 Latihan Tambahan: Automorfisme

1. Misalkan $\mathrm{Aut}(G)$ adalah himpunan semua automorfisme dari G; yaitu, isomorfisma dari G ke dirinya sendiri. Buktikan bahwa himpunan ini membentuk grup dan merupakan subgrup dari grup permutasi pada G; yaitu, $\mathrm{Aut}(G) \leq S_G$.

2. Sebuah **automorfisme dalam** dari G,

$$i_g : G \to G,$$

didefinisikan oleh pemetaan

$$i_g(x) = gxg^{-1},$$

untuk $g \in G$. Tunjukkan bahwa $i_g \in \mathrm{Aut}(G)$.

3. Himpunan semua automorfisme dalam dinotasikan dengan $\mathrm{Inn}(G)$. Tunjukkan bahwa $\mathrm{Inn}(G)$ merupakan subgrup dari $\mathrm{Aut}(G)$.

4. Carilah automorfisme dari suatu grup G yang bukan automorfisme dalam.

5. Misalkan G adalah grup dan i_g merupakan automorfisme dalam dari G, lalu definisikan pemetaan

$$G \to \mathrm{Aut}(G)$$

melalui

$$g \mapsto i_g.$$

Buktikan bahwa pemetaan ini merupakan homomorfisma dengan citra $\mathrm{Inn}(G)$ dan kernel $Z(G)$. Gunakan hasil ini untuk menyimpulkan bahwa

$$G/Z(G) \cong \mathrm{Inn}(G).$$

6. Hitung $\mathrm{Aut}(S_3)$ dan $\mathrm{Inn}(S_3)$. Lakukan hal yang sama untuk D_4.

7. Carilah semua homomorfisma $\phi : \mathbb{Z} \to \mathbb{Z}$. Apakah $\mathrm{Aut}(\mathbb{Z})$?

8. Carilah semua automorfisme dari $\mathbb{Z}_8$. Buktikan bahwa $\mathrm{Aut}(\mathbb{Z}_8) \cong U(8)$.

9. Untuk $k \in \mathbb{Z}_n$, definisikan pemetaan $\phi_k : \mathbb{Z}_n \to \mathbb{Z}_n$ melalui $a \mapsto ka$. Buktikan bahwa ϕ_k merupakan homomorfisma.

10. Buktikan bahwa ϕ_k merupakan isomorfisma jika dan hanya jika k adalah pembangkit dari $\mathbb{Z}_n$.

11. Tunjukkan bahwa setiap automorfisme dari $\mathbb{Z}_n$ berbentuk ϕ_k, dengan k sebagai pembangkit dari $\mathbb{Z}_n$.

12. Buktikan bahwa $\psi : U(n) \to \text{Aut}(\mathbb{Z}_n)$ merupakan isomorfisma, dengan $\psi : k \mapsto \phi_k$.

12

Grup Matriks dan Simetri

Ketika Felix Klein (1849–1925) menerima jabatan profesor di Universitas Erlangen, dalam pidato pelantikannya ia menguraikan suatu program untuk mengklasifikasikan berbagai geometri. Teori grup merupakan inti program Klein: ia memandang geometri sebagai kajian tentang sifat-sifat yang tetap invarian di bawah grup transformasi. Grup, khususnya grup matriks, kini menjadi penting dalam kajian simetri dan telah diterapkan dalam bidang seperti kimia dan fisika. Pada bagian pertama bab ini, kita akan memeriksa beberapa grup matriks klasik, seperti grup linear umum, grup linear khusus, dan grup ortogonal. Selanjutnya, kita akan menggunakan grup-grup matriks tersebut untuk menyelidiki beberapa gagasan yang mendasari simetri geometris.

12.1 Grup Matriks

12.1.1 Beberapa Fakta dari Aljabar Linear

Sebelum mempelajari grup matriks, kita perlu mengingat kembali beberapa fakta dasar dari aljabar linear. Salah satu gagasan paling mendasar dalam aljabar linear ialah transformasi linear. Suatu **transformasi linear** atau **pemetaan linear** $T : \mathbb{R}^n \to \mathbb{R}^m$ adalah pemetaan yang mempertahankan penjumlahan vektor dan perkalian skalar; yaitu, untuk vektor $\mathbf{x}$ dan $\mathbf{y}$ dalam $\mathbb{R}^n$ serta skalar $\alpha \in \mathbb{R}$,

$$\begin{aligned} T(\mathbf{x}+\mathbf{y}) &= T(\mathbf{x}) + T(\mathbf{y}) \\ T(\alpha\mathbf{y}) &= \alpha T(\mathbf{y}). \end{aligned}$$

Suatu matriks $m \times n$ dengan entri dalam $\mathbb{R}$ merepresentasikan transformasi linear dari $\mathbb{R}^n$ ke $\mathbb{R}^m$. Jika vektor $\mathbf{x} = (x_1, \ldots, x_n)^{\mathrm{t}}$ dan $\mathbf{y} = (y_1, \ldots, y_n)^{\mathrm{t}}$ dalam $\mathbb{R}^n$ kita tuliskan sebagai matriks kolom, maka matriks $m \times n$

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

memetakan vektor-vektor tersebut secara linear ke $\mathbb{R}^m$ melalui perkalian matriks. Perhatikan bahwa jika α suatu bilangan real,

$$A(\mathbf{x}+\mathbf{y}) = A\mathbf{x} + A\mathbf{y} \qquad \text{dan} \qquad \alpha A\mathbf{x} = A(\alpha\mathbf{x}),$$

dengan

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Kita akan sering menyingkat matriks A dengan menuliskan (a_{ij}).

Sebaliknya, jika $T : \mathbb{R}^n \to \mathbb{R}^m$ suatu pemetaan linear, kita dapat mengaitkan suatu matriks A dengan T dengan memperhatikan tindakan T pada vektor-vektor

$$\begin{aligned} \mathbf{e}_1 &= (1, 0, \ldots, 0)^{\mathrm{t}} \\ \mathbf{e}_2 &= (0, 1, \ldots, 0)^{\mathrm{t}} \\ &\vdots \\ \mathbf{e}_n &= (0, 0, \ldots, 1)^{\mathrm{t}}. \end{aligned}$$

Setiap vektor $\mathbf{x} = (x_1, \ldots, x_n)^{\mathrm{t}}$ dapat kita tuliskan sebagai

$$x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \cdots + x_n\mathbf{e}_n.$$

Akibatnya, jika

$$\begin{aligned} T(\mathbf{e}_1) &= (a_{11}, a_{21}, \ldots, a_{m1})^{\mathrm{t}}, \\ T(\mathbf{e}_2) &= (a_{12}, a_{22}, \ldots, a_{m2})^{\mathrm{t}}, \\ &\vdots \\ T(\mathbf{e}_n) &= (a_{1n}, a_{2n}, \ldots, a_{mn})^{\mathrm{t}}, \end{aligned}$$

maka

$$\begin{aligned} T(\mathbf{x}) &= T(x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \cdots + x_n\mathbf{e}_n) \\ &= x_1T(\mathbf{e}_1) + x_2T(\mathbf{e}_2) + \cdots + x_nT(\mathbf{e}_n) \\ &= \left(\sum_{k=1}^{n} a_{1k}x_k, \ldots, \sum_{k=1}^{n} a_{mk}x_k \right)^{\mathrm{t}} \\ &= A\mathbf{x}. \end{aligned}$$

Contoh 12.1.1 Jika $T : \mathbb{R}^2 \to \mathbb{R}^2$ kita tetapkan sebagai pemetaan yang diberikan oleh

$$T(x_1, x_2) = (2x_1 + 5x_2, -4x_1 + 3x_2),$$

aksioma-aksioma yang harus dipenuhi T agar menjadi transformasi linear dapat diverifikasi dengan mudah. Vektor kolom $T\mathbf{e}_1 = (2, -4)^{\mathrm{t}}$ dan $T\mathbf{e}_2 = (5, 3)^{\mathrm{t}}$ menunjukkan bahwa T diberikan oleh matriks

$$A = \begin{pmatrix} 2 & 5 \\ -4 & 3 \end{pmatrix}.$$

▲

Karena kita tertarik pada grup matriks, kita perlu mengetahui matriks mana yang mempunyai invers perkalian. Ingat bahwa matriks $n \times n$ A disebut **dapat dibalik** tepat ketika terdapat matriks lain A^{-1} sedemikian sehingga

$AA^{-1} = A^{-1}A = I$, dengan

$$I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

merupakan matriks identitas $n \times n$. Dari aljabar linear, kita mengetahui bahwa A dapat dibalik jika dan hanya jika determinan A tidak nol. Matriks yang dapat dibalik kadang-kadang disebut **nonsingular**.

Contoh 12.1.2 Jika A adalah matriks

$$\begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix},$$

maka invers A adalah

$$A^{-1} = \begin{pmatrix} 3 & -1 \\ -5 & 2 \end{pmatrix}.$$

Keberadaan A^{-1} terjamin karena $\det(A) = 2 \cdot 3 - 5 \cdot 1 = 1$ tidak nol. ▲

Beberapa fakta lain mengenai determinan juga akan berguna dalam bab ini. Misalkan A dan B matriks $n \times n$. Dari aljabar linear, kita memperoleh sifat-sifat determinan berikut.

- Determinan merupakan homomorfisma ke grup perkalian bilangan real; yaitu, $\det(AB) = (\det A)(\det B)$.
- Jika A merupakan matriks yang dapat dibalik, maka $\det(A^{-1}) = 1/\det A$.
- Jika transpos dari matriks $A = (a_{ij})$ kita definisikan sebagai $A^{\mathrm{t}} = (a_{ji})$, maka $\det(A^{\mathrm{t}}) = \det A$.
- Misalkan T transformasi linear yang berkaitan dengan matriks $n \times n$ A. Maka T mengalikan volume dengan faktor $|\det A|$. Dalam kasus $\mathbb{R}^2$, ini berarti bahwa T mengalikan luas dengan $|\det A|$.

Pemetaan linear, matriks, dan determinan dibahas dalam setiap buku teks aljabar linear elementer; akan tetapi, jika Anda belum pernah mengikuti mata kuliah aljabar linear, sifat-sifat ini dapat diverifikasi secara langsung dengan mudah untuk matriks 2×2, yaitu kasus yang paling kita perhatikan.

12.1.2 Grup Linear Umum dan Grup Linear Khusus

Himpunan semua matriks $n \times n$ yang dapat dibalik membentuk suatu grup yang disebut **grup linear umum**. Kita akan menyatakan grup ini dengan $GL_n(\mathbb{R})$. Grup linear umum memiliki beberapa subgrup penting. Sifat perkalian determinan menyiratkan bahwa himpunan matriks berdeterminan satu merupakan subgrup dari grup linear umum. Dengan kata lain, andaikan $\det(A) = 1$ dan $\det(B) = 1$. Maka $\det(AB) = \det(A)\det(B) = 1$ dan $\det(A^{-1}) = 1/\det A = 1$. Subgrup ini disebut **grup linear khusus** dan dinyatakan dengan $SL_n(\mathbb{R})$.

Contoh 12.1.3 Diberikan suatu matriks 2×2

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

determinan A adalah $ad - bc$. Grup $GL_2(\mathbb{R})$ terdiri atas matriks-matriks yang memenuhi $ad - bc \neq 0$. Invers A adalah

$$A^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

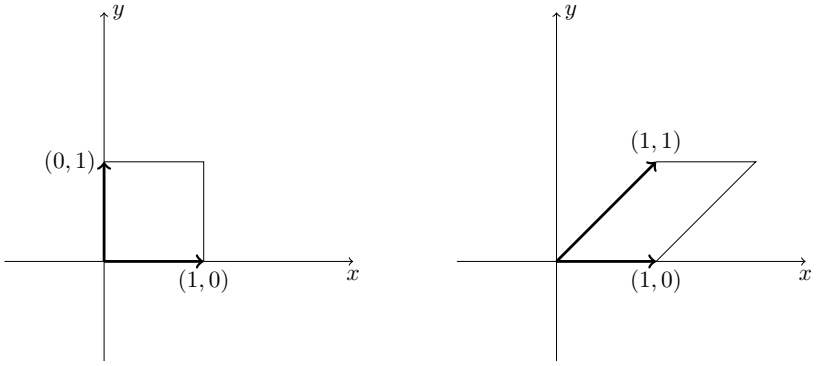
Jika A berada dalam $SL_2(\mathbb{R})$, maka

$$A^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Secara geometris, $SL_2(\mathbb{R})$ merupakan grup yang mempertahankan luas jajar genjang. Misalkan

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

berada dalam $SL_2(\mathbb{R})$. Dalam Gambar 12.1.4, persegi satuan yang bersesuaian dengan vektor $\mathbf{x} = (1,0)^t$ dan $\mathbf{y} = (0,1)^t$ dipetakan oleh A ke jajar genjang dengan sisi $(1,0)^t$ dan $(1,1)^t$; yaitu, $A\mathbf{x} = (1,0)^t$ dan $A\mathbf{y} = (1,1)^t$. Perhatikan bahwa kedua jajar genjang ini mempunyai luas yang sama. ▲



Gambar 12.1.4 Tindakan $SL_2(\mathbb{R})$ pada persegi satuan

12.1.3 Grup Ortogonal $O(n)$

Subgrup lain dari $GL_n(\mathbb{R})$ ialah grup ortogonal. Suatu matriks A disebut **ortogonal** jika $A^{-1} = A^t$. **Grup ortogonal** terdiri atas himpunan semua matriks ortogonal. Kita menuliskan $O(n)$ untuk grup ortogonal $n \times n$. Pembuktian bahwa $O(n)$ merupakan subgrup dari $GL_n(\mathbb{R})$ diserahkan sebagai latihan.

Contoh 12.1.5 Matriks-matriks berikut bersifat ortogonal:

$$\begin{pmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{pmatrix}, \quad \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}, \quad \begin{pmatrix} -1/\sqrt{2} & 0 & 1/\sqrt{2} \\ 1/\sqrt{6} & -2/\sqrt{6} & 1/\sqrt{6} \\ 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \end{pmatrix}.$$

▲

Terdapat cara yang lebih geometris untuk memandang grup $O(n)$. Matriks ortogonal tepat merupakan matriks yang mempertahankan panjang vektor. Kita dapat mendefinisikan panjang vektor dengan menggunakan **hasil kali dalam Euklides**, atau **hasil kali titik**, dari dua vektor. Hasil kali dalam

Euklides dari dua vektor $\mathbf{x} = (x_1, \ldots, x_n)^{\mathrm{t}}$ dan $\mathbf{y} = (y_1, \ldots, y_n)^{\mathrm{t}}$ adalah

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^{\mathrm{t}}\mathbf{y} = (x_1, x_2, \ldots, x_n) \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = x_1 y_1 + \cdots + x_n y_n.$$

Panjang vektor $\mathbf{x} = (x_1, \ldots, x_n)^{\mathrm{t}}$ kita definisikan sebagai

$$\|\mathbf{x}\| = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle} = \sqrt{x_1^2 + \cdots + x_n^2}.$$

Gagasan jarak antara dua vektor berkaitan dengan konsep panjang vektor. Kita mendefinisikan **jarak** antara dua vektor $\mathbf{x}$ dan $\mathbf{y}$ sebagai $\|\mathbf{x} - \mathbf{y}\|$. Pembuktian proposisi berikut mengenai sifat hasil kali dalam Euklides diserahkan sebagai latihan.

Proposisi 12.1.6 *Misalkan* $\mathbf{x}$, $\mathbf{y}$, *dan* $\mathbf{w}$ *vektor-vektor dalam* $\mathbb{R}^n$, *serta* $\alpha \in \mathbb{R}$. *Maka*

1. $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$.
2. $\langle \mathbf{x}, \mathbf{y} + \mathbf{w} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{x}, \mathbf{w} \rangle$.
3. $\langle \alpha\mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{x}, \alpha\mathbf{y} \rangle = \alpha \langle \mathbf{x}, \mathbf{y} \rangle$.
4. $\langle \mathbf{x}, \mathbf{x} \rangle \geq 0$, *dengan kesamaan tepat ketika* $\mathbf{x} = 0$.
5. *Jika* $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ *untuk semua* $\mathbf{x}$ *dalam* $\mathbb{R}^n$, *maka* $\mathbf{y} = 0$.

Contoh 12.1.7 Vektor $\mathbf{x} = (3, 4)^{\mathrm{t}}$ mempunyai panjang $\sqrt{3^2 + 4^2} = 5$. Kita juga dapat melihat bahwa matriks ortogonal

$$A = \begin{pmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{pmatrix}$$

mempertahankan panjang vektor tersebut. Vektor $A\mathbf{x} = (-7/5, 24/5)^{\mathrm{t}}$ juga mempunyai panjang 5. ▲

Karena $\det(AA^{\mathrm{t}}) = \det(I) = 1$ dan $\det(A) = \det(A^{\mathrm{t}})$, determinan setiap matriks ortogonal bernilai 1 atau -1. Perhatikan vektor-vektor kolom

$$\mathbf{a}_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix}$$

dari matriks ortogonal $A = (a_{ij})$. Karena $AA^{\mathrm{t}} = I$, $\langle \mathbf{a}_r, \mathbf{a}_s \rangle = \delta_{rs}$, dengan

$$\delta_{rs} = \begin{cases} 1 & r = s \\ 0 & r \neq s \end{cases}$$

merupakan delta Kronecker. Dengan demikian, semua vektor kolom suatu matriks ortogonal mempunyai panjang 1; dan hasil kali dalam Euklides dari vektor-vektor kolom yang berbeda bernilai nol. Setiap himpunan vektor yang memenuhi sifat-sifat ini disebut **himpunan ortonormal**. Sebaliknya, jika diberikan matriks $n \times n$ A yang kolom-kolomnya membentuk himpunan ortonormal, maka $A^{-1} = A^{\mathrm{t}}$.

Suatu matriks A disebut **mempertahankan jarak**, **mempertahankan panjang**, atau **mempertahankan hasil kali dalam** apabila $\|A\mathbf{x} - A\mathbf{y}\| = \|\mathbf{x} - \mathbf{y}\|$, $\|A\mathbf{x}\| = \|\mathbf{x}\|$, atau $\langle A\mathbf{x}, A\mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{y}\rangle$, secara berturut-turut. Teorema berikut, yang mengarakterisasi grup ortogonal, menyatakan bahwa gagasan-gagasan tersebut ekuivalen.

Teorema 12.1.8 *Misalkan A suatu matriks $n \times n$. Pernyataan-pernyataan berikut ekuivalen.*

1. *Kolom-kolom matriks A membentuk suatu himpunan ortonormal.*
2. $A^{-1} = A^t$.
3. *Untuk vektor $\mathbf{x}$ dan $\mathbf{y}$, $\langle A\mathbf{x}, A\mathbf{y}\rangle = \langle \mathbf{x}, \mathbf{y}\rangle$.*
4. *Untuk vektor $\mathbf{x}$ dan $\mathbf{y}$, $\|A\mathbf{x} - A\mathbf{y}\| = \|\mathbf{x} - \mathbf{y}\|$.*
5. *Untuk setiap vektor $\mathbf{x}$, $\|A\mathbf{x}\| = \|\mathbf{x}\|$.*

Bukti. Kita telah menunjukkan bahwa (1) dan (2) ekuivalen.
(2) $\Rightarrow$ (3).

$$\begin{aligned}\langle A\mathbf{x}, A\mathbf{y}\rangle &= (A\mathbf{x})^{\mathrm{t}} A\mathbf{y} \\ &= \mathbf{x}^{\mathrm{t}} A^{\mathrm{t}} A\mathbf{y} \\ &= \mathbf{x}^{\mathrm{t}}\mathbf{y} \\ &= \langle \mathbf{x}, \mathbf{y}\rangle.\end{aligned}$$

(3) $\Rightarrow$ (2). Pertama-tama, $\langle A\mathbf{x}, A\mathbf{y}\rangle = (A\mathbf{x})^{\mathrm{t}} A\mathbf{y} = \mathbf{x}^{\mathrm{t}} A^{\mathrm{t}} A\mathbf{y} = \mathbf{x}^{\mathrm{t}}\mathbf{y}$. Jika M suatu matriks $n \times n$ sembarang, maka $\mathbf{e}_i^{\mathrm{t}} M \mathbf{e}_j^{\mathrm{t}} = M_{ij}$, dengan M_{ij} merupakan entri ke-ij dari matriks M. Dengan memperhatikan bahwa $\mathbf{x}^{\mathrm{t}} A^{\mathrm{t}} A\mathbf{y} = \mathbf{x}^{\mathrm{t}}\mathbf{y}$, misalkan $\mathbf{x} = \mathbf{e}_i$ dan $\mathbf{y} = \mathbf{e}_j$. Maka

$$\mathbf{e}_i^{\mathrm{t}} A^{\mathrm{t}} A \mathbf{e}_j = \mathbf{e}_i^{\mathrm{t}} \mathbf{e}_j.$$

Jadi, komponen ke-ij dari $A^{\mathrm{t}}A$ bernilai 1 ketika $i = j$ dan 0 selainnya. Dengan kata lain, $A^{\mathrm{t}}A = I$, dan $A^{-1} = A^{\mathrm{t}}$.

(3) $\Rightarrow$ (4). Jika A mempertahankan hasil kali dalam, maka A mempertahankan jarak, sebab

$$\begin{aligned}\|A\mathbf{x} - A\mathbf{y}\|^2 &= \|A(\mathbf{x} - \mathbf{y})\|^2 \\ &= \langle A(\mathbf{x} - \mathbf{y}), A(\mathbf{x} - \mathbf{y})\rangle \\ &= \langle \mathbf{x} - \mathbf{y}, \mathbf{x} - \mathbf{y}\rangle \\ &= \|\mathbf{x} - \mathbf{y}\|^2.\end{aligned}$$

(4) $\Rightarrow$ (5). Jika A mempertahankan jarak, maka A mempertahankan panjang. Dengan mengambil $\mathbf{y} = 0$, kita memperoleh

$$\|A\mathbf{x}\| = \|A\mathbf{x} - A\mathbf{y}\| = \|\mathbf{x} - \mathbf{y}\| = \|\mathbf{x}\|.$$

(5) $\Rightarrow$ (3). Kita menggunakan identitas berikut untuk menunjukkan bahwa sifat mempertahankan panjang menyiratkan sifat mempertahankan hasil kali dalam:

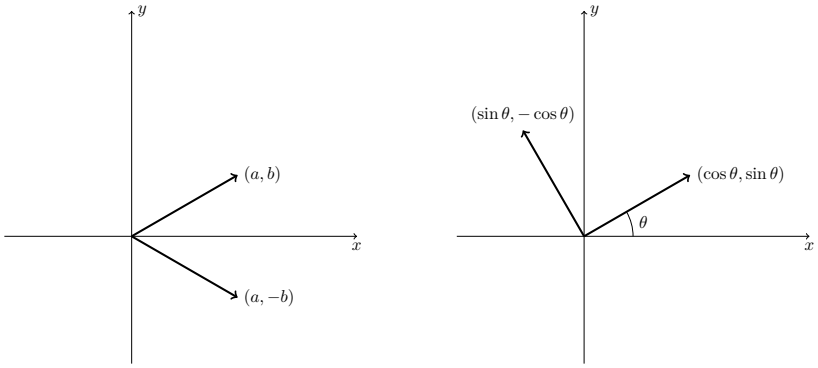
$$\langle \mathbf{x}, \mathbf{y}\rangle = \frac{1}{2}\left[\|\mathbf{x} + \mathbf{y}\|^2 - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2\right].$$

Perhatikan bahwa

$$\langle A\mathbf{x}, A\mathbf{y}\rangle = \frac{1}{2}\left[\|A\mathbf{x} + A\mathbf{y}\|^2 - \|A\mathbf{x}\|^2 - \|A\mathbf{y}\|^2\right]$$

$$
\begin{aligned}
&= \frac{1}{2}\left[\|A(\mathbf{x}+\mathbf{y})\|^2 - \|A\mathbf{x}\|^2 - \|A\mathbf{y}\|^2\right] \\
&= \frac{1}{2}\left[\|\mathbf{x}+\mathbf{y}\|^2 - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2\right] \\
&= \langle \mathbf{x}, \mathbf{y}\rangle.
\end{aligned}
$$

■



Gambar 12.1.9 Tindakan $O(2)$ pada $\mathbb{R}^2$

Contoh 12.1.10 Mari kita periksa grup ortogonal pada $\mathbb{R}^2$ dengan lebih saksama. Suatu elemen $A \in O(2)$ ditentukan oleh tindakannya pada $\mathbf{e}_1 = (1,0)^{\mathrm{t}}$ dan $\mathbf{e}_2 = (0,1)^{\mathrm{t}}$. Jika $A\mathbf{e}_1 = (a,b)^{\mathrm{t}}$, maka $a^2 + b^2 = 1$, karena panjang suatu vektor harus dipertahankan ketika vektor tersebut dikalikan dengan A. Karena perkalian dengan elemen $O(2)$ mempertahankan panjang dan keortogonalan, $A\mathbf{e}_2 = \pm(-b,a)^{\mathrm{t}}$. Jika kita memilih $A\mathbf{e}_2 = (-b,a)^{\mathrm{t}}$, maka

$$
A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},
$$

dengan $0 \le \theta < 2\pi$. Matriks A memutar suatu vektor dalam $\mathbb{R}^2$ berlawanan arah jarum jam mengelilingi titik asal sejauh sudut θ (Gambar 12.1.9).

Jika kita memilih $A\mathbf{e}_2 = (b,-a)^{\mathrm{t}}$, maka kita memperoleh matriks

$$
B = \begin{pmatrix} a & b \\ b & -a \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}.
$$

Di sini, $\det B = -1$ dan

$$
B^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.
$$

Pencerminan terhadap sumbu horizontal diberikan oleh matriks

$$
C = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},
$$

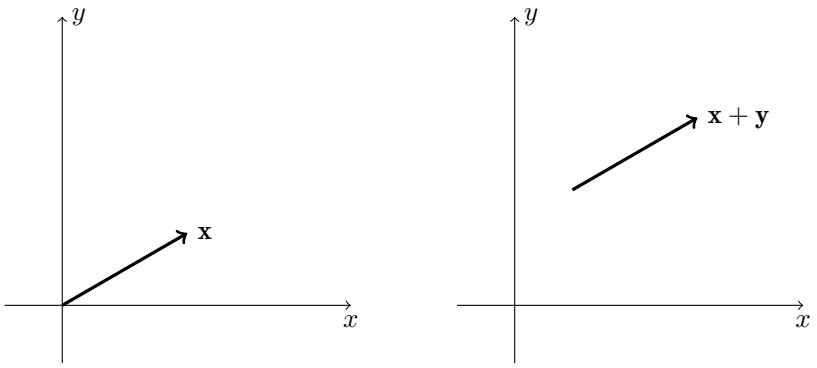
dan $B = AC$ (lihat Gambar 12.1.9). Jadi, pencerminan terhadap garis ℓ tidak lain adalah pencerminan terhadap sumbu horizontal yang diikuti oleh rotasi. ▲

Dua grup matriks atau grup yang berkaitan dengan matriks lainnya yang akan kita perhatikan ialah grup ortogonal khusus dan grup gerak Euklides. **Grup ortogonal khusus**, $SO(n)$, tidak lain adalah irisan $O(n)$ dan $SL_n(\mathbb{R})$; yaitu, elemen-elemen dalam $O(n)$ yang berdeterminan satu. **Grup Euklides**, $E(n)$, dapat dituliskan sebagai pasangan terurut $(A, \mathbf{x})$, dengan A berada da-

lam $O(n)$ dan $\mathbf{x}$ berada dalam $\mathbb{R}^n$. Kita mendefinisikan perkalian dengan

$$(A, \mathbf{x})(B, \mathbf{y}) = (AB, A\mathbf{y} + \mathbf{x}).$$

Identitas grup tersebut adalah $(I, \mathbf{0})$; invers dari $(A, \mathbf{x})$ adalah $(A^{-1}, -A^{-1}\mathbf{x})$. Dalam Latihan 12.4.6, Anda diminta memeriksa bahwa $E(n)$ benar-benar merupakan grup di bawah operasi ini.



Gambar 12.1.11 Translasi dalam $\mathbb{R}^2$

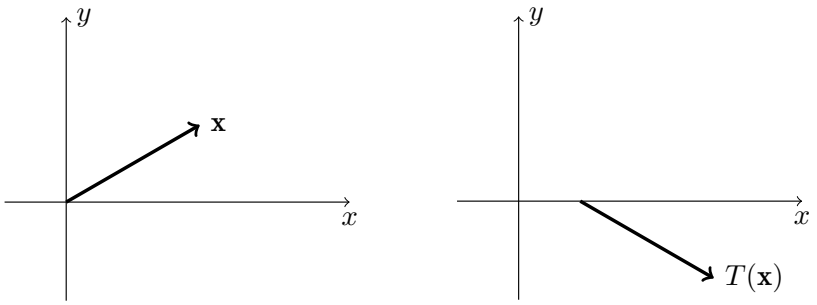
12.2 Simetri

Suatu **isometri** atau **gerak kaku** dalam $\mathbb{R}^n$ adalah fungsi f yang mempertahankan jarak dari $\mathbb{R}^n$ ke $\mathbb{R}^n$. Ini berarti bahwa f harus memenuhi

$$\|f(\mathbf{x}) - f(\mathbf{y})\| = \|\mathbf{x} - \mathbf{y}\|$$

untuk semua $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. Tidak sulit untuk menunjukkan bahwa f harus merupakan pemetaan satu-satu. Berdasarkan Teorema 12.1.8, setiap elemen dalam $O(n)$ merupakan isometri pada $\mathbb{R}^n$; akan tetapi, $O(n)$ tidak mencakup semua isometri yang mungkin pada $\mathbb{R}^n$. Translasi oleh vektor $\mathbf{x}$, $T_{\mathbf{y}}(\mathbf{x}) = \mathbf{x} + \mathbf{y}$, juga merupakan isometri (Gambar 12.1.11); akan tetapi, T tidak dapat berada dalam $O(n)$ karena bukan pemetaan linear.

Kita terutama tertarik pada isometri dalam $\mathbb{R}^2$. Sesungguhnya, satu-satunya isometri dalam $\mathbb{R}^2$ ialah rotasi dan pencerminan terhadap titik asal, translasi, serta kombinasi keduanya. Sebagai contoh, **pencerminan luncur** merupakan translasi yang diikuti oleh pencerminan (Gambar 12.2.1). Dalam $\mathbb{R}^n$, semua isometri diberikan dengan cara yang sama. Pembuktiannya sangat mudah diperumum.



Gambar 12.2.1 Pencerminan luncur

Lema 12.2.2 *Suatu isometri f yang mempertahankan titik asal dalam $\mathbb{R}^2$ merupakan transformasi linear. Secara khusus, f diberikan oleh suatu elemen*

dalam $O(2)$.

BUKTI. Misalkan f suatu isometri dalam $\mathbb{R}^2$ yang mempertahankan titik asal. Pertama-tama kita akan menunjukkan bahwa f mempertahankan hasil kali dalam. Karena $f(0) = 0$, $\|f(\mathbf{x})\| = \|\mathbf{x}\|$; oleh karena itu,

$$\begin{aligned}\|\mathbf{x}\|^2 - 2\langle f(\mathbf{x}), f(\mathbf{y})\rangle + \|\mathbf{y}\|^2 &= \|f(\mathbf{x})\|^2 - 2\langle f(\mathbf{x}), f(\mathbf{y})\rangle + \|f(\mathbf{y})\|^2 \\ &= \langle f(\mathbf{x}) - f(\mathbf{y}), f(\mathbf{x}) - f(\mathbf{y})\rangle \\ &= \|f(\mathbf{x}) - f(\mathbf{y})\|^2 \\ &= \|\mathbf{x} - \mathbf{y}\|^2 \\ &= \langle \mathbf{x} - \mathbf{y}, \mathbf{x} - \mathbf{y}\rangle \\ &= \|\mathbf{x}\|^2 - 2\langle \mathbf{x}, \mathbf{y}\rangle + \|\mathbf{y}\|^2.\end{aligned}$$

Akibatnya,

$$\langle f(\mathbf{x}), f(\mathbf{y})\rangle = \langle \mathbf{x}, \mathbf{y}\rangle.$$

Sekarang misalkan $\mathbf{e}_1$ dan $\mathbf{e}_2$ adalah $(1,0)^{\mathrm{t}}$ dan $(0,1)^{\mathrm{t}}$, secara berturut-turut. Jika

$$\mathbf{x} = (x_1, x_2) = x_1\mathbf{e}_1 + x_2\mathbf{e}_2,$$

maka

$$f(\mathbf{x}) = \langle f(\mathbf{x}), f(\mathbf{e}_1)\rangle f(\mathbf{e}_1) + \langle f(\mathbf{x}), f(\mathbf{e}_2)\rangle f(\mathbf{e}_2) = x_1 f(\mathbf{e}_1) + x_2 f(\mathbf{e}_2).$$

Linearitas f segera diperoleh. ■

Untuk setiap isometri sembarang f, $T_{\mathbf{x}}f$ akan mempertahankan titik asal untuk suatu vektor $\mathbf{x}$ dalam $\mathbb{R}^2$; jadi, $T_{\mathbf{x}}f(\mathbf{y}) = A\mathbf{y}$ untuk suatu matriks $A \in O(2)$. Akibatnya, $f(\mathbf{y}) = A\mathbf{y} + \mathbf{x}$. Diberikan isometri-isometri

$$\begin{aligned}f(\mathbf{y}) &= A\mathbf{y} + \mathbf{x}_1 \\ g(\mathbf{y}) &= B\mathbf{y} + \mathbf{x}_2,\end{aligned}$$

komposisinya adalah

$$f(g(\mathbf{y})) = f(B\mathbf{y} + \mathbf{x}_2) = AB\mathbf{y} + A\mathbf{x}_2 + \mathbf{x}_1.$$

Perhitungan terakhir ini memungkinkan kita mengidentifikasi grup isometri pada $\mathbb{R}^2$ dengan $E(2)$.

Teorema 12.2.3 *Grup isometri pada $\mathbb{R}^2$ merupakan grup Euklides, $E(2)$.*

Suatu **grup simetri** dalam $\mathbb{R}^n$ adalah subgrup dari grup isometri pada $\mathbb{R}^n$ yang mempertahankan suatu himpunan titik $X \subset \mathbb{R}^n$. Penting untuk disadari bahwa grup simetri X bergantung *baik* pada $\mathbb{R}^n$ maupun pada X. Sebagai contoh, grup simetri titik asal dalam $\mathbb{R}^1$ adalah $\mathbb{Z}_2$, sedangkan grup simetri titik asal dalam $\mathbb{R}^2$ adalah $O(2)$.

Teorema 12.2.4 *Satu-satunya grup simetri hingga dalam $\mathbb{R}^2$ adalah $\mathbb{Z}_n$ dan D_n.*

BUKTI. Kita hanya perlu mencari semua subgrup hingga G dari $E(2)$. Setiap grup simetri hingga G dalam $\mathbb{R}^2$ harus mempertahankan titik asal dan merupakan subgrup hingga dari $O(2)$, karena translasi dan pencerminan luncur berorde takhingga. Berdasarkan Contoh 12.1.10, elemen-elemen dalam $O(2)$ berupa rotasi berbentuk

$$R_\theta = \begin{pmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}$$

atau pencerminan berbentuk

$$T_\phi = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{pmatrix}.$$

Perhatikan bahwa $\det(R_\theta) = 1$, $\det(T_\phi) = -1$, dan $T_\phi^2 = I$. Kita dapat membagi pembuktian menjadi dua kasus. Dalam kasus pertama, semua elemen dalam G berdeterminan satu. Dalam kasus kedua, terdapat setidaknya satu elemen dalam G yang berdeterminan -1.

Kasus 1. Determinan setiap elemen dalam G adalah satu. Dalam kasus ini, setiap elemen dalam G harus berupa rotasi. Karena G hingga, terdapat sudut terkecil, misalkan θ_0, sedemikian sehingga elemen yang bersesuaian R_{θ_0} merupakan rotasi terkecil dalam arah positif. Kita menyatakan bahwa R_{θ_0} membangkitkan G. Jika tidak, maka untuk suatu bilangan bulat positif n terdapat sudut θ_1 di antara $n\theta_0$ dan $(n+1)\theta_0$. Jika demikian, $(n+1)\theta_0 - \theta_1$ bersesuaian dengan rotasi yang lebih kecil daripada θ_0, bertentangan dengan keminimalan θ_0.

Kasus 2. Grup G memuat suatu pencerminan T. Kernel homomorfisma $\phi : G \to \{-1, 1\}$ yang diberikan oleh $A \mapsto \det(A)$ terdiri atas elemen-elemen yang determinannya 1. Oleh karena itu, $|G/\ker\phi| = 2$. Berdasarkan kasus pertama, kita mengetahui bahwa kernel tersebut siklik dan merupakan subgrup dari G yang, misalnya, berorde n. Jadi, $|G| = 2n$. Elemen-elemen G adalah

$$R_\theta, \ldots, R_\theta^{n-1}, TR_\theta, \ldots, TR_\theta^{n-1}.$$

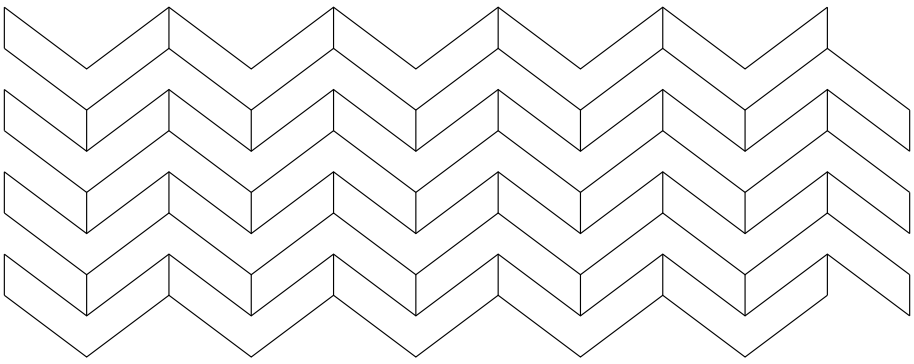
Elemen-elemen tersebut memenuhi relasi

$$TR_\theta T = R_\theta^{-1}.$$

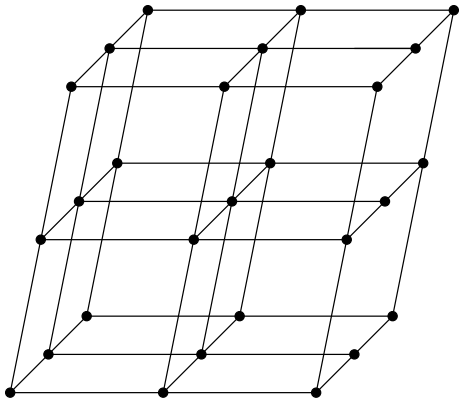
Akibatnya, dalam kasus ini G harus isomorfik dengan D_n. ■

12.2.1 Grup Kertas Dinding

Andaikan kita ingin mempelajari pola kertas dinding pada bidang atau kristal dalam tiga dimensi. Pola kertas dinding tidak lain adalah pola berulang pada bidang (Gambar 12.2.5). Analogi pola kertas dinding dalam $\mathbb{R}^3$ ialah kristal, yang dapat kita pandang sebagai pola molekul berulang dalam tiga dimensi (Gambar 12.2.6). Padanan matematis pola kertas dinding atau pola kristal disebut kisi.



Gambar 12.2.5 Pola kertas dinding dalam $\mathbb{R}^2$



Gambar 12.2.6 Struktur kristal dalam $\mathbb{R}^3$

Mari kita periksa pola kertas dinding pada bidang dengan lebih saksama. Andaikan $\mathbf{x}$ dan $\mathbf{y}$ merupakan vektor-vektor bebas linear dalam $\mathbb{R}^2$; yaitu, salah satu vektor bukan kelipatan skalar dari vektor lainnya. **Kisi** dari $\mathbf{x}$ dan $\mathbf{y}$ adalah himpunan semua kombinasi linear $m\mathbf{x}+n\mathbf{y}$, dengan m dan n bilangan bulat. Vektor $\mathbf{x}$ dan $\mathbf{y}$ disebut **basis** bagi kisi tersebut.

Perhatikan bahwa suatu kisi dapat memiliki beberapa basis. Sebagai contoh, vektor $(1,1)^{\mathrm{t}}$ dan $(2,0)^{\mathrm{t}}$ mempunyai kisi yang sama dengan vektor $(-1,1)^{\mathrm{t}}$ dan $(-1,-1)^{\mathrm{t}}$ (Gambar 12.2.7). Akan tetapi, setiap kisi ditentukan sepenuhnya oleh suatu basis. Diberikan dua basis bagi kisi yang sama, misalnya $\{\mathbf{x}_1, \mathbf{x}_2\}$ dan $\{\mathbf{y}_1, \mathbf{y}_2\}$, kita dapat menuliskan

$$\begin{aligned}\mathbf{y}_1 &= \alpha_1\mathbf{x}_1 + \alpha_2\mathbf{x}_2\\ \mathbf{y}_2 &= \beta_1\mathbf{x}_1 + \beta_2\mathbf{x}_2,\end{aligned}$$

dengan α_1, α_2, β_1, dan β_2 bilangan bulat. Matriks yang bersesuaian dengan transformasi ini adalah

$$U = \begin{pmatrix}\alpha_1 & \alpha_2\\ \beta_1 & \beta_2\end{pmatrix}.$$

Jika kita ingin menyatakan $\mathbf{x}_1$ dan $\mathbf{x}_2$ dalam $\mathbf{y}_1$ dan $\mathbf{y}_2$, kita hanya perlu menghitung U^{-1}; yaitu,

$$U^{-1}\begin{pmatrix}\mathbf{y}_1\\ \mathbf{y}_2\end{pmatrix} = \begin{pmatrix}\mathbf{x}_1\\ \mathbf{x}_2\end{pmatrix}.$$

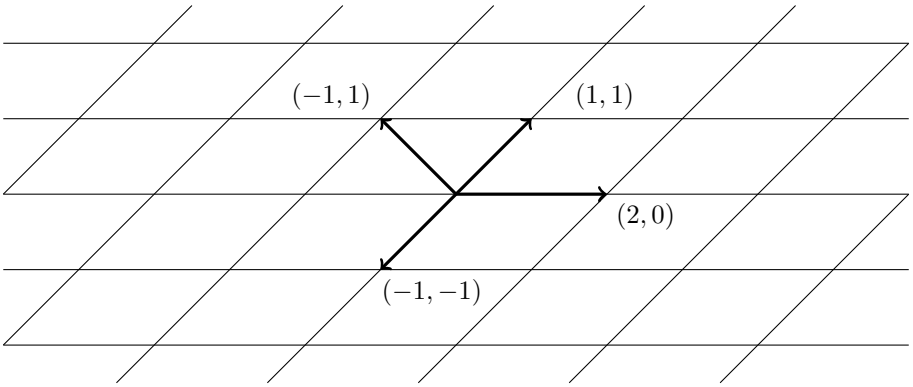
Karena U mempunyai entri bilangan bulat, U^{-1} juga harus mempunyai entri bilangan bulat; jadi, determinan U maupun U^{-1} harus berupa bilangan bulat. Karena $UU^{-1} = I$,

$$\det(UU^{-1}) = \det(U)\det(U^{-1}) = 1;$$

akibatnya, $\det(U) = \pm 1$. Matriks dengan determinan ± 1 dan entri bilangan bulat disebut **unimodular**. Sebagai contoh, matriks

$$\begin{pmatrix}3 & 1\\ 5 & 2\end{pmatrix}$$

bersifat unimodular. Jelas bahwa terdapat panjang minimum bagi vektor dalam suatu kisi.



Gambar 12.2.7 Kisi dalam $\mathbb{R}^2$

Kita dapat mengklasifikasikan kisi dengan mempelajari grup simetrinya. Grup simetri suatu kisi adalah subgrup dari $E(2)$ yang memetakan kisi tersebut ke dirinya sendiri. Dua kisi dalam $\mathbb{R}^2$ kita anggap ekuivalen jika mempunyai grup simetri yang sama. Demikian pula, klasifikasi kristal dalam $\mathbb{R}^3$ dilakukan dengan mengaitkan suatu grup simetri, yang disebut **grup ruang**, dengan setiap jenis kristal. Dua kisi dianggap berbeda jika grup ruangnya tidak sama. Pertanyaan wajar yang kini muncul ialah berapa banyak grup ruang yang ada.

Suatu grup ruang tersusun atas dua bagian: **subgrup translasi** dan suatu **titik**. Subgrup translasi merupakan subgrup abelian takhingga dari grup ruang yang tersusun atas simetri translasi kristal; grup titik merupakan grup hingga yang terdiri atas rotasi dan pencerminan kristal terhadap suatu titik. Secara lebih khusus, suatu grup ruang merupakan subgrup dari $G \subset E(2)$ yang translasinya berupa himpunan berbentuk $\{(I,t) : t \in L\}$, dengan L suatu kisi. Grup ruang tentu saja takhingga. Dengan menggunakan argumen geometris, kita dapat membuktikan teorema berikut (lihat [5] atau [6]).

Teorema 12.2.8 *Setiap grup translasi dalam* $\mathbb{R}^2$ *isomorfik dengan* $\mathbb{Z} \times \mathbb{Z}$.

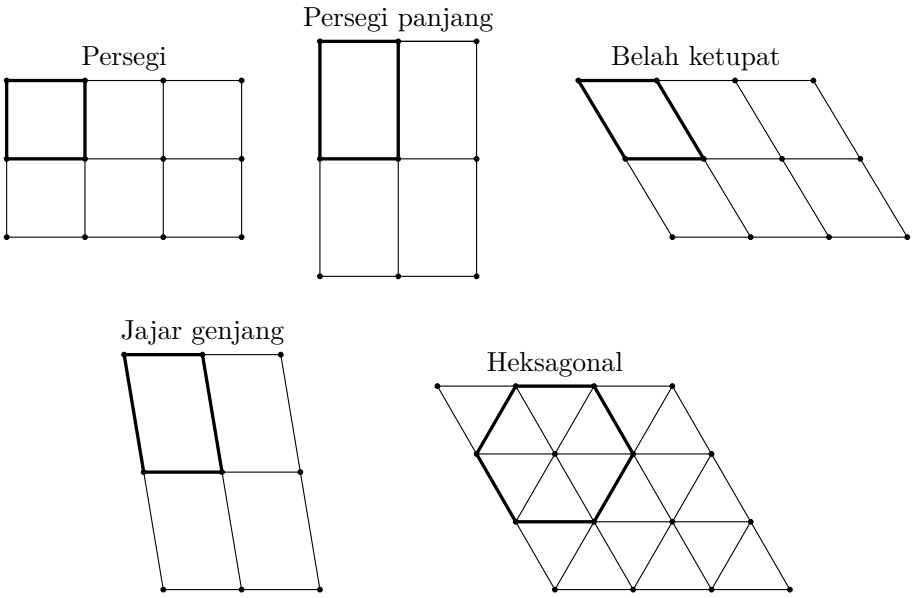
Grup titik dari G adalah $G_0 = \{A : (A,b) \in G \text{ untuk suatu } b\}$. Secara khusus, G_0 harus merupakan subgrup dari $O(2)$. Andaikan $\mathbf{x}$ suatu vektor dalam kisi L dengan grup ruang G, grup translasi H, dan grup titik G_0. Untuk setiap elemen $(A, \mathbf{y})$ dalam G,

$$\begin{aligned}(A,\mathbf{y})(I,\mathbf{x})(A,\mathbf{y})^{-1} &= (A, A\mathbf{x}+\mathbf{y})(A^{-1}, -A^{-1}\mathbf{y}) \\ &= (AA^{-1}, -AA^{-1}\mathbf{y} + A\mathbf{x} + \mathbf{y}) \\ &= (I, A\mathbf{x});\end{aligned}$$

jadi, $(I, A\mathbf{x})$ berada dalam grup translasi G. Secara lebih khusus, $A\mathbf{x}$ harus berada dalam kisi L. Penting untuk dicatat bahwa G_0 biasanya bukan subgrup dari grup ruang G; akan tetapi, jika T merupakan subgrup translasi dari G, maka $G/T \cong G_0$. Pembuktian teorema berikut dapat ditemukan dalam [2], [5], atau [6].

Teorema 12.2.9 *Grup titik dalam grup kertas dinding isomorfik dengan* $\mathbb{Z}_n$ *atau* D_n*, dengan* $n = 1, 2, 3, 4, 6$.

Untuk menjawab bagaimana grup titik dan grup translasi dapat digabungkan, kita harus memperhatikan berbagai jenis kisi. Kisi dapat diklasifikasikan berdasarkan struktur satu sel kisi. Bentuk sel yang mungkin ialah jajar genjang, persegi panjang, persegi, belah ketupat, dan heksagonal (Gambar 12.2.10). Grup kertas dinding kini dapat diklasifikasikan menurut jenis pencerminan yang muncul dalam setiap grup: pencerminan biasa, pencerminan luncur, keduanya, atau tidak satu pun.

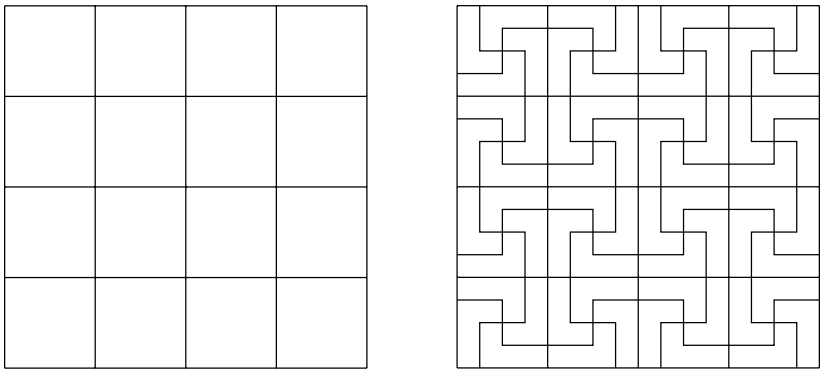


Gambar 12.2.10 Jenis kisi dalam $\mathbb{R}^2$

Tabel 12.2.11 Ke-17 Grup Kertas Dinding

Notasi dan Grup Ruang	Grup Titik	Jenis Kisi	Pencerminan atau Pencerminan Luncur?
p1	$\mathbb{Z}_1$	jajar genjang	tidak ada
p2	$\mathbb{Z}_2$	jajar genjang	tidak ada
p3	$\mathbb{Z}_3$	heksagonal	tidak ada
p4	$\mathbb{Z}_4$	persegi	tidak ada
p6	$\mathbb{Z}_6$	heksagonal	tidak ada
pm	D_1	persegi panjang	pencerminan
pg	D_1	persegi panjang	pencerminan luncur
cm	D_1	belah ketupat	keduanya
pmm	D_2	persegi panjang	pencerminan
pmg	D_2	persegi panjang	pencerminan luncur
pgg	D_2	persegi panjang	keduanya
c2mm	D_2	belah ketupat	keduanya
p3m1, p31m	D_3	heksagonal	keduanya
p4m, p4g	D_4	persegi	keduanya
p6m	D_6	heksagonal	keduanya

Teorema 12.2.12 *Terdapat tepat 17 grup kertas dinding.*



Gambar 12.2.13 Grup kertas dinding p4m dan p4g

Ke-17 grup kertas dinding dicantumkan dalam Tabel 12.2.11. Grup p3m1 dan p31m dapat dibedakan berdasarkan apakah semua pusat berorde tiganya terletak pada sumbu pencerminan: semua pusat p3m1 harus terletak pada sumbu tersebut, sedangkan pusat p31m tidak harus demikian. Demikian pula, pusat berorde empat p4m harus terletak pada sumbu pencerminan, sedangkan pusat p4g tidak harus demikian (Gambar 12.2.13). Pembuktian lengkap teorema ini dapat ditemukan dalam beberapa rujukan pada akhir bab, termasuk [5], [6], [10], dan [11].

Catatan Sejarah

Grup simetri telah lama memikat para matematikawan. Leonardo da Vinci mungkin merupakan orang pertama yang mengetahui semua grup titik. Pada Kongres Matematikawan Internasional tahun 1900, David Hilbert menyampaikan pidato yang kini terkenal, yang menguraikan 23 masalah untuk memandu matematika pada abad kedua puluh. Masalah kedelapan belas Hilbert menanyakan apakah grup kristalografi dalam n dimensi selalu hingga. Pada tahun 1910, L. Bieberbach membuktikan bahwa grup kristalografi hingga dalam setiap dimensi. Menentukan berapa banyak grup tersebut dalam setiap dimensi merupakan persoalan lain. Dalam $\mathbb{R}^3$ terdapat 230 grup ruang yang berbeda; dalam $\mathbb{R}^4$ terdapat 4894; dalam $\mathbb{R}^5$ terdapat 222097. Belum ada yang berhasil menghitung banyaknya grup ruang untuk $\mathbb{R}^6$ dan dimensi yang lebih tinggi (oeis.org/A006227). Menarik untuk dicatat bahwa grup kristalografi untuk $\mathbb{R}^3$ telah ditemukan secara matematis sebelum 230 jenis kristal yang berbeda benar-benar ditemukan di alam.

12.3 Pertanyaan Bacaan

1. Apakah matriks nonsingular itu? Berikan contoh matriks nonsingular 2×2. Bagaimana Anda mengetahui bahwa contoh tersebut nonsingular?
2. Apakah isometri dalam $\mathbb{R}^n$ itu? Dapatkah Anda memberikan contoh isometri dalam $\mathbb{R}^2$?
3. Apakah himpunan vektor ortonormal itu?
4. Apakah perbedaan antara grup ortogonal dan grup ortogonal khusus?
5. Apakah kisi itu?

12.4 Latihan

1. Buktikan identitas

$$\langle \mathbf{x}, \mathbf{y} \rangle = \frac{1}{2} \left[\|\mathbf{x} + \mathbf{y}\|^2 - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2 \right].$$

Petunjuk.

$$\begin{aligned} \frac{1}{2} \left[\|\mathbf{x} + \mathbf{y}\|^2 + \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2 \right] &= \frac{1}{2} \left[\langle x + y, x + y \rangle - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2 \right] \\ &= \frac{1}{2} \left[\|\mathbf{x}\|^2 + 2\langle x, y \rangle + \|\mathbf{y}\|^2 - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2 \right] \\ &= \langle \mathbf{x}, \mathbf{y} \rangle. \end{aligned}$$

2. Tunjukkan bahwa $O(n)$ merupakan sebuah grup.

3. Buktikan bahwa matriks-matriks berikut ortogonal. Adakah di antara matriks tersebut yang berada dalam $SO(n)$?

(a)
$$\begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$$

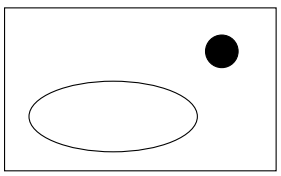
(b)
$$\begin{pmatrix} 1/\sqrt{5} & 2/\sqrt{5} \\ -2/\sqrt{5} & 1/\sqrt{5} \end{pmatrix}$$

(c)
$$\begin{pmatrix} 4/5 & 0 & 3/5 \\ -3/5 & 0 & 4/5 \\ 0 & -1 & 0 \end{pmatrix}$$

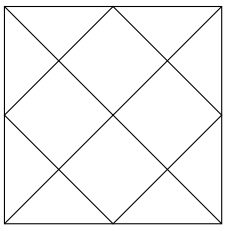
(d)
$$\begin{pmatrix} 1/3 & 2/3 & -2/3 \\ -2/3 & 2/3 & 1/3 \\ 2/3 & 1/3 & 2/3 \end{pmatrix}$$

Petunjuk. (a) berada dalam $SO(2)$; (c) tidak berada dalam $O(3)$.

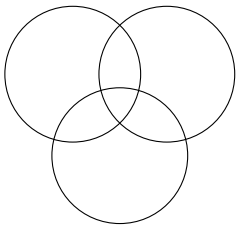
4. Tentukan grup simetri setiap gambar di bawah ini.



(a)



(b)



(c)

5. Misalkan $\mathbf{x}$, $\mathbf{y}$, dan $\mathbf{w}$ vektor-vektor dalam $\mathbb{R}^n$, serta $\alpha \in \mathbb{R}$. Buktikan setiap sifat hasil kali dalam berikut.

(a) $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$.

(b) $\langle \mathbf{x}, \mathbf{y} + \mathbf{w} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle + \langle \mathbf{x}, \mathbf{w} \rangle$.

(c) $\langle \alpha\mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{x}, \alpha\mathbf{y} \rangle = \alpha \langle \mathbf{x}, \mathbf{y} \rangle$.

(d) $\langle \mathbf{x}, \mathbf{x} \rangle \geq 0$, dengan kesamaan tepat ketika $\mathbf{x} = 0$.

(e) Jika $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ untuk semua $\mathbf{x}$ dalam $\mathbb{R}^n$, maka $\mathbf{y} = 0$.

Petunjuk. (a) $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$.

6. Verifikasi bahwa

$$E(n) = \{(A, \mathbf{x}) : A \in O(n) \text{ dan } \mathbf{x} \in \mathbb{R}^n\}$$

merupakan sebuah grup.

7. Buktikan bahwa $\{(2,1),(1,1)\}$ dan $\{(12,5),(7,3)\}$ merupakan basis bagi kisi yang sama.

Petunjuk. Gunakan matriks unimodular

$$\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}.$$

8. Misalkan G suatu subgrup dari $E(2)$ dan andaikan T subgrup translasi dari G. Buktikan bahwa grup titik dari G isomorfik dengan G/T.

9. Misalkan $A \in SL_2(\mathbb{R})$ dan andaikan vektor $\mathbf{x}$ serta $\mathbf{y}$ membentuk dua sisi suatu jajar genjang dalam $\mathbb{R}^2$. Buktikan bahwa luas jajar genjang tersebut sama dengan luas jajar genjang yang bersisi $A\mathbf{x}$ dan $A\mathbf{y}$.

10. Buktikan bahwa $SO(n)$ merupakan subgrup normal dari $O(n)$.

Petunjuk. Tunjukkan bahwa kernel pemetaan $\det : O(n) \to \mathbb{R}^*$ adalah $SO(n)$.

11. Tunjukkan bahwa setiap isometri f dalam $\mathbb{R}^n$ merupakan pemetaan satu-satu.

12. Buktikan atau bantah: suatu elemen dalam $E(2)$ yang berbentuk $(A, \mathbf{x})$, dengan $\mathbf{x} \neq 0$, berorde takhingga.

13. Buktikan atau bantah: Terdapat subgrup abelian takhingga dari $O(n)$.

Petunjuk. Benar.

14. Misalkan $\mathbf{x} = (x_1, x_2)$ suatu titik pada lingkaran satuan dalam $\mathbb{R}^2$; yaitu, $x_1^2 + x_2^2 = 1$. Jika $A \in O(2)$, tunjukkan bahwa $A\mathbf{x}$ juga merupakan titik pada lingkaran satuan.

15. Misalkan G suatu grup dengan subgrup H (tidak harus normal) dan subgrup normal N. Maka G merupakan **hasil kali semilangsung** dari N oleh H jika

- $H \cap N = \{\mathrm{id}\}$;
- $HN = G$.

Tunjukkan bahwa setiap pernyataan berikut benar.

(a) S_3 merupakan hasil kali semilangsung dari A_3 oleh $H = \{(1), (1\,2)\}$.

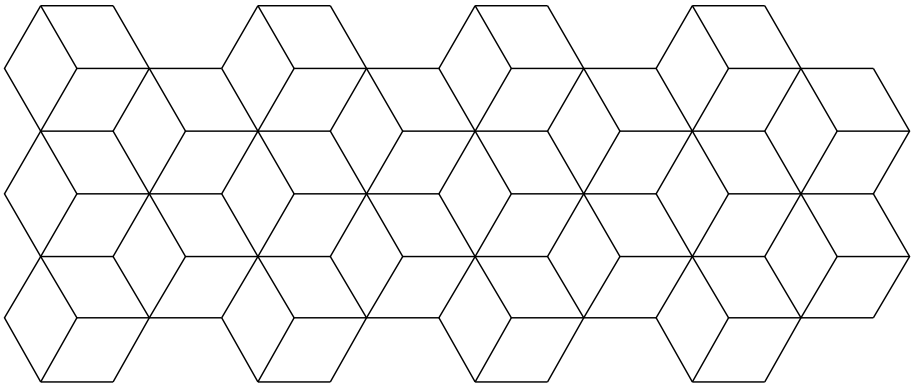
(b) Grup kuaternion Q_8 tidak dapat dituliskan sebagai hasil kali semilangsung.

(c) $E(2)$ merupakan hasil kali semilangsung dari $O(2)$ oleh H, dengan H terdiri atas semua translasi dalam $\mathbb{R}^2$.

16. Tentukan grup mana di antara 17 grup kertas dinding yang mempertahankan simetri pola dalam Gambar 12.2.5.

17. Tentukan grup mana di antara 17 grup kertas dinding yang mempertahankan simetri pola dalam Gambar 12.4.1.

Petunjuk. $p6m$



Gambar 12.4.1 Kisi untuk Latihan 12.4.17

18. Carilah grup rotasi suatu dodekahedron.

19. Untuk masing-masing dari 17 grup kertas dinding, gambarlah pola kertas dinding yang mempunyai grup tersebut sebagai grup simetri.

12.5 Referensi dan Bacaan yang Disarankan

[1] Coxeter, H. M. and Moser, W. O. J. *Generators and Relations for Discrete Groups*, 3rd ed. Springer-Verlag, New York, 1972.

[2] Grove, L. C. and Benson, C. T. *Finite Reflection Groups.* 2nd ed. Springer-Verlag, New York, 1985.

[3] Hiller, H. "Crystallography and Cohomology of Groups," *American Mathematical Monthly* 93 (1986), 765–79.

[4] Lockwood, E. H. and Macmillan, R. H. *Geometric Symmetry.* Cambridge University Press, Cambridge, 1978.

[5] Mackiw, G. *Applications of Abstract Algebra.* Wiley, New York, 1985.

[6] Martin, G. *Transformation Groups: An Introduction to Symmetry.* Springer-Verlag, New York, 1982.

[7] Milnor, J. "Hilbert's Problem 18: On Crystallographic Groups, Fundamental Domains, and Sphere Packing," *t Proceedings of Symposia in Pure Mathematics* 18, American Mathematical Society, 1976.

[8] Phillips, F. C. *An Introduction to Crystallography.* 4th ed. Wiley, New York, 1971.

[9] Rose, B. I. and Stafford, R. D. "An Elementary Course in Mathematical Symmetry," *American Mathematical Monthly* 88 (1980), 54–64.

[10] Schattschneider, D. "The Plane Symmetry Groups: Their Recognition and Their Notation," *American Mathematical Monthly* 85 (1978), 439–50.

[11] Schwarzenberger, R. L. "The 17 Plane Symmetry Groups," *Mathematical Gazette* 58 (1974), 123–31.

[12] Weyl, H. *Symmetry.* Princeton University Press, Princeton, NJ, 1952.

13

Struktur Grup

Tujuan akhir teori grup adalah mengklasifikasikan semua grup hingga isomorfisma; yaitu, jika diberikan suatu grup tertentu, kita seharusnya dapat memadankannya dengan grup yang telah dikenal melalui suatu isomorfisma. Sebagai contoh, kita telah membuktikan bahwa setiap grup siklik hingga berorde n isomorfik dengan $\mathbb{Z}_n$; dengan demikian, kita "mengenal" semua grup siklik hingga. Mungkin tidak masuk akal untuk berharap bahwa suatu saat kita akan mengenal semua grup; namun, kita sering dapat mengklasifikasikan jenis grup tertentu atau membedakan grup-grup dalam kasus khusus.

Dalam bab ini, kita akan mengarakterisasi semua grup abelian hingga. Kita juga akan menyelidiki grup yang memiliki barisan subgrup. Jika suatu grup memiliki barisan subgrup, katakanlah

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\},$$

dengan setiap subgrup H_i normal dalam H_{i+1} dan setiap grup hasil bagi H_{i+1}/H_i abelian, maka G merupakan grup solvabel. Selain memungkinkan kita membedakan kelas-kelas grup tertentu, grup solvabel ternyata berperan sentral dalam kajian penyelesaian persamaan polinomial.

13.1 Grup Abelian Hingga

Dalam penyelidikan grup siklik, kita menemukan bahwa setiap grup berorde prima isomorfik dengan $\mathbb{Z}_p$, dengan p suatu bilangan prima. Kita juga menentukan bahwa $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ ketika $\gcd(m, n) = 1$. Bahkan, berlaku hasil yang jauh lebih kuat. Setiap grup abelian hingga isomorfik dengan hasil kali langsung grup-grup siklik yang ordenya berupa pangkat prima; yaitu, setiap grup abelian hingga isomorfik dengan grup berbentuk

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}},$$

dengan setiap p_k prima (tidak harus berbeda).

Pertama-tama, mari kita telaah sedikit perumuman dari grup abelian hingga. Misalkan G suatu grup dan misalkan $\{g_i\}$ suatu himpunan elemen dalam G, dengan i berada dalam suatu himpunan indeks I (yang tidak harus hingga). Subgrup terkecil dari G yang memuat semua g_i adalah subgrup dari G yang **dibangkitkan** oleh g_i tersebut. Jika subgrup dari G ini ternyata merupakan seluruh G, maka G dibangkitkan oleh himpunan $\{g_i : i \in I\}$. Dalam hal ini, g_i tersebut disebut **pembangkit** dari G. Jika terdapat himpunan hingga

$\{g_i : i \in I\}$ yang membangkitkan G, maka G disebut **dibangkitkan secara hingga**.

Contoh 13.1.1 Jelas bahwa semua grup hingga dibangkitkan secara hingga. Sebagai contoh, grup S_3 dibangkitkan oleh permutasi $(1\,2)$ dan $(1\,2\,3)$. Grup $\mathbb{Z} \times \mathbb{Z}_n$ merupakan grup tak hingga, tetapi dibangkitkan secara hingga oleh $\{(1,0),(0,1)\}$. ▲

Contoh 13.1.2 Tidak semua grup dibangkitkan secara hingga. Tinjau bilangan rasional $\mathbb{Q}$ terhadap operasi penjumlahan. Andaikan $\mathbb{Q}$ dibangkitkan secara hingga oleh pembangkit $p_1/q_1, \ldots, p_n/q_n$, dengan setiap p_i/q_i merupakan pecahan yang dinyatakan dalam bentuk paling sederhana. Misalkan p suatu bilangan prima yang tidak membagi satu pun penyebut $q_1, \ldots, q_n$. Kita menyatakan bahwa $1/p$ tidak mungkin berada dalam subgrup dari $\mathbb{Q}$ yang dibangkitkan oleh $p_1/q_1, \ldots, p_n/q_n$, karena p tidak membagi penyebut elemen mana pun dalam subgrup ini. Fakta ini mudah dilihat karena jumlah sebarang dua pembangkit adalah

$$p_i/q_i + p_j/q_j = (p_i q_j + p_j q_i)/(q_i q_j).$$

▲

Proposisi 13.1.3 *Misalkan H subgrup dari suatu grup G yang dibangkitkan oleh $\{g_i \in G : i \in I\}$. Maka $h \in H$ tepat ketika elemen tersebut merupakan hasil kali berbentuk*

$$h = g_{i_1}^{\alpha_1} \cdots g_{i_n}^{\alpha_n},$$

dengan g_{i_k} yang tidak harus berbeda.

Bukti. Misalkan K himpunan semua hasil kali berbentuk $g_{i_1}^{\alpha_1} \cdots g_{i_n}^{\alpha_n}$, dengan g_{i_k} yang tidak harus berbeda. Jelas bahwa K merupakan himpunan bagian dari H. Kita hanya perlu menunjukkan bahwa K merupakan subgrup dari G. Jika demikian, maka $K = H$, karena H merupakan subgrup terkecil yang memuat semua g_i.

Jelas bahwa himpunan K tertutup terhadap operasi grup. Karena $g_i^0 = 1$, identitas berada dalam K. Tinggal menunjukkan bahwa invers dari suatu elemen $g = g_{i_1}^{k_1} \cdots g_{i_n}^{k_n}$ dalam K juga harus berada dalam K. Memang,

$$g^{-1} = (g_{i_1}^{k_1} \cdots g_{i_n}^{k_n})^{-1} = (g_{i_n}^{-k_n} \cdots g_{i_1}^{-k_1}).$$

■

Pangkat-pangkat dari suatu g_i tetap dapat muncul beberapa kali dalam hasil kali karena grupnya mungkin nonabelian. Namun, jika grup tersebut abelian, maka setiap g_i hanya perlu muncul satu kali. Sebagai contoh, hasil kali seperti $a^{-3}b^5a^7$ dalam suatu grup abelian selalu dapat disederhanakan (dalam kasus ini menjadi a^4b^5).

Sekarang mari kita batasi perhatian pada grup abelian hingga. Kita dapat menyatakan setiap grup abelian hingga sebagai hasil kali langsung hingga dari grup-grup siklik. Secara lebih khusus, dengan p prima, kita mendefinisikan suatu grup G sebagai **grup-p** jika orde setiap elemen dalam G merupakan suatu pangkat dari p. Sebagai contoh, $\mathbb{Z}_2 \times \mathbb{Z}_2$ maupun $\mathbb{Z}_4$ merupakan grup-2, sedangkan $\mathbb{Z}_{27}$ merupakan grup-3. Kita akan membuktikan Teorema Dasar Grup Abelian Hingga, yang menyatakan bahwa setiap grup abelian hingga isomorfik dengan hasil kali langsung grup-p siklik.

Teorema 13.1.4 Teorema Dasar Grup Abelian Hingga. *Setiap grup*

abelian hingga G isomorfik dengan hasil kali langsung grup-grup siklik berbentuk

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}}$$

dengan p_i bilangan-bilangan prima (yang tidak harus berbeda).

Contoh 13.1.5 Misalkan kita ingin mengklasifikasikan semua grup abelian berorde $540 = 2^2 \cdot 3^3 \cdot 5$. Teorema Dasar Grup Abelian Hingga menyatakan bahwa terdapat enam kemungkinan berikut.

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$;
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$;
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$;
- $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$;
- $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$;
- $\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$.

▲

Pembuktian Teorema Dasar Grup Abelian Hingga bergantung pada beberapa lema.

Lema 13.1.6 *Misalkan G suatu grup abelian hingga berorde n. Jika p merupakan bilangan prima yang membagi n, maka G memuat elemen berorde p.*

BUKTI. Kita akan membuktikan lema ini dengan induksi. Jika $n = 1$, tidak ada yang perlu dibuktikan. Sekarang andaikan bahwa lema tersebut benar untuk semua grup berorde k, dengan $k < n$. Selanjutnya, misalkan p suatu bilangan prima yang membagi n.

Jika G tidak memiliki subgrup sejati nontrivial, maka $G = \langle a \rangle$, dengan a sebarang elemen selain identitas. Berdasarkan Latihan 4.5.39, orde G harus prima. Karena p membagi n, kita mengetahui bahwa $p = n$, dan G memuat $p - 1$ elemen berorde p.

Sekarang misalkan G memuat subgrup sejati nontrivial H. Maka $1 < |H| < n$. Jika $p \mid |H|$, maka berdasarkan induksi, H memuat elemen berorde p sehingga lema terbukti. Misalkan p tidak membagi orde H. Karena G abelian, H harus merupakan subgrup normal dari G, dan $|G| = |H| \cdot |G/H|$. Akibatnya, p harus membagi $|G/H|$. Karena $|G/H| < |G| = n$, berdasarkan hipotesis induksi kita mengetahui bahwa G/H memuat elemen aH berorde p. Jadi,

$$H = (aH)^p = a^p H,$$

dan $a^p \in H$, tetapi $a \notin H$. Jika $|H| = r$, maka p dan r relatif prima, dan terdapat bilangan bulat s dan t sedemikian sehingga $sp + tr = 1$. Selanjutnya, orde a^p harus membagi r, dan $(a^p)^r = (a^r)^p = 1$.

Kita menyatakan bahwa a^r berorde p. Kita harus menunjukkan bahwa $a^r \neq 1$. Andaikan $a^r = 1$. Maka

$$\begin{aligned} a &= a^{sp+tr} \\ &= a^{sp} a^{tr} \\ &= (a^p)^s (a^r)^t \\ &= (a^p)^s 1 \\ &= (a^p)^s. \end{aligned}$$

Karena $a^p \in H$, harus berlaku bahwa $a = (a^p)^s \in H$, yang merupakan suatu kontradiksi. Oleh karena itu, $a^r \neq 1$ merupakan elemen berorde p dalam G. ■

Lema 13.1.6 merupakan kasus khusus Teorema Cauchy (Teorema 15.1.1), yang menyatakan bahwa jika G suatu grup hingga dan p suatu bilangan prima sedemikian sehingga p membagi orde G, maka G memuat subgrup berorde p. Kita akan membuktikan Teorema Cauchy dalam Bab 15.

Lema 13.1.7 *Suatu grup abelian hingga merupakan grup-p jika dan hanya jika ordenya merupakan pangkat dari p.*

BUKTI. Jika $|G| = p^n$, maka berdasarkan Teorema Lagrange, orde setiap $g \in G$ harus membagi p^n, sehingga harus merupakan pangkat dari p. Sebaliknya, jika $|G|$ bukan merupakan pangkat dari p, maka bilangan tersebut memiliki pembagi prima lain q, sehingga berdasarkan Lema 13.1.6, G memiliki elemen berorde q dan dengan demikian bukan merupakan grup-p. ■

Lema 13.1.8 *Misalkan G suatu grup abelian hingga berorde $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, dengan $p_1, \ldots, p_k$ bilangan-bilangan prima yang berbeda dan $\alpha_1, \alpha_2, \ldots, \alpha_k$ bilangan-bilangan bulat positif. Maka G merupakan hasil kali langsung internal dari subgrup-subgrup $G_1, G_2, \ldots, G_k$, dengan G_i subgrup dari G yang terdiri atas semua elemen berorde p_i^r untuk suatu bilangan bulat r.*

BUKTI. Karena G merupakan grup abelian, terjamin bahwa G_i merupakan subgrup dari G untuk $i = 1, \ldots, k$. Karena identitas berorde $p_i^0 = 1$, kita mengetahui bahwa $1 \in G_i$. Jika $g \in G_i$ berorde p_i^r, maka g^{-1} juga harus berorde p_i^r. Terakhir, jika $h \in G_i$ berorde p_i^s, maka

$$(gh)^{p_i^t} = g^{p_i^t} h^{p_i^t} = 1 \cdot 1 = 1,$$

dengan t nilai maksimum dari r dan s.

Kita harus menunjukkan bahwa

$$G = G_1 G_2 \cdots G_k$$

dan $G_i \cap G_j = \{1\}$ untuk $i \neq j$. Misalkan $g_1 \in G_1$ berada dalam subgrup yang dibangkitkan oleh $G_2, G_3, \ldots, G_k$. Maka $g_1 = g_2 g_3 \cdots g_k$ untuk $g_i \in G_i$. Karena g_i berorde $p_i^{\alpha_i}$, kita mengetahui bahwa $g_i^{p_i^{\alpha_i}} = 1$ untuk $i = 2, 3, \ldots, k$, dan $g_1^{p_2^{\alpha_2} \cdots p_k^{\alpha_k}} = 1$. Karena orde g_1 merupakan pangkat dari p_1 dan $\gcd(p_1, p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = 1$, harus berlaku bahwa $g_1 = 1$ dan irisan G_1 dengan setiap subgrup $G_2, G_3, \ldots, G_k$ hanyalah identitas. Argumen serupa menunjukkan bahwa $G_i \cap G_j = \{1\}$ untuk $i \neq j$.

Selanjutnya, kita harus menunjukkan bahwa setiap $g \in G$ dapat ditulis sebagai hasil kali $g_1 \cdots g_k$, dengan $g_i \in G_i$. Karena orde g membagi orde G, kita mengetahui bahwa

$$|g| = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

untuk suatu bilangan bulat $\beta_1, \ldots, \beta_k$. Dengan menetapkan $a_i = |g|/p_i^{\beta_i}$, bilangan-bilangan a_i relatif prima; dengan demikian, terdapat bilangan bulat $b_1, \ldots, b_k$ sedemikian sehingga $a_1 b_1 + \cdots + a_k b_k = 1$. Akibatnya,

$$g = g^{a_1 b_1 + \cdots + a_k b_k} = g^{a_1 b_1} \cdots g^{a_k b_k}.$$

Karena

$$g^{(a_i b_i) p_i^{\beta_i}} = g^{b_i |g|} = e,$$

diperoleh bahwa $g^{a_i b_i}$ harus berada dalam G_i. Misalkan $g_i = g^{a_i b_i}$. Maka $g = g_1 \cdots g_k \in G_1 G_2 \cdots G_k$. Oleh karena itu, $G = G_1 G_2 \cdots G_k$ merupakan hasil kali langsung internal dari subgrup-subgrup. ■

Tinggal menentukan kemungkinan struktur setiap grup-p_i G_i dalam Lema 13.1.8.

Lema 13.1.9 *Misalkan G suatu grup-p abelian hingga dan andaikan $g \in G$ memiliki orde maksimum. Maka G isomorfik dengan $\langle g \rangle \times H$ untuk suatu subgrup H dari G.*

Bukti. Berdasarkan Lema 13.1.7, kita dapat mengandaikan bahwa orde G adalah p^n. Kita akan melakukan induksi pada n. Jika $n = 1$, maka G siklik berorde p dan harus dibangkitkan oleh g. Sekarang andaikan bahwa pernyataan lema berlaku untuk semua bilangan bulat k dengan $1 \leq k < n$, dan misalkan g memiliki orde maksimum dalam G, katakanlah $|g| = p^m$. Maka $a^{p^m} = e$ untuk semua $a \in G$. Sekarang pilih h dalam G sedemikian sehingga $h \notin \langle g \rangle$, dengan h memiliki orde sekecil mungkin. Elemen h semacam itu tentu ada; jika tidak, $G = \langle g \rangle$ dan pembuktian selesai. Misalkan $H = \langle h \rangle$.

Kita menyatakan bahwa $\langle g \rangle \cap H = \{e\}$. Cukup ditunjukkan bahwa $|H| = p$. Karena $|h^p| = |h|/p$, orde h^p lebih kecil daripada orde h dan harus berada dalam $\langle g \rangle$ berdasarkan minimalitas h; yaitu, $h^p = g^r$ untuk suatu bilangan r. Dengan demikian,

$$(g^r)^{p^{m-1}} = (h^p)^{p^{m-1}} = h^{p^m} = e,$$

dan orde g^r harus kurang dari atau sama dengan p^{m-1}. Oleh karena itu, g^r tidak dapat membangkitkan $\langle g \rangle$. Perhatikan bahwa p harus merupakan faktor dari r, katakanlah $r = ps$, dan $h^p = g^r = g^{ps}$. Definisikan a sebagai $g^{-s}h$. Maka a tidak mungkin berada dalam $\langle g \rangle$; jika tidak, h juga harus berada dalam $\langle g \rangle$. Selain itu,

$$a^p = g^{-sp}h^p = g^{-r}h^p = h^{-p}h^p = e.$$

Sekarang kita telah membentuk elemen a berorde p sedemikian sehingga $a \notin \langle g \rangle$. Karena h dipilih sebagai elemen berorde terkecil di antara semua elemen yang tidak berada dalam $\langle g \rangle$, $|H| = p$.

Sekarang kita akan menunjukkan bahwa orde gH dalam grup hasil bagi G/H harus sama dengan orde g dalam G. Jika $|gH| < |g| = p^m$, maka

$$H = (gH)^{p^{m-1}} = g^{p^{m-1}}H;$$

dengan demikian, $g^{p^{m-1}}$ harus berada dalam $\langle g \rangle \cap H = \{e\}$, yang bertentangan dengan fakta bahwa orde g adalah p^m. Oleh karena itu, gH harus memiliki orde maksimum dalam G/H. Berdasarkan Teorema Korespondensi dan hipotesis induksi,

$$G/H \cong \langle gH \rangle \times K/H$$

untuk suatu subgrup K dari G yang memuat H. Kita menyatakan bahwa $\langle g \rangle \cap K = \{e\}$. Jika $b \in \langle g \rangle \cap K$, maka $bH \in \langle gH \rangle \cap K/H = \{H\}$ dan $b \in \langle g \rangle \cap H = \{e\}$. Dengan demikian, $G = \langle g \rangle K$ mengakibatkan $G \cong \langle g \rangle \times K$. ■

Pembuktian Teorema Dasar Grup Abelian Hingga mengikuti dengan cepat dari Lema 13.1.8 dan Lema 13.1.9. Berdasarkan Lema 13.1.8, G merupakan hasil kali dari grup-grup yang masing-masing merupakan grup-p. Misalkan G suatu grup-p dan misalkan g elemen berorde maksimum dalam G. Jika $\langle g \rangle = G$, pembuktian selesai; jika tidak, $G \cong \mathbb{Z}_{|g|} \times H$ untuk suatu subgrup H yang termuat dalam G berdasarkan Lema 13.1.9. Karena $|H| < |G|$, kita dapat menerapkan induksi matematika.

Sekarang kita nyatakan teorema yang lebih umum untuk semua grup abelian yang dibangkitkan secara hingga. Pembuktian teorema ini dapat ditemukan

dalam setiap referensi pada akhir bab ini.

Teorema 13.1.10 Teorema Dasar Grup Abelian yang Dibangkitkan secara Hingga. *Setiap grup abelian G yang dibangkitkan secara hingga isomorfik dengan hasil kali langsung grup-grup siklik berbentuk*

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

dengan p_i bilangan-bilangan prima (yang tidak harus berbeda).

13.2 Grup Solvabel

Deret subnormal dari suatu grup G adalah barisan hingga subgrup

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\},$$

dengan H_i merupakan subgrup normal dari H_{i+1}. Jika setiap subgrup H_i normal dalam G, maka deret tersebut disebut **deret normal**. **Panjang** suatu deret subnormal atau deret normal adalah banyaknya inklusi sejati.

Contoh 13.2.1 Setiap deret subgrup dari suatu grup abelian merupakan deret normal. Tinjau deret grup berikut:

$$\mathbb{Z} \supset 9\mathbb{Z} \supset 45\mathbb{Z} \supset 180\mathbb{Z} \supset \{0\},$$
$$\mathbb{Z}_{24} \supset \langle 2\rangle \supset \langle 6\rangle \supset \langle 12\rangle \supset \{0\}.$$

▲

Contoh 13.2.2 Deret subnormal tidak harus merupakan deret normal. Tinjau deret subnormal berikut dari grup D_4:

$$D_4 \supset \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \supset \{(1), (1\,2)(3\,4)\} \supset \{(1)\}.$$

Subgrup $\{(1), (1\,2)(3\,4)\}$ tidak normal dalam D_4; akibatnya, deret ini bukan deret normal. ▲

Suatu deret subnormal (normal) $\{K_j\}$ merupakan **perhalusan dari deret subnormal (normal)** $\{H_i\}$ jika $\{H_i\} \subset \{K_j\}$. Artinya, setiap H_i merupakan salah satu K_j.

Contoh 13.2.3 Deret

$$\mathbb{Z} \supset 3\mathbb{Z} \supset 9\mathbb{Z} \supset 45\mathbb{Z} \supset 90\mathbb{Z} \supset 180\mathbb{Z} \supset \{0\}$$

merupakan perhalusan dari deret

$$\mathbb{Z} \supset 9\mathbb{Z} \supset 45\mathbb{Z} \supset 180\mathbb{Z} \supset \{0\}.$$

▲

Cara terbaik untuk mempelajari suatu deret subnormal atau normal dari subgrup-subgrup $\{H_i\}$ dari G sebenarnya adalah mempelajari grup hasil bagi H_{i+1}/H_i. Kita mengatakan bahwa dua deret subnormal (normal) $\{H_i\}$ dan $\{K_j\}$ dari suatu grup G **isomorfik** jika terdapat korespondensi satu-satu antara koleksi grup hasil bagi $\{H_{i+1}/H_i\}$ dan $\{K_{j+1}/K_j\}$.

Contoh 13.2.4 Kedua deret normal

$$\mathbb{Z}_{60} \supset \langle 3\rangle \supset \langle 15\rangle \supset \{0\}$$
$$\mathbb{Z}_{60} \supset \langle 4\rangle \supset \langle 20\rangle \supset \{0\}$$

dari grup $\mathbb{Z}_{60}$ isomorfik karena

$$\mathbb{Z}_{60}/\langle 3\rangle \cong \langle 20\rangle/\{0\} \cong \mathbb{Z}_3$$
$$\langle 3\rangle/\langle 15\rangle \cong \langle 4\rangle/\langle 20\rangle \cong \mathbb{Z}_5$$
$$\langle 15\rangle/\{0\} \cong \mathbb{Z}_{60}/\langle 4\rangle \cong \mathbb{Z}_4.$$

▲

Suatu deret subnormal $\{H_i\}$ dari grup G disebut **deret komposisi** jika semua grup hasil baginya sederhana; yaitu, jika tidak satu pun grup hasil bagi dalam deret tersebut memuat subgrup normal. Suatu deret normal $\{H_i\}$ dari G disebut **deret prinsipal** jika semua grup hasil baginya sederhana.

Contoh 13.2.5 Grup $\mathbb{Z}_{60}$ memiliki deret komposisi

$$\mathbb{Z}_{60} \supset \langle 3\rangle \supset \langle 15\rangle \supset \langle 30\rangle \supset \{0\}$$

dengan grup-grup hasil bagi

$$\mathbb{Z}_{60}/\langle 3\rangle \cong \mathbb{Z}_3$$
$$\langle 3\rangle/\langle 15\rangle \cong \mathbb{Z}_5$$
$$\langle 15\rangle/\langle 30\rangle \cong \mathbb{Z}_2$$
$$\langle 30\rangle/\{0\} \cong \mathbb{Z}_2.$$

Karena $\mathbb{Z}_{60}$ merupakan grup abelian, deret ini secara otomatis merupakan deret prinsipal. Perhatikan bahwa deret komposisi tidak harus tunggal. Deret

$$\mathbb{Z}_{60} \supset \langle 2\rangle \supset \langle 4\rangle \supset \langle 20\rangle \supset \{0\}$$

juga merupakan deret komposisi. ▲

Contoh 13.2.6 Untuk $n \geq 5$, deret

$$S_n \supset A_n \supset \{(1)\}$$

merupakan deret komposisi untuk S_n karena $S_n/A_n \cong \mathbb{Z}_2$ dan A_n sederhana. ▲

Contoh 13.2.7 Tidak setiap grup memiliki deret komposisi atau deret prinsipal. Misalkan

$$\{0\} = H_0 \subset H_1 \subset \cdots \subset H_{n-1} \subset H_n = \mathbb{Z}$$

merupakan deret subnormal untuk bilangan bulat terhadap penjumlahan. Maka H_1 harus berbentuk $k\mathbb{Z}$ untuk suatu $k \in \mathbb{N}$. Dalam hal ini, $H_1/H_0 \cong k\mathbb{Z}$ merupakan grup siklik tak hingga dengan banyak subgrup normal sejati nontrivial. ▲

Meskipun deret komposisi tidak harus tunggal, seperti dalam kasus $\mathbb{Z}_{60}$, ternyata sebarang dua deret komposisi saling berkaitan. Grup-grup hasil bagi dari kedua deret komposisi untuk $\mathbb{Z}_{60}$ adalah $\mathbb{Z}_2$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, dan $\mathbb{Z}_5$; yaitu, kedua deret komposisi tersebut isomorfik. Teorema Jordan-Hölder menyatakan bahwa hal ini selalu berlaku.

Teorema 13.2.8 Jordan-Hölder. *Sebarang dua deret komposisi dari G isomorfik.*

Bukti. Kita akan menggunakan induksi matematika pada panjang deret komposisi. Jika panjang suatu deret komposisi adalah 1, maka G harus merupakan grup sederhana. Dalam kasus ini, sebarang dua deret komposisi isomorfik.

Sekarang andaikan bahwa teorema tersebut benar untuk semua grup yang

memiliki deret komposisi dengan panjang k, dengan $1 \leq k < n$. Misalkan

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\}$$
$$G = K_m \supset K_{m-1} \supset \cdots \supset K_1 \supset K_0 = \{e\}$$

merupakan dua deret komposisi untuk G. Kita dapat membentuk dua deret subnormal baru untuk G karena $H_i \cap K_{m-1}$ normal dalam $H_{i+1} \cap K_{m-1}$ dan $K_j \cap H_{n-1}$ normal dalam $K_{j+1} \cap H_{n-1}$:

$$G = H_n \supset H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_0 \cap K_{m-1} = \{e\}$$
$$G = K_m \supset K_{m-1} \supset K_{m-1} \cap H_{n-1} \supset \cdots \supset K_0 \cap H_{n-1} = \{e\}.$$

Karena $H_i \cap K_{m-1}$ normal dalam $H_{i+1} \cap K_{m-1}$, Teorema Isomorfisma Kedua (Teorema 11.2.3) mengakibatkan bahwa

$$\begin{aligned}(H_{i+1} \cap K_{m-1})/(H_i \cap K_{m-1}) &= (H_{i+1} \cap K_{m-1})/(H_i \cap (H_{i+1} \cap K_{m-1})) \\ &\cong H_i(H_{i+1} \cap K_{m-1})/H_i,\end{aligned}$$

dengan H_i normal dalam $H_i(H_{i+1} \cap K_{m-1})$. Karena $\{H_i\}$ merupakan deret komposisi, H_{i+1}/H_i harus sederhana; akibatnya, $H_i(H_{i+1} \cap K_{m-1})/H_i$ adalah H_{i+1}/H_i atau H_i/H_i. Artinya, $H_i(H_{i+1} \cap K_{m-1})$ harus merupakan H_i atau H_{i+1}. Dengan menghapus setiap inklusi yang tidak sejati dari deret

$$H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_0 \cap K_{m-1} = \{e\},$$

kita memperoleh deret komposisi untuk H_{n-1}. Hipotesis induksi menyatakan bahwa deret ini harus ekuivalen dengan deret komposisi

$$H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\}.$$

Dengan demikian, deret komposisi

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\}$$

dan

$$G = H_n \supset H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_0 \cap K_{m-1} = \{e\}$$

ekuivalen. Jika $H_{n-1} = K_{m-1}$, maka deret komposisi $\{H_i\}$ dan $\{K_j\}$ ekuivalen dan pembuktian selesai; jika tidak, $H_{n-1}K_{m-1}$ merupakan subgrup normal dari G yang memuat H_{n-1} secara sejati. Dalam hal ini, $H_{n-1}K_{m-1} = G$ dan kita dapat menerapkan Teorema Isomorfisma Kedua sekali lagi; yaitu,

$$K_{m-1}/(K_{m-1} \cap H_{n-1}) \cong (H_{n-1}K_{m-1})/H_{n-1} = G/H_{n-1}.$$

Oleh karena itu,

$$G = H_n \supset H_{n-1} \supset H_{n-1} \cap K_{m-1} \supset \cdots \supset H_0 \cap K_{m-1} = \{e\}$$

dan

$$G = K_m \supset K_{m-1} \supset K_{m-1} \cap H_{n-1} \supset \cdots \supset K_0 \cap H_{n-1} = \{e\}$$

ekuivalen, dan pembuktian teorema selesai. ■

Suatu grup G disebut **solvabel** jika grup tersebut memiliki deret subnormal $\{H_i\}$ sedemikian sehingga semua grup hasil bagi H_{i+1}/H_i abelian. Grup solvabel akan memainkan peran mendasar ketika kita mempelajari teori Galois dan penyelesaian persamaan polinomial.

Contoh 13.2.9 Grup S_4 solvabel karena

$$S_4 \supset A_4 \supset \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \supset \{(1)\}$$

memiliki grup-grup hasil bagi abelian; namun, untuk $n \geq 5$, deret

$$S_n \supset A_n \supset \{(1)\}$$

merupakan deret komposisi untuk S_n dengan suatu grup hasil bagi nonabelian. Oleh karena itu, S_n bukan grup solvabel untuk $n \geq 5$. ▲

13.3 Pertanyaan Bacaan

1. Ada berapa banyak grup abelian berorde $200 = 2^3 5^2$?

2. Ada berapa banyak grup abelian berorde $729 = 3^6$?

3. Temukan subgrup berorde 6 dalam $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

4. Dapat ditunjukkan bahwa suatu grup abelian berorde 72 memuat subgrup berorde 8. Apa saja kemungkinan untuk subgrup ini?

5. Apakah deret prinsipal dari grup G itu? Jawaban Anda tidak boleh menggunakan istilah baru yang didefinisikan dalam bab ini.

13.4 Latihan

1. Temukan semua grup abelian berorde kurang dari atau sama dengan 40 hingga isomorfisma.

Petunjuk. Terdapat tiga grup yang mungkin.

2. Temukan semua grup abelian berorde 200 hingga isomorfisma.

3. Temukan semua grup abelian berorde 720 hingga isomorfisma.

4. Temukan semua deret komposisi untuk setiap grup berikut.

(a) $\mathbb{Z}_{12}$

(b) $\mathbb{Z}_{48}$

(c) Kuaternion, Q_8

(d) D_4

(e) $S_3 \times \mathbb{Z}_4$

(f) S_4

(g) S_n, $n \geq 5$

(h) $\mathbb{Q}$

Petunjuk. (a) $\{0\} \subset \langle 6\rangle \subset \langle 3\rangle \subset \mathbb{Z}_{12}$; (e) $\{(1)\} \times \{0\} \subset \{(1), (1\,2\,3), (1\,3\,2)\} \times \{0\} \subset S_3 \times \{0\} \subset S_3 \times \langle 2\rangle \subset S_3 \times \mathbb{Z}_4$.

5. Tunjukkan bahwa hasil kali langsung tak hingga $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$ tidak dibangkitkan secara hingga.

6. Misalkan G suatu grup abelian berorde m. Jika n membagi m, buktikan bahwa G memiliki subgrup berorde n.

7. Suatu grup G disebut **grup torsi** jika setiap elemen G memiliki orde hingga. Buktikan bahwa grup torsi abelian yang dibangkitkan secara hingga harus merupakan grup hingga.

Petunjuk. Gunakan Teorema Dasar Grup Abelian yang Dibangkitkan secara Hingga.

8. Misalkan G, H, dan K merupakan grup-grup abelian yang dibangkitkan secara hingga. Tunjukkan bahwa jika $G \times H \cong G \times K$, maka $H \cong K$. Berikan contoh penyangkal untuk menunjukkan bahwa pernyataan ini tidak selalu benar secara umum.

9. Misalkan G dan H merupakan grup solvabel. Tunjukkan bahwa $G \times H$ juga solvabel.

10. Jika G memiliki deret komposisi (prinsipal) dan jika N merupakan subgrup normal sejati dari G, tunjukkan bahwa terdapat deret komposisi (prinsipal) yang memuat N.

11. Buktikan atau bantah: Misalkan N suatu subgrup normal dari G. Jika N dan G/N memiliki deret komposisi, maka G juga harus memiliki deret komposisi.

12. Misalkan N suatu subgrup normal dari G. Jika N dan G/N merupakan grup solvabel, tunjukkan bahwa G juga merupakan grup solvabel.

Petunjuk. Jika N dan G/N solvabel, maka keduanya memiliki deret solvabel

$$N = N_n \supset N_{n-1} \supset \cdots \supset N_1 \supset N_0 = \{e\}$$
$$G/N = G_n/N \supset G_{n-1}/N \supset \cdots G_1/N \supset G_0/N = \{N\}.$$

13. Buktikan bahwa G merupakan grup solvabel jika dan hanya jika G memiliki deret subgrup

$$G = P_n \supset P_{n-1} \supset \cdots \supset P_1 \supset P_0 = \{e\}$$

dengan P_i normal dalam P_{i+1} dan orde P_{i+1}/P_i prima.

14. Misalkan G suatu grup solvabel. Buktikan bahwa setiap subgrup dari G juga solvabel.

15. Misalkan G suatu grup solvabel dan N suatu subgrup normal dari G. Buktikan bahwa G/N solvabel.

16. Buktikan bahwa D_n solvabel untuk semua bilangan bulat n.

Petunjuk. Gunakan fakta bahwa D_n memiliki subgrup siklik berindeks 2.

17. Misalkan G memiliki deret komposisi. Jika N merupakan subgrup normal dari G, tunjukkan bahwa N dan G/N juga memiliki deret komposisi.

18. Misalkan G suatu grup-p siklik dengan subgrup H dan K. Buktikan bahwa H termuat dalam K atau K termuat dalam H.

19. Misalkan G suatu grup solvabel berorde $n \geq 2$. Tunjukkan bahwa G memuat subgrup abelian normal nontrivial.

20. Ingat bahwa **subgrup komutator** G' dari suatu grup G didefinisikan sebagai subgrup dari G yang dibangkitkan oleh elemen-elemen berbentuk $a^{-1}b^{-1}ab$ untuk $a, b \in G$. Kita dapat mendefinisikan deret subgrup dari G dengan $G^{(0)} = G$, $G^{(1)} = G'$, dan $G^{(i+1)} = (G^{(i)})'$.

(a) Buktikan bahwa $G^{(i+1)}$ normal dalam $(G^{(i)})'$. Deret subgrup

$$G^{(0)} = G \supset G^{(1)} \supset G^{(2)} \supset \cdots$$

disebut **deret turunan** dari G.

(b) Tunjukkan bahwa G solvabel jika dan hanya jika $G^{(n)} = \{e\}$ untuk suatu bilangan bulat n.

21. Misalkan G suatu grup solvabel berorde $n \geq 2$. Tunjukkan bahwa G memuat grup hasil bagi abelian normal nontrivial.

Petunjuk. G/G' abelian.

22. **Lema Zassenhaus.** Misalkan H dan K merupakan subgrup dari suatu grup G. Andaikan pula bahwa H^* dan K^* berturut-turut merupakan subgrup normal dari H dan K. Maka

(a) $H^*(H \cap K^*)$ merupakan subgrup normal dari $H^*(H \cap K)$.

(b) $K^*(H^* \cap K)$ merupakan subgrup normal dari $K^*(H \cap K)$.

(c) $H^*(H \cap K)/H^*(H \cap K^*) \cong K^*(H \cap K)/K^*(H^* \cap K) \cong (H \cap K)/(H^* \cap K)(H \cap K^*)$.

23. **Teorema Schreier.** Gunakan Lema Zassenhaus untuk membuktikan bahwa dua deret subnormal (normal) dari suatu grup G memiliki perhalusan yang isomorfik.

24. Gunakan Teorema Schreier untuk membuktikan Teorema Jordan-Hölder.

13.5 Latihan Pemrograman

1. Tulis program yang menghitung semua kemungkinan grup abelian berorde n. Berapakah nilai n terbesar yang dapat ditangani program Anda?

13.6 Referensi dan Bacaan yang Disarankan

[1] Hungerford, T. W. *Algebra*. Springer, New York, 1974.

[2] Lang, S. *Algebra*. 3rd ed. Springer, New York, 2002.

[3] Rotman, J. J. *An Introduction to the Theory of Groups*. 4th ed. Springer, New York, 1995.

14

Aksi Grup

Aksi grup memperumum perkalian grup. Jika G adalah suatu grup dan X adalah himpunan sebarang, aksi grup dari suatu unsur $g \in G$ pada $x \in X$ adalah hasil kali gx yang berada dalam X. Banyak masalah dalam aljabar paling baik ditangani melalui aksi grup. Sebagai contoh, pembuktian teorema-teorema Sylow dan Teorema Pencacahan Burnside paling mudah dipahami apabila dirumuskan dalam aksi grup.

14.1 Grup yang Beraksi pada Himpunan

Misalkan X adalah suatu himpunan dan G adalah suatu grup. Suatu **aksi (kiri)** dari G pada X adalah pemetaan $G \times X \to X$ yang diberikan oleh $(g, x) \mapsto gx$, dengan

1. $ex = x$ untuk semua $x \in X$;
2. $(g_1 g_2)x = g_1(g_2 x)$ untuk semua $x \in X$ dan semua $g_1, g_2 \in G$.

Dalam keadaan ini, X disebut **himpunan-G**. Perhatikan bahwa kita tidak mensyaratkan X berhubungan dengan G dengan cara apa pun. Memang, setiap grup G beraksi pada setiap himpunan X melalui aksi trivial $(g, x) \mapsto x$; namun, aksi grup lebih menarik apabila himpunan X memiliki hubungan tertentu dengan grup G.

Contoh 14.1.1 Misalkan $G = GL_2(\mathbb{R})$ dan $X = \mathbb{R}^2$. Maka G beraksi pada X melalui perkalian kiri. Jika $v \in \mathbb{R}^2$ dan I adalah matriks identitas, maka $Iv = v$. Jika A dan B adalah matriks invertibel 2×2, maka $(AB)v = A(Bv)$ karena perkalian matriks bersifat asosiatif. ▲

Contoh 14.1.2 Misalkan $G = D_4$ adalah grup simetri sebuah persegi. Jika $X = \{1, 2, 3, 4\}$ adalah himpunan titik sudut persegi tersebut, maka kita dapat memandang D_4 sebagai himpunan yang terdiri atas permutasi-permutasi berikut:

$$\{(1), (1\,3), (2\,4), (1\,4\,3\,2), (1\,2\,3\,4), (1\,2)(3\,4), (1\,4)(2\,3), (1\,3)(2\,4)\}.$$

Unsur-unsur D_4 beraksi pada X sebagai fungsi. Permutasi $(1\,3)(2\,4)$ beraksi pada titik sudut 1 dengan memetakannya ke titik sudut 3, pada titik sudut 2 dengan memetakannya ke titik sudut 4, dan seterusnya. Mudah dilihat bahwa aksi tersebut memenuhi aksioma-aksioma aksi grup. ▲

Secara umum, jika X adalah sebarang himpunan dan G adalah subgrup dari S_X, yaitu grup semua permutasi yang beraksi pada X, maka X merupakan himpunan-G di bawah aksi grup

$$(\sigma, x) \mapsto \sigma(x)$$

untuk $\sigma \in G$ dan $x \in X$.

Contoh 14.1.3 Jika kita menetapkan $X = G$, maka setiap grup G beraksi pada dirinya sendiri melalui representasi reguler kiri; yaitu, $(g, x) \mapsto \lambda_g(x) = gx$, dengan λ_g sebagai perkalian kiri:

$$e \cdot x = \lambda_e x = ex = x$$
$$(gh) \cdot x = \lambda_{gh} x = \lambda_g \lambda_h x = \lambda_g(hx) = g \cdot (h \cdot x).$$

Jika H adalah subgrup dari G, maka G merupakan himpunan-H di bawah perkalian kiri oleh unsur-unsur H. ▲

Contoh 14.1.4 Misalkan G adalah suatu grup dan misalkan $X = G$. Jika H adalah subgrup dari G, maka G merupakan himpunan-H di bawah **konjugasi**; yaitu, kita dapat mendefinisikan suatu aksi H pada G,

$$H \times G \to G,$$

melalui

$$(h, g) \mapsto hgh^{-1}$$

untuk $h \in H$ dan $g \in G$. Jelas bahwa aksioma pertama aksi grup berlaku. Dengan memperhatikan bahwa

$$\begin{aligned}(h_1h_2, g) &= h_1h_2g(h_1h_2)^{-1} \\ &= h_1(h_2gh_2^{-1})h_1^{-1} \\ &= (h_1, (h_2, g)),\end{aligned}$$

kita melihat bahwa syarat kedua juga dipenuhi. ▲

Contoh 14.1.5 Misalkan H adalah subgrup dari G dan $\mathcal{L}_H$ adalah himpunan koset kiri H. Himpunan $\mathcal{L}_H$ merupakan himpunan-G di bawah aksi

$$(g, xH) \mapsto gxH.$$

Sekali lagi, mudah dilihat bahwa aksioma pertama berlaku. Karena $(gg')xH = g(g'xH)$, aksioma kedua juga berlaku. ▲

Jika G beraksi pada suatu himpunan X dan $x, y \in X$, maka x dikatakan **ekuivalen-G** dengan y jika terdapat $g \in G$ sedemikian sehingga $gx = y$. Kita menulis $x \sim_G y$ atau $x \sim y$ jika kedua unsur ekuivalen-G.

Proposisi 14.1.6 *Misalkan X merupakan himpunan-G. Maka ekuivalensi-G merupakan relasi ekuivalensi pada X.*

Bukti. Relasi $\sim$ bersifat refleksif karena $ex = x$. Misalkan $x \sim y$ untuk $x, y \in X$. Maka terdapat g sedemikian sehingga $gx = y$. Dalam hal ini $g^{-1}y = x$; jadi, $y \sim x$. Untuk menunjukkan bahwa relasi tersebut transitif, misalkan $x \sim y$ dan $y \sim z$. Maka harus terdapat unsur-unsur grup g dan h sedemikian sehingga $gx = y$ dan $hy = z$. Jadi, $z = hy = (hg)x$, dan x ekuivalen dengan z. ■

Jika X merupakan himpunan-G, maka setiap partisi X yang terkait dengan ekuivalensi-G disebut **orbit** dari X di bawah G. Kita akan menyatakan orbit yang memuat suatu unsur x dari X dengan $\mathcal{O}_x$.

Contoh 14.1.7 Misalkan G adalah grup permutasi yang didefinisikan oleh

$$G = \{(1), (1\,2\,3), (1\,3\,2), (4\,5), (1\,2\,3)(4\,5), (1\,3\,2)(4\,5)\}$$

dan $X = \{1, 2, 3, 4, 5\}$. Maka X merupakan himpunan-G. Orbit-orbitnya adalah $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1, 2, 3\}$ dan $\mathcal{O}_4 = \mathcal{O}_5 = \{4, 5\}$. ▲

Sekarang, misalkan G adalah grup yang beraksi pada suatu himpunan X dan misalkan g adalah unsur G. **Himpunan titik tetap** dari g dalam X, yang dinyatakan dengan X_g, adalah himpunan semua $x \in X$ sedemikian sehingga $gx = x$. Kita juga dapat mempelajari unsur-unsur grup g yang menetapkan suatu $x \in X$. Himpunan ini bukan sekadar himpunan bagian dari G, melainkan suatu subgrup. Subgrup ini disebut **subgrup penstabil** atau **subgrup isotropi** dari x. Kita akan menyatakan subgrup penstabil dari x dengan G_x.

Catatan 14.1.8 Penting untuk diingat bahwa $X_g \subset X$ dan $G_x \subset G$.

Contoh 14.1.9 Misalkan $X = \{1, 2, 3, 4, 5, 6\}$ dan misalkan G adalah grup permutasi yang diberikan oleh permutasi-permutasi

$$\{(1), (1\,2)(3\,4\,5\,6), (3\,5)(4\,6), (1\,2)(3\,6\,5\,4)\}.$$

Maka himpunan-himpunan titik tetap dari X di bawah aksi G adalah

$$\begin{aligned} X_{(1)} &= X, \\ X_{(3\,5)(4\,6)} &= \{1, 2\}, \\ X_{(1\,2)(3\,4\,5\,6)} &= X_{(1\,2)(3\,6\,5\,4)} = \emptyset, \end{aligned}$$

dan subgrup-subgrup penstabilnya adalah

$$\begin{aligned} G_1 = G_2 &= \{(1), (3\,5)(4\,6)\}, \\ G_3 = G_4 = G_5 &= G_6 = \{(1)\}. \end{aligned}$$

Mudah dilihat bahwa G_x merupakan subgrup dari G untuk setiap $x \in X$. ▲

Proposisi 14.1.10 *Misalkan G adalah grup yang beraksi pada suatu himpunan X dan $x \in X$. Grup penstabil dari x, G_x, merupakan subgrup dari G.*

Bukti. Jelas bahwa $e \in G_x$ karena identitas menetapkan setiap unsur dalam himpunan X. Misalkan $g, h \in G_x$. Maka $gx = x$ dan $hx = x$. Jadi, $(gh)x = g(hx) = gx = x$; dengan demikian, hasil kali dua unsur dalam G_x juga berada dalam G_x. Terakhir, jika $g \in G_x$, maka $x = ex = (g^{-1}g)x = (g^{-1})gx = g^{-1}x$. Jadi, g^{-1} berada dalam G_x. ■

Kita akan menyatakan banyaknya unsur dalam himpunan titik tetap suatu unsur $g \in G$ dengan $|X_g|$ dan banyaknya unsur dalam orbit $x \in X$ dengan $|\mathcal{O}_x|$. Teorema berikut menunjukkan hubungan antara orbit suatu unsur $x \in X$ dan koset-koset kiri G_x dalam G.

Teorema 14.1.11 *Misalkan G adalah grup hingga dan X adalah himpunan-G hingga. Jika $x \in X$, maka $|\mathcal{O}_x| = [G : G_x]$.*

Bukti. Kita mengetahui bahwa $|G|/|G_x|$ adalah banyaknya koset kiri G_x dalam G berdasarkan Teorema Lagrange (Teorema 6.2.2). Kita akan mendefinisikan pemetaan bijektif ϕ antara orbit $\mathcal{O}_x$ dari X dan himpunan koset kiri $\mathcal{L}_{G_x}$ dari G_x dalam G. Misalkan $y \in \mathcal{O}_x$. Maka terdapat g dalam G sedemikian sehingga $gx = y$. Definisikan ϕ dengan $\phi(y) = gG_x$. Untuk menunjukkan bahwa ϕ satu-satu, asumsikan bahwa $\phi(y_1) = \phi(y_2)$. Maka

$$\phi(y_1) = g_1G_x = g_2G_x = \phi(y_2),$$

dengan $g_1x = y_1$ dan $g_2x = y_2$. Karena $g_1G_x = g_2G_x$, terdapat $g \in G_x$ sedemikian sehingga $g_2 = g_1g$,

$$y_2 = g_2x = g_1gx = g_1x = y_1;$$

akibatnya, pemetaan ϕ satu-satu. Terakhir, kita harus menunjukkan bahwa pemetaan ϕ surjektif. Misalkan gG_x adalah suatu koset kiri. Jika $gx = y$, maka $\phi(y) = gG_x$. ■

14.2 Persamaan Kelas

Misalkan X adalah himpunan-G hingga dan X_G adalah himpunan titik tetap dalam X; yaitu,

$$X_G = \{x \in X : gx = x \text{ untuk semua } g \in G\}.$$

Karena orbit-orbit aksi tersebut mempartisi X,

$$|X| = |X_G| + \sum_{i=k}^{n} |\mathcal{O}_{x_i}|,$$

dengan $x_k, \ldots, x_n$ sebagai wakil dari orbit-orbit taktrivial yang berbeda dari X.

Sekarang, tinjau kasus khusus ketika G beraksi pada dirinya sendiri melalui konjugasi, $(g, x) \mapsto gxg^{-1}$. **Pusat** dari G,

$$Z(G) = \{x : xg = gx \text{ untuk semua } g \in G\},$$

adalah himpunan titik yang tetap di bawah konjugasi. Orbit-orbit taktrivial dari aksi tersebut disebut **kelas konjugasi** dari G. Jika $x_1, \ldots, x_k$ merupakan wakil dari setiap kelas konjugasi taktrivial dari G dan $|\mathcal{O}_{x_1}| = n_1, \ldots, |\mathcal{O}_{x_k}| = n_k$, maka

$$|G| = |Z(G)| + n_1 + \cdots + n_k.$$

Subgrup penstabil dari setiap x_i, yaitu $C(x_i) = \{g \in G : gx_i = x_ig\}$, disebut **subgrup pemusat** dari x_i. Dari Teorema 14.1.11, kita memperoleh **persamaan kelas**:

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)].$$

Salah satu konsekuensi persamaan kelas adalah bahwa orde setiap kelas konjugasi harus membagi orde G.

Contoh 14.2.1 Mudah diperiksa bahwa kelas-kelas konjugasi dalam S_3 adalah sebagai berikut:

$$\{(1)\}, \quad \{(1\,2\,3), (1\,3\,2)\}, \quad \{(1\,2), (1\,3), (2\,3)\}.$$

Persamaan kelasnya adalah $6 = 1 + 2 + 3$. ▲

Contoh 14.2.2 Pusat D_4 adalah $\{(1), (1\,3)(2\,4)\}$, dan kelas-kelas konjugasinya adalah

$$\{(1\,3), (2\,4)\}, \quad \{(1\,4\,3\,2), (1\,2\,3\,4)\}, \quad \{(1\,2)(3\,4), (1\,4)(2\,3)\}.$$

Jadi, persamaan kelas untuk D_4 adalah $8 = 2 + 2 + 2 + 2$. ▲

Contoh 14.2.3 Untuk S_n, diperlukan sedikit usaha untuk mencari kelas-kelas konjugasinya. Kita mulai dengan siklus. Misalkan $\sigma = (a_1, \ldots, a_k)$ adalah suatu siklus dan misalkan $\tau \in S_n$. Berdasarkan Teorema 6.2.8,

$$\tau\sigma\tau^{-1} = (\tau(a_1), \ldots, \tau(a_k)).$$

Akibatnya, setiap dua siklus yang panjangnya sama saling berkonjugasi. Sekarang, misalkan $\sigma = \sigma_1\sigma_2\cdots\sigma_r$ adalah suatu dekomposisi siklus, dengan panjang setiap siklus σ_i adalah r_i. Maka σ berkonjugasi dengan setiap $\tau \in S_n$ lain yang dekomposisi siklusnya mempunyai panjang yang sama.

Banyaknya kelas konjugasi dalam S_n sama dengan banyaknya cara n dapat dipartisi menjadi jumlah bilangan bulat positif. Dalam kasus S_3, sebagai contoh, kita dapat mempartisi bilangan bulat 3 menjadi tiga jumlah berikut:

$$\begin{aligned} 3 &= 1+1+1 \\ 3 &= 1+2 \\ 3 &= 3; \end{aligned}$$

oleh karena itu, terdapat tiga kelas konjugasi. Ada variasi dari masalah pencarian banyaknya partisi semacam itu untuk sebarang bilangan bulat positif n yang disebut ilmuwan komputer sebagai **NP-complete**. Hal ini pada praktiknya berarti bahwa masalah tersebut tidak dapat diselesaikan untuk n yang besar karena perhitungannya akan memakan waktu terlalu lama, bahkan bagi komputer terbesar sekalipun. ▲

Teorema 14.2.4 *Misalkan G adalah grup berorde p^n dengan p prima. Maka G memiliki pusat taktrivial.*

Bukti. Kita menerapkan persamaan kelas

$$|G| = |Z(G)| + n_1 + \cdots + n_k.$$

Karena setiap $n_i > 1$ dan $n_i \mid |G|$, diperoleh bahwa p harus membagi setiap n_i. Selain itu, $p \mid |G|$; jadi, p harus membagi $|Z(G)|$. Karena identitas selalu berada dalam pusat G, $|Z(G)| \geq 1$. Oleh karena itu, $|Z(G)| \geq p$, dan terdapat suatu $g \in Z(G)$ sedemikian sehingga $g \neq 1$. ■

Korolari 14.2.5 *Misalkan G adalah grup berorde p^2 dengan p prima. Maka G abelian.*

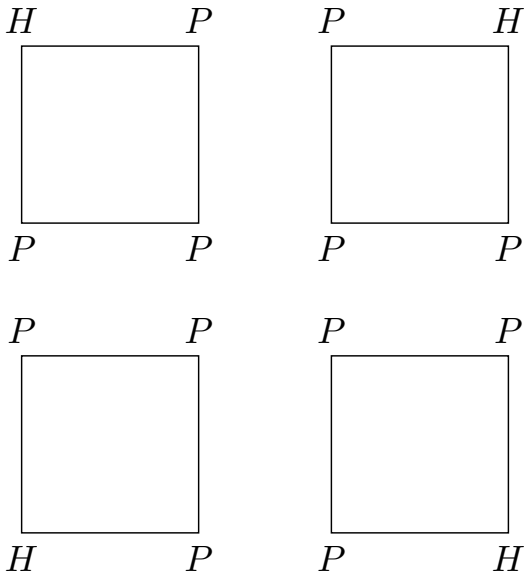
Bukti. Berdasarkan Teorema 14.2.4, $|Z(G)| = p$ atau p^2. Misalkan $|Z(G)| = p$. Maka $Z(G)$ dan $G/Z(G)$ keduanya berorde p dan keduanya pasti merupakan grup siklik. Dengan memilih pembangkit $aZ(G)$ untuk $G/Z(G)$, kita dapat menulis setiap unsur $gZ(G)$ dalam grup hasil bagi sebagai $a^mZ(G)$ untuk suatu bilangan bulat m; jadi, $g = a^mx$ untuk suatu x dalam pusat G. Demikian pula, jika $hZ(G) \in G/Z(G)$, terdapat y dalam $Z(G)$ sedemikian sehingga $h = a^ny$ untuk suatu bilangan bulat n. Karena x dan y berada dalam pusat G, keduanya komutatif dengan semua unsur lain dari G; oleh karena itu,

$$gh = a^mxa^ny = a^{m+n}xy = a^nya^mx = hg,$$

dan G pasti abelian. Jadi, $|Z(G)| = p^2$. ■

14.3 Teorema Pencacahan Burnside

Misalkan kita ingin mewarnai titik-titik sudut suatu persegi dengan dua warna berbeda, misalnya hitam dan putih. Kita mungkin menduga bahwa terdapat $2^4 = 16$ pewarnaan yang berbeda. Namun, sebagian pewarnaan tersebut ekuivalen. Jika kita mewarnai titik sudut pertama dengan hitam dan titik-titik sudut lainnya dengan putih, hasilnya sama dengan mewarnai titik sudut kedua dengan hitam dan yang lainnya dengan putih, sebab pewarnaan kedua dapat diperoleh hanya dengan memutar persegi tersebut sebesar 90° (Gambar 14.3.1).



Gambar 14.3.1 Pewarnaan persegi yang ekuivalen

Teorema Pencacahan Burnside memberikan metode untuk menghitung banyaknya cara yang dapat dibedakan dalam melakukan sesuatu. Selain penerapan geometrisnya, teorema ini memiliki penerapan menarik dalam teori pensakelaran dan kimia. Pembuktian Teorema Pencacahan Burnside bergantung pada lema berikut.

Lema 14.3.2 *Misalkan X adalah himpunan-G dan misalkan $x \sim y$. Maka G_x isomorfik dengan G_y. Secara khusus, $|G_x| = |G_y|$.*

Bukti. Misalkan G beraksi pada X melalui $(g, x) \mapsto g \cdot x$. Karena $x \sim y$, terdapat $g \in G$ sedemikian sehingga $g \cdot x = y$. Misalkan $a \in G_x$. Karena

$$gag^{-1} \cdot y = ga \cdot g^{-1}y = ga \cdot x = g \cdot x = y,$$

kita dapat mendefinisikan pemetaan $\phi : G_x \to G_y$ dengan $\phi(a) = gag^{-1}$. Pemetaan ϕ merupakan homomorfisma karena

$$\phi(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \phi(a)\phi(b).$$

Misalkan $\phi(a) = \phi(b)$. Maka $gag^{-1} = gbg^{-1}$ atau $a = b$; jadi, pemetaan tersebut injektif. Untuk menunjukkan bahwa ϕ surjektif, misalkan b berada dalam G_y; maka $g^{-1}bg$ berada dalam G_x karena

$$g^{-1}bg \cdot x = g^{-1}b \cdot gx = g^{-1}b \cdot y = g^{-1} \cdot y = x;$$

dan $\phi(g^{-1}bg) = b$. ■

Teorema 14.3.3 Burnside. *Misalkan G adalah grup hingga yang beraksi pada suatu himpunan X dan misalkan k menyatakan banyaknya orbit X. Maka*

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

BUKTI. Kita meninjau semua titik tetap x dari semua unsur $g \in G$; artinya, kita meninjau semua g dan semua x sedemikian sehingga $gx = x$. Jika dipandang dari segi himpunan titik tetap, banyaknya semua g yang menetapkan x adalah

$$\sum_{g \in G} |X_g|.$$

Namun, jika dipandang dari segi subgrup penstabil, bilangan ini adalah

$$\sum_{x \in X} |G_x|;$$

jadi, $\sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|$. Berdasarkan Lema 14.3.2,

$$\sum_{y \in \mathcal{O}_x} |G_y| = |\mathcal{O}_x| \cdot |G_x|.$$

Berdasarkan Teorema 14.1.11 dan Teorema Lagrange, ekspresi ini sama dengan $|G|$. Dengan menjumlahkan atas semua k orbit yang berbeda, kita menyimpulkan bahwa

$$\sum_{g \in G} |X_g| = \sum_{x \in X} |G_x| = k \cdot |G|.$$

■

Contoh 14.3.4 Misalkan $X = \{1, 2, 3, 4, 5\}$ dan misalkan G adalah grup permutasi $G = \{(1), (1\,3), (1\,3)(2\,5), (2\,5)\}$. Orbit-orbit X adalah $\{1, 3\}$, $\{2, 5\}$, dan $\{4\}$. Himpunan-himpunan titik tetapnya adalah

$$\begin{aligned} X_{(1)} &= X \\ X_{(1\,3)} &= \{2, 4, 5\} \\ X_{(1\,3)(2\,5)} &= \{4\} \\ X_{(2\,5)} &= \{1, 3, 4\}. \end{aligned}$$

Teorema Burnside menyatakan bahwa

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g| = \frac{1}{4}(5 + 3 + 1 + 3) = 3.$$

▲

14.3.1 Contoh Geometris

Sebelum kita menerapkan Teorema Burnside pada masalah teori pensakelaran, mari kita periksa banyaknya cara titik-titik sudut suatu persegi dapat diwarnai hitam atau putih. Perhatikan bahwa terkadang kita dapat memperoleh pewarnaan yang ekuivalen hanya dengan menerapkan gerak kaku pada persegi tersebut. Sebagai contoh, seperti telah kita tunjukkan, jika salah satu titik sudut kita warnai hitam dan tiga lainnya putih, titik sudut mana yang diwarnai hitam tidaklah penting karena suatu rotasi akan menghasilkan pewarnaan

yang ekuivalen.

Grup simetri suatu persegi, D_4, diberikan oleh permutasi-permutasi berikut:

(1)	$(1\,3)$	$(2\,4)$	$(1\,4\,3\,2)$
$(1\,2\,3\,4)$	$(1\,2)(3\,4)$	$(1\,4)(2\,3)$	$(1\,3)(2\,4)$

Grup G beraksi pada himpunan titik sudut $\{1, 2, 3, 4\}$ dengan cara biasa. Kita dapat mendeskripsikan pewarnaan-pewarnaan yang berbeda melalui pemetaan dari X ke $Y = \{H, P\}$, dengan H dan P masing-masing merepresentasikan warna hitam dan putih. Setiap pemetaan $f : X \to Y$ mendeskripsikan suatu cara mewarnai sudut-sudut persegi. Setiap $\sigma \in D_4$ menginduksi suatu permutasi $\widetilde{\sigma}$ pada semua pewarnaan yang mungkin, yang diberikan oleh $\widetilde{\sigma}(f) = f \circ \sigma$ untuk $f : X \to Y$. Sebagai contoh, misalkan f didefinisikan oleh

$$\begin{aligned} f(1) &= B \\ f(2) &= W \\ f(3) &= W \\ f(4) &= W \end{aligned}$$

dan $\sigma = (12)(34)$. Maka $\widetilde{\sigma}(f) = f \circ \sigma$ memetakan titik sudut 2 ke H dan titik-titik sudut lainnya ke P. Himpunan semua $\widetilde{\sigma}$ semacam ini merupakan grup permutasi $\widetilde{G}$ pada himpunan semua pewarnaan yang mungkin. Misalkan $\widetilde{X}$ menyatakan himpunan semua pewarnaan yang mungkin; yaitu, $\widetilde{X}$ adalah himpunan semua pemetaan yang mungkin dari X ke Y. Sekarang kita harus menghitung banyaknya kelas ekuivalensi-$\widetilde{G}$.

1. $\widetilde{X}_{(1)} = \widetilde{X}$ karena identitas menetapkan setiap pewarnaan yang mungkin. $|\widetilde{X}| = 2^4 = 16$.
2. $\widetilde{X}_{(1\,2\,3\,4)}$ terdiri atas semua $f \in \widetilde{X}$ sedemikian sehingga f tidak berubah oleh permutasi $(1\,2\,3\,4)$. Dalam kasus ini $f(1) = f(2) = f(3) = f(4)$, sehingga semua nilai f harus sama; yaitu, $f(x) = B$ atau $f(x) = W$ untuk setiap titik sudut x dari persegi tersebut. Jadi, $|\widetilde{X}_{(1\,2\,3\,4)}| = 2$.
3. $|\widetilde{X}_{(1\,4\,3\,2)}| = 2$.
4. Untuk $\widetilde{X}_{(1\,3)(2\,4)}$, $f(1) = f(3)$ dan $f(2) = f(4)$. Jadi, $|\widetilde{X}_{(1\,3)(2\,4)}| = 2^2 = 4$.
5. $|\widetilde{X}_{(1\,2)(3\,4)}| = 4$.
6. $|\widetilde{X}_{(1\,4)(2\,3)}| = 4$.
7. Untuk $\widetilde{X}_{(1\,3)}$, $f(1) = f(3)$ dan sudut-sudut lainnya dapat memiliki warna sebarang; jadi, $|\widetilde{X}_{(1\,3)}| = 2^3 = 8$.
8. $|\widetilde{X}_{(2\,4)}| = 8$.

Berdasarkan Teorema Burnside, kita dapat menyimpulkan bahwa terdapat tepat

$$\frac{1}{8}(2^4 + 2^1 + 2^2 + 2^1 + 2^2 + 2^2 + 2^3 + 2^3) = 6$$

cara untuk mewarnai titik-titik sudut persegi tersebut.

Proposisi 14.3.5 *Misalkan G adalah grup permutasi dari X dan $\widetilde{X}$ adalah himpunan fungsi dari X ke Y. Maka G menginduksi suatu grup $\widetilde{G}$ yang mempermutasikan unsur-unsur $\widetilde{X}$, dengan $\widetilde{\sigma} \in \widetilde{G}$ didefinisikan oleh $\widetilde{\sigma}(f) = f \circ \sigma$ untuk $\sigma \in G$ dan $f \in \widetilde{X}$. Lebih lanjut, jika n adalah banyaknya siklus dalam dekomposisi siklus σ, maka $|\widetilde{X}_\sigma| = |Y|^n$.*

BUKTI. Misalkan $\sigma \in G$ dan $f \in \widetilde{X}$. Karena σ mempermutasikan unsur-unsur X, $f \circ \sigma$ juga harus berada dalam $\widetilde{X}$. Misalkan g adalah fungsi lain dari X ke Y sedemikian sehingga $\widetilde{\sigma}(f) = \widetilde{\sigma}(g)$. Maka untuk setiap $x \in X$,

$$f(\sigma(x)) = \widetilde{\sigma}(f)(x) = \widetilde{\sigma}(g)(x) = g(\sigma(x)).$$

Karena σ merupakan permutasi dari X, setiap unsur x' dalam X adalah citra suatu x dalam X di bawah σ; jadi, f dan g sama pada semua unsur X. Oleh karena itu, $f = g$ dan $\widetilde{\sigma}$ injektif. Pemetaan $\sigma \mapsto \widetilde{\sigma}$ surjektif, karena kedua himpunan memiliki ukuran yang sama.

Misalkan σ adalah permutasi dari X dengan dekomposisi siklus $\sigma = \sigma_1\sigma_2 \cdots \sigma_n$. Setiap f dalam $\widetilde{X}_\sigma$ harus memiliki nilai yang sama pada setiap siklus σ. Karena terdapat n siklus dan $|Y|$ nilai yang mungkin untuk setiap siklus, $|\widetilde{X}_\sigma| = |Y|^n$. ■

Contoh 14.3.6 Misalkan $X = \{1, 2, \ldots, 7\}$ dan misalkan $Y = \{A, B, C\}$. Jika g adalah permutasi dari X yang diberikan oleh $(1\,3)(2\,4\,5) = (1\,3)(2\,4\,5)(6)(7)$, maka $n = 4$. Setiap $f \in \widetilde{X}_g$ harus memiliki nilai yang sama pada setiap siklus dalam g. Terdapat $|Y| = 3$ pilihan semacam itu untuk setiap nilai, sehingga $|\widetilde{X}_g| = 3^4 = 81$. ▲

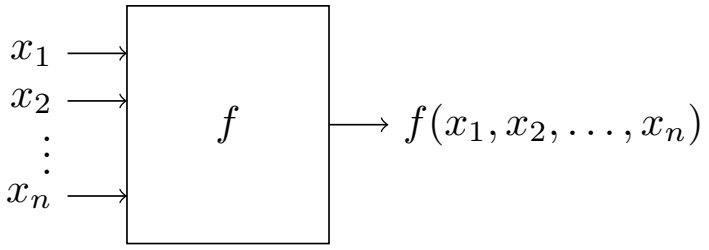
Contoh 14.3.7 Misalkan kita ingin mewarnai titik-titik sudut suatu persegi dengan empat warna berbeda. Berdasarkan Proposisi 14.3.5, kita dapat segera menentukan bahwa terdapat

$$\frac{1}{8}(4^4 + 4^1 + 4^2 + 4^1 + 4^2 + 4^2 + 4^3 + 4^3) = 55$$

cara yang mungkin. ▲

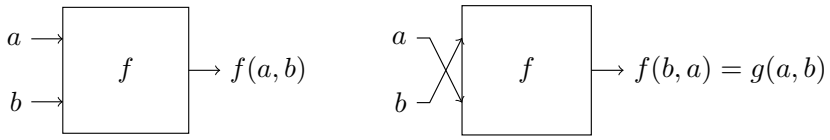
14.3.2 Fungsi Pensakelaran

Dalam teori pensakelaran, kita membahas perancangan rangkaian elektronik dengan masukan dan keluaran biner. Rangkaian yang paling sederhana adalah fungsi pensakelaran yang memiliki n masukan dan satu keluaran (Gambar 14.3.8). Rangkaian elektronik besar sering kali dapat dikonstruksi dengan menggabungkan modul-modul kecil semacam ini. Masalah yang melekat di sini adalah bahwa bahkan untuk rangkaian sederhana, sejumlah besar fungsi pensakelaran yang berbeda dapat dikonstruksi. Hanya dengan empat masukan dan satu keluaran, kita dapat mengonstruksi 65,536 fungsi pensakelaran yang berbeda. Namun, kita sering dapat mengganti suatu fungsi pensakelaran dengan fungsi lainnya hanya dengan mempermutasikan kabel masukan ke rangkaian tersebut (Gambar 14.3.9).



Gambar 14.3.8 Fungsi pensakelaran dengan n variabel

Kita mendefinisikan **fungsi pensakelaran** atau **fungsi Boolean** dengan n variabel sebagai fungsi dari $\mathbb{Z}_2^n$ ke $\mathbb{Z}_2$. Karena setiap fungsi pensakelaran dapat memiliki dua nilai yang mungkin untuk setiap tupel-n biner dan terdapat 2^n tupel-n biner, terdapat 2^{2^n} fungsi pensakelaran yang mungkin untuk n variabel. Secara umum, mengizinkan permutasi masukan sangat mengurangi banyaknya jenis modul berbeda yang diperlukan untuk membangun rangkaian besar.



Gambar 14.3.9 Fungsi pensakelaran dalam dua variabel

Fungsi pensakelaran yang mungkin dengan dua variabel masukan a dan b tercantum dalam Tabel 14.3.10. Dua fungsi pensakelaran f dan g ekuivalen jika g dapat diperoleh dari f melalui permutasi variabel masukan. Sebagai contoh, $g(a,b,c) = f(b,c,a)$. Dalam kasus ini $g \sim f$ melalui permutasi (a,c,b). Dalam kasus fungsi pensakelaran dua variabel, permutasi (a,b) mereduksi 16 fungsi pensakelaran yang mungkin menjadi 12 fungsi ekuivalen karena

$$f_2 \sim f_4$$
$$f_3 \sim f_5$$
$$f_{10} \sim f_{12}$$
$$f_{11} \sim f_{13}.$$

Tabel 14.3.10 Fungsi pensakelaran dalam dua variabel

Masukan		Keluaran							
		f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7
0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1
Masukan		Keluaran							
		f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1

Untuk tiga variabel masukan terdapat $2^{2^3} = 256$ fungsi pensakelaran yang mungkin; dalam kasus empat variabel terdapat $2^{2^4} = 65{,}536$. Banyaknya kelas ekuivalensi terlalu besar untuk dihitung secara langsung dengan wajar. Kita perlu menggunakan Teorema Burnside.

Tinjau suatu fungsi pensakelaran dengan tiga masukan yang mungkin, a, b, dan c. Seperti telah disebutkan, dua fungsi pensakelaran f dan g ekuivalen jika suatu permutasi variabel masukan f menghasilkan g. Penting untuk diperhatikan bahwa permutasi fungsi pensakelaran bukan sekadar permutasi nilai masukan $\{a, b, c\}$. Suatu fungsi pensakelaran merupakan himpunan nilai keluaran untuk masukan a, b, dan c, sehingga ketika kita meninjau fungsi-fungsi pensakelaran yang ekuivalen, kita mempermutasikan 2^3 keluaran yang mungkin, bukan hanya tiga nilai masukan. Sebagai contoh, setiap tripel biner (a, b, c) memiliki keluaran tertentu yang terkait dengannya. Permutasi (acb) mengubah keluaran sebagai berikut:

$$\begin{aligned}(0,0,0) &\mapsto (0,0,0)\\ (0,0,1) &\mapsto (0,1,0)\\ (0,1,0) &\mapsto (1,0,0)\\ &\vdots\\ (1,1,0) &\mapsto (1,0,1)\\ (1,1,1) &\mapsto (1,1,1).\end{aligned}$$

Misalkan X adalah himpunan nilai keluaran bagi fungsi pensakelaran dalam n variabel. Maka $|X| = 2^n$. Kita dapat mengenumerasi nilai-nilai tersebut sebagai berikut:

$$\begin{aligned}(0,\ldots,0,1) &\mapsto 0\\ (0,\ldots,1,0) &\mapsto 1\\ (0,\ldots,1,1) &\mapsto 2\\ &\vdots\\ (1,\ldots,1,1) &\mapsto 2^n - 1.\end{aligned}$$

Sekarang, mari kita tinjau suatu rangkaian dengan empat variabel masukan dan satu keluaran. Misalkan kita dapat mempermutasikan kabel pada sebarang rangkaian menurut grup permutasi berikut:

$$\begin{gathered}(a), \quad (a,c), \quad (b,d), \quad (a,d,c,b),\\ (a,b,c,d), \quad (a,b)(c,d), \quad (a,d)(b,c), \quad (a,c)(b,d).\end{gathered}$$

Permutasi empat variabel masukan yang mungkin menginduksi permutasi nilai keluaran dalam Tabel 14.3.11.

Jadi, terdapat

$$\frac{1}{8}(2^{16} + 2 \cdot 2^{12} + 2 \cdot 2^6 + 3 \cdot 2^{10}) = 9616$$

fungsi pensakelaran empat variabel yang mungkin di bawah grup permutasi ini. Bilangan ini akan lebih kecil lagi jika kita meninjau grup simetris penuh pada empat huruf.

Tabel 14.3.11 Permutasi fungsi pensakelaran dalam empat variabel

Grup Permutasi	Permutasi Fungsi Pensakelaran	Banyaknya Siklus
(a)	(0)	16
(a,c)	$(2,8)(3,9)(6,12)(7,13)$	12
(b,d)	$(1,4)(3,6)(9,12)(11,14)$	12
(a,d,c,b)	$(1,2,4,8)(3,6.12,9)(5,10)(7,14,13,11)$	6
(a,b,c,d)	$(1,8,4,2)(3,9,12,6)(5,10)(7,11,13,14)$	6
$(a,b)(c,d)$	$(1,2)(4,8)(5,10)(6,9)(7,11)(13,14)$	10
$(a,d)(b,c)$	$(1,8)(2,4)(3,12)(5,10)(7,14)(11,13)$	10
$(a,c)(b,d)$	$(1,4)(2,8)(3,12)(6,9)(7,13)(11,14)$	10

Catatan Sejarah

William Burnside lahir di London pada tahun 1852. Ia menempuh pendidikan di Universitas Cambridge dari tahun 1871 hingga 1875 dan memenangkan Smith's Prize pada tahun terakhirnya. Setelah lulus, ia mengajar di Cambridge. Ia diangkat menjadi anggota Royal Society pada tahun 1893. Burnside menulis sekitar 150 makalah tentang matematika terapan, geometri diferensial, dan probabilitas, tetapi sumbangannya yang paling terkenal adalah dalam teori grup. Beberapa konjektur Burnside telah mendorong penelitian hingga kini. Salah satu konjektur tersebut menyatakan bahwa setiap grup berorde ganjil dapat dipecahkan; yaitu, untuk suatu grup G berorde ganjil, terdapat suatu barisan subgrup

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\}$$

sedemikian sehingga H_i normal dalam H_{i+1} dan H_{i+1}/H_i abelian. Konjektur ini akhirnya dibuktikan oleh W. Feit dan J. Thompson pada tahun 1963. Burnside's *The Theory of Groups of Finite Order*, yang diterbitkan pada tahun 1897, merupakan salah satu buku pertama yang membahas grup dalam konteks modern, bukan hanya sebagai grup permutasi. Edisi keduanya, yang diterbitkan pada tahun 1911, tetap menjadi karya klasik.

14.4 Pertanyaan Bacaan

1. Berikan deskripsi informal tentang aksi grup.

2. Jelaskan persamaan kelas.

3. Apa saja grup berorde 49?

4. Berapa banyak fungsi pensakelaran dengan lima masukan? (Berikan ekspresi sederhana maupun jumlah keseluruhannya sebagai satu bilangan bulat.)

5. Bagian "Catatan Sejarah" menyebutkan pembuktian Konjektur Burnside. Berapa panjang pembuktian tersebut?

14.5 Latihan

1. Contoh-contoh 14.1.1–14.1.5 dalam bagian pertama masing-masing mendeskripsikan aksi suatu grup G pada suatu himpunan X, yang menghasilkan relasi ekuivalensi yang didefinisikan oleh ekuivalensi-G. Untuk setiap contoh, hitung kelas-kelas ekuivalensi dari relasi ekuivalensi tersebut, yai-

tu G-**kelas ekuivalensi**.

Petunjuk. Contoh 14.1.1: 0, $\mathbb{R}^2 \setminus \{0\}$. Contoh 14.1.2: $X = \{1,2,3,4\}$.

2. Hitung semua X_g dan semua G_x untuk setiap grup permutasi berikut.

(a) $X = \{1,2,3\}$, $G = S_3 = \{(1), (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$

(b) $X = \{1,2,3,4,5,6\}$, $G = \{(1), (1\,2), (3\,4\,5), (3\,5\,4), (1\,2)(3\,4\,5), (1\,2)(3\,5\,4)\}$

Petunjuk. (a) $X_{(1)} = \{1,2,3\}$, $X_{(1\,2)} = \{3\}$, $X_{(1\,3)} = \{2\}$, $X_{(2\,3)} = \{1\}$, $X_{(1\,2\,3)} = X_{(1\,3\,2)} = \emptyset$. $G_1 = \{(1), (2\,3)\}$, $G_2 = \{(1), (1\,3)\}$, $G_3 = \{(1), (1\,2)\}$.

3. Hitung kelas ekuivalensi-G dari X untuk setiap himpunan-G dalam Latihan 14.5.2. Untuk setiap $x \in X$, verifikasikan bahwa $|G| = |\mathcal{O}_x| \cdot |G_x|$.

Petunjuk. (a) $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1,2,3\}$.

4. Misalkan G adalah grup aditif bilangan real. Misalkan aksi $\theta \in G$ pada bidang real $\mathbb{R}^2$ diberikan dengan memutar bidang tersebut berlawanan arah jarum jam terhadap titik asal sejauh θ radian. Misalkan P adalah suatu titik pada bidang selain titik asal.

(a) Tunjukkan bahwa $\mathbb{R}^2$ merupakan himpunan-G.

(b) Deskripsikan secara geometris orbit yang memuat P.

(c) Carilah grup G_P.

5. Misalkan $G = A_4$ dan misalkan G beraksi pada dirinya sendiri melalui konjugasi; yaitu, $(g,h) \mapsto ghg^{-1}$.

(a) Tentukan kelas-kelas konjugasi (orbit) dari setiap unsur G.

(b) Tentukan semua subgrup isotropi untuk setiap unsur G.

6. Carilah kelas-kelas konjugasi dan persamaan kelas untuk setiap grup berikut.

(a) S_4 (b) D_5 (c) $\mathbb{Z}_9$ (d) Q_8

Petunjuk. Kelas-kelas konjugasi untuk S_4 adalah

$$\begin{gathered}\mathcal{O}_{(1)} = \{(1)\},\\ \mathcal{O}_{(12)} = \{(1\,2), (1\,3), (1\,4), (2\,3), (2\,4), (3\,4)\},\\ \mathcal{O}_{(1\,2)(3\,4)} = \{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\},\\ \mathcal{O}_{(123)} = \{(1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3)\},\\ \mathcal{O}_{(1234)} = \{(1\,2\,3\,4), (1\,2\,4\,3), (1\,3\,2\,4), (1\,3\,4\,2), (1\,4\,2\,3), (1\,4\,3\,2)\}.\end{gathered}$$

Persamaan kelasnya adalah $1 + 3 + 6 + 6 + 8 = 24$.

7. Tuliskan persamaan kelas untuk S_5 dan untuk A_5.

8. Jika suatu persegi tetap pada tempatnya di bidang, berapa banyak cara berbeda sudut-sudut persegi tersebut dapat diwarnai apabila digunakan tiga warna?

Petunjuk. $(3^4 + 3^1 + 3^2 + 3^1 + 3^2 + 3^2 + 3^3 + 3^3)/8 = 21$.

9. Berapa banyak cara titik-titik sudut segitiga sama sisi dapat diwarnai dengan menggunakan tiga warna berbeda?

10. Carilah banyaknya cara sebuah dadu bersisi enam dapat dibuat jika setiap sisinya diberi tanda yang berbeda dengan $1, \ldots, 6$ titik.

11. Hingga rotasi, berapa banyak cara permukaan sebuah kubus dapat diwarnai dengan tiga warna berbeda?

Petunjuk. Grup gerak kaku kubus dapat dideskripsikan oleh permutasi yang diizinkan pada keenam permukaannya dan isomorfik dengan S_4. Terdapat siklus identitas, 6 permutasi berstruktur $(abcd)$ yang bersesuaian dengan putaran seperempat, 3 permutasi berstruktur $(ab)(cd)$ yang bersesuaian dengan putaran setengah, 6 permutasi berstruktur $(ab)(cd)(ef)$ yang bersesuaian dengan rotasi kubus terhadap pusat sisi-sisi yang berhadapan, dan 8 permutasi berstruktur $(abc)(def)$ yang bersesuaian dengan rotasi kubus terhadap titik-titik sudut yang berhadapan.

12. Tinjau 12 kawat lurus yang sama panjang dengan ujung-ujungnya disolder menjadi satu untuk membentuk rusuk-rusuk kubus. Kawat perak atau tembaga dapat digunakan untuk setiap rusuk. Berapa banyak cara berbeda kubus tersebut dapat dibuat?

13. Misalkan kita mewarnai setiap sudut dari delapan sudut suatu kubus. Dengan menggunakan tiga warna berbeda, berapa banyak cara sudut-sudut tersebut dapat diwarnai hingga rotasi kubus?

14. Setiap permukaan tetrahedron beraturan dapat dicat merah atau putih. Hingga rotasi, berapa banyak cara berbeda tetrahedron tersebut dapat dicat?

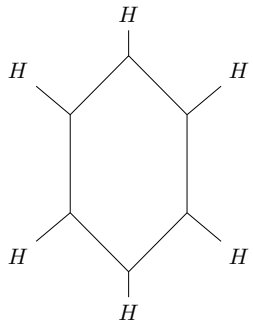
15. Misalkan titik-titik sudut segi enam beraturan akan diwarnai merah atau putih. Berapa banyak cara hal ini dapat dilakukan hingga simetri segi enam tersebut?

Petunjuk. $(1 \cdot 2^6 + 3 \cdot 2^4 + 4 \cdot 2^3 + 2 \cdot 2^2 + 2 \cdot 2^1)/12 = 13$.

16. Suatu molekul benzena terdiri atas enam atom karbon dan enam atom hidrogen, yang saling terhubung dalam bentuk segi enam seperti dalam Gambar 14.5.1.

(a) Berapa banyak senyawa berbeda yang dapat dibentuk dengan mengganti satu atau lebih atom hidrogen dengan atom klorin?

(b) Carilah banyaknya senyawa kimia berbeda yang dapat dibentuk dengan mengganti tiga dari enam atom hidrogen dalam cincin benzena dengan radikal CH_3.



Gambar 14.5.1 Cincin benzena

17. Berapa banyak kelas ekuivalensi fungsi pensakelaran jika variabel masukan x_1, x_2, dan x_3 dapat dipermutasi oleh sebarang permutasi dalam S_3? Bagaimana jika variabel masukan x_1, x_2, x_3, dan x_4 dapat dipermutasi oleh sebarang permutasi dalam S_4?

Petunjuk. $(1 \cdot 2^8 + 3 \cdot 2^6 + 2 \cdot 2^4)/6 = 80$.

18. Berapa banyak kelas ekuivalensi fungsi pensakelaran jika variabel masukan x_1, x_2, x_3, dan x_4 dapat dipermutasi oleh sebarang permutasi dalam subgrup S_4 yang dibangkitkan oleh permutasi (x_1, x_2, x_3, x_4)?

19. Sebuah dasi bergaris memiliki 12 pita warna. Setiap pita dapat diwarnai dengan salah satu dari empat warna yang mungkin. Berapa banyak dasi dengan pewarnaan berbeda yang mungkin?

20. Suatu grup beraksi **secara setia** pada himpunan-G X jika identitas merupakan satu-satunya unsur G yang menetapkan setiap unsur X. Tunjukkan bahwa G beraksi secara setia pada X jika dan hanya jika tidak ada dua unsur berbeda dari G yang mempunyai aksi sama pada setiap unsur X.

21. Misalkan p prima. Tunjukkan bahwa banyaknya grup abelian berbeda berorde p^n (hingga isomorfisma) sama dengan banyaknya kelas konjugasi dalam S_n.

22. Misalkan $a \in G$. Tunjukkan bahwa untuk sebarang $g \in G$, $gC(a)g^{-1} = C(gag^{-1})$.

Petunjuk. Gunakan fakta bahwa $x \in gC(a)g^{-1}$ jika dan hanya jika $g^{-1}xg \in C(a)$.

23. Misalkan $|G| = p^n$ adalah grup nonabelian dengan p prima. Buktikan bahwa $|Z(G)| < p^{n-1}$.

24. Misalkan G adalah grup berorde p^n dengan p prima dan X adalah himpunan-G hingga. Jika $X_G = \{x \in X : gx = x \text{ untuk semua } g \in G\}$ adalah himpunan unsur dalam X yang tetap di bawah aksi grup, buktikan bahwa $|X| \equiv |X_G| \pmod{p}$.

25. Jika G adalah grup berorde p^n, dengan p prima dan $n \geq 2$, tunjukkan bahwa G pasti memiliki subgrup sejati berorde p. Jika $n \geq 3$, benarkah bahwa G memiliki subgrup sejati berorde p^2?

14.6 Latihan Pemrograman

1. Tulislah program untuk menghitung banyaknya kelas konjugasi dalam S_n. Berapakah n terbesar yang dapat ditangani oleh program Anda?

14.7 Referensi dan Bacaan yang Disarankan

[1] Bruijin, de, N. G. "Pólya's Theory of Counting," in *Applied Combinatorial Mathematics*, Beckenbach, E. F., ed. Wiley, New York, 1964.

[2] Eidswick, J. A. "Cubelike Puzzles—What Are They and How Do You Solve Them?" *American Mathematical Monthly* 93 (1986), 157–76.

[3] Harary, F., Palmer, E. M., and Robinson, R. W. "Pólya's Contributions to Chemical Enumeration," in *Chemical Applications of Graph Theory*, Balaban, A. T., ed. Academic Press, London, 1976.

[4] Gårding, L. and Tambour, T. *Algebra for Computer Science*. Springer-Verlag, New York, 1988.

[5] Laufer, H. B. *Discrete Mathematics and Applied Modern Algebra*. PWS-Kent, Boston, 1984.

[6] Pólya, G. and Read, R. C. *Combinatorial Enumeration of Groups, Graphs, and Chemical Compounds*. Springer-Verlag, New York, 1985.

[7] Shapiro, L. W. "Finite Groups Acting on Sets with Applications," *Mathematics Magazine*, May–June 1973, 136–47.

15

Teorema Sylow

Kita telah mengetahui bahwa kebalikan Teorema Lagrange tidak berlaku. Jika G adalah grup berorde m dan n membagi m, G belum tentu memiliki subgrup berorde n. Sebagai contoh, A_4 berorde 12, tetapi tidak memiliki subgrup berorde 6. Meskipun demikian, Teorema Sylow memberikan kebalikan parsial bagi Teorema Lagrange—dalam kasus tertentu, teorema-teorema ini menjamin keberadaan subgrup dengan orde tertentu. Teorema-teorema ini menyediakan seperangkat alat yang ampuh untuk mengklasifikasikan semua grup hingga nonabelian.

15.1 Teorema Sylow

Kita akan menggunakan apa yang telah dipelajari tentang aksi grup untuk membuktikan Teorema Sylow. Ingat kembali makna G beraksi pada dirinya sendiri melalui konjugasi serta cara kelas-kelas konjugasi tersebar di dalam grup menurut persamaan kelas, yang dibahas dalam Bab 14. Grup G beraksi pada dirinya sendiri melalui konjugasi dengan pemetaan $(g, x) \mapsto gxg^{-1}$. Misalkan $x_1, \ldots, x_k$ merupakan wakil dari setiap kelas konjugasi berbeda di G yang terdiri atas lebih dari satu elemen. Persamaan kelas kemudian dapat ditulis sebagai

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)],$$

dengan $Z(G) = \{g \in G : gx = xg \text{ untuk semua } x \in G\}$ merupakan pusat G dan $C(x_i) = \{g \in G : gx_i = x_i g\}$ merupakan subgrup pemusat dari x_i.

Kita memulai kajian Teorema Sylow dengan memeriksa subgrup berorde p, dengan p prima. Grup G disebut **grup-p** jika orde setiap elemen di G merupakan suatu pangkat dari p, dengan p bilangan prima. Subgrup dari grup G disebut **subgrup-p** jika subgrup itu merupakan grup-p.

Teorema 15.1.1 Cauchy. *Misalkan G grup hingga dan p bilangan prima sedemikian sehingga p membagi orde G. Maka G memuat subgrup berorde p.*

Bukti. Kita menggunakan induksi pada orde G. Jika $|G| = p$, jelas bahwa G sendiri merupakan subgrup yang diperlukan. Sekarang andaikan setiap grup berorde k, dengan $p \leq k < n$ dan p membagi k, memiliki elemen berorde p. Andaikan $|G| = n$ dan $p \mid n$, lalu tinjau persamaan kelas G:

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)].$$

Ada dua kasus.

Kasus 1. Andaikan orde salah satu subgrup pemusat, $C(x_i)$, habis dibagi p untuk suatu i, $i = 1, \ldots, k$. Dalam kasus ini, hipotesis induksi menyelesaikan pembuktian. Karena $C(x_i)$ merupakan subgrup sejati dari G dan p membagi $|C(x_i)|$, $C(x_i)$ harus memuat elemen berorde p. Jadi, G harus memuat elemen berorde p.

Kasus 2. Andaikan orde tidak satu pun subgrup pemusat habis dibagi p. Maka p membagi $[G : C(x_i)]$, yaitu orde setiap kelas konjugasi dalam persamaan kelas; karena itu, p harus membagi orde pusat G, yaitu $Z(G)$. Karena $Z(G)$ abelian, Teorema Dasar Grup Abelian Hingga menyatakan bahwa pusat tersebut harus memiliki subgrup berorde p. Oleh karena itu, pusat G memuat elemen berorde p. ■

Korolari 15.1.2 *Misalkan G grup hingga. Maka G merupakan grup-p jika dan hanya jika $|G| = p^n$.*

Contoh 15.1.3 Tinjau grup A_5. Kita mengetahui bahwa $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$. Berdasarkan Teorema Cauchy, A_5 dijamin memiliki subgrup berorde 2, 3, dan 5. Teorema Sylow akan memberi kita lebih banyak informasi tentang subgrup-subgrup yang mungkin dari A_5. ▲

Sekarang kita siap menyatakan dan membuktikan Teorema Sylow yang pertama. Pembuktiannya sangat mirip dengan pembuktian Teorema Cauchy.

Teorema 15.1.4 Teorema Sylow Pertama. *Misalkan G grup hingga dan p bilangan prima sedemikian sehingga p^r membagi $|G|$. Maka G memuat subgrup berorde p^r.*

Bukti. Sekali lagi kita melakukan induksi pada orde G. Jika $|G| = p$, pembuktian selesai. Sekarang andaikan orde G adalah n dengan $n > p$ dan teorema ini berlaku bagi semua grup yang ordenya kurang dari n, dengan p membagi n. Kita kembali menerapkan persamaan kelas:

$$|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_k)].$$

Pertama, andaikan p tidak membagi $[G : C(x_i)]$ untuk suatu i. Maka $p^r \mid |C(x_i)|$, sebab p^r membagi $|G| = |C(x_i)| \cdot [G : C(x_i)]$. Sekarang kita dapat menerapkan hipotesis induksi pada $C(x_i)$.

Jadi, kita boleh mengandaikan bahwa p membagi $[G : C(x_i)]$ untuk setiap i. Karena p membagi $|G|$, persamaan kelas menyatakan bahwa p harus membagi $|Z(G)|$; karena itu, berdasarkan Teorema Cauchy, $Z(G)$ memiliki elemen berorde p, misalkan g. Misalkan N adalah grup yang dibangkitkan oleh g. Jelas bahwa N merupakan subgrup normal dari $Z(G)$ karena $Z(G)$ abelian; oleh karena itu, N normal di G karena setiap elemen dalam $Z(G)$ komutatif dengan setiap elemen dalam G. Sekarang tinjau grup hasil bagi G/N yang berorde $|G|/p$. Berdasarkan hipotesis induksi, G/N memuat subgrup H berorde p^{r-1}. Pracitra H di bawah homomorfisma kanonik $\phi : G \to G/N$ merupakan subgrup berorde p^r di G. ■

Subgrup Sylow-p P dari grup G adalah subgrup-p maksimal dari G. Untuk membuktikan dua Teorema Sylow lainnya, kita perlu meninjau subgrup-subgrup konjugat, bukan elemen-elemen konjugat dalam grup. Untuk grup G, misalkan $\mathcal{S}$ adalah koleksi semua subgrup dari G. Untuk sebarang subgrup H, $\mathcal{S}$ merupakan himpunan-H, dengan H beraksi pada $\mathcal{S}$ melalui konjugasi. Dengan kata lain, terdapat aksi

$$H \times \mathcal{S} \to \mathcal{S}$$

yang didefinisikan oleh

$$h \cdot K \mapsto hKh^{-1}$$

untuk K dalam $\mathcal{S}$.

Himpunan

$$N(H) = \{g \in G : gHg^{-1} = H\}$$

merupakan subgrup dari G yang disebut **penormal** H di G. Perhatikan bahwa H merupakan subgrup normal dari $N(H)$. Bahkan, $N(H)$ adalah subgrup terbesar dari G tempat H normal.

Lema 15.1.5 *Misalkan P subgrup Sylow-p dari grup hingga G dan orde x merupakan suatu pangkat dari p. Jika $x^{-1}Px = P$, maka $x \in P$.*

BUKTI. Jelas bahwa $x \in N(P)$, dan subgrup siklik $\langle xP\rangle \subset N(P)/P$ berorde suatu pangkat dari p. Berdasarkan Teorema Korespondensi, terdapat subgrup H dari $N(P)$ yang memuat P sedemikian sehingga $H/P = \langle xP\rangle$. Karena $|H| = |P| \cdot |\langle xP\rangle|$, orde H harus merupakan suatu pangkat dari p. Namun, P merupakan subgrup Sylow-p yang termuat dalam H. Karena orde P adalah pangkat terbesar dari p yang membagi $|G|$, $H = P$. Jadi, H/P merupakan subgrup trivial dan $xP = P$, atau $x \in P$. ■

Lema 15.1.6 *Misalkan H dan K subgrup dari G. Banyaknya konjugat-H yang berbeda dari K adalah $[H : N(K) \cap H]$.*

BUKTI. Kita mendefinisikan bijeksi antara kelas-kelas konjugasi K dan koset-koset kanan dari $N(K) \cap H$ melalui $h^{-1}Kh \mapsto (N(K) \cap H)h$. Untuk menunjukkan bahwa pemetaan ini bijektif, misalkan $h_1, h_2 \in H$ dan andaikan $(N(K) \cap H)h_1 = (N(K) \cap H)h_2$. Maka $h_2h_1^{-1} \in N(K)$. Jadi, $K = h_2h_1^{-1}Kh_1h_2^{-1}$ atau $h_1^{-1}Kh_1 = h_2^{-1}Kh_2$, sehingga pemetaan tersebut injektif. Mudah dilihat bahwa pemetaan ini surjektif; karena itu, terdapat pemetaan satu-satu dan pada antara konjugat-konjugat-H dari K dan koset-koset kanan dari $N(K) \cap H$ di H. ■

Teorema 15.1.7 Teorema Sylow Kedua. *Misalkan G grup hingga dan p bilangan prima yang membagi $|G|$. Maka semua subgrup Sylow-p dari G saling konjugat. Artinya, jika P_1 dan P_2 adalah dua subgrup Sylow-p, terdapat $g \in G$ sedemikian sehingga $gP_1g^{-1} = P_2$.*

BUKTI. Misalkan P subgrup Sylow-p dari G dan andaikan $|G| = p^r m$ dengan $|P| = p^r$. Misalkan

$$\mathcal{S} = \{P = P_1, P_2, \ldots, P_k\}$$

terdiri atas konjugat-konjugat berbeda dari P di G. Berdasarkan Lema 15.1.6, $k = [G : N(P)]$. Perhatikan bahwa

$$|G| = p^r m = |N(P)| \cdot [G : N(P)] = |N(P)| \cdot k.$$

Karena p^r membagi $|N(P)|$, p tidak mungkin membagi k.

Diberikan sebarang subgrup Sylow-p lain Q, kita harus menunjukkan bahwa $Q \in \mathcal{S}$. Tinjau kelas konjugasi-Q dari setiap P_i. Jelas bahwa kelas-kelas konjugasi ini mempartisi $\mathcal{S}$. Ukuran bagian yang memuat P_i adalah $[Q : N(P_i) \cap Q]$ berdasarkan Lema 15.1.6, dan Teorema Lagrange menyatakan bahwa $|Q| = [Q : N(P_i) \cap Q]|N(P_i) \cap Q|$. Jadi, $[Q : N(P_i) \cap Q]$ harus membagi $|Q| = p^r$. Dengan demikian, banyaknya konjugat dalam setiap kelas ekuivalensi pada partisi tersebut merupakan suatu pangkat dari p. Namun, karena p tidak membagi k, salah satu kelas ekuivalensi ini harus hanya memuat satu subgrup Sylow-p, misalkan P_j. Dalam hal ini, $x^{-1}P_jx = P_j$ untuk setiap $x \in Q$. Berdasarkan Lema 15.1.5, $P_j = Q$. ■

Teorema 15.1.8 Teorema Sylow Ketiga. *Misalkan G grup hingga dan p bilangan prima yang membagi orde G. Maka banyaknya subgrup Sylow-p*

kongruen dengan $1 \pmod{p}$ *dan membagi* $|G|$.

BUKTI. Misalkan P subgrup Sylow-p yang beraksi pada himpunan subgrup Sylow-p,

$$\mathcal{S} = \{P = P_1, P_2, \ldots, P_k\},$$

melalui konjugasi. Dari pembuktian Teorema Sylow Kedua, satu-satunya konjugat-P dari P adalah dirinya sendiri dan orde kelas-kelas konjugasi-P lainnya merupakan suatu pangkat dari p. Setiap kelas konjugasi-P menyumbangkan suatu pangkat positif dari p terhadap $|\mathcal{S}|$, kecuali kelas ekuivalensi $\{P\}$. Karena $|\mathcal{S}|$ merupakan jumlah beberapa pangkat positif dari p dan 1, $|\mathcal{S}| \equiv 1 \pmod{p}$.

Sekarang andaikan G beraksi pada $\mathcal{S}$ melalui konjugasi. Karena semua subgrup Sylow-p saling konjugat, hanya ada satu orbit di bawah aksi ini. Untuk $P \in \mathcal{S}$,

$$|\mathcal{S}| = |\text{orbit dari } P| = [G : N(P)]$$

berdasarkan Lema 15.1.6. Namun, $[G : N(P)]$ membagi $|G|$; akibatnya, banyaknya subgrup Sylow-p dari suatu grup hingga harus membagi orde grup tersebut. ■

Catatan Sejarah

Peter Ludvig Mejdell Sylow lahir pada tahun 1832 di Christiania, Norwegia (sekarang Oslo). Setelah menempuh pendidikan di Universitas Christiania, Sylow mengajar di sekolah menengah. Pada tahun 1862 ia memperoleh jabatan sementara di Universitas Christiania. Meskipun masa jabatannya relatif singkat, ia memengaruhi mahasiswa seperti Sophus Lie (1842–1899). Pada tahun 1869 Sylow berkesempatan memperoleh jabatan profesor tetap, tetapi tidak berhasil mendapatkannya. Pada tahun 1872, ia menerbitkan makalah sepuluh halaman yang memaparkan teorema-teorema yang kini menyandang namanya. Kemudian Lie dan Sylow bekerja sama menyusun edisi baru karya-karya Abel. Pada tahun 1898, berkat upaya Lie sebagai mantan mahasiswa sekaligus koleganya, sebuah jabatan profesor di Universitas Christiania akhirnya dibentuk untuk Sylow. Sylow meninggal pada tahun 1918.

15.2 Contoh dan Penerapan

Contoh 15.2.1 Dengan menggunakan Teorema Sylow, kita dapat menentukan bahwa A_5 memiliki subgrup berorde 2, 3, 4, dan 5. Subgrup Sylow-p dari A_5 berorde 3, 4, dan 5. Teorema Sylow Ketiga menyatakan dengan tepat banyaknya subgrup Sylow-p yang dimiliki A_5. Karena banyaknya subgrup Sylow-5 harus membagi 60 dan juga kongruen dengan 1 (mod 5), terdapat satu atau enam subgrup Sylow-5 di A_5. Semua subgrup Sylow-5 saling konjugat. Jika hanya ada satu subgrup Sylow-5, subgrup itu akan konjugat dengan dirinya sendiri; artinya, subgrup tersebut normal di A_5. Karena A_5 tidak memiliki subgrup normal, hal ini mustahil; jadi, kita telah menentukan bahwa terdapat tepat enam subgrup Sylow-5 yang berbeda di A_5. ▲

Teorema Sylow memungkinkan kita membuktikan banyak hasil yang berguna tentang grup hingga. Dengan menggunakannya, kita sering kali dapat menyimpulkan banyak hal tentang grup berorde tertentu jika hipotesis tertentu dipenuhi.

Teorema 15.2.2 *Jika p dan q bilangan prima berbeda dengan $p < q$, maka setiap grup G berorde pq memiliki tepat satu subgrup berorde q, dan subgrup ini normal di G. Jadi, G tidak mungkin sederhana. Lebih lanjut, jika $q \not\equiv 1$*

(mod p), *maka* G *siklik.*

BUKTI. Kita mengetahui bahwa G memuat subgrup H berorde q. Banyaknya konjugat dari H membagi pq dan sama dengan $1 + kq$ untuk $k = 0, 1, \ldots$. Namun, $1 + q$ sudah terlalu besar untuk membagi orde grup; karena itu, H hanya dapat konjugat dengan dirinya sendiri. Artinya, H harus normal di G.

Grup G juga memiliki subgrup Sylow-p, misalkan K. Banyaknya konjugat dari K harus membagi q dan sama dengan $1+kp$ untuk $k = 0, 1, \ldots$. Karena q prima, berlaku salah satu dari $1+kp = q$ atau $1+kp = 1$. Jika $1+kp = 1$, maka K normal di G. Dalam kasus ini, mudah ditunjukkan bahwa G memenuhi kriteria, yang diberikan dalam Bab 9, bagi hasil kali langsung internal dari H dan K. Karena H isomorfik dengan $\mathbb{Z}_q$ dan K isomorfik dengan $\mathbb{Z}_p$, $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ berdasarkan Teorema 9.2.9. ■

Contoh 15.2.3 Setiap grup berorde 15 bersifat siklik. Hal ini berlaku karena $15 = 5 \cdot 3$ dan $5 \not\equiv 1 \pmod 3$. ▲

Contoh 15.2.4 Mari kita klasifikasikan semua grup berorde $99 = 3^2 \cdot 11$ hingga isomorfisma. Pertama, kita akan menunjukkan bahwa setiap grup G berorde 99 bersifat abelian. Berdasarkan Teorema Sylow Ketiga, terdapat $1 + 3k$ subgrup Sylow-3, masing-masing berorde 9, untuk suatu $k = 0, 1, 2, \ldots$. Selain itu, $1 + 3k$ harus membagi 11; jadi, hanya mungkin ada satu subgrup Sylow-3 normal H di G. Serupa dengan itu, terdapat $1 + 11k$ subgrup Sylow-11 dan $1 + 11k$ harus membagi 9. Akibatnya, hanya ada satu subgrup Sylow-11 K di G. Berdasarkan Korolari 14.2.5, setiap grup berorde p^2 bersifat abelian untuk p prima; karena itu, H isomorfik dengan $\mathbb{Z}_3 \times \mathbb{Z}_3$ atau $\mathbb{Z}_9$. Karena K berorde 11, grup ini harus isomorfik dengan $\mathbb{Z}_{11}$. Oleh karena itu, hingga isomorfisma, satu-satunya grup yang mungkin berorde 99 adalah $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11}$ atau $\mathbb{Z}_9 \times \mathbb{Z}_{11}$. ▲

Untuk menentukan semua grup berorde $5 \cdot 7 \cdot 47 = 1645$, kita memerlukan teorema berikut.

Teorema 15.2.5 *Misalkan* $G' = \langle aba^{-1}b^{-1} : a, b \in G \rangle$ *adalah subgrup yang terdiri atas semua hasil kali hingga elemen berbentuk* $aba^{-1}b^{-1}$ *dalam grup* G. *Maka* G' *merupakan subgrup normal dari* G *dan* G/G' *abelian.*

Subgrup G' dari G disebut **subgrup komutator** dari G. Pembuktian teorema ini diserahkan sebagai latihan (Latihan 10.4.14 dalam Bab 10).

Contoh 15.2.6 Sekarang kita akan menunjukkan bahwa setiap grup berorde $5 \cdot 7 \cdot 47 = 1645$ bersifat abelian, dan bersifat siklik berdasarkan Teorema 9.2.9. Menurut Teorema Sylow Ketiga, G hanya memiliki satu subgrup H_1 berorde 47. Jadi, G/H_1 berorde 35 dan harus abelian berdasarkan Teorema 15.2.2. Karena itu, subgrup komutator dari G termuat dalam H, sehingga $|G'|$ sama dengan 1 atau 47. Jika $|G'| = 1$, pembuktian selesai. Andaikan $|G'| = 47$. Teorema Sylow Ketiga menyatakan bahwa G hanya memiliki satu subgrup berorde 5 dan satu subgrup berorde 7. Jadi, terdapat subgrup normal H_2 dan H_3 di G, dengan $|H_2| = 5$ dan $|H_3| = 7$. Dalam kedua kasus, grup hasil baginya abelian; karena itu, G' harus merupakan subgrup dari H_i, $i = 1, 2$. Dengan demikian, orde G' adalah 1, 5, atau 7. Namun, sebelumnya kita telah menentukan bahwa $|G'| = 1$ atau 47. Jadi, subgrup komutator dari G trivial, dan akibatnya G abelian. ▲

15.2.1 Grup Sederhana Hingga

Diberikan suatu grup hingga, kita dapat bertanya apakah grup tersebut memiliki subgrup normal. Ingat bahwa grup sederhana tidak memiliki subgrup

normal nontrivial sejati. Seperti pada kasus A_5, membuktikan bahwa suatu grup sederhana dapat menjadi tugas yang sangat sulit; namun, Teorema Sylow merupakan alat yang berguna untuk membuktikan bahwa suatu grup tidak sederhana. Biasanya, pembuktiannya melibatkan suatu argumen pencacahan.

Contoh 15.2.7 Mari kita tunjukkan bahwa tidak ada grup G berorde 20 yang sederhana. Berdasarkan Teorema Sylow Ketiga, G memuat satu atau lebih subgrup Sylow-5. Banyaknya subgrup tersebut kongruen dengan 1 (mod 5) dan juga harus membagi 20. Satu-satunya bilangan yang mungkin adalah 1. Karena hanya ada satu subgrup Sylow-5 dan semua subgrup Sylow-5 saling konjugat, subgrup ini harus normal. ▲

Contoh 15.2.8 Misalkan G grup hingga berorde p^n, dengan $n > 1$ dan p prima. Berdasarkan Teorema 14.2.4, G memiliki pusat yang nontrivial. Karena pusat sebarang grup G merupakan subgrup normal, G tidak mungkin sederhana. Oleh karena itu, grup-grup berorde 4, 8, 9, 16, 25, 27, 32, 49, 64, dan 81 tidak sederhana. Bahkan, grup-grup berorde 4, 9, 25, dan 49 bersifat abelian berdasarkan Korolari 14.2.5. ▲

Contoh 15.2.9 Tidak ada grup berorde $56 = 2^3 \cdot 7$ yang sederhana. Kita telah melihat bahwa jika dapat ditunjukkan hanya ada satu subgrup Sylow-p untuk suatu bilangan prima p yang membagi 56, maka subgrup ini harus normal dan pembuktian selesai. Berdasarkan Teorema Sylow Ketiga, terdapat satu atau delapan subgrup Sylow-7. Jika hanya ada satu subgrup Sylow-7, subgrup itu harus normal.

Di sisi lain, andaikan terdapat delapan subgrup Sylow-7. Setiap subgrup tersebut harus siklik; karena itu, irisan sebarang dua subgrup tersebut hanya memuat identitas grup. Dengan demikian terdapat $8 \cdot 6 = 48$ elemen berbeda dalam grup, masing-masing berorde 7. Sekarang mari kita cacah subgrup Sylow-2. Terdapat satu atau tujuh subgrup Sylow-2. Setiap elemen selain identitas dalam subgrup Sylow-2 harus berorde suatu pangkat dari 2; karena itu, elemen tersebut tidak mungkin termasuk salah satu dari 48 elemen berorde 7 dalam subgrup Sylow-7. Karena subgrup Sylow-2 berorde 8, hanya tersedia cukup banyak elemen untuk satu subgrup Sylow-2 dalam grup berorde 56. Jika hanya ada satu subgrup Sylow-2, subgrup itu harus normal. ▲

Untuk grup-grup G lainnya, membuktikan bahwa G tidak sederhana lebih sulit. Andaikan G berorde 48. Dalam kasus ini, teknik yang digunakan pada contoh terakhir tidak akan berhasil. Kita memerlukan lema berikut untuk membuktikan bahwa tidak ada grup berorde 48 yang sederhana.

Lema 15.2.10 *Misalkan H dan K subgrup hingga dari grup G. Maka*

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Bukti. Ingat bahwa

$$HK = \{hk : h \in H, k \in K\}.$$

Tentu saja, $|HK| \leq |H| \cdot |K|$ karena suatu elemen dalam HK mungkin dapat ditulis sebagai hasil kali elemen-elemen berbeda dari H dan K. Sangat mungkin bahwa $h_1k_1 = h_2k_2$ untuk $h_1, h_2 \in H$ dan $k_1, k_2 \in K$. Jika demikian, misalkan

$$a = (h_1)^{-1}h_2 = k_1(k_2)^{-1}.$$

Perhatikan bahwa $a \in H \cap K$, karena $(h_1)^{-1}h_2$ berada dalam H dan $k_2(k_1)^{-1}$ berada dalam K; akibatnya,

$$h_2 = h_1a^{-1}$$

$$k_2 = ak_1.$$

Sebaliknya, misalkan $h = h_1 b^{-1}$ dan $k = bk_1$ untuk $b \in H \cap K$. Maka $hk = h_1 k_1$, dengan $h \in H$ dan $k \in K$. Jadi, sebarang elemen $hk \in HK$ dapat ditulis dalam bentuk $h_i k_i$ untuk $h_i \in H$ dan $k_i \in K$, sebanyak jumlah elemen dalam $H \cap K$; yaitu sebanyak $|H \cap K|$ kali. Oleh karena itu, $|HK| = (|H| \cdot |K|)/|H \cap K|$. ■

Contoh 15.2.11 Untuk menunjukkan bahwa grup G berorde 48 tidak sederhana, kita akan menunjukkan bahwa G memuat subgrup normal berorde 8 atau subgrup normal berorde 16. Berdasarkan Teorema Sylow Ketiga, G memiliki satu atau tiga subgrup Sylow-2 berorde 16. Jika hanya ada satu subgrup, maka subgrup itu harus normal.

Andaikan kasus lainnya berlaku, dan dua dari ketiga subgrup Sylow-2 itu adalah H dan K. Kita mengklaim bahwa $|H \cap K| = 8$. Jika $|H \cap K| \leq 4$, maka berdasarkan Lema 15.2.10,

$$|HK| \geq \frac{16 \cdot 16}{4} = 64,$$

yang mustahil. Perhatikan bahwa $H \cap K$ berindeks dua dalam H maupun K, sehingga normal di keduanya, dan dengan demikian H serta K masing-masing termuat dalam penormal $H \cap K$. Karena H merupakan subgrup dari $N(H \cap K)$ dan karena $N(H \cap K)$ memiliki lebih dari 16 elemen, $|N(H \cap K)|$ harus merupakan kelipatan 16 yang lebih besar dari 1, sekaligus membagi 48. Satu-satunya kemungkinan adalah $|N(H \cap K)| = 48$. Jadi, $N(H \cap K) = G$. ▲

Konjektur Burnside yang terkenal berikut dibuktikan oleh Feit dan Thompson dalam sebuah makalah yang panjang dan sulit [2].

Teorema 15.2.12 Teorema Orde Ganjil. *Setiap grup sederhana hingga yang ordenya bukan prima harus berorde genap.*

Pembuktian teorema ini meletakkan dasar bagi suatu program pada dekade 1960-an dan 1970-an yang mengklasifikasikan semua grup sederhana hingga. Keberhasilan program ini merupakan salah satu pencapaian luar biasa dalam matematika modern.

15.3 Pertanyaan Bacaan

1. Nyatakan Teorema Sylow Pertama.

2. Ada berapa grup berorde 69? Mengapa?

3. Berikan dua deskripsi yang sifatnya benar-benar berbeda tentang penormal suatu subgrup.

4. Andaikan G grup abelian. Apa subgrup komutator dari G, dan bagaimana Anda mengetahuinya?

5. Mengapa Teorema Sylow begitu penting?

15.4 Latihan

1. Tentukan orde semua subgrup Sylow-p ketika G berorde 18, 24, 54, 72, dan 80?

Petunjuk. Jika $|G| = 18 = 2 \cdot 3^2$, maka orde subgrup Sylow-2 adalah 2, dan orde subgrup Sylow-3 adalah 9.

2. Tentukan semua subgrup Sylow-3 dari S_4 dan tunjukkan bahwa semuanya saling konjugat.

Petunjuk. Keempat subgrup Sylow-3 dari S_4 adalah $P_1 = \{(1), (1\,2\,3), (1\,3\,2)\}$, $P_2 = \{(1), (1\,2\,4), (1\,4\,2)\}$, $P_3 = \{(1), (1\,3\,4), (1\,4\,3)\}$, $P_4 = \{(1), (2\,3\,4), (2\,4\,3)\}$.

3. Tunjukkan bahwa setiap grup berorde 45 memiliki subgrup normal berorde 9.

4. Misalkan H subgrup Sylow-p dari G. Buktikan bahwa H adalah satu-satunya subgrup Sylow-p dari G yang termuat dalam $N(H)$.

5. Buktikan bahwa tidak ada grup berorde 96 yang sederhana.

Petunjuk. Karena $|G| = 96 = 2^5 \cdot 3$, menurut Teorema Sylow Ketiga, G memiliki satu atau tiga subgrup Sylow-2. Jika hanya ada satu subgrup, pembuktian selesai. Jika terdapat tiga subgrup Sylow-2, misalkan H dan K dua di antaranya. Maka $|H \cap K| \geq 16$; jika tidak, HK akan memiliki $(32 \cdot 32)/8 = 128$ elemen, yang mustahil. Jadi, $H \cap K$ normal di H maupun K karena berindeks 2 dalam kedua grup.

6. Buktikan bahwa tidak ada grup berorde 160 yang sederhana.

7. Jika H subgrup normal dari grup hingga G dan $|H| = p^k$ untuk suatu bilangan prima p, tunjukkan bahwa H termuat dalam setiap subgrup Sylow-p dari G.

8. Misalkan G grup berorde p^2q^2, dengan p dan q bilangan prima berbeda sedemikian sehingga $q \nmid p^2 - 1$ dan $p \nmid q^2 - 1$. Buktikan bahwa G harus abelian. Tentukan sepasang bilangan prima yang memenuhi kondisi ini.

Petunjuk. Tunjukkan bahwa G memiliki subgrup Sylow-p normal berorde p^2 dan subgrup Sylow-q normal berorde q^2.

9. Tunjukkan bahwa grup berorde 33 hanya memiliki satu subgrup Sylow-3.

10. Misalkan H subgrup dari grup G. Buktikan atau sangkal bahwa penormal H normal di G.

Petunjuk. Salah.

11. Misalkan G grup hingga yang ordenya habis dibagi bilangan prima p. Buktikan bahwa jika hanya ada satu subgrup Sylow-p di G, subgrup tersebut harus normal di G.

12. Misalkan G grup berorde p^r, dengan p prima. Buktikan bahwa G memuat subgrup normal berorde p^{r-1}.

13. Andaikan G grup hingga berorde $p^n k$, dengan $k < p$. Tunjukkan bahwa G harus memuat subgrup normal nontrivial sejati.

14. Misalkan H subgrup dari grup hingga G. Buktikan bahwa $gN(H)g^{-1} = N(gHg^{-1})$ untuk setiap $g \in G$.

15. Buktikan bahwa grup berorde 108 harus memiliki subgrup normal nontrivial sejati.

16. Klasifikasikan semua grup berorde 175 hingga isomorfisma.

17. Tunjukkan bahwa setiap grup berorde 255 bersifat siklik.

Petunjuk. Jika G abelian, maka G siklik, karena $|G| = 3 \cdot 5 \cdot 17$. Sekarang perhatikan Contoh 15.2.6.

18. Misalkan G berorde $p_1^{e_1} \cdots p_n^{e_n}$ dan andaikan G memiliki n subgrup Sylow-p $P_1, \ldots, P_n$ dengan $|P_i| = p_i^{e_i}$. Buktikan bahwa G isomorfik dengan $P_1 \times \cdots \times P_n$.

19. Misalkan P subgrup Sylow-p normal dari G. Buktikan bahwa setiap automorfisme dalam dari G menetapkan P.

20. Berapakah orde terkecil yang mungkin bagi grup G sedemikian sehingga G nonabelian dan $|G|$ ganjil? Dapatkah Anda menemukan grup semacam itu?

21. **Lema Frattini.** Jika H subgrup normal dari grup hingga G dan P subgrup Sylow-p dari H, untuk setiap $g \in G$, tunjukkan bahwa terdapat h dalam H sedemikian sehingga $gPg^{-1} = hPh^{-1}$. Tunjukkan pula bahwa jika N adalah penormal P, maka $G = HN$.

22. Tunjukkan bahwa jika orde G adalah $p^n q$, dengan p dan q bilangan prima serta $p > q$, maka G memuat subgrup normal nontrivial sejati.

23. Buktikan bahwa banyaknya konjugat berbeda dari subgrup H pada grup hingga G adalah $[G : N(H)]$.

Petunjuk. Definisikan pemetaan antara koset-koset kanan dari $N(H)$ di G dan konjugat-konjugat dari H di G melalui $N(H)g \mapsto g^{-1}Hg$. Buktikan bahwa pemetaan ini bijektif.

24. Buktikan bahwa subgrup Sylow-2 dari S_5 isomorfik dengan D_4.

25. **Pembuktian Lain Teorema Sylow.**

(a) Andaikan p prima dan p tidak membagi m. Tunjukkan bahwa

$$p \nmid \binom{p^k m}{p^k}.$$

(b) Misalkan $\mathcal{S}$ menyatakan himpunan semua himpunan bagian beranggotakan p^k elemen dari G. Tunjukkan bahwa p tidak membagi $|\mathcal{S}|$.

(c) Definisikan aksi G pada $\mathcal{S}$ melalui perkalian kiri, $aT = \{at : t \in T\}$ untuk $a \in G$ dan $T \in \mathcal{S}$. Buktikan bahwa ini merupakan aksi grup.

(d) Buktikan bahwa $p \nmid |\mathcal{O}_T|$ untuk suatu $T \in \mathcal{S}$.

(e) Misalkan $\{T_1, \ldots, T_u\}$ suatu orbit sedemikian sehingga $p \nmid u$ dan $H = \{g \in G : gT_1 = T_1\}$. Buktikan bahwa H merupakan subgrup dari G dan tunjukkan bahwa $|G| = u|H|$.

(f) Tunjukkan bahwa p^k membagi $|H|$ dan $p^k \leq |H|$.

(g) Tunjukkan bahwa $|H| = |\mathcal{O}_T| \leq p^k$; simpulkan bahwa $p^k = |H|$.

26. Misalkan G suatu grup. Buktikan bahwa $G' = \langle aba^{-1}b^{-1} : a, b \in G \rangle$ merupakan subgrup normal dari G dan G/G' abelian. Temukan contoh yang menunjukkan bahwa $\{aba^{-1}b^{-1} : a, b \in G\}$ belum tentu merupakan grup.

Petunjuk. Misalkan $aG', bG' \in G/G'$. Maka $(aG')(bG') = abG' = ab(b^{-1}a^{-1}ba)G' = (abb^{-1}a^{-1})baG' = baG'$.

15.5 Proyek

Tujuan utama teori grup hingga adalah mengklasifikasikan semua grup hingga yang mungkin hingga isomorfisma. Masalah ini sangat sulit, bahkan jika kita hanya mencoba mengklasifikasikan grup yang ordenya kurang dari atau sama dengan 60. Namun, kita dapat membagi masalah ini menjadi beberapa masalah antara. Proyek ini menantang dan memerlukan penguasaan praktis atas teori grup yang telah Anda pelajari sampai titik ini. Meskipun tidak menyelesaikannya, Anda akan belajar banyak tentang grup hingga. Anda dapat

menggunakan Tabel 15.5.1 sebagai panduan.

Tabel 15.5.1 Banyaknya grup berbeda G, $|G| \leq 60$

Orde	Banyaknya	Orde	Banyaknya	Orde	Banyaknya	Orde	Banyaknya
1	?	16	14	31	1	46	2
2	?	17	1	32	51	47	1
3	?	18	?	33	1	48	52
4	?	19	?	34	?	49	?
5	?	20	5	35	1	50	5
6	?	21	?	36	14	51	?
7	?	22	2	37	1	52	?
8	?	23	1	38	?	53	?
9	?	24	?	39	2	54	15
10	?	25	2	40	14	55	2
11	?	26	2	41	1	56	?
12	5	27	5	42	?	57	2
13	?	28	?	43	1	58	?
14	?	29	1	44	4	59	1
15	1	30	4	45	?	60	13

1. Tentukan semua grup sederhana G ($|G| \leq 60$). *Jangan gunakan Teorema Orde Ganjil kecuali Anda siap membuktikannya.*

2. Tentukan banyaknya grup berbeda G, dengan orde G adalah n untuk $n = 1, \ldots, 60$.

3. Tentukan grup-grupnya (hingga isomorfisma) untuk setiap n.

15.6 Referensi dan Bacaan yang Disarankan

[1] Edwards, H. "A Short History of the Fields Medal," *Mathematical Intelligencer* 1 (1978), 127–29.

[2] Feit, W. and Thompson, J. G. "Solvability of Groups of Odd Order," *Pacific Journal of Mathematics* 13 (1963), 775–1029.

[3] Gallian, J. A. "The Search for Finite Simple Groups," *Mathematics Magazine* 49 (1976), 163–79.

[4] Gorenstein, D. "Classifying the Finite Simple Groups," *Bulletin of the American Mathematical Society* 14 (1986), 1–98.

[5] Gorenstein, D. *Finite Groups.* AMS Chelsea Publishing, Providence RI, 1968.

[6] Gorenstein, D., Lyons, R., and Solomon, R. *The Classification of Finite Simple Groups.* American Mathematical Society, Providence RI, 1994.

16

Gelanggang

Sampai tahap ini, kita telah mempelajari himpunan dengan satu operasi biner yang memenuhi aksioma-aksioma tertentu, tetapi sering kali kita lebih tertarik bekerja dengan himpunan yang memiliki dua operasi biner. Sebagai contoh, salah satu struktur aljabar yang paling alami untuk dipelajari adalah bilangan bulat dengan operasi penjumlahan dan perkalian. Kedua operasi ini saling berkaitan melalui sifat distributif. Jika kita meninjau suatu himpunan dengan dua operasi biner yang saling berkaitan dan memenuhi aksioma-aksioma tertentu, kita memperoleh struktur aljabar yang disebut gelanggang. Dalam suatu gelanggang, kita menjumlahkan dan mengalikan elemen seperti bilangan real, bilangan kompleks, matriks, dan fungsi.

16.1 Gelanggang

Suatu himpunan takkosong R disebut **gelanggang** jika memiliki dua operasi biner tertutup, yaitu penjumlahan dan perkalian, yang memenuhi syarat-syarat berikut.

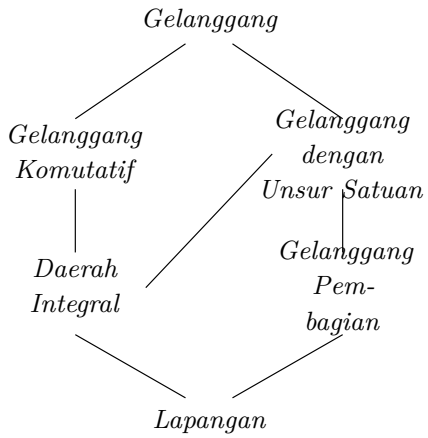
1. $a + b = b + a$ untuk $a, b \in R$.
2. $(a + b) + c = a + (b + c)$ untuk $a, b, c \in R$.
3. Terdapat elemen 0 dalam R sedemikian sehingga $a + 0 = a$ untuk semua $a \in R$.
4. Untuk setiap elemen $a \in R$, terdapat elemen $-a$ dalam R sedemikian sehingga $a + (-a) = 0$.
5. $(ab)c = a(bc)$ untuk $a, b, c \in R$.
6. Untuk $a, b, c \in R$,

$$a(b + c) = ab + ac$$
$$(a + b)c = ac + bc.$$

Syarat terakhir ini, yakni aksioma distributif, menghubungkan operasi biner penjumlahan dan perkalian. Perhatikan bahwa empat aksioma pertama hanya mensyaratkan suatu gelanggang menjadi grup abelian terhadap penjumlahan, sehingga kita juga dapat mendefinisikan gelanggang sebagai grup abelian

$(R, +)$ beserta operasi biner kedua yang memenuhi syarat kelima dan keenam di atas.

Jika terdapat elemen $1 \in R$ sedemikian sehingga $1 \neq 0$ dan $1a = a1 = a$ untuk setiap elemen $a \in R$, kita mengatakan bahwa R merupakan gelanggang dengan **satuan** atau **identitas**. Suatu gelanggang R yang memenuhi $ab = ba$ untuk semua a, b dalam R disebut **gelanggang komutatif**. Suatu gelanggang komutatif R dengan identitas disebut **daerah integral** jika, untuk setiap $a, b \in R$ sedemikian sehingga $ab = 0$, berlaku $a = 0$ atau $b = 0$. **Gelanggang pembagian** adalah gelanggang R dengan identitas, yang setiap elemen taknol dalam R merupakan suatu **unsur satuan**; yaitu, untuk setiap $a \in R$ dengan $a \neq 0$, terdapat elemen tunggal a^{-1} sedemikian sehingga $a^{-1}a = aa^{-1} = 1$. Gelanggang pembagian komutatif disebut **lapangan**. Hubungan antara gelanggang, daerah integral, gelanggang pembagian, dan lapangan ditunjukkan dalam Gambar 16.1.1.



Gambar 16.1.1 Jenis-jenis gelanggang

Contoh 16.1.2 Seperti telah disebutkan sebelumnya, bilangan bulat membentuk gelanggang. Bahkan, $\mathbb{Z}$ merupakan daerah integral. Jelas bahwa jika $ab = 0$ untuk dua bilangan bulat a dan b, maka $a = 0$ atau $b = 0$. Namun, $\mathbb{Z}$ bukan lapangan. Tidak ada bilangan bulat yang merupakan invers multiplikatif dari 2, karena $1/2$ bukan bilangan bulat. Satu-satunya bilangan bulat yang memiliki invers multiplikatif adalah 1 dan -1. ▲

Contoh 16.1.3 Terhadap operasi penjumlahan dan perkalian biasa, semua sistem bilangan yang dikenal merupakan gelanggang: bilangan rasional, $\mathbb{Q}$; bilangan real, $\mathbb{R}$; dan bilangan kompleks, $\mathbb{C}$. Setiap gelanggang ini merupakan lapangan. ▲

Contoh 16.1.4 Kita dapat mendefinisikan hasil kali dua elemen a dan b dalam $\mathbb{Z}_n$ dengan $ab \pmod{n}$. Sebagai contoh, dalam $\mathbb{Z}_{12}$, $5 \cdot 7 \equiv 11 \pmod{12}$. Hasil kali ini menjadikan grup abelian $\mathbb{Z}_n$ suatu gelanggang. Jelas bahwa $\mathbb{Z}_n$ merupakan gelanggang komutatif; namun, gelanggang tersebut mungkin bukan daerah integral. Jika kita meninjau $3 \cdot 4 \equiv 0 \pmod{12}$ dalam $\mathbb{Z}_{12}$, mudah dilihat bahwa hasil kali dua elemen taknol dalam gelanggang dapat sama dengan nol. ▲

Elemen taknol a dalam gelanggang komutatif R disebut **pembagi nol** jika terdapat elemen taknol b dalam R sedemikian sehingga $ab = 0$. Dalam contoh sebelumnya, 3 dan 4 merupakan pembagi nol dalam $\mathbb{Z}_{12}$.

Contoh 16.1.5 Dalam kalkulus, fungsi kontinu bernilai real pada suatu interval $[a, b]$ membentuk gelanggang komutatif. Kita menjumlahkan atau menga-

likan dua fungsi dengan menjumlahkan atau mengalikan nilai-nilai fungsi tersebut. Jika $f(x) = x^2$ dan $g(x) = \cos x$, maka $(f+g)(x) = f(x) + g(x) = x^2 + \cos x$ dan $(fg)(x) = f(x)g(x) = x^2 \cos x$. ▲

Contoh 16.1.6 Matriks 2×2 dengan entri dalam $\mathbb{R}$ membentuk gelanggang terhadap operasi penjumlahan dan perkalian matriks biasa. Gelanggang ini nonkomutatif, karena biasanya berlaku $AB \neq BA$. Perhatikan pula bahwa dapat berlaku $AB = 0$ ketika A maupun B tidak nol. ▲

Contoh 16.1.7 Sebagai contoh gelanggang pembagian nonkomutatif, misalkan

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

dengan $i^2 = -1$. Elemen-elemen ini memenuhi relasi berikut:

$$\begin{aligned} \mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 &= -1 \\ \mathbf{ij} &= \mathbf{k} \\ \mathbf{jk} &= \mathbf{i} \\ \mathbf{ki} &= \mathbf{j} \\ \mathbf{ji} &= -\mathbf{k} \\ \mathbf{kj} &= -\mathbf{i} \\ \mathbf{ik} &= -\mathbf{j}. \end{aligned}$$

Misalkan $\mathbb{H}$ terdiri atas elemen berbentuk $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, dengan a, b, c, d bilangan real. Secara ekuivalen, $\mathbb{H}$ dapat dipandang sebagai himpunan semua matriks 2×2 berbentuk

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix},$$

dengan $\alpha = a + di$ dan $\beta = b + ci$ merupakan bilangan kompleks. Kita dapat mendefinisikan penjumlahan dan perkalian pada $\mathbb{H}$ melalui operasi matriks biasa atau berdasarkan pembangkit 1, $\mathbf{i}$, $\mathbf{j}$, dan $\mathbf{k}$:

$$\begin{aligned} &(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k}) + (a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) \\ &= (a_1 + a_2) + (b_1 + b_2)\mathbf{i} + (c_1 + c_2)\mathbf{j} + (d_1 + d_2)\mathbf{k} \end{aligned}$$

dan

$$(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k})(a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) = \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k},$$

dengan

$$\begin{aligned} \alpha &= a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 \\ \beta &= a_1b_2 + a_2b_1 + c_1d_2 - d_1c_2 \\ \gamma &= a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2 \\ \delta &= a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2. \end{aligned}$$

Meskipun perkaliannya tampak rumit, perhitungannya sebenarnya langsung jika kita mengingat bahwa elemen-elemen dalam $\mathbb{H}$ cukup dijumlahkan dan dikalikan seperti polinomial sambil memperhatikan relasi antara pembangkit $\mathbf{i}$, $\mathbf{j}$, dan $\mathbf{k}$. Gelanggang $\mathbb{H}$ disebut gelanggang **kuaternion**.

Untuk menunjukkan bahwa kuaternion merupakan gelanggang pembagian, kita harus dapat menemukan invers bagi setiap elemen taknol. Perhatikan bahwa

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) = a^2 + b^2 + c^2 + d^2.$$

Elemen ini hanya dapat bernilai nol jika a, b, c, dan d semuanya nol. Jadi, jika $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \neq 0$,

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) \left(\frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2} \right) = 1.$$

▲

Proposisi 16.1.8 *Misalkan R suatu gelanggang dengan $a, b \in R$. Maka*

1. $a0 = 0a = 0$;
2. $a(-b) = (-a)b = -ab$;
3. $(-a)(-b) = ab$.

BUKTI. Untuk membuktikan (1), perhatikan bahwa

$$a0 = a(0 + 0) = a0 + a0;$$

dengan demikian, $a0 = 0$. Demikian pula, $0a = 0$. Untuk (2), kita memiliki $ab + a(-b) = a(b - b) = a0 = 0$; akibatnya, $-ab = a(-b)$. Demikian pula, $-ab = (-a)b$. Bagian (3) mengikuti langsung dari (2) karena $(-a)(-b) = -(a(-b)) = -(-ab) = ab$. ■

Sebagaimana grup memiliki subgrup, gelanggang memiliki kelas substruktur yang analog. Suatu **subgelanggang** S dari gelanggang R adalah himpunan bagian S dari R sedemikian sehingga S juga merupakan gelanggang terhadap operasi yang diwarisi dari R.

Contoh 16.1.9 Gelanggang $n\mathbb{Z}$ merupakan subgelanggang dari $\mathbb{Z}$. Perhatikan bahwa meskipun gelanggang asal mungkin memiliki identitas, kita tidak mensyaratkan subgelanggangnya memiliki identitas. Kita memiliki rantai subgelanggang berikut:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

▲

Proposisi berikut memberikan beberapa kriteria mudah untuk menentukan apakah suatu himpunan bagian dari gelanggang benar-benar merupakan subgelanggang. (Pembuktian proposisi ini diserahkan sebagai latihan.)

Proposisi 16.1.10 *Misalkan R suatu gelanggang dan S suatu himpunan bagian dari R. Maka S merupakan subgelanggang dari R jika dan hanya jika syarat-syarat berikut terpenuhi.*

1. $S \neq \emptyset$.
2. $rs \in S$ *untuk semua* $r, s \in S$.
3. $r - s \in S$ *untuk semua* $r, s \in S$.

Contoh 16.1.11 Misalkan $R = \mathbb{M}_2(\mathbb{R})$ gelanggang matriks 2×2 dengan entri dalam $\mathbb{R}$. Jika T merupakan himpunan matriks segitiga atas dalam R; yaitu,

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\},$$

maka T merupakan subgelanggang dari R. Jika

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \quad \text{dan} \quad B = \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}$$

berada dalam T, maka jelas bahwa $A - B$ juga berada dalam T. Selain itu,

$$AB = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix}$$

berada dalam T. ▲

16.2 Daerah Integral dan Lapangan

Mari kita ingat kembali beberapa definisi secara singkat. Jika R merupakan gelanggang komutatif dan r elemen taknol dalam R, maka r disebut **pembagi nol** jika terdapat elemen taknol $s \in R$ sedemikian sehingga $rs = 0$. Gelanggang komutatif dengan identitas disebut **daerah integral** jika tidak memiliki pembagi nol. Jika suatu elemen a dalam gelanggang R dengan identitas memiliki invers multiplikatif, kita mengatakan bahwa a merupakan **unsur satuan**. Jika setiap elemen taknol dalam gelanggang R merupakan unsur satuan, maka R disebut **gelanggang pembagian**. Gelanggang pembagian komutatif disebut **lapangan**.

Contoh 16.2.1 Jika $i^2 = -1$, maka himpunan $\mathbb{Z}[i] = \{m + ni : m, n \in \mathbb{Z}\}$ membentuk gelanggang yang dikenal sebagai **bilangan bulat Gauss**. Mudah dilihat bahwa bilangan bulat Gauss merupakan subgelanggang dari bilangan kompleks karena tertutup terhadap penjumlahan dan perkalian. Misalkan $\alpha = a + bi$ suatu unsur satuan dalam $\mathbb{Z}[i]$. Maka $\overline{\alpha} = a - bi$ juga merupakan unsur satuan karena jika $\alpha\beta = 1$, maka $\overline{\alpha}\overline{\beta} = 1$. Jika $\beta = c + di$, maka

$$1 = \alpha\beta\overline{\alpha}\overline{\beta} = (a^2 + b^2)(c^2 + d^2).$$

Oleh karena itu, $a^2 + b^2$ harus bernilai 1 atau -1; atau, secara ekuivalen, $a+bi = \pm 1$ atau $a+bi = \pm i$. Jadi, unsur-unsur satuan gelanggang ini adalah ± 1 dan $\pm i$; dengan demikian, bilangan bulat Gauss bukan lapangan. Pembuktian bahwa bilangan bulat Gauss merupakan daerah integral diserahkan sebagai latihan. ▲

Contoh 16.2.2 Himpunan matriks

$$F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

dengan entri dalam $\mathbb{Z}_2$ membentuk lapangan. ▲

Contoh 16.2.3 Himpunan $\mathbb{Q}(\sqrt{2}\,) = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ merupakan lapangan. Invers suatu elemen $a + b\sqrt{2}$ dalam $\mathbb{Q}(\sqrt{2}\,)$ adalah

$$\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}.$$

▲

Kita memiliki karakterisasi alternatif berikut untuk daerah integral.

Proposisi 16.2.4 Hukum Kanselasi. *Misalkan D suatu gelanggang komutatif dengan identitas. Maka D merupakan daerah integral jika dan hanya jika untuk semua elemen taknol $a \in D$ dengan $ab = ac$, berlaku $b = c$.*

Bukti. Misalkan D suatu daerah integral. Maka D tidak memiliki pembagi nol. Misalkan $ab = ac$ dengan $a \neq 0$. Maka $a(b - c) = 0$. Dengan demikian, $b - c = 0$ dan $b = c$.

Sebaliknya, andaikan kanselasi dapat dilakukan dalam D. Artinya, andaik-

an $ab = ac$ mengakibatkan $b = c$. Misalkan $ab = 0$. Jika $a \neq 0$, maka $ab = a0$ atau $b = 0$. Oleh karena itu, a tidak mungkin merupakan pembagi nol. ■

Teorema mengejutkan berikut dikemukakan oleh Wedderburn.

Teorema 16.2.5 *Setiap daerah integral hingga merupakan lapangan.*

BUKTI. Misalkan D suatu daerah integral hingga dan D^* himpunan elemen taknol dari D. Kita harus menunjukkan bahwa setiap elemen dalam D^* memiliki invers. Untuk setiap $a \in D^*$, kita dapat mendefinisikan pemetaan $\lambda_a : D^* \to D^*$ dengan $\lambda_a(d) = ad$. Pemetaan ini masuk akal karena jika $a \neq 0$ dan $d \neq 0$, maka $ad \neq 0$. Pemetaan λ_a injektif, karena untuk $d_1, d_2 \in D^*$,

$$ad_1 = \lambda_a(d_1) = \lambda_a(d_2) = ad_2$$

mengakibatkan $d_1 = d_2$ berdasarkan kanselasi kiri. Karena D^* merupakan himpunan hingga, pemetaan λ_a juga harus surjektif; dengan demikian, untuk suatu $d \in D^*$, $\lambda_a(d) = ad = 1$. Oleh karena itu, a memiliki invers kiri. Karena D komutatif, d juga harus merupakan invers kanan bagi a. Akibatnya, D merupakan lapangan. ■

Untuk setiap bilangan bulat taknegatif n dan setiap elemen r dalam suatu gelanggang R, kita tuliskan $r + \cdots + r$ (n kali) sebagai nr. Kita mendefinisikan **karakteristik** suatu gelanggang R sebagai bilangan bulat positif terkecil n sedemikian sehingga $nr = 0$ untuk semua $r \in R$. Jika tidak terdapat bilangan bulat semacam itu, maka karakteristik R didefinisikan sebagai 0. Kita akan menyatakan karakteristik R dengan $\operatorname{char} R$.

Contoh 16.2.6 Untuk setiap bilangan prima p, $\mathbb{Z}_p$ merupakan lapangan berkarakteristik p. Berdasarkan Proposisi 3.1.4, setiap elemen taknol dalam $\mathbb{Z}_p$ memiliki invers; dengan demikian, $\mathbb{Z}_p$ merupakan lapangan. Jika a sebarang elemen taknol dalam lapangan tersebut, maka $pa = 0$, karena orde setiap elemen taknol dalam grup abelian $\mathbb{Z}_p$ adalah p. ▲

Lema 16.2.7 *Misalkan R suatu gelanggang dengan identitas. Jika 1 berorde n, maka karakteristik R adalah n.*

BUKTI. Jika 1 berorde n, maka n merupakan bilangan bulat positif terkecil sedemikian sehingga $n1 = 0$. Jadi, untuk semua $r \in R$,

$$nr = n(1r) = (n1)r = 0r = 0.$$

Di sisi lain, jika tidak terdapat n positif sedemikian sehingga $n1 = 0$, maka karakteristik R adalah nol. ■

Teorema 16.2.8 *Karakteristik suatu daerah integral adalah prima atau nol.*

BUKTI. Misalkan D suatu daerah integral dan andaikan karakteristik D adalah n dengan $n \neq 0$. Jika n tidak prima, maka $n = ab$, dengan $1 < a < n$ dan $1 < b < n$. Berdasarkan Lema 16.2.7, kita hanya perlu meninjau kasus $n1 = 0$. Karena $0 = n1 = (ab)1 = (a1)(b1)$ dan tidak ada pembagi nol dalam D, berlaku $a1 = 0$ atau $b1 = 0$. Dengan demikian, karakteristik D harus kurang dari n, yang merupakan suatu kontradiksi. Oleh karena itu, n harus prima. ■

16.3 Homomorfisma Gelanggang dan Ideal

Dalam kajian grup, homomorfisma adalah pemetaan yang mempertahankan operasi grup. Demikian pula, homomorfisma antara gelanggang mempertahankan operasi penjumlahan dan perkalian dalam gelanggang. Secara lebih

khusus, jika R dan S adalah gelanggang, maka **homomorfisma gelanggang** adalah pemetaan $\phi : R \to S$ yang memenuhi

$$\begin{aligned}\phi(a+b) &= \phi(a) + \phi(b)\\ \phi(ab) &= \phi(a)\phi(b)\end{aligned}$$

untuk semua $a, b \in R$. Jika $\phi : R \to S$ adalah homomorfisma yang injektif dan surjektif, maka ϕ disebut **isomorfisma** gelanggang.

Himpunan unsur yang dipetakan ke 0 oleh suatu homomorfisma gelanggang memainkan peran mendasar dalam teori gelanggang. Untuk sebarang homomorfisma gelanggang $\phi : R \to S$, kita mendefinisikan **kernel** homomorfisma gelanggang sebagai himpunan

$$\ker \phi = \{r \in R : \phi(r) = 0\}.$$

Contoh 16.3.1 Untuk sebarang bilangan bulat n, kita dapat mendefinisikan homomorfisma gelanggang $\phi : \mathbb{Z} \to \mathbb{Z}_n$ dengan $a \mapsto a \pmod n$. Pemetaan ini memang merupakan homomorfisma gelanggang, karena

$$\begin{aligned}\phi(a+b) &= (a+b) \pmod n\\ &= a \pmod n + b \pmod n\\ &= \phi(a) + \phi(b)\end{aligned}$$

dan

$$\begin{aligned}\phi(ab) &= ab \pmod n\\ &= a \pmod n \cdot b \pmod n\\ &= \phi(a)\phi(b).\end{aligned}$$

Kernel homomorfisma ϕ adalah $n\mathbb{Z}$. ▲

Contoh 16.3.2 Misalkan $C[a, b]$ adalah gelanggang fungsi kontinu bernilai real pada interval $[a, b]$ seperti dalam Contoh 16.1.5. Untuk suatu $\alpha \in [a, b]$ yang tetap, kita dapat mendefinisikan homomorfisma gelanggang $\phi_\alpha : C[a, b] \to \mathbb{R}$ dengan $\phi_\alpha(f) = f(\alpha)$. Pemetaan ini merupakan homomorfisma gelanggang karena

$$\begin{aligned}\phi_\alpha(f+g) = (f+g)(\alpha) = f(\alpha) + g(\alpha) = \phi_\alpha(f) + \phi_\alpha(g)\\ \phi_\alpha(fg) = (fg)(\alpha) = f(\alpha)g(\alpha) = \phi_\alpha(f)\phi_\alpha(g).\end{aligned}$$

Homomorfisma gelanggang bertipe ϕ_α disebut **homomorfisma evaluasi**. ▲

Dalam proposisi berikut, kita akan memeriksa beberapa sifat mendasar homomorfisma gelanggang. Pembuktian proposisi tersebut diserahkan sebagai latihan.

Proposisi 16.3.3 *Misalkan $\phi : R \to S$ adalah homomorfisma gelanggang.*

1. *Jika R adalah gelanggang komutatif, maka $\phi(R)$ adalah gelanggang komutatif.*
2. $\phi(0) = 0$.
3. *Misalkan 1_R dan 1_S masing-masing adalah identitas untuk R dan S. Jika ϕ surjektif, maka $\phi(1_R) = 1_S$.*
4. *Jika R adalah lapangan dan $\phi(R) \neq \{0\}$, maka $\phi(R)$ adalah lapangan.*

Dalam teori grup, kita mendapati bahwa subgrup normal memainkan peran khusus. Subgrup-subgrup ini memiliki karakteristik baik yang membuatnya lebih menarik untuk dikaji daripada subgrup sebarang. Dalam teori gelanggang, objek yang bersesuaian dengan subgrup normal adalah suatu kelas khusus subgelanggang yang disebut ideal. **Ideal** dalam gelanggang R adalah subgelanggang I dari R sedemikian sehingga jika a berada dalam I dan r berada dalam R, maka ar dan ra keduanya berada dalam I; yaitu, $rI \subset I$ dan $Ir \subset I$ untuk semua $r \in R$.

Contoh 16.3.4 Setiap gelanggang R memiliki sekurang-kurangnya dua ideal, yaitu $\{0\}$ dan R. Ideal-ideal ini disebut **ideal trivial**. ▲

Misalkan R adalah gelanggang dengan identitas dan andaikan I adalah ideal dalam R sedemikian sehingga 1 berada dalam I. Karena untuk sebarang $r \in R$, $r1 = r \in I$ berdasarkan definisi ideal, maka $I = R$.

Contoh 16.3.5 Jika a adalah sebarang unsur dalam gelanggang komutatif R dengan identitas, maka himpunan

$$\langle a \rangle = \{ar : r \in R\}$$

adalah ideal dalam R. Jelas bahwa $\langle a \rangle$ tidak kosong karena $0 = a0$ dan $a = a1$ keduanya berada dalam $\langle a \rangle$. Jumlah dua unsur dalam $\langle a \rangle$ kembali berada dalam $\langle a \rangle$ karena $ar + ar' = a(r + r')$. Invers dari ar adalah $-ar = a(-r) \in \langle a \rangle$. Terakhir, jika kita mengalikan unsur $ar \in \langle a \rangle$ dengan sebarang unsur $s \in R$, kita memperoleh $s(ar) = a(sr)$. Oleh karena itu, $\langle a \rangle$ memenuhi definisi ideal. ▲

Jika R adalah gelanggang komutatif dengan identitas, maka ideal berbentuk $\langle a \rangle = \{ar : r \in R\}$ disebut **ideal utama**.

Teorema 16.3.6 *Setiap ideal dalam gelanggang bilangan bulat $\mathbb{Z}$ adalah ideal utama.*

Bukti. Ideal nol $\{0\}$ adalah ideal utama karena $\langle 0 \rangle = \{0\}$. Jika I adalah sebarang ideal taknol dalam $\mathbb{Z}$, maka I harus memuat suatu bilangan bulat positif m. Berdasarkan Prinsip Terurut Baik, terdapat bilangan bulat positif terkecil n dalam I. Sekarang misalkan a adalah sebarang unsur dalam I. Dengan menggunakan algoritma pembagian, kita mengetahui bahwa terdapat bilangan bulat q dan r sedemikian sehingga

$$a = nq + r$$

dengan $0 \leq r < n$. Persamaan ini menunjukkan bahwa $r = a - nq \in I$, tetapi r harus sama dengan 0 karena n adalah unsur positif terkecil dalam I. Oleh karena itu, $a = nq$ dan $I = \langle n \rangle$. ■

Contoh 16.3.7 Himpunan $n\mathbb{Z}$ adalah ideal dalam gelanggang bilangan bulat. Jika na berada dalam $n\mathbb{Z}$ dan b berada dalam $\mathbb{Z}$, maka nab berada dalam $n\mathbb{Z}$ sebagaimana disyaratkan. Bahkan, berdasarkan Teorema 16.3.6, himpunan-himpunan ini merupakan satu-satunya ideal dari $\mathbb{Z}$. ▲

Proposisi 16.3.8 *Kernel dari sebarang homomorfisma gelanggang $\phi : R \to S$ adalah ideal dalam R.*

Bukti. Dari teori grup, kita mengetahui bahwa $\ker \phi$ adalah subgrup aditif dari R. Andaikan $r \in R$ dan $a \in \ker \phi$. Maka kita harus menunjukkan bahwa ar dan ra berada dalam $\ker \phi$. Namun,

$$\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$$

dan

$$\phi(ra) = \phi(r)\phi(a) = \phi(r)0 = 0.$$

■

Catatan 16.3.9 Dalam definisi ideal, kita mensyaratkan $rI \subset I$ dan $Ir \subset I$ untuk semua $r \in R$. Ideal semacam itu kadang-kadang disebut **ideal dua sisi**. Kita juga dapat meninjau **ideal satu sisi**; yaitu, kita dapat mensyaratkan hanya salah satu dari $rI \subset I$ atau $Ir \subset I$ untuk $r \in R$, tetapi tidak keduanya. Ideal semacam itu masing-masing disebut **ideal kiri** dan **ideal kanan**. Tentu saja, dalam gelanggang komutatif setiap ideal harus dua sisi. Dalam buku ini, kita akan berfokus pada ideal dua sisi.

Teorema 16.3.10 *Misalkan I adalah ideal dari R. Grup hasil bagi R/I adalah gelanggang dengan perkalian yang didefinisikan oleh*

$$(r + I)(s + I) = rs + I.$$

BUKTI. Kita telah mengetahui bahwa R/I adalah grup abelian terhadap penjumlahan. Misalkan $r+I$ dan $s+I$ berada dalam R/I. Kita harus menunjukkan bahwa hasil kali $(r+I)(s+I) = rs+I$ tidak bergantung pada pemilihan koset; yaitu, jika $r' \in r + I$ dan $s' \in s + I$, maka $r's'$ harus berada dalam $rs + I$. Karena $r' \in r + I$, terdapat unsur a dalam I sedemikian sehingga $r' = r + a$. Demikian pula, terdapat $b \in I$ sedemikian sehingga $s' = s + b$. Perhatikan bahwa

$$r's' = (r + a)(s + b) = rs + as + rb + ab$$

dan $as + rb + ab \in I$ karena I adalah ideal; akibatnya, $r's' \in rs + I$. Verifikasi hukum asosiatif untuk perkalian dan hukum-hukum distributif diserahkan sebagai latihan. ■

Gelanggang R/I dalam Teorema 16.3.10 disebut **gelanggang hasil bagi** atau **gelanggang hasil bagi**. Sebagaimana pada homomorfisma grup dan subgrup normal, terdapat hubungan antara homomorfisma gelanggang dan ideal.

Teorema 16.3.11 *Misalkan I adalah ideal dari R. Pemetaan $\phi : R \to R/I$ yang didefinisikan oleh $\phi(r) = r + I$ adalah homomorfisma gelanggang dari R ke R/I yang surjektif dengan kernel I.*

BUKTI. Jelas bahwa $\phi : R \to R/I$ adalah homomorfisma grup abelian yang surjektif. Tinggal menunjukkan bahwa ϕ berperilaku sebagaimana mestinya terhadap perkalian gelanggang. Misalkan r dan s berada dalam R. Maka

$$\phi(r)\phi(s) = (r + I)(s + I) = rs + I = \phi(rs),$$

yang melengkapi pembuktian teorema. ■

Pemetaan $\phi : R \to R/I$ sering disebut homomorfisma **alami** atau **homomorfisma kanonik**. Dalam teori gelanggang, terdapat teorema-teorema isomorfisma yang menghubungkan ideal dengan homomorfisma gelanggang, serupa dengan teorema isomorfisma grup yang menghubungkan subgrup normal dengan homomorfisma dalam Bab 11. Dalam bab ini, kita hanya akan membuktikan Teorema Isomorfisma Pertama untuk gelanggang dan menyerahkan pembuktian dua teorema lainnya sebagai latihan. Semua pembuktian tersebut serupa dengan pembuktian teorema isomorfisma untuk grup.

Teorema 16.3.12 Teorema Isomorfisma Pertama. *Misalkan $\psi : R \to S$ adalah homomorfisma gelanggang. Maka $\ker \psi$ adalah ideal dari R. Jika $\phi : R \to R/\ker \psi$ adalah homomorfisma kanonik, maka terdapat isomorfisma tunggal $\eta : R/\ker \psi \to \psi(R)$ sedemikian sehingga $\psi = \eta\phi$.*

BUKTI. Misalkan $K = \ker \psi$. Berdasarkan Teorema Isomorfisma Pertama untuk grup, terdapat homomorfisma grup terdefinisi dengan baik $\eta : R/K \to \psi(R)$ yang didefinisikan oleh $\eta(r+K) = \psi(r)$ untuk grup abelian aditif R dan R/K. Untuk menunjukkan bahwa pemetaan ini merupakan homomorfisma gelanggang, kita hanya perlu menunjukkan bahwa $\eta((r+K)(s+K)) = \eta(r+K)\eta(s+K)$; tetapi

$$\begin{aligned}\eta((r+K)(s+K)) &= \eta(rs+K)\\ &= \psi(rs)\\ &= \psi(r)\psi(s)\\ &= \eta(r+K)\eta(s+K).\end{aligned}$$

■

Teorema 16.3.13 Teorema Isomorfisma Kedua. *Misalkan I adalah subgelanggang dari gelanggang R dan J adalah ideal dari R. Maka $I \cap J$ adalah ideal dari I dan*

$$I/I \cap J \cong (I+J)/J.$$

Teorema 16.3.14 Teorema Isomorfisma Ketiga. *Misalkan R adalah gelanggang serta I dan J adalah ideal dari R dengan $J \subset I$. Maka*

$$R/I \cong \frac{R/J}{I/J}.$$

Teorema 16.3.15 Teorema Korespondensi. *Misalkan I adalah ideal dari gelanggang R. Maka $S \mapsto S/I$ merupakan korespondensi satu-ke-satu antara himpunan subgelanggang S yang memuat I dan himpunan subgelanggang dari R/I. Lebih lanjut, ideal-ideal dari R yang memuat I bersesuaian dengan ideal-ideal dari R/I.*

16.4 Ideal Maksimal dan Ideal Prima

Dalam bagian ini, kita secara khusus tertarik pada ideal-ideal tertentu dari gelanggang komutatif. Ideal-ideal ini menghasilkan jenis gelanggang hasil bagi yang khusus. Secara lebih khusus, kita ingin mencirikan ideal-ideal I dari gelanggang komutatif R sedemikian sehingga R/I merupakan daerah integral atau lapangan.

Ideal sejati M dari gelanggang R adalah **ideal maksimal** dari R jika ideal M bukan himpunan bagian sejati dari ideal mana pun dari R, kecuali R sendiri. Dengan kata lain, M adalah ideal maksimal jika untuk setiap ideal I yang memuat M secara sejati, $I = R$. Teorema berikut mencirikan sepenuhnya ideal maksimal pada gelanggang komutatif dengan identitas melalui gelanggang hasil bagi yang bersesuaian.

Teorema 16.4.1 *Misalkan R adalah gelanggang komutatif dengan identitas dan M adalah ideal dalam R. Maka M adalah ideal maksimal dari R jika dan hanya jika R/M merupakan lapangan.*

BUKTI. Misalkan M adalah ideal maksimal dalam R. Jika R adalah gelanggang komutatif, maka R/M juga harus merupakan gelanggang komutatif. Jelas bahwa $1+M$ bertindak sebagai identitas untuk R/M. Kita juga harus menunjukkan bahwa setiap unsur taknol dalam R/M memiliki invers. Jika $a+M$ adalah unsur taknol dalam R/M, maka $a \notin M$. Definisikan I sebagai himpunan $\{ra+m : r \in R \text{ dan } m \in M\}$. Kita akan menunjukkan bahwa I adalah ideal dalam R. Himpunan I tidak kosong karena $0a+0 = 0$ berada

dalam I. Jika $r_1a + m_1$ dan $r_2a + m_2$ adalah dua unsur dalam I, maka

$$(r_1a + m_1) - (r_2a + m_2) = (r_1 - r_2)a + (m_1 - m_2)$$

berada dalam I. Selain itu, untuk sebarang $r \in R$ berlaku $rI \subset I$; dengan demikian, I tertutup terhadap perkalian dan memenuhi syarat-syarat yang diperlukan untuk menjadi ideal. Oleh karena itu, berdasarkan Proposisi 16.1.10 dan definisi ideal, I adalah ideal yang memuat M secara sejati. Karena M adalah ideal maksimal, $I = R$; akibatnya, berdasarkan definisi I, harus terdapat m dalam M dan unsur b dalam R sedemikian sehingga $1 = ab + m$. Oleh karena itu,

$$1 + M = ab + M = ba + M = (a + M)(b + M).$$

Sebaliknya, andaikan M adalah ideal dan R/M merupakan lapangan. Karena R/M merupakan lapangan, gelanggang tersebut harus memuat sekurang-kurangnya dua unsur: $0+M = M$ dan $1+M$. Jadi, M adalah ideal sejati dari R. Misalkan I adalah sebarang ideal yang memuat M secara sejati. Kita perlu menunjukkan bahwa $I = R$. Pilih a dalam I, tetapi tidak dalam M. Karena $a+M$ adalah unsur taknol dalam suatu lapangan, terdapat unsur $b+M$ dalam R/M sedemikian sehingga $(a + M)(b + M) = ab + M = 1 + M$. Akibatnya, terdapat unsur $m \in M$ sedemikian sehingga $ab + m = 1$ dan 1 berada dalam I. Oleh karena itu, $r1 = r \in I$ untuk semua $r \in R$. Akibatnya, $I = R$. ■

Contoh 16.4.2 Misalkan $p\mathbb{Z}$ adalah ideal dalam $\mathbb{Z}$, dengan p prima. Maka $p\mathbb{Z}$ adalah ideal maksimal karena $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ merupakan lapangan. ▲

Ideal sejati P dalam gelanggang komutatif R disebut **ideal prima** jika setiap kali $ab \in P$, berlaku $a \in P$ atau $b \in P$.[1]

Contoh 16.4.3 Mudah diperiksa bahwa himpunan $P = \{0, 2, 4, 6, 8, 10\}$ adalah ideal dalam $\mathbb{Z}_{12}$. Ideal ini adalah ideal prima. Bahkan, ideal ini merupakan ideal maksimal. ▲

Proposisi 16.4.4 *Misalkan R adalah gelanggang komutatif dengan identitas 1, dengan $1 \neq 0$. Maka P adalah ideal prima dalam R jika dan hanya jika R/P merupakan daerah integral.*

Bukti. Pertama, andaikan P adalah ideal dalam R dan R/P merupakan daerah integral. Andaikan $ab \in P$. Jika $a + P$ dan $b + P$ adalah dua unsur dari R/P sedemikian sehingga $(a + P)(b + P) = 0 + P = P$, maka berlaku $a+P = P$ atau $b+P = P$. Ini berarti bahwa a berada dalam P atau b berada dalam P, yang menunjukkan bahwa P harus merupakan ideal prima.

Sebaliknya, andaikan P adalah ideal prima dan

$$(a + P)(b + P) = ab + P = 0 + P = P.$$

Maka $ab \in P$. Jika $a \notin P$, maka b harus berada dalam P berdasarkan definisi ideal prima; dengan demikian, $b + P = 0 + P$ dan R/P merupakan daerah integral. ■

Contoh 16.4.5 Setiap ideal dalam $\mathbb{Z}$ berbentuk $n\mathbb{Z}$. Gelanggang hasil bagi $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ merupakan daerah integral hanya ketika n prima. Bahkan, gelanggang tersebut merupakan lapangan. Jadi, ideal prima taknol dalam $\mathbb{Z}$ adalah ideal-ideal $p\mathbb{Z}$, dengan p prima. Contoh ini sungguh membenarkan penggunaan kata "prima" dalam definisi ideal prima. ▲

[1] Ideal prima dapat pula didefinisikan dalam gelanggang takkomutatif. Lihat [1] atau [3].

Karena setiap lapangan merupakan daerah integral, kita memperoleh akibat berikut.

Korolari 16.4.6 *Setiap ideal maksimal dalam gelanggang komutatif dengan identitas juga merupakan ideal prima.*

Catatan Sejarah

Amalie Emmy Noether, salah seorang matematikawan terkemuka abad kedua puluh, lahir di Erlangen, Jerman, pada tahun 1882. Ia adalah putri Max Noether (1844–1921), seorang matematikawan terkemuka di University of Erlangen. Bersama Paul Gordon (1837–1912), ayah Emmy Noether sangat memengaruhi pendidikan awalnya. Ia memasuki University of Erlangen pada usia 18 tahun. Meskipun perempuan telah diterima di universitas-universitas di Inggris, Prancis, dan Italia selama puluhan tahun, terdapat penolakan besar terhadap kehadiran mereka di universitas-universitas di Jerman. Noether merupakan satu dari hanya dua perempuan di antara 986 mahasiswa universitas tersebut. Setelah menyelesaikan gelar doktornya di bawah bimbingan Gordon pada tahun 1907, ia melanjutkan penelitian di Erlangen, dan sesekali memberi kuliah ketika ayahnya sakit.

Noether pergi ke Göttingen untuk belajar pada tahun 1916. David Hilbert dan Felix Klein berusaha tanpa hasil untuk memperoleh jabatan baginya di Göttingen. Beberapa anggota fakultas menentang dosen perempuan dengan mengatakan, "Apa yang akan dipikirkan para prajurit kita ketika mereka kembali ke universitas dan diharapkan belajar di bawah bimbingan seorang perempuan?" Hilbert, yang kesal dengan pertanyaan itu, menjawab, "Meine Herren, saya tidak melihat bahwa jenis kelamin seorang kandidat merupakan alasan untuk menolak penerimaannya sebagai Privatdozent. Lagi pula, Senat bukanlah rumah pemandian." Pada akhir Perang Dunia I, sikap berubah dan kondisi bagi perempuan sangat membaik. Setelah Noether lulus ujian habilitasi pada tahun 1919, ia diberi gelar dan dibayar sejumlah kecil uang untuk kuliah-kuliahnya.

Pada tahun 1922, Noether menjadi Privatdozent di Göttingen. Selama 11 tahun berikutnya, ia menggunakan metode aksiomatik untuk mengembangkan teori abstrak mengenai gelanggang dan ideal. Meskipun tidak mahir memberi kuliah, Noether adalah pengajar yang menginspirasi. Salah seorang dari banyak mahasiswanya adalah B. L. van der Waerden, penulis buku pertama yang membahas aljabar abstrak dari sudut pandang modern. Beberapa matematikawan lain yang dipengaruhi Noether atau bekerja erat dengannya ialah Alexandroff, Artin, Brauer, Courant, Hasse, Hopf, Pontryagin, von Neumann, dan Weyl. Salah satu puncak kariernya adalah undangan untuk berbicara di Kongres Matematikawan Internasional di Zurich pada tahun 1932. Terlepas dari segala pengakuan yang diterimanya dari para kolega, kemampuan Noether tidak pernah diakui sebagaimana mestinya semasa hidupnya. Ia tidak pernah dipromosikan menjadi profesor penuh oleh birokrasi akademik Prusia.

Pada tahun 1933, Noether, yang beretnis Yahudi, dilarang berpartisipasi dalam seluruh kegiatan akademik di Jerman. Ia beremigrasi ke Amerika Serikat, menerima jabatan di Bryn Mawr College, dan menjadi anggota Institute for Advanced Study di Princeton. Noether meninggal secara mendadak pada 14 April 1935. Setelah kematiannya, ilmuwan terkemuka seperti Albert Einstein menyampaikan pujian mengenangnya.

16.5 Penerapan pada Perancangan Perangkat Lunak

Teorema Sisa Cina merupakan hasil dalam teori bilangan elementer mengenai penyelesaian sistem kongruensi simultan. Matematikawan Cina Sun-tsï menulis tentang teorema ini pada abad pertama Masehi. Teorema ini memiliki beberapa konsekuensi menarik bagi perancangan perangkat lunak untuk prosesor paralel.

Lema 16.5.1 *Misalkan m dan n adalah bilangan bulat positif sedemikian sehingga* $\gcd(m, n) = 1$. *Maka, untuk $a, b \in \mathbb{Z}$, sistem*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

mempunyai solusi. Jika x_1 dan x_2 adalah dua solusi sistem tersebut, maka $x_1 \equiv x_2 \pmod{mn}$.

Bukti. Persamaan $x \equiv a \pmod{m}$ mempunyai solusi karena $a + km$ memenuhi persamaan tersebut untuk setiap $k \in \mathbb{Z}$. Kita harus menunjukkan bahwa terdapat bilangan bulat k_1 sedemikian sehingga

$$a + k_1 m \equiv b \pmod{n}.$$

Hal ini ekuivalen dengan menunjukkan bahwa

$$k_1 m \equiv (b - a) \pmod{n}$$

mempunyai solusi untuk k_1. Karena m dan n relatif prima, terdapat bilangan bulat s dan t sedemikian sehingga $ms + nt = 1$. Akibatnya,

$$(b - a)ms = (b - a) - (b - a)nt,$$

atau

$$[(b - a)s]m \equiv (b - a) \pmod{n}.$$

Sekarang ambil $k_1 = (b - a)s$.

Untuk menunjukkan bahwa sembarang dua solusi kongruen modulo mn, misalkan c_1 dan c_2 adalah dua solusi sistem tersebut. Artinya,

$$\begin{aligned} c_i &\equiv a \pmod{m} \\ c_i &\equiv b \pmod{n} \end{aligned}$$

untuk $i = 1, 2$. Maka

$$\begin{aligned} c_2 &\equiv c_1 \pmod{m} \\ c_2 &\equiv c_1 \pmod{n}. \end{aligned}$$

Oleh karena itu, m maupun n membagi $c_1 - c_2$. Akibatnya, $c_2 \equiv c_1 \pmod{mn}$. ■

Contoh 16.5.2 Mari kita selesaikan sistem

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5}. \end{aligned}$$

Dengan menggunakan algoritma Euklides, kita dapat menemukan bilangan bulat s dan t sedemikian sehingga $4s + 5t = 1$. Dua bilangan bulat yang memenuhi syarat itu adalah $s = 4$ dan $t = -3$. Akibatnya,

$$x = a + k_1 m = 3 + 4k_1 = 3 + 4[(5 - 4)4] = 19.$$

▲

Teorema 16.5.3 Teorema Sisa Cina. *Misalkan $n_1, n_2, \ldots, n_k$ adalah bilangan bulat positif sedemikian sehingga $\gcd(n_i, n_j) = 1$ untuk $i \neq j$. Maka, untuk sembarang bilangan bulat $a_1, \ldots, a_k$, sistem*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

mempunyai solusi. Selain itu, sembarang dua solusi sistem tersebut kongruen modulo $n_1 n_2 \cdots n_k$.

Bukti. Kita akan menggunakan induksi matematika pada banyaknya persamaan dalam sistem. Jika terdapat $k = 2$ persamaan, teorema ini benar berdasarkan Lema 16.5.1. Sekarang andaikan hasil tersebut benar untuk suatu sistem yang terdiri atas k persamaan atau kurang dan kita hendak mencari solusi dari

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_{k+1} \pmod{n_{k+1}}. \end{aligned}$$

Dengan meninjau k persamaan pertama, terdapat solusi yang tunggal modulo $n_1 \cdots n_k$, katakanlah a. Karena $n_1 \cdots n_k$ dan n_{k+1} relatif prima, sistem

$$\begin{aligned} x &\equiv a \pmod{n_1 \cdots n_k} \\ x &\equiv a_{k+1} \pmod{n_{k+1}} \end{aligned}$$

mempunyai solusi yang tunggal modulo $n_1 \ldots n_{k+1}$ berdasarkan lemma tersebut. ■

Contoh 16.5.4 Mari kita selesaikan sistem

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 1 \pmod{9} \\ x &\equiv 5 \pmod{7}. \end{aligned}$$

Dari Contoh 16.5.2 kita mengetahui bahwa 19 merupakan solusi dari dua kongruensi pertama dan setiap solusi lain dari sistem tersebut kongruen dengan 19 (mod 20). Jadi, kita dapat mereduksi sistem tersebut menjadi sistem tiga kongruensi:

$$\begin{aligned} x &\equiv 19 \pmod{20} \\ x &\equiv 1 \pmod{9} \end{aligned}$$

$$x \equiv 5 \pmod 7.$$

Dengan menyelesaikan dua persamaan berikutnya, kita dapat mereduksi sistem menjadi

$$\begin{aligned} x &\equiv 19 \pmod{180} \\ x &\equiv 5 \pmod 7. \end{aligned}$$

Dengan menyelesaikan sistem terakhir ini, kita memperoleh bahwa 19 merupakan solusi sistem yang tunggal modulo 1260. ▲

Salah satu penerapan menarik Teorema Sisa Cina dalam perancangan perangkat lunak komputer ialah bahwa teorema tersebut memungkinkan kita memecah perhitungan yang melibatkan bilangan bulat besar menjadi beberapa perhitungan yang lebih mudah ditangani. Karena ukuran cip prosesornya, komputer hanya dapat menangani perhitungan bilangan bulat sampai ukuran tertentu; cip prosesor tersebut biasanya berukuran 32 atau 64 bit. Sebagai contoh, bilangan bulat terbesar yang tersedia pada komputer dengan cip prosesor 64 bit adalah

$$2^{63} - 1 = 9{,}223{,}372{,}036{,}854{,}775{,}807.$$

Prosesor yang lebih besar, seperti prosesor 128 atau 256 bit, telah diusulkan atau sedang dikembangkan. Bahkan, cip prosesor 512 bit pernah dibicarakan. Bilangan bulat terbesar yang dapat disimpan oleh cip semacam itu adalah $2^{511} - 1$, yakni bilangan yang terdiri atas 154 digit. Namun, kita perlu menangani bilangan yang jauh lebih besar untuk memecahkan sistem enkripsi canggih.

Perangkat lunak khusus diperlukan untuk perhitungan yang melibatkan bilangan bulat lebih besar yang tidak dapat dijumlahkan secara langsung oleh mesin. Dengan menggunakan Teorema Sisa Cina, kita dapat memecah penjumlahan dan perkalian bilangan bulat besar menjadi perhitungan yang dapat ditangani komputer secara langsung. Hal ini sangat berguna pada komputer pemrosesan paralel yang mampu menjalankan beberapa program secara bersamaan.

Kebanyakan komputer memiliki satu unit pemrosesan pusat (CPU) yang memuat satu cip prosesor dan hanya dapat menjumlahkan dua bilangan pada satu waktu. Untuk menjumlahkan daftar yang berisi sepuluh bilangan, CPU harus melakukan sembilan penjumlahan secara berurutan. Namun, komputer pemrosesan paralel memiliki lebih dari satu CPU. Sebagai contoh, komputer dengan 10 CPU dapat melakukan 10 penjumlahan yang berbeda secara bersamaan. Jika kita dapat memecah bilangan bulat besar menjadi beberapa bagian dan mengirim setiap bagian ke CPU yang berbeda, dengan melakukan beberapa penjumlahan atau perkalian secara serentak pada bagian-bagian tersebut, kita dapat bekerja dengan bilangan bulat yang tidak dapat ditangani komputer secara utuh.

Contoh 16.5.5 Andaikan kita hendak mengalikan 2134 dengan 1531. Kita akan menggunakan bilangan bulat 95, 97, 98, dan 99 karena bilangan-bilangan tersebut saling relatif prima. Kita dapat memecah setiap bilangan bulat menjadi empat bagian:

$$\begin{aligned} 2134 &\equiv 44 \pmod{95} \\ 2134 &\equiv 0 \pmod{97} \\ 2134 &\equiv 76 \pmod{98} \\ 2134 &\equiv 55 \pmod{99} \end{aligned}$$

dan

$$\begin{aligned} 1531 &\equiv 11 \pmod{95} \\ 1531 &\equiv 76 \pmod{97} \\ 1531 &\equiv 61 \pmod{98} \\ 1531 &\equiv 46 \pmod{99}. \end{aligned}$$

Dengan mengalikan persamaan-persamaan yang bersesuaian, kita memperoleh

$$\begin{aligned} 2134 \cdot 1531 &\equiv 44 \cdot 11 \equiv 9 \pmod{95} \\ 2134 \cdot 1531 &\equiv 0 \cdot 76 \equiv 0 \pmod{97} \\ 2134 \cdot 1531 &\equiv 76 \cdot 61 \equiv 30 \pmod{98} \\ 2134 \cdot 1531 &\equiv 55 \cdot 46 \equiv 55 \pmod{99}. \end{aligned}$$

Jika komputer kita memiliki beberapa CPU, masing-masing dari keempat perhitungan ini dapat dikirim ke prosesor yang berbeda. Berdasarkan perhitungan di atas, kita mengetahui bahwa $2134 \cdot 1531$ merupakan solusi dari sistem

$$\begin{aligned} x &\equiv 9 \pmod{95} \\ x &\equiv 0 \pmod{97} \\ x &\equiv 30 \pmod{98} \\ x &\equiv 55 \pmod{99}. \end{aligned}$$

Teorema Sisa Cina menyatakan bahwa solusi-solusi sistem tersebut tunggal modulo $95 \cdot 97 \cdot 98 \cdot 99 = 89{,}403{,}930$. Dengan menyelesaikan sistem kongruensi ini untuk x, kita memperoleh $2134 \cdot 1531 = 3{,}267{,}154$.

Pengubahan perhitungan menjadi empat subperhitungan memerlukan sejumlah waktu komputasi. Selain itu, penyelesaian sistem kongruensi juga dapat memerlukan waktu yang cukup lama. Namun, jika kita perlu melakukan banyak perhitungan pada suatu himpunan bilangan tertentu, masuk akal untuk mengubah masalah seperti yang kita lakukan di atas dan menjalankan perhitungan yang diperlukan secara serentak. ▲

16.6 Pertanyaan Bacaan

1. Apa perbedaan mendasar antara grup dan gelanggang?

2. Berikan dua karakterisasi daerah integral.

3. Berikan dua contoh lapangan, satu tak hingga dan satu berhingga.

4. Siapakah Emmy Noether?

5. Bayangkan sebuah program komputer yang mungkin menggunakan Teorema Sisa Cina untuk mempercepat komputasi dengan bilangan bulat besar.

16.7 Latihan

1. Manakah di antara himpunan berikut yang merupakan gelanggang terhadap operasi penjumlahan dan perkalian biasa? Jika himpunan tersebut merupakan gelanggang, apakah himpunan itu juga merupakan lapangan?

(a) $7\mathbb{Z}$

(b) $\mathbb{Z}_{18}$

(c) $\mathbb{Q}(\sqrt{2}\,) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$

(d) $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\}$

(e) $\mathbb{Z}[\sqrt{3}\,] = \{a + b\sqrt{3} : a, b \in \mathbb{Z}\}$

(f) $R = \{a + b\sqrt[3]{3} : a, b \in \mathbb{Q}\}$

(g) $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \text{ dan } i^2 = -1\}$

(h) $\mathbb{Q}(\sqrt[3]{3}\,) = \{a + b\sqrt[3]{3} + c\sqrt[3]{9} : a, b, c \in \mathbb{Q}\}$

Petunjuk. (a) $7\mathbb{Z}$ merupakan gelanggang tetapi bukan lapangan; (c) $\mathbb{Q}(\sqrt{2}\,)$ merupakan lapangan; (f) R bukan gelanggang.

2. Misalkan R adalah gelanggang matriks 2×2 berbentuk

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},$$

dengan $a, b \in \mathbb{R}$. Tunjukkan bahwa meskipun R merupakan gelanggang yang tidak memiliki identitas, kita dapat menemukan subgelanggang S dari R yang memiliki identitas.

3. Daftarkan atau karakterisasikan semua unsur satuan dalam setiap gelanggang berikut.

(a) $\mathbb{Z}_{10}$

(b) $\mathbb{Z}_{12}$

(c) $\mathbb{Z}_7$

(d) $\mathbb{M}_2(\mathbb{Z})$, yaitu matriks 2×2 dengan entri dalam $\mathbb{Z}$

(e) $\mathbb{M}_2(\mathbb{Z}_2)$, yaitu matriks 2×2 dengan entri dalam $\mathbb{Z}_2$

Petunjuk. (a) $\{1, 3, 7, 9\}$; (c) $\{1, 2, 3, 4, 5, 6\}$; (e)

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \right\}.$$

4. Tentukan semua ideal dalam setiap gelanggang berikut. Manakah di antara ideal-ideal tersebut yang maksimal dan manakah yang prima?

(a) $\mathbb{Z}_{18}$

(b) $\mathbb{Z}_{25}$

(c) $\mathbb{M}_2(\mathbb{R})$, yaitu matriks 2×2 dengan entri dalam $\mathbb{R}$

(d) $\mathbb{M}_2(\mathbb{Z})$, yaitu matriks 2×2 dengan entri dalam $\mathbb{Z}$

(e) $\mathbb{Q}$

Petunjuk. (a) $\{0\}$, $\{0, 9\}$, $\{0, 6, 12\}$, $\{0, 3, 6, 9, 12, 15\}$, $\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$; (c) tidak ada ideal taktrivial.

5. Untuk setiap gelanggang R berikut beserta ideal I, berikan tabel penjumlahan dan tabel perkalian untuk R/I.

(a) $R = \mathbb{Z}$ dan $I = 6\mathbb{Z}$

(b) $R = \mathbb{Z}_{12}$ dan $I = \{0, 3, 6, 9\}$

6. Tentukan semua homomorfisma $\phi : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$.

7. Buktikan bahwa $\mathbb{R}$ tidak isomorfik dengan $\mathbb{C}$.

Petunjuk. Andaikan terdapat isomorfisma $\phi : \mathbb{C} \to \mathbb{R}$ dengan $\phi(i) = a$.

8. Buktikan atau sangkal: Gelanggang $\mathbb{Q}(\sqrt{2}\,) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ isomorfik dengan gelanggang $\mathbb{Q}(\sqrt{3}\,) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\}$.

Petunjuk. Salah. Andaikan terdapat isomorfisma $\phi : \mathbb{Q}(\sqrt{2}\,) \to \mathbb{Q}(\sqrt{3}\,)$ sedemikian sehingga $\phi(\sqrt{2}\,) = a$.

9. Berapakah karakteristik lapangan yang dibentuk oleh himpunan matriks

$$F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

dengan entri dalam $\mathbb{Z}_2$?

10. Definisikan pemetaan $\phi : \mathbb{C} \to \mathbb{M}_2(\mathbb{R})$ dengan

$$\phi(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Tunjukkan bahwa ϕ merupakan isomorfisma dari $\mathbb{C}$ ke citranya dalam $\mathbb{M}_2(\mathbb{R})$.

11. Buktikan bahwa bilangan bulat Gauss, $\mathbb{Z}[i]$, membentuk daerah integral.

12. Buktikan bahwa $\mathbb{Z}[\sqrt{3}\,i] = \{a + b\sqrt{3}\,i : a, b \in \mathbb{Z}\}$ merupakan daerah integral.

13. Selesaikan setiap sistem kongruensi berikut.

(a)
$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 6 \pmod{11} \end{aligned}$$

(b)
$$\begin{aligned} x &\equiv 3 \pmod 7 \\ x &\equiv 0 \pmod 8 \\ x &\equiv 5 \pmod{15} \end{aligned}$$

(c)
$$x \equiv 2 \pmod 4$$
$$\begin{aligned} x &\equiv 4 \pmod 7 \\ x &\equiv 7 \pmod 9 \\ x &\equiv 5 \pmod{11} \end{aligned}$$

(d)
$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 0 \pmod 8 \\ x &\equiv 1 \pmod{11} \\ x &\equiv 5 \pmod{13} \end{aligned}$$

Petunjuk. (a) $x \equiv 17 \pmod{55}$; (c) $x \equiv 214 \pmod{2772}$.

14. Gunakan metode komputasi paralel yang diuraikan dalam teks untuk menghitung $2234 + 4121$ dengan membagi perhitungan menjadi empat penjumlahan terpisah modulo 95, 97, 98, dan 99.

15. Jelaskan mengapa metode komputasi paralel yang diuraikan dalam teks gagal untuk $2134 \cdot 1531$ jika kita mencoba memecah perhitungan menjadi dua perhitungan yang lebih kecil modulo 98 dan 99.

16. Jika R merupakan lapangan, tunjukkan bahwa dua ideal satu-satunya dari R adalah $\{0\}$ dan R sendiri.

Petunjuk. Jika $I \neq \{0\}$, tunjukkan bahwa $1 \in I$.

17. Misalkan a adalah sembarang unsur dalam gelanggang R yang memiliki identitas. Tunjukkan bahwa $(-1)a = -a$.

18. Misalkan $\phi : R \to S$ adalah homomorfisma gelanggang. Buktikan setiap pernyataan berikut.

(a) Jika R merupakan gelanggang komutatif, maka $\phi(R)$ merupakan gelanggang komutatif.

(b) $\phi(0) = 0$.

(c) Misalkan 1_R dan 1_S masing-masing merupakan identitas untuk R dan S. Jika ϕ surjektif, maka $\phi(1_R) = 1_S$.

(d) Jika R merupakan lapangan dan $\phi(R) \neq 0$, maka $\phi(R)$ merupakan lapangan.

Petunjuk. (a) $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$.

19. Buktikan bahwa hukum asosiatif untuk perkalian dan hukum-hukum distributif berlaku dalam R/I.

20. Buktikan Teorema Isomorfisma Kedua untuk gelanggang: Misalkan I adalah subgelanggang dari gelanggang R dan J adalah ideal dalam R. Maka $I \cap J$ merupakan ideal dalam I dan

$$I/I \cap J \cong I + J/J.$$

21. Buktikan Teorema Isomorfisma Ketiga untuk gelanggang: Misalkan R adalah gelanggang dan I serta J adalah ideal-ideal dari R, dengan $J \subset I$. Maka

$$R/I \cong \frac{R/J}{I/J}.$$

22. Buktikan Teorema Korespondensi: Misalkan I adalah ideal dari gelanggang R. Maka $S \to S/I$ merupakan korespondensi satu-satu antara himpunan subgelanggang S yang memuat I dan himpunan subgelanggang dari R/I. Selain itu, ideal-ideal dari R berkorespondensi dengan ideal-ideal dari R/I.

23. Misalkan R adalah gelanggang dan S merupakan himpunan bagian dari R. Tunjukkan bahwa S merupakan subgelanggang dari R jika dan hanya jika setiap syarat berikut dipenuhi.

(a) $S \neq \emptyset$.

(b) $rs \in S$ untuk semua $r, s \in S$.

(c) $r - s \in S$ untuk semua $r, s \in S$.

24. Misalkan R adalah gelanggang dengan koleksi subgelanggang $\{R_\alpha\}$. Buktikan bahwa $\bigcap R_\alpha$ merupakan subgelanggang dari R. Berikan contoh untuk menunjukkan bahwa gabungan dua subgelanggang belum tentu merupakan subgelanggang.

25. Misalkan $\{I_\alpha\}_{\alpha \in A}$ adalah koleksi ideal dalam gelanggang R. Buktikan bahwa $\bigcap_{\alpha \in A} I_\alpha$ juga merupakan ideal dalam R. Berikan contoh untuk menunjukkan bahwa jika I_1 dan I_2 adalah ideal-ideal dalam R, maka $I_1 \cup I_2$ mungkin bukan ideal.

26. Misalkan R adalah daerah integral. Tunjukkan bahwa jika ideal satu-satunya dalam R adalah $\{0\}$ dan R sendiri, maka R harus merupakan lapangan.

Petunjuk. Misalkan $a \in R$ dengan $a \neq 0$. Maka ideal utama yang dibangun oleh a adalah R. Jadi, terdapat $b \in R$ sedemikian sehingga $ab = 1$.

27. Misalkan R adalah gelanggang komutatif. Unsur a dalam R disebut **nilpoten** jika $a^n = 0$ untuk suatu bilangan bulat positif n. Tunjukkan bahwa himpunan semua unsur nilpoten membentuk ideal dalam R.

28. Gelanggang R disebut **gelanggang Boolean** jika untuk setiap $a \in R$, $a^2 = a$. Tunjukkan bahwa setiap gelanggang Boolean merupakan gelanggang komutatif.

Petunjuk. Hitung $(a + b)^2$ dan $(-ab)^2$.

29. Misalkan R adalah gelanggang dengan $a^3 = a$ untuk semua $a \in R$. Buktikan bahwa R harus merupakan gelanggang komutatif.

30. Misalkan R adalah gelanggang dengan identitas 1_R dan S adalah subgelanggang dari R dengan identitas 1_S. Buktikan atau sangkal bahwa $1_R = 1_S$.

31. Jika kita tidak mensyaratkan identitas gelanggang berbeda dari 0, kita tidak akan memperoleh struktur matematika yang terlalu menarik. Misalkan R adalah gelanggang sedemikian sehingga $1 = 0$. Buktikan bahwa $R = \{0\}$.

32. Misalkan R adalah gelanggang. Definisikan **pusat** dari R sebagai

$$Z(R) = \{a \in R : ar = ra \text{ untuk semua } r \in R\}.$$

Buktikan bahwa $Z(R)$ merupakan subgelanggang komutatif dari R.

33. Misalkan p adalah bilangan prima. Buktikan bahwa

$$\mathbb{Z}_{(p)} = \{a/b : a, b \in \mathbb{Z} \text{ dan } \gcd(b, p) = 1\}$$

merupakan gelanggang. Gelanggang $\mathbb{Z}_{(p)}$ disebut **gelanggang bilangan bulat yang dilokalkan di** p.

Petunjuk. Misalkan $a/b, c/d \in \mathbb{Z}_{(p)}$. Maka $a/b + c/d = (ad + bc)/bd$ dan $(a/b) \cdot (c/d) = (ac)/(bd)$ keduanya berada dalam $\mathbb{Z}_{(p)}$, karena $\gcd(bd, p) = 1$.

34. Buktikan atau sangkal: Setiap daerah integral berhingga isomorfik dengan $\mathbb{Z}_p$.

35. Misalkan R adalah gelanggang dengan identitas.

(a) Misalkan u adalah unsur satuan dalam R. Definisikan pemetaan $i_u : R \to R$ dengan $r \mapsto uru^{-1}$. Buktikan bahwa i_u merupakan automorfisme dari R. Automorfisme R semacam ini disebut automorfisme dalam dari R. Nyatakan himpunan semua automorfisme dalam dari R dengan $\text{Inn}(R)$.

(b) Nyatakan himpunan semua automorfisme dari R dengan $\text{Aut}(R)$. Buktikan bahwa $\text{Inn}(R)$ merupakan subgrup normal dari $\text{Aut}(R)$.

(c) Misalkan $U(R)$ adalah grup unsur satuan dalam R. Buktikan bahwa pemetaan

$$\phi : U(R) \to \text{Inn}(R)$$

yang didefinisikan oleh $u \mapsto i_u$ merupakan homomorfisma. Tentukan kernel dari ϕ.

(d) Hitung $\mathrm{Aut}(\mathbb{Z})$, $\mathrm{Inn}(\mathbb{Z})$, dan $U(\mathbb{Z})$.

36. Misalkan R dan S adalah gelanggang sembarang. Tunjukkan bahwa hasil kali Cartesiusnya merupakan gelanggang jika kita mendefinisikan penjumlahan dan perkalian dalam $R \times S$ dengan

(a) $(r, s) + (r', s') = (r + r', s + s')$

(b) $(r, s)(r', s') = (rr', ss')$

37. Unsur x dalam suatu gelanggang disebut **idempoten** jika $x^2 = x$. Buktikan bahwa idempoten satu-satunya dalam daerah integral adalah 0 dan 1. Temukan gelanggang dengan suatu idempoten x yang tidak sama dengan 0 ataupun 1.

Petunjuk. Misalkan $x^2 = x$ dan $x \neq 0$. Karena R merupakan daerah integral, $x = 1$. Untuk menemukan idempoten taktrivial, carilah dalam $\mathbb{M}_2(\mathbb{R})$.

38. Misalkan $\gcd(a, n) = d$ dan $\gcd(b, d) \neq 1$. Buktikan bahwa $ax \equiv b \pmod{n}$ tidak mempunyai solusi.

39. **Teorema Sisa Cina untuk Gelanggang.** Misalkan R adalah gelanggang dan I serta J adalah ideal-ideal dalam R sedemikian sehingga $I + J = R$.

(a) Tunjukkan bahwa untuk sembarang r dan s dalam R, sistem persamaan

$$\begin{aligned} x &\equiv r \pmod{I} \\ x &\equiv s \pmod{J} \end{aligned}$$

mempunyai solusi.

(b) Selain itu, buktikan bahwa sembarang dua solusi sistem tersebut kongruen modulo $I \cap J$.

(c) Misalkan I dan J adalah ideal-ideal dalam gelanggang R sedemikian sehingga $I + J = R$. Tunjukkan bahwa terdapat isomorfisma gelanggang

$$R/(I \cap J) \cong R/I \times R/J.$$

16.8 Latihan Pemrograman

1. Tulislah program komputer yang menerapkan penjumlahan dan perkalian cepat dengan menggunakan Teorema Sisa Cina dan metode yang diuraikan dalam teks.

16.9 Referensi dan Bacaan yang Disarankan

[1] Anderson, F. W. and Fuller, K. R. *Rings and Categories of Modules*. 2nd ed. Springer, New York, 1992.

[2] Atiyah, M. F. and MacDonald, I. G. *Introduction to Commutative Algebra*. Westview Press, Boulder, CO, 1994.

[3] Herstein, I. N. *Noncommutative Rings*. Mathematical Association of America, Washington, DC, 1994.

[4] Kaplansky, I. *Commutative Rings*. Revised edition. University of Chicago Press, Chicago, 1974.

[5] Knuth, D. E. *The Art of Computer Programming: Semi-Numerical Algorithms*, vol. 2. 3rd ed. Addison-Wesley Professional, Boston, 1997.

[6] Lidl, R. and Pilz, G. *Applied Abstract Algebra*. 2nd ed. Springer, New York, 1998. Sumber yang baik untuk penerapan.

[7] Mackiw, G. *Applications of Abstract Algebra*. Wiley, New York, 1985.

[8] McCoy, N. H. *Rings and Ideals*. Carus Monograph Series, No. 8. Mathematical Association of America, Washington, DC, 1968.

[9] McCoy, N. H. *The Theory of Rings*. Chelsea, New York, 1972.

[10] Zariski, O. and Samuel, P. *Commutative Algebra*, vols. I and II. Springer, New York, 1975, 1960.

17

Polinomial

Kebanyakan orang sudah cukup mengenal polinomial ketika mulai mempelajari aljabar abstrak. Ketika kita menelaah ekspresi polinomial seperti

$$p(x) = x^3 - 3x + 2$$
$$q(x) = 3x^2 - 6x + 5,$$

kita telah memiliki gambaran yang cukup baik tentang makna $p(x) + q(x)$ dan $p(x)q(x)$. Kita cukup menjumlahkan dan mengalikan polinomial sebagai fungsi; yaitu,

$$\begin{aligned}(p+q)(x) &= p(x) + q(x) \\ &= (x^3 - 3x + 2) + (3x^2 - 6x + 5) \\ &= x^3 + 3x^2 - 9x + 7\end{aligned}$$

dan

$$\begin{aligned}(pq)(x) &= p(x)q(x) \\ &= (x^3 - 3x + 2)(3x^2 - 6x + 5) \\ &= 3x^5 - 6x^4 - 4x^3 + 24x^2 - 27x + 10.\end{aligned}$$

Mungkin tidak mengherankan bahwa polinomial membentuk suatu gelanggang. Dalam bab ini kita akan menekankan struktur aljabar polinomial dengan mempelajari gelanggang polinomial. Kita dapat membuktikan banyak hasil untuk gelanggang polinomial yang serupa dengan teorema-teorema yang telah kita buktikan untuk bilangan bulat. Padanan bilangan prima, algoritma pembagian, dan algoritma Euklides juga ada untuk polinomial.

17.1 Gelanggang Polinomial

Sepanjang bab ini kita akan mengasumsikan bahwa R adalah gelanggang komutatif dengan identitas. Setiap ekspresi berbentuk

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

dengan $a_i \in R$ dan $a_n \neq 0$, disebut **polinomial atas** R dengan **peubah tak tentu** x. Elemen-elemen $a_0, a_1, \ldots, a_n$ disebut **koefisien** dari f. Koefisien

a_n disebut **koefisien utama**. Suatu polinomial disebut **monik** jika koefisien utamanya adalah 1. Jika n adalah bilangan taknegatif terbesar yang memenuhi $a_n \neq 0$, kita mengatakan bahwa **derajat** dari f adalah n dan menulis $\deg f(x) = n$. Jika tidak ada n semacam itu—yakni, jika $f = 0$ adalah polinomial nol—maka derajat f didefinisikan sebagai $-\infty$. Kita akan menyatakan himpunan semua polinomial dengan koefisien di gelanggang R dengan $R[x]$. Dua polinomial sama tepat ketika koefisien-koefisien yang bersesuaian sama; yaitu, jika kita ambil

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$
$$q(x) = b_0 + b_1x + \cdots + b_mx^m,$$

maka $p(x) = q(x)$ jika dan hanya jika $a_i = b_i$ untuk semua $i \geq 0$.

Untuk menunjukkan bahwa himpunan semua polinomial membentuk suatu gelanggang, pertama-tama kita harus mendefinisikan penjumlahan dan perkalian. Kita mendefinisikan jumlah dua polinomial sebagai berikut. Misalkan

$$p(x) = a_0 + a_1x + \cdots + a_nx^n$$
$$q(x) = b_0 + b_1x + \cdots + b_mx^m.$$

Maka jumlah $p(x)$ dan $q(x)$ adalah

$$p(x) + q(x) = c_0 + c_1x + \cdots + c_kx^k,$$

dengan $c_i = a_i + b_i$ untuk setiap i. Kita mendefinisikan hasil kali $p(x)$ dan $q(x)$ sebagai

$$p(x)q(x) = c_0 + c_1x + \cdots + c_{m+n}x^{m+n},$$

dengan

$$c_i = \sum_{k=0}^{i} a_kb_{i-k} = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0$$

untuk setiap i. Perhatikan bahwa dalam setiap kasus beberapa koefisien mungkin bernilai nol.

Contoh 17.1.1 Misalkan

$$p(x) = 3 + 0x + 0x^2 + 2x^3 + 0x^4$$

dan

$$q(x) = 2 + 0x - x^2 + 0x^3 + 4x^4$$

adalah polinomial-polinomial di $\mathbb{Z}[x]$. Jika koefisien suatu suku dalam polinomial bernilai nol, biasanya kita cukup menghilangkan suku tersebut. Dalam kasus ini kita akan menulis $p(x) = 3 + 2x^3$ dan $q(x) = 2 - x^2 + 4x^4$. Jumlah kedua polinomial ini adalah

$$p(x) + q(x) = 5 - x^2 + 2x^3 + 4x^4.$$

Hasil kalinya,

$$p(x)q(x) = (3 + 2x^3)(2 - x^2 + 4x^4) = 6 - 3x^2 + 4x^3 + 12x^4 - 2x^5 + 8x^7,$$

dapat dihitung dengan menentukan setiap c_i dalam definisi atau cukup dengan mengalikan polinomial seperti yang biasa kita lakukan. ▲

Contoh 17.1.2 Misalkan

$$p(x) = 3 + 3x^3 \qquad \text{dan} \qquad q(x) = 4 + 4x^2 + 4x^4$$

adalah polinomial-polinomial di $\mathbb{Z}_{12}[x]$. Jumlah $p(x)$ dan $q(x)$ adalah $7+4x^2+3x^3+4x^4$. Hasil kali kedua polinomial tersebut adalah polinomial nol. Contoh ini menunjukkan bahwa kita tidak dapat mengharapkan $R[x]$ menjadi daerah integral jika R bukan daerah integral. ▲

Teorema 17.1.3 *Misalkan R gelanggang komutatif dengan identitas. Maka $R[x]$ adalah gelanggang komutatif dengan identitas.*

BUKTI. Tugas pertama kita adalah menunjukkan bahwa $R[x]$ merupakan grup abelian terhadap penjumlahan polinomial. Polinomial nol, $f(x) = 0$, adalah identitas aditif. Untuk suatu polinomial $p(x) = \sum_{i=0}^{n} a_i x^i$, invers $p(x)$ mudah diverifikasi sebagai $-p(x) = \sum_{i=0}^{n}(-a_i)x^i = -\sum_{i=0}^{n} a_i x^i$. Komutativitas dan asosiativitas langsung mengikuti dari definisi penjumlahan polinomial dan fakta bahwa penjumlahan di R bersifat komutatif sekaligus asosiatif.

Untuk menunjukkan bahwa perkalian polinomial bersifat asosiatif, misalkan

$$p(x) = \sum_{i=0}^{m} a_i x^i,$$
$$q(x) = \sum_{i=0}^{n} b_i x^i,$$
$$r(x) = \sum_{i=0}^{p} c_i x^i.$$

Maka

$$\begin{aligned}
[p(x)q(x)]r(x) &= \left[\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right)\right]\left(\sum_{i=0}^{p} c_i x^i\right) \\
&= \left[\sum_{i=0}^{m+n}\left(\sum_{j=0}^{i} a_j b_{i-j}\right)x^i\right]\left(\sum_{i=0}^{p} c_i x^i\right) \\
&= \sum_{i=0}^{m+n+p}\left[\sum_{j=0}^{i}\left(\sum_{k=0}^{j} a_k b_{j-k}\right)c_{i-j}\right]x^i \\
&= \sum_{i=0}^{m+n+p}\left(\sum_{j+k+l=i} a_j b_k c_l\right)x^i \\
&= \sum_{i=0}^{m+n+p}\left[\sum_{j=0}^{i} a_j\left(\sum_{k=0}^{i-j} b_k c_{i-j-k}\right)\right]x^i \\
&= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\sum_{i=0}^{n+p}\left(\sum_{j=0}^{i} b_j c_{i-j}\right)x^i\right] \\
&= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\left(\sum_{i=0}^{n} b_i x^i\right)\left(\sum_{i=0}^{p} c_i x^i\right)\right] \\
&= p(x)[q(x)r(x)]
\end{aligned}$$

Sifat komutatif dan distributif perkalian polinomial dibuktikan dengan cara serupa. Bukti sifat-sifat ini kita serahkan sebagai latihan. ■

Proposisi 17.1.4 *Misalkan $p(x)$ dan $q(x)$ polinomial-polinomial di $R[x]$, dengan R suatu daerah integral. Maka* $\deg p(x)+\deg q(x) = \deg(p(x)q(x))$. *Lebih lanjut, $R[x]$ adalah daerah integral.*

BUKTI. Misalkan kita memiliki dua polinomial taknol

$$p(x) = a_m x^m + \cdots + a_1 x + a_0$$

dan

$$q(x) = b_n x^n + \cdots + b_1 x + b_0$$

dengan $a_m \neq 0$ dan $b_n \neq 0$. Derajat $p(x)$ dan $q(x)$ masing-masing adalah m dan n. Suku utama $p(x)q(x)$ adalah $a_m b_n x^{m+n}$, yang tidak mungkin nol karena R merupakan daerah integral; jadi, derajat $p(x)q(x)$ adalah $m+n$, dan $p(x)q(x) \neq 0$. Karena $p(x) \neq 0$ dan $q(x) \neq 0$ mengakibatkan $p(x)q(x) \neq 0$, kita mengetahui bahwa $R[x]$ juga merupakan daerah integral. ■

Kita juga ingin mempertimbangkan polinomial dalam dua variabel atau lebih, seperti $x^2 - 3xy + 2y^3$. Misalkan R gelanggang dan kita diberikan dua peubah tak tentu x dan y. Tentu saja kita dapat membentuk gelanggang $(R[x])[y]$. Menunjukkan bahwa $(R[x])[y] \cong R([y])[x]$ tidak sulit, meskipun mungkin menjemukan. Kita akan mengidentifikasi kedua gelanggang ini melalui isomorfisma tersebut dan cukup menulis $R[x, y]$. Gelanggang $R[x, y]$ disebut **gelanggang polinomial dalam dua peubah tak tentu x dan y dengan koefisien di R.** Dengan cara serupa, kita dapat mendefinisikan **gelanggang polinomial dalam n peubah tak tentu dengan koefisien di R.** Kita akan menyatakan gelanggang ini dengan $R[x_1, x_2, \ldots, x_n]$.

Teorema 17.1.5 *Misalkan R gelanggang komutatif dengan identitas dan $\alpha \in R$. Maka kita memiliki homomorfisma gelanggang $\phi_\alpha : R[x] \to R$ yang didefinisikan oleh*

$$\phi_\alpha(p(x)) = p(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0,$$

dengan $p(x) = a_n x^n + \cdots + a_1 x + a_0$.

BUKTI. Misalkan $p(x) = \sum_{i=0}^{n} a_i x^i$ dan $q(x) = \sum_{i=0}^{m} b_i x^i$. Mudah ditunjukkan bahwa $\phi_\alpha(p(x) + q(x)) = \phi_\alpha(p(x)) + \phi_\alpha(q(x))$. Untuk menunjukkan bahwa perkalian dipertahankan oleh pemetaan ϕ_α, perhatikan bahwa

$$\begin{aligned}
\phi_\alpha(p(x))\phi_\alpha(q(x)) &= p(\alpha)q(\alpha) \\
&= \left(\sum_{i=0}^{n} a_i\alpha^i\right)\left(\sum_{i=0}^{m} b_i\alpha^i\right) \\
&= \sum_{i=0}^{m+n}\left(\sum_{k=0}^{i} a_k b_{i-k}\right)\alpha^i \\
&= \phi_\alpha(p(x)q(x)).
\end{aligned}$$

■

Pemetaan $\phi_\alpha : R[x] \to R$ disebut **homomorfisma evaluasi** di α.

17.2 Algoritma Pembagian

Ingat bahwa algoritma pembagian untuk bilangan bulat (Teorema 2.2.1) menyatakan bahwa jika a dan b bilangan bulat dengan $b > 0$, maka terdapat bilangan bulat tunggal q dan r sedemikian sehingga $a = bq + r$, dengan $0 \leq r < b$.

Algoritma untuk memperoleh q dan r hanyalah pembagian bersusun. Teorema serupa berlaku untuk polinomial. Algoritma pembagian untuk polinomial memiliki beberapa konsekuensi penting. Karena buktinya sangat mirip dengan bukti yang bersesuaian untuk bilangan bulat, ada baiknya kita meninjau kembali Teorema 2.2.1 pada tahap ini.

Teorema 17.2.1 Algoritma Pembagian. *Misalkan $f(x)$ dan $g(x)$ polinomial-polinomial di $F[x]$, dengan F suatu lapangan dan $g(x)$ polinomial taknol. Maka terdapat polinomial tunggal $q(x), r(x) \in F[x]$ sedemikian sehingga*

$$f(x) = g(x)q(x) + r(x),$$

dengan $\deg r(x) < \deg g(x)$ atau $r(x)$ merupakan polinomial nol.

Bukti. Pertama-tama kita akan meninjau keberadaan $q(x)$ dan $r(x)$. Jika $f(x)$ adalah polinomial nol, maka

$$0 = 0 \cdot g(x) + 0;$$

jadi, q dan r juga harus merupakan polinomial nol. Sekarang misalkan $f(x)$ bukan polinomial nol serta $\deg f(x) = n$ dan $\deg g(x) = m$. Jika $m > n$, kita dapat mengambil $q(x) = 0$ dan $r(x) = f(x)$. Jadi, kita boleh mengasumsikan bahwa $m \leq n$ dan melanjutkan dengan induksi pada n. Jika

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \\ g(x) &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \end{aligned}$$

maka polinomial

$$f'(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$$

berderajat kurang dari n atau merupakan polinomial nol. Berdasarkan induksi, terdapat polinomial $q'(x)$ dan $r(x)$ sedemikian sehingga

$$f'(x) = q'(x)g(x) + r(x),$$

dengan $r(x) = 0$ atau derajat $r(x)$ kurang dari derajat $g(x)$. Sekarang ambil

$$q(x) = q'(x) + \frac{a_n}{b_m} x^{n-m}.$$

Maka

$$f(x) = g(x)q(x) + r(x),$$

dengan $r(x)$ polinomial nol atau $\deg r(x) < \deg g(x)$.

Untuk menunjukkan bahwa $q(x)$ dan $r(x)$ tunggal, misalkan terdapat dua polinomial lain $q_1(x)$ dan $r_1(x)$ sedemikian sehingga $f(x) = g(x)q_1(x) + r_1(x)$ dengan $\deg r_1(x) < \deg g(x)$ atau $r_1(x) = 0$, sehingga

$$f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x),$$

dan

$$g(x)[q(x) - q_1(x)] = r_1(x) - r(x).$$

Jika $q(x) - q_1(x)$ bukan polinomial nol, maka

$$\deg(g(x)[q(x) - q_1(x)]) = \deg(r_1(x) - r(x)) \geq \deg g(x).$$

Akan tetapi, derajat $r(x)$ dan $r_1(x)$ keduanya lebih kecil secara tegas daripada derajat $g(x)$; oleh karena itu, $r(x) = r_1(x)$ dan $q(x) = q_1(x)$. ■

Contoh 17.2.2 Algoritma pembagian sekadar memformalkan pembagian bersusun polinomial, suatu tugas yang telah kita kenal sejak sekolah menengah. Sebagai contoh, misalkan kita membagi $x^3 - x^2 + 2x - 3$ dengan $x - 2$.

$$\begin{array}{rrr|rcrcrcr} & & & x^2 & + & x & + & 4 & & \\ \hline x & - & 2 & x^3 & - & x^2 & + & 2x & - & 3 \\ & & & x^3 & - & 2x^2 & & & & \\ \hline & & & & & x^2 & + & 2x & - & 3 \\ & & & & & x^2 & - & 2x & & \\ \hline & & & & & & & 4x & - & 3 \\ & & & & & & & 4x & - & 8 \\ \hline & & & & & & & & & 5 \end{array}$$

Jadi, $x^3 - x^2 + 2x - 3 = (x - 2)(x^2 + x + 4) + 5$. ▲

Misalkan $p(x)$ suatu polinomial di $F[x]$ dan $\alpha \in F$. Kita mengatakan bahwa α merupakan **nol** atau **akar** dari $p(x)$ jika $p(x)$ berada dalam kernel homomorfisma evaluasi ϕ_α. Pernyataan ini sebenarnya hanya mengatakan bahwa α adalah nol dari $p(x)$ jika $p(\alpha) = 0$.

Korolari 17.2.3 *Misalkan F suatu lapangan. Elemen $\alpha \in F$ merupakan nol dari $p(x) \in F[x]$ jika dan hanya jika $x - \alpha$ merupakan faktor dari $p(x)$ di $F[x]$.*

BUKTI. Misalkan $\alpha \in F$ dan $p(\alpha) = 0$. Berdasarkan algoritma pembagian, terdapat polinomial $q(x)$ dan $r(x)$ sedemikian sehingga

$$p(x) = (x - \alpha)q(x) + r(x)$$

dan derajat $r(x)$ harus kurang dari derajat $x - \alpha$. Karena derajat $r(x)$ kurang dari 1, $r(x) = a$ untuk suatu $a \in F$; oleh karena itu,

$$p(x) = (x - \alpha)q(x) + a.$$

Namun,

$$0 = p(\alpha) = 0 \cdot q(\alpha) + a = a;$$

akibatnya, $p(x) = (x - \alpha)q(x)$, dan $x - \alpha$ merupakan faktor dari $p(x)$.

Sebaliknya, misalkan $x - \alpha$ merupakan faktor dari $p(x)$; katakanlah $p(x) = (x - \alpha)q(x)$. Maka $p(\alpha) = 0 \cdot q(\alpha) = 0$. ■

Korolari 17.2.4 *Misalkan F suatu lapangan. Polinomial taknol $p(x)$ berderajat n di $F[x]$ dapat memiliki paling banyak n nol yang berbeda di F.*

BUKTI. Kita akan menggunakan induksi pada derajat $p(x)$. Jika $\deg p(x) = 0$, maka $p(x)$ merupakan polinomial konstan dan tidak memiliki nol. Misalkan $\deg p(x) = 1$. Maka $p(x) = ax + b$ untuk suatu a dan b di F. Jika α_1 dan α_2 merupakan nol dari $p(x)$, maka $a\alpha_1 + b = a\alpha_2 + b$, sehingga $\alpha_1 = \alpha_2$.

Sekarang asumsikan bahwa $\deg p(x) > 1$. Jika $p(x)$ tidak memiliki nol di F, pembuktian selesai. Sebaliknya, jika α merupakan nol dari $p(x)$, maka $p(x) = (x - \alpha)q(x)$ untuk suatu $q(x) \in F[x]$ berdasarkan Korolari 17.2.3. Derajat $q(x)$ adalah $n - 1$ berdasarkan Proposisi 17.1.4. Misalkan β suatu nol lain dari $p(x)$ yang berbeda dari α. Maka $p(\beta) = (\beta - \alpha)q(\beta) = 0$. Karena $\alpha \neq \beta$ dan F merupakan lapangan, $q(\beta) = 0$. Berdasarkan hipotesis induksi, $q(x)$ dapat memiliki paling banyak $n - 1$ nol di F yang berbeda dari α. Oleh karena itu, $p(x)$ memiliki paling banyak n nol yang berbeda di F. ■

Misalkan F suatu lapangan. Polinomial monik $d(x)$ merupakan **faktor persekutuan terbesar** (FPB) dari polinomial $p(x), q(x) \in F[x]$ jika $d(x)$ membagi habis $p(x)$ dan $q(x)$; dan, untuk setiap polinomial lain $d'(x)$ yang

membagi $p(x)$ maupun $q(x)$, berlaku $d'(x) \mid d(x)$. Kita menulis $d(x) = \gcd(p(x), q(x))$. Dua polinomial $p(x)$ dan $q(x)$ disebut **relatif prima** jika $\gcd(p(x), q(x)) = 1$.

Proposisi 17.2.5 *Misalkan F suatu lapangan dan $d(x)$ merupakan faktor persekutuan terbesar dari dua polinomial $p(x)$ dan $q(x)$ di $F[x]$. Maka terdapat polinomial $r(x)$ dan $s(x)$ sedemikian sehingga*

$$d(x) = r(x)p(x) + s(x)q(x).$$

Lebih lanjut, faktor persekutuan terbesar dari dua polinomial bersifat tunggal.

Bukti. Misalkan $d(x)$ polinomial monik berderajat terkecil dalam himpunan

$$S = \{f(x)p(x) + g(x)q(x) : f(x), g(x) \in F[x]\}.$$

Kita dapat menulis $d(x) = r(x)p(x) + s(x)q(x)$ untuk dua polinomial $r(x)$ dan $s(x)$ di $F[x]$. Kita perlu menunjukkan bahwa $d(x)$ membagi $p(x)$ dan $q(x)$. Pertama-tama kita akan menunjukkan bahwa $d(x)$ membagi $p(x)$. Berdasarkan algoritma pembagian, terdapat polinomial $a(x)$ dan $b(x)$ sedemikian sehingga $p(x) = a(x)d(x) + b(x)$, dengan $b(x)$ merupakan polinomial nol atau $\deg b(x) < \deg d(x)$. Oleh karena itu,

$$\begin{aligned} b(x) &= p(x) - a(x)d(x) \\ &= p(x) - a(x)(r(x)p(x) + s(x)q(x)) \\ &= p(x) - a(x)r(x)p(x) - a(x)s(x)q(x) \\ &= p(x)(1 - a(x)r(x)) + q(x)(-a(x)s(x)) \end{aligned}$$

merupakan kombinasi linear dari $p(x)$ dan $q(x)$, sehingga harus berada di S. Akan tetapi, $b(x)$ harus merupakan polinomial nol karena $d(x)$ dipilih berderajat terkecil; akibatnya, $d(x)$ membagi $p(x)$. Argumen simetris menunjukkan bahwa $d(x)$ juga harus membagi $q(x)$; jadi, $d(x)$ merupakan faktor persekutuan dari $p(x)$ dan $q(x)$.

Untuk menunjukkan bahwa $d(x)$ merupakan faktor persekutuan terbesar dari $p(x)$ dan $q(x)$, misalkan $d'(x)$ faktor persekutuan lain dari $p(x)$ dan $q(x)$. Kita akan menunjukkan bahwa $d'(x) \mid d(x)$. Karena $d'(x)$ merupakan faktor persekutuan dari $p(x)$ dan $q(x)$, terdapat polinomial $u(x)$ dan $v(x)$ sedemikian sehingga $p(x) = u(x)d'(x)$ dan $q(x) = v(x)d'(x)$. Oleh karena itu,

$$\begin{aligned} d(x) &= r(x)p(x) + s(x)q(x) \\ &= r(x)u(x)d'(x) + s(x)v(x)d'(x) \\ &= d'(x)[r(x)u(x) + s(x)v(x)]. \end{aligned}$$

Karena $d'(x) \mid d(x)$, $d(x)$ merupakan faktor persekutuan terbesar dari $p(x)$ dan $q(x)$.

Terakhir, kita harus menunjukkan bahwa faktor persekutuan terbesar dari $p(x)$ dan $q(x)$ bersifat tunggal. Misalkan $d'(x)$ faktor persekutuan terbesar lain dari $p(x)$ dan $q(x)$. Kita baru saja menunjukkan bahwa terdapat polinomial $u(x)$ dan $v(x)$ di $F[x]$ sedemikian sehingga $d(x) = d'(x)[r(x)u(x) + s(x)v(x)]$. Karena

$$\deg d(x) = \deg d'(x) + \deg[r(x)u(x) + s(x)v(x)]$$

dan $d(x)$ serta $d'(x)$ keduanya merupakan faktor persekutuan terbesar, $\deg d(x) = \deg d'(x)$. Karena $d(x)$ dan $d'(x)$ keduanya polinomial monik berderajat sama, haruslah $d(x) = d'(x)$. ■

Perhatikan kemiripan antara bukti Proposisi 17.2.5 dan bukti Teorema 2.2.2.

17.3 Polinomial Tak Tereduksi

Polinomial takkonstan $f(x) \in F[x]$ disebut **tak tereduksi** atas lapangan F jika $f(x)$ tidak dapat dinyatakan sebagai hasil kali dua polinomial $g(x)$ dan $h(x)$ di $F[x]$, dengan derajat $g(x)$ dan $h(x)$ keduanya lebih kecil daripada derajat $f(x)$. Polinomial tak tereduksi berperan sebagai "bilangan prima" dalam gelanggang polinomial.

Contoh 17.3.1 Polinomial $x^2 - 2 \in \mathbb{Q}[x]$ tak tereduksi karena tidak dapat difaktorkan lebih lanjut atas bilangan rasional. Demikian pula, $x^2 + 1$ tak tereduksi atas bilangan real. ▲

Contoh 17.3.2 Polinomial $p(x) = x^3 + x^2 + 2$ tak tereduksi atas $\mathbb{Z}_3[x]$. Misalkan polinomial ini tereduksi atas $\mathbb{Z}_3[x]$. Berdasarkan algoritma pembagian, harus ada faktor berbentuk $x - a$, dengan a suatu elemen di $\mathbb{Z}_3[x]$. Dengan demikian, harus berlaku $p(a) = 0$. Akan tetapi,

$$\begin{aligned} p(0) &= 2 \\ p(1) &= 1 \\ p(2) &= 2. \end{aligned}$$

Oleh karena itu, $p(x)$ tidak memiliki nol di $\mathbb{Z}_3$ dan harus tak tereduksi. ▲

Lema 17.3.3 *Misalkan $p(x) \in \mathbb{Q}[x]$. Maka*

$$p(x) = \frac{r}{s}(a_0 + a_1 x + \cdots + a_n x^n),$$

dengan $r, s, a_0, \ldots, a_n$ bilangan bulat, setiap a_i relatif prima secara bersama, serta r dan s relatif prima.

Bukti. Misalkan

$$p(x) = \frac{b_0}{c_0} + \frac{b_1}{c_1}x + \cdots + \frac{b_n}{c_n}x^n,$$

dengan setiap b_i dan c_i bilangan bulat. Kita dapat menulis ulang $p(x)$ sebagai

$$p(x) = \frac{1}{c_0 \cdots c_n}(d_0 + d_1 x + \cdots + d_n x^n),$$

dengan $d_0, \ldots, d_n$ bilangan bulat. Misalkan d faktor persekutuan terbesar dari $d_0, \ldots, d_n$. Maka

$$p(x) = \frac{d}{c_0 \cdots c_n}(a_0 + a_1 x + \cdots + a_n x^n),$$

dengan $d_i = da_i$ dan setiap a_i relatif prima secara bersama. Setelah menyederhanakan $d/(c_0 \cdots c_n)$ ke bentuk paling sederhana, kita dapat menulis

$$p(x) = \frac{r}{s}(a_0 + a_1 x + \cdots + a_n x^n),$$

dengan $\gcd(r, s) = 1$. ■

Teorema 17.3.4 Lema Gauss. *Misalkan $p(x) \in \mathbb{Z}[x]$ polinomial monik sedemikian sehingga $p(x)$ terfaktor sebagai hasil kali dua polinomial $\alpha(x)$ dan*

$\beta(x)$ di $\mathbb{Q}[x]$, dengan derajat $\alpha(x)$ dan $\beta(x)$ keduanya kurang dari derajat $p(x)$. Maka $p(x) = a(x)b(x)$, dengan $a(x)$ dan $b(x)$ polinomial monik di $\mathbb{Z}[x]$ yang memenuhi $\deg \alpha(x) = \deg a(x)$ dan $\deg \beta(x) = \deg b(x)$.

BUKTI. Berdasarkan Lema 17.3.3, kita dapat mengasumsikan bahwa

$$\alpha(x) = \frac{c_1}{d_1}(a_0 + a_1x + \cdots + a_mx^m) = \frac{c_1}{d_1}\alpha_1(x)$$
$$\beta(x) = \frac{c_2}{d_2}(b_0 + b_1x + \cdots + b_nx^n) = \frac{c_2}{d_2}\beta_1(x),$$

dengan setiap a_i relatif prima secara bersama dan setiap b_i relatif prima secara bersama. Akibatnya,

$$p(x) = \alpha(x)\beta(x) = \frac{c_1c_2}{d_1d_2}\alpha_1(x)\beta_1(x) = \frac{c}{d}\alpha_1(x)\beta_1(x),$$

dengan c/d hasil kali c_1/d_1 dan c_2/d_2 yang dinyatakan dalam bentuk paling sederhana. Jadi, $dp(x) = c\alpha_1(x)\beta_1(x)$.

Jika $d = 1$, maka $ca_mb_n = 1$ karena $p(x)$ polinomial monik. Jadi, $c = 1$ atau $c = -1$. Jika $c = 1$, maka $a_m = b_n = 1$ atau $a_m = b_n = -1$. Dalam kasus pertama, $p(x) = \alpha_1(x)\beta_1(x)$, dengan $\alpha_1(x)$ dan $\beta_1(x)$ polinomial monik yang memenuhi $\deg \alpha(x) = \deg \alpha_1(x)$ dan $\deg \beta(x) = \deg \beta_1(x)$. Dalam kasus kedua, $a(x) = -\alpha_1(x)$ dan $b(x) = -\beta_1(x)$ merupakan polinomial monik yang tepat karena $p(x) = (-\alpha_1(x))(-\beta_1(x)) = a(x)b(x)$. Kasus $c = -1$ dapat ditangani dengan cara serupa.

Sekarang misalkan $d \neq 1$. Karena $\gcd(c, d) = 1$, terdapat bilangan prima p sedemikian sehingga $p \mid d$ dan $p \nmid c$. Selain itu, karena koefisien-koefisien $\alpha_1(x)$ relatif prima secara bersama, terdapat koefisien a_i sedemikian sehingga $p \nmid a_i$. Demikian pula, terdapat koefisien b_j dari $\beta_1(x)$ sedemikian sehingga $p \nmid b_j$. Misalkan $\alpha_1'(x)$ dan $\beta_1'(x)$ adalah polinomial di $\mathbb{Z}_p[x]$ yang diperoleh dengan mereduksi koefisien $\alpha_1(x)$ dan $\beta_1(x)$ modulo p. Karena $p \mid d$, $\alpha_1'(x)\beta_1'(x) = 0$ di $\mathbb{Z}_p[x]$. Namun, hal ini mustahil karena $\alpha_1'(x)$ maupun $\beta_1'(x)$ bukan polinomial nol dan $\mathbb{Z}_p[x]$ merupakan daerah integral. Oleh karena itu, $d = 1$ dan teorema terbukti. ■

Korolari 17.3.5 *Misalkan $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ polinomial dengan koefisien di $\mathbb{Z}$ dan $a_0 \neq 0$. Jika $p(x)$ memiliki nol di $\mathbb{Q}$, maka $p(x)$ juga memiliki nol α di $\mathbb{Z}$. Lebih lanjut, α membagi a_0.*

BUKTI. Misalkan $p(x)$ memiliki nol $a \in \mathbb{Q}$. Maka $p(x)$ harus memiliki faktor linear $x - a$. Berdasarkan Lema Gauss, $p(x)$ memiliki faktorisasi dengan faktor linear di $\mathbb{Z}[x]$. Jadi, untuk suatu $\alpha \in \mathbb{Z}$

$$p(x) = (x - \alpha)(x^{n-1} + \cdots - a_0/\alpha).$$

Dengan demikian, $a_0/\alpha \in \mathbb{Z}$ dan karenanya $\alpha \mid a_0$. ■

Contoh 17.3.6 Misalkan $p(x) = x^4 - 2x^3 + x + 1$. Kita akan menunjukkan bahwa $p(x)$ tak tereduksi atas $\mathbb{Q}[x]$. Asumsikan bahwa $p(x)$ tereduksi. Maka $p(x)$ memiliki faktor linear, katakanlah $p(x) = (x - \alpha)q(x)$, dengan $q(x)$ polinomial berderajat tiga, atau $p(x)$ memiliki dua faktor kuadratik.

Jika $p(x)$ memiliki faktor linear di $\mathbb{Q}[x]$, maka polinomial itu memiliki nol di $\mathbb{Z}$. Berdasarkan Korolari 17.3.5, setiap nol harus membagi 1 dan karenanya harus berupa ± 1; akan tetapi, $p(1) = 1$ dan $p(-1) = 3$. Akibatnya, kita telah menyingkirkan kemungkinan bahwa $p(x)$ memiliki faktor linear.

Oleh karena itu, jika $p(x)$ tereduksi, polinomial itu harus terfaktor menjadi dua polinomial kuadratik, katakanlah

$$\begin{aligned} p(x) &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd, \end{aligned}$$

dengan setiap faktor berada di $\mathbb{Z}[x]$ berdasarkan Lema Gauss. Jadi,

$$\begin{aligned} a + c &= -2 \\ ac + b + d &= 0 \\ ad + bc &= 1 \\ bd &= 1. \end{aligned}$$

Karena $bd = 1$, maka $b = d = 1$ atau $b = d = -1$. Dalam kedua kasus, $b = d$, sehingga

$$ad + bc = b(a + c) = 1.$$

Karena $a + c = -2$, kita mengetahui bahwa $-2b = 1$. Hal ini mustahil karena b bilangan bulat. Oleh karena itu, $p(x)$ harus tak tereduksi atas $\mathbb{Q}$. ▲

Teorema 17.3.7 Kriteria Eisenstein. *Misalkan p bilangan prima dan*

$$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x].$$

Jika $p \mid a_i$ untuk $i = 0, 1, \ldots, n-1$, tetapi $p \nmid a_n$ dan $p^2 \nmid a_0$, maka $f(x)$ tak tereduksi atas $\mathbb{Q}$.

Bukti. Berdasarkan Lema Gauss (lihat Teorema 17.3.7 dan Lema 18.2.19), kita hanya perlu menunjukkan bahwa $f(x)$ tidak terfaktor menjadi polinomial-polinomial berderajat lebih rendah di $\mathbb{Z}[x]$. Misalkan

$$f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$$

merupakan suatu faktorisasi di $\mathbb{Z}[x]$, dengan b_r dan c_s taknol serta $r, s < n$. Karena p^2 tidak membagi $a_0 = b_0 c_0$, salah satu dari b_0 atau c_0 tidak habis dibagi p. Misalkan $p \nmid b_0$ dan $p \mid c_0$. Karena $p \nmid a_n$ dan $a_n = b_r c_s$, baik b_r maupun c_s tidak habis dibagi p. Misalkan m nilai terkecil dari k yang memenuhi $p \nmid c_k$. Maka

$$a_m = b_0 c_m + b_1 c_{m-1} + \cdots + b_m c_0$$

tidak habis dibagi p, karena setiap suku di ruas kanan persamaan habis dibagi p, kecuali $b_0 c_m$. Oleh karena itu, $m = n$ karena a_i habis dibagi p untuk $m < n$. Jadi, $f(x)$ tidak dapat difaktorkan menjadi polinomial-polinomial berderajat lebih rendah dan karenanya harus tak tereduksi. ■

Contoh 17.3.8 Polinomial

$$f(x) = 16x^5 - 9x^4 + 3x^2 + 6x - 21$$

mudah dilihat tak tereduksi atas $\mathbb{Q}$ berdasarkan Kriteria Eisenstein jika kita mengambil $p = 3$. ▲

Kriteria Eisenstein lebih berguna untuk membangun polinomial tak tereduksi berderajat tertentu atas $\mathbb{Q}$ daripada untuk menentukan ketaktereduksian sembarang polinomial di $\mathbb{Q}[x]$: untuk sembarang polinomial yang diberikan, kecil kemungkinan kita dapat menerapkan Kriteria Eisenstein. Nilai penting Teorema 17.3.7 adalah bahwa kini kita memiliki metode mudah untuk meng-

hasilkan polinomial tak tereduksi dengan derajat berapa pun.

17.3.1 Ideal dalam $F[x]$

Misalkan F suatu lapangan. Ingat bahwa ideal utama di $F[x]$ adalah ideal $\langle p(x)\rangle$ yang dibangkitkan oleh suatu polinomial $p(x)$; yaitu,

$$\langle p(x)\rangle = \{p(x)q(x) : q(x) \in F[x]\}.$$

Contoh 17.3.9 Polinomial x^2 di $F[x]$ membangkitkan ideal $\langle x^2\rangle$ yang terdiri atas semua polinomial tanpa suku konstan maupun suku berderajat 1. ▲

Teorema 17.3.10 *Jika F suatu lapangan, maka setiap ideal di $F[x]$ merupakan ideal utama.*

BUKTI. Misalkan I suatu ideal dari $F[x]$. Jika I adalah ideal nol, teorema ini jelas benar. Misalkan I ideal taktrivial di $F[x]$, dan ambil elemen taknol $p(x) \in I$ dengan derajat minimum. Jika $\deg p(x) = 0$, maka $p(x)$ merupakan konstanta taknol dan 1 harus berada di I. Karena 1 membangkitkan seluruh $F[x]$, $\langle 1\rangle = I = F[x]$ dan I sekali lagi merupakan ideal utama.

Sekarang asumsikan bahwa $\deg p(x) \geq 1$ dan misalkan $f(x)$ sembarang elemen di I. Berdasarkan algoritma pembagian, terdapat $q(x)$ dan $r(x)$ di $F[x]$ sedemikian sehingga $f(x) = p(x)q(x) + r(x)$ dan $\deg r(x) < \deg p(x)$. Karena $f(x), p(x) \in I$ dan I suatu ideal, $r(x) = f(x) - p(x)q(x)$ juga berada di I. Akan tetapi, karena kita memilih $p(x)$ berderajat minimum, $r(x)$ harus merupakan polinomial nol. Karena kita dapat menulis setiap elemen $f(x)$ di I sebagai $p(x)q(x)$ untuk suatu $q(x) \in F[x]$, haruslah $I = \langle p(x)\rangle$. ■

Contoh 17.3.11 Tidak setiap ideal dalam gelanggang $F[x, y]$ merupakan ideal utama. Tinjau ideal dari $F[x, y]$ yang dibangkitkan oleh polinomial x dan y. Ideal ini terdiri atas semua polinomial di $F[x, y]$ tanpa suku konstan. Karena x dan y keduanya berada dalam ideal tersebut, tidak ada satu polinomial pun yang dapat membangkitkan seluruh ideal. ▲

Teorema 17.3.12 *Misalkan F suatu lapangan dan $p(x) \in F[x]$. Maka ideal yang dibangkitkan oleh $p(x)$ maksimal jika dan hanya jika $p(x)$ tak tereduksi.*

BUKTI. Misalkan $p(x)$ membangkitkan ideal maksimal dari $F[x]$. Maka $\langle p(x)\rangle$ juga merupakan ideal prima dari $F[x]$. Karena ideal maksimal harus termuat secara sejati di dalam $F[x]$, $p(x)$ tidak mungkin merupakan polinomial konstan. Asumsikan bahwa $p(x)$ terfaktor menjadi dua polinomial berderajat lebih kecil, katakanlah $p(x) = f(x)g(x)$. Karena $\langle p(x)\rangle$ merupakan ideal prima, salah satu faktor ini, katakanlah $f(x)$, berada di $\langle p(x)\rangle$ dan karenanya merupakan kelipatan $p(x)$. Namun, hal ini akan mengakibatkan $\langle p(x)\rangle \subset \langle f(x)\rangle$, yang mustahil karena $\langle p(x)\rangle$ maksimal.

Sebaliknya, misalkan $p(x)$ tak tereduksi atas $F[x]$. Misalkan I suatu ideal di $F[x]$ yang memuat $\langle p(x)\rangle$. Berdasarkan Teorema 17.3.10, I merupakan ideal utama; jadi, $I = \langle f(x)\rangle$ untuk suatu $f(x) \in F[x]$. Karena $p(x) \in I$, haruslah $p(x) = f(x)g(x)$ untuk suatu $g(x) \in F[x]$. Akan tetapi, $p(x)$ tak tereduksi; jadi, $f(x)$ atau $g(x)$ merupakan polinomial konstan. Jika $f(x)$ konstan, maka $I = F[x]$ dan pembuktian selesai. Jika $g(x)$ konstan, maka $f(x)$ merupakan kelipatan konstan dari I dan $I = \langle p(x)\rangle$. Dengan demikian, tidak ada ideal sejati dari $F[x]$ yang secara sejati memuat $\langle p(x)\rangle$. ■

Catatan Sejarah

Sepanjang sejarah, penyelesaian persamaan polinomial merupakan masalah yang menantang. Bangsa Babilonia mengetahui cara menyelesaikan persa-

maan $ax^2 + bx + c = 0$. Omar Khayyam (1048–1131) merancang metode untuk menyelesaikan persamaan kubik dengan menggunakan konstruksi geometri dan irisan kerucut. Penyelesaian aljabar untuk persamaan kubik umum $ax^3 + bx^2 + cx + d = 0$ baru ditemukan pada abad keenam belas. Seorang matematikawan Italia, Luca Pacioli (ca. 1445–1509), menulis dalam *Summa de Arithmetica* bahwa persamaan kubik mustahil diselesaikan. Pernyataan ini diterima sebagai tantangan oleh komunitas matematika lainnya.

Scipione del Ferro (1465–1526), dari Universitas Bologna, menyelesaikan "persamaan kubik tereduksi,"

$$ax^3 + cx + d = 0.$$

Ia merahasiakan mutlak penyelesaiannya. Hal ini mungkin tampak mengejutkan pada masa kini, ketika para matematikawan biasanya sangat ingin menerbitkan hasil mereka, tetapi pada zaman Renaisans Italia kerahasiaan merupakan hal yang lazim. Jabatan akademik tidak mudah diperoleh dan bergantung pada kemampuan untuk menang dalam kompetisi publik. Tantangan semacam itu dapat diajukan kapan saja. Akibatnya, setiap penemuan baru yang besar menjadi senjata berharga dalam kompetisi tersebut. Jika seorang lawan menyajikan daftar masalah untuk diselesaikan, del Ferro dapat menyajikan daftar persamaan kubik tereduksi sebagai balasan. Ia menyimpan rahasia penemuannya sepanjang hidup, dan baru mewariskannya di ranjang kematian kepada muridnya, Antonio Fior (ca. 1506–?).

Meskipun kemampuan Fior tidak menyamai gurunya, ia segera mengajukan tantangan kepada Niccolo Fontana (1499–1557). Fontana dikenal sebagai Tartaglia (Si Gagap). Ketika muda, ia terkena sabetan pedang seorang prajurit Prancis dalam serangan terhadap desanya. Ia selamat dari luka parah tersebut, tetapi kemampuan bicaranya terganggu secara permanen. Tartaglia mengirimkan kepada Fior daftar 30 masalah matematika yang beragam; Fior membalas dengan mengirimkan kepada Tartaglia daftar 30 persamaan kubik tereduksi. Tartaglia harus menyelesaikan seluruh 30 masalah itu atau gagal sama sekali. Setelah berusaha keras, Tartaglia akhirnya berhasil menyelesaikan persamaan kubik tereduksi dan mengalahkan Fior, yang kemudian tenggelam dalam ketidaktenaran.

Pada titik ini, seorang matematikawan lain, Gerolamo Cardano (1501–1576), memasuki kisah ini. Cardano menulis kepada Tartaglia, memohon kepadanya agar memberikan penyelesaian persamaan kubik tereduksi. Tartaglia menolak beberapa permintaannya, lalu akhirnya mengungkapkan penyelesaian itu kepada Cardano setelah Cardano bersumpah tidak akan menerbitkan rahasia tersebut atau menyampaikannya kepada orang lain. Dengan menggunakan pengetahuan yang diperolehnya dari Tartaglia, Cardano akhirnya menyelesaikan persamaan kubik umum

$$ax^3 + bx^2 + cx + d = 0.$$

Cardano membagikan rahasia itu kepada muridnya, Ludovico Ferrari (1522–1565), yang menyelesaikan persamaan kuartik umum,

$$ax^4 + bx^3 + cx^2 + dx + e = 0.$$

Pada 1543, Cardano dan Ferrari memeriksa naskah-naskah del Ferro dan menemukan bahwa ia juga telah menyelesaikan persamaan kubik tereduksi. Cardano merasa bahwa penemuan ini membebaskannya dari kewajibannya kepada Tartaglia, sehingga ia kemudian menerbitkan penyelesaian-penyelesaian itu dalam *Ars Magna* (1545), yang di dalamnya ia mengakui jasa del Ferro atas penyelesaian kasus khusus persamaan kubik. Hal ini menimbulkan perselisihan sengit antara Cardano dan Tartaglia, yang menerbitkan kisah mengenai sumpah tersebut setahun kemudian.

17.4 Pertanyaan Bacaan

1. Misalkan $p(x)$ polinomial berderajat n dengan koefisien dari sembarang lapangan. Berapa banyak akar yang dapat dimiliki $p(x)$? Bagaimana hal ini memperumum pengalaman aljabar Anda di sekolah menengah?

2. Apa definisi polinomial tak tereduksi?

3. Tentukan sisa pembagian $8\,x^5 - 18\,x^4 + 20\,x^3 - 25\,x^2 + 20$ oleh $4\,x^2 - x - 2$.

4. Satu teorema dalam bab ini menghubungkan banyak gagasan dalam bab ini dengan banyak gagasan dalam bab sebelumnya. Nyatakan versi parafrasa dari teorema tersebut.

5. Pada awal bab ini, kita mengatakan, "Kita dapat membuktikan banyak hasil untuk gelanggang polinomial yang serupa dengan teorema-teorema yang telah kita buktikan untuk bilangan bulat." Tulislah esai singkat (atau paragraf yang sangat panjang) yang membenarkan pernyataan ini.

17.5 Latihan

1. Daftarkan semua polinomial berderajat 3 atau kurang di $\mathbb{Z}_2[x]$.

2. Hitung setiap ekspresi berikut.

(a) $(5x^2 + 3x - 4) + (4x^2 - x + 9)$ di $\mathbb{Z}_{12}[x]$

(b) $(5x^2 + 3x - 4)(4x^2 - x + 9)$ di $\mathbb{Z}_{12}[x]$

(c) $(7x^3 + 3x^2 - x) + (6x^2 - 8x + 4)$ di $\mathbb{Z}_9[x]$

(d) $(3x^2 + 2x - 4) + (4x^2 + 2)$ di $\mathbb{Z}_5[x]$

(e) $(3x^2 + 2x - 4)(4x^2 + 2)$ di $\mathbb{Z}_5[x]$

(f) $(5x^2 + 3x - 2)^2$ di $\mathbb{Z}_{12}[x]$

Petunjuk. (a) $9x^2 + 2x + 5$; (b) $8x^4 + 7x^3 + 2x^2 + 7x$.

3. Gunakan algoritma pembagian untuk menentukan $q(x)$ dan $r(x)$ sedemikian sehingga $a(x) = q(x)b(x) + r(x)$ dengan $\deg r(x) < \deg b(x)$ untuk setiap pasangan polinomial berikut.

(a) $a(x) = 5x^3 + 6x^2 - 3x + 4$ dan $b(x) = x - 2$ di $\mathbb{Z}_7[x]$

(b) $a(x) = 6x^4 - 2x^3 + x^2 - 3x + 1$ dan $b(x) = x^2 + x - 2$ di $\mathbb{Z}_7[x]$

(c) $a(x) = 4x^5 - x^3 + x^2 + 4$ dan $b(x) = x^3 - 2$ di $\mathbb{Z}_5[x]$

(d) $a(x) = x^5 + x^3 - x^2 - x$ dan $b(x) = x^3 + x$ di $\mathbb{Z}_2[x]$

Petunjuk. (a) $5x^3 + 6x^2 - 3x + 4 = (5x^2 + 2x + 1)(x - 2) + 6$; (c) $4x^5 - x^3 + x^2 + 4 = (4x^2 + 4)(x^3 + 3) + 4x^2 + 2$.

4. Tentukan faktor persekutuan terbesar dari setiap pasangan polinomial $p(x)$ dan $q(x)$ berikut. Jika $d(x) = \gcd(p(x), q(x))$, tentukan dua polinomial $a(x)$ dan $b(x)$ sedemikian sehingga $a(x)p(x) + b(x)q(x) = d(x)$.

(a) $p(x) = x^3 - 6x^2 + 14x - 15$ dan $q(x) = x^3 - 8x^2 + 21x - 18$, dengan $p(x), q(x) \in \mathbb{Q}[x]$

(b) $p(x) = x^3 + x^2 - x + 1$ dan $q(x) = x^3 + x - 1$, dengan $p(x), q(x) \in \mathbb{Z}_2[x]$

(c) $p(x) = x^3 + x^2 - 4x + 4$ dan $q(x) = x^3 + 3x - 2$, dengan $p(x), q(x) \in \mathbb{Z}_5[x]$

(d) $p(x) = x^3 - 2x + 4$ dan $q(x) = 4x^3 + x + 3$, dengan $p(x), q(x) \in \mathbb{Q}[x]$

5. Tentukan semua nol dari setiap polinomial berikut.

(a) $5x^3 + 4x^2 - x + 9$ di $\mathbb{Z}_{12}[x]$

(b) $3x^3 - 4x^2 - x + 4$ di $\mathbb{Z}_5[x]$

(c) $5x^4 + 2x^2 - 3$ di $\mathbb{Z}_7[x]$

(d) $x^3 + x + 1$ di $\mathbb{Z}_2[x]$

Petunjuk. (a) Tidak ada nol di $\mathbb{Z}_{12}$; (c) 3, 4.

6. Tentukan semua unit di $\mathbb{Z}[x]$.

7. Tentukan suatu unit $p(x)$ di $\mathbb{Z}_4[x]$ sedemikian sehingga $\deg p(x) > 1$.

Petunjuk. Tinjau $(2x + 1)$.

8. Manakah di antara polinomial berikut yang tak tereduksi atas $\mathbb{Q}[x]$?

(a) $x^4 - 2x^3 + 2x^2 + x + 4$

(b) $x^4 - 5x^3 + 3x - 2$

(c) $3x^5 - 4x^3 - 6x^2 + 6$

(d) $5x^5 - 6x^4 - 3x^2 + 9x - 15$

Petunjuk. (a) Tereduksi; (c) tak tereduksi.

9. Tentukan semua polinomial tak tereduksi berderajat 2 dan 3 di $\mathbb{Z}_2[x]$.

10. Berikan dua faktorisasi berbeda dari $x^2 + x + 8$ di $\mathbb{Z}_{10}[x]$.

Petunjuk. Salah satu faktorisasinya adalah $x^2 + x + 8 = (x + 2)(x + 9)$.

11. Buktikan atau sangkal: Terdapat polinomial $p(x)$ di $\mathbb{Z}_6[x]$ berderajat n dengan lebih dari n nol yang berbeda.

12. Jika F suatu lapangan, tunjukkan bahwa $F[x_1, \ldots, x_n]$ merupakan daerah integral.

13. Tunjukkan bahwa algoritma pembagian tidak berlaku untuk $\mathbb{Z}[x]$. Mengapa algoritma itu gagal?

Petunjuk. Bilangan bulat $\mathbb{Z}$ tidak membentuk lapangan.

14. Buktikan atau sangkal: $x^p + a$ tak tereduksi untuk setiap $a \in \mathbb{Z}_p$, dengan p prima.

Petunjuk. Salah.

15. Misalkan $f(x)$ tak tereduksi di $F[x]$, dengan F suatu lapangan. Jika $f(x) \mid p(x)q(x)$, buktikan bahwa $f(x) \mid p(x)$ atau $f(x) \mid q(x)$.

16. Misalkan R dan S gelanggang-gelanggang isomorfik. Buktikan bahwa $R[x] \cong S[x]$.

Petunjuk. Misalkan $\phi : R \to S$ suatu isomorfisma. Definisikan $\overline{\phi} : R[x] \to S[x]$ dengan $\overline{\phi}(a_0 + a_1x + \cdots + a_nx^n) = \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n$.

17. Misalkan F suatu lapangan dan $a \in F$. Jika $p(x) \in F[x]$, tunjukkan bahwa $p(a)$ adalah sisa yang diperoleh ketika $p(x)$ dibagi dengan $x - a$.

18. Teorema Akar Rasional. Misalkan

$$p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x],$$

dengan $a_n \neq 0$. Buktikan bahwa jika $p(r/s) = 0$, dengan $\gcd(r, s) = 1$, maka $r \mid a_0$ dan $s \mid a_n$.

19. Misalkan $\mathbb{Q}^*$ grup perkalian bilangan rasional positif. Buktikan bahwa $\mathbb{Q}^*$ isomorfik dengan $(\mathbb{Z}[x], +)$.

20. Polinomial Siklotomik. Polinomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

untuk p prima disebut **polinomial siklotomik.** Tunjukkan bahwa $\Phi_p(x)$ tak tereduksi atas $\mathbb{Q}$ untuk setiap bilangan prima p.

Petunjuk. Polinomial

$$\Phi_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1$$

disebut **polinomial siklotomik.** Tunjukkan bahwa $\Phi_p(x)$ tak tereduksi atas $\mathbb{Q}$ untuk setiap bilangan prima p.

21. Jika F suatu lapangan, tunjukkan bahwa terdapat tak terhingga banyak polinomial tak tereduksi di $F[x]$.

22. Misalkan R gelanggang komutatif dengan identitas. Buktikan bahwa perkalian di $R[x]$ bersifat komutatif.

23. Misalkan R gelanggang komutatif dengan identitas. Buktikan bahwa perkalian di $R[x]$ bersifat distributif.

24. Tunjukkan bahwa $x^p - x$ memiliki p nol yang berbeda di $\mathbb{Z}_p$, untuk setiap bilangan prima p. Simpulkan bahwa

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)).$$

25. Misalkan F suatu lapangan dan $f(x) = a_0 + a_1x + \cdots + a_nx^n$ berada di $F[x]$. Definisikan $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$ sebagai **turunan** dari $f(x)$.

(a) Buktikan bahwa

$$(f+g)'(x) = f'(x) + g'(x).$$

Simpulkan bahwa kita dapat mendefinisikan homomorfisma grup abelian $D : F[x] \to F[x]$ dengan $D(f(x)) = f'(x)$.

(b) Hitung kernel D jika $\operatorname{char} F = 0$.

(c) Hitung kernel D jika $\operatorname{char} F = p$.

(d) Buktikan bahwa

$$(fg)'(x) = f'(x)g(x) + f(x)g'(x).$$

(e) Misalkan kita dapat memfaktorkan polinomial $f(x) \in F[x]$ menjadi faktor-faktor linear, katakanlah

$$f(x) = a(x-a_1)(x-a_2)\cdots(x-a_n).$$

Buktikan bahwa $f(x)$ tidak memiliki faktor berulang jika dan hanya jika $f(x)$ dan $f'(x)$ relatif prima.

26. Misalkan F suatu lapangan. Tunjukkan bahwa $F[x]$ tidak pernah merupakan lapangan.

Petunjuk. Tentukan ideal sejati taktrivial di $F[x]$.

27. Misalkan R suatu daerah integral. Buktikan bahwa $R[x_1, \ldots, x_n]$ merupakan daerah integral.

28. Misalkan R gelanggang komutatif dengan identitas. Tunjukkan bahwa $R[x]$ memiliki subgelanggang R' yang isomorfik dengan R.

29. Misalkan $p(x)$ dan $q(x)$ polinomial-polinomial di $R[x]$, dengan R gelanggang komutatif dengan identitas. Buktikan bahwa $\deg(p(x) + q(x)) \leq \max(\deg p(x), \deg q(x))$.

17.6 Latihan Tambahan: Menyelesaikan Persamaan Kubik dan Kuartik

1. Sempurnakan kuadrat untuk menyelesaikan persamaan kuadrat umum

$$ax^2 + bx + c = 0$$

sehingga diperoleh

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Diskriminan dari persamaan kuadrat, $\Delta = b^2 - 4ac$, menentukan sifat penyelesaian persamaan tersebut. Jika $\Delta > 0$, persamaan memiliki dua penyelesaian real yang berbeda. Jika $\Delta = 0$, persamaan memiliki satu akar real berulang. Jika $\Delta < 0$, terdapat dua penyelesaian imajiner yang berbeda.

2. Tunjukkan bahwa setiap persamaan kubik berbentuk

$$x^3 + bx^2 + cx + d = 0$$

dapat direduksi ke bentuk $y^3 + py + q = 0$ dengan melakukan substitusi $x = y - b/3$.

3. Buktikan bahwa akar pangkat tiga dari 1 diberikan oleh

$$\omega = \frac{-1 + i\sqrt{3}}{2}$$
$$\omega^2 = \frac{-1 - i\sqrt{3}}{2}$$
$$\omega^3 = 1.$$

4. Lakukan substitusi

$$y = z - \frac{p}{3z}$$

untuk y dalam persamaan $y^3 + py + q = 0$ dan peroleh dua penyelesaian A dan B untuk z^3.

5. Tunjukkan bahwa hasil kali penyelesaian yang diperoleh dalam (4) adalah $-p^3/27$, dan simpulkan bahwa $\sqrt[3]{AB} = -p/3$.

6. Buktikan bahwa semua penyelesaian yang mungkin untuk z dalam (4) diberikan oleh

$$\sqrt[3]{A}, \quad \omega\sqrt[3]{A}, \quad \omega^2\sqrt[3]{A}, \quad \sqrt[3]{B}, \quad \omega\sqrt[3]{B}, \quad \omega^2\sqrt[3]{B}$$

dan gunakan hasil ini untuk menunjukkan bahwa tiga penyelesaian yang

mungkin untuk y adalah

$$\omega^i \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}}+\omega^{2i}\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{p^3}{27}+\frac{q^2}{4}}},$$

dengan $i = 0, 1, 2$.

7. **Diskriminan** dari persamaan kubik adalah

$$\Delta = \frac{p^3}{27}+\frac{q^2}{4}.$$

Tunjukkan bahwa $y^3 + py + q = 0$

(a) memiliki tiga akar real, dengan sedikitnya dua di antaranya sama, jika $\Delta = 0$.

(b) memiliki satu akar real dan dua akar imajiner konjugat jika $\Delta > 0$.

(c) memiliki tiga akar real yang berbeda jika $\Delta < 0$.

8. Selesaikan persamaan-persamaan kubik berikut.

(a) $x^3 - 4x^2 + 11x + 30 = 0$

(b) $x^3 - 3x + 5 = 0$

(c) $x^3 - 3x + 2 = 0$

(d) $x^3 + x + 3 = 0$

9. Tunjukkan bahwa persamaan kuartik umum

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

dapat direduksi menjadi

$$y^4 + py^2 + qy + r = 0$$

dengan menggunakan substitusi $x = y - a/4$.

10. Tunjukkan bahwa

$$\left(y^2+\frac{1}{2}z\right)^2 = (z-p)y^2 - qy + \left(\frac{1}{4}z^2 - r\right).$$

11. Tunjukkan bahwa ruas kanan Latihan 17.6.10 dapat dinyatakan dalam bentuk $(my + k)^2$ jika dan hanya jika

$$q^2 - 4(z-p)\left(\frac{1}{4}z^2 - r\right) = 0.$$

12. Dari Latihan 17.6.11, peroleh **persamaan kubik resolven**

$$z^3 - pz^2 - 4rz + (4pr - q^2) = 0.$$

Dengan menyelesaikan persamaan kubik resolven, nyatakan persamaan yang ditemukan dalam Latihan 17.6.10 dalam bentuk

$$\left(y^2+\frac{1}{2}z\right)^2 = (my+k)^2$$

untuk memperoleh penyelesaian persamaan kuartik.

13. Gunakan metode ini untuk menyelesaikan persamaan-persamaan kuartik berikut.

(a) $x^4 - x^2 - 3x + 2 = 0$

(b) $x^4 + x^3 - 7x^2 - x + 6 = 0$

(c) $x^4 - 2x^2 + 4x - 3 = 0$

(d) $x^4 - 4x^3 + 3x^2 - 5x + 2 = 0$

18

Daerah Integral

Salah satu gelanggang terpenting yang kita pelajari adalah gelanggang bilangan bulat. Gelanggang ini merupakan contoh pertama kita tentang struktur aljabar: gelanggang polinomial pertama yang kita kaji adalah $\mathbb{Z}[x]$. Kita juga mengetahui bahwa bilangan bulat termuat secara alami di dalam lapangan bilangan rasional, $\mathbb{Q}$. Gelanggang bilangan bulat merupakan model bagi semua daerah integral. Dalam bab ini kita akan mengkaji daerah integral secara umum, menjawab pertanyaan mengenai struktur ideal pada daerah integral, gelanggang polinomial di atas daerah integral, serta apakah suatu daerah integral dapat disematkan ke dalam suatu lapangan.

18.1 Lapangan Pecahan

Setiap lapangan juga merupakan daerah integral; tetapi, terdapat banyak daerah integral yang bukan lapangan. Sebagai contoh, bilangan bulat $\mathbb{Z}$ membentuk daerah integral, tetapi bukan lapangan. Pertanyaan yang secara alami muncul adalah bagaimana kita dapat mengaitkan suatu daerah integral dengan suatu lapangan. Terdapat cara alami untuk membangun bilangan rasional $\mathbb{Q}$ dari bilangan bulat: bilangan rasional dapat direpresentasikan sebagai hasil bagi formal dari dua bilangan bulat. Bilangan rasional tentu saja membentuk lapangan. Bahkan, dapat ditunjukkan bahwa bilangan rasional merupakan lapangan terkecil yang memuat bilangan bulat. Diberikan suatu daerah integral D, pertanyaan kita sekarang adalah bagaimana membangun lapangan terkecil F yang memuat D. Kita akan melakukannya dengan cara yang sama seperti ketika kita membangun bilangan rasional dari bilangan bulat.

Suatu elemen $p/q \in \mathbb{Q}$ adalah hasil bagi dua bilangan bulat p dan q; tetapi, pasangan bilangan bulat yang berbeda dapat merepresentasikan bilangan rasional yang sama. Misalnya, $1/2 = 2/4 = 3/6$. Kita mengetahui bahwa

$$\frac{a}{b} = \frac{c}{d}$$

jika dan hanya jika $ad = bc$. Cara yang lebih formal untuk meninjau masalah ini adalah mengkaji pecahan melalui relasi ekuivalensi. Kita dapat memandang elemen-elemen dalam $\mathbb{Q}$ sebagai pasangan terurut dalam $\mathbb{Z} \times \mathbb{Z}$. Hasil bagi p/q dapat ditulis sebagai (p, q). Misalnya, $(3, 7)$ merepresentasikan pecahan $3/7$. Akan tetapi, timbul masalah jika kita meninjau semua pasangan yang mungkin dalam $\mathbb{Z}\times\mathbb{Z}$. Tidak ada pecahan $5/0$ yang bersesuaian dengan pasangan $(5, 0)$. Selain itu, pasangan $(3, 6)$ dan $(2, 4)$ sama-sama merepresentasikan

pecahan 1/2. Masalah pertama mudah diselesaikan dengan mensyaratkan koordinat kedua tidak nol. Masalah kedua diselesaikan dengan menganggap dua pasangan (a, b) dan (c, d) ekuivalen jika $ad = bc$.

Jika kita menggunakan pendekatan pasangan terurut alih-alih pecahan, kita dapat mempelajari daerah integral secara umum. Misalkan D sebarang daerah integral dan misalkan

$$S = \{(a, b) : a, b \in D \text{ dan } b \neq 0\}.$$

Definisikan suatu relasi pada S dengan $(a, b) \sim (c, d)$ jika $ad = bc$.

Lema 18.1.1 *Relasi $\sim$ antara elemen-elemen S merupakan relasi ekuivalensi.*

BUKTI. Karena D komutatif, $ab = ba$; jadi, $\sim$ bersifat refleksif pada D. Sekarang andaikan bahwa $(a, b) \sim (c, d)$. Maka $ad = bc$ atau $cb = da$. Oleh karena itu, $(c, d) \sim (a, b)$ dan relasi tersebut bersifat simetris. Terakhir, untuk menunjukkan bahwa relasi tersebut bersifat transitif, misalkan $(a, b) \sim (c, d)$ dan $(c, d) \sim (e, f)$. Dalam hal ini $ad = bc$ dan $cf = de$. Mengalikan kedua ruas $ad = bc$ dengan f menghasilkan

$$afd = adf = bcf = bde = bed.$$

Karena D merupakan daerah integral, kita dapat menyimpulkan bahwa $af = be$ atau $(a, b) \sim (e, f)$. ■

Kita akan menyatakan himpunan kelas ekuivalensi pada S dengan F_D. Sekarang kita perlu mendefinisikan operasi penjumlahan dan perkalian pada F_D. Ingat kembali bagaimana pecahan dijumlahkan dan dikalikan dalam $\mathbb{Q}$:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd};$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Wajar jika operasi penjumlahan dan perkalian pada F_D didefinisikan dengan cara serupa. Jika kita menyatakan kelas ekuivalensi dari $(a, b) \in S$ dengan $[a, b]$, kita terdorong untuk mendefinisikan operasi penjumlahan dan perkalian pada F_D dengan

$$[a, b] + [c, d] = [ad + bc, bd]$$

dan

$$[a, b] \cdot [c, d] = [ac, bd],$$

secara berturut-turut. Lema berikut menunjukkan bahwa operasi-operasi ini tidak bergantung pada pilihan wakil dari setiap kelas ekuivalensi.

Lema 18.1.2 *Operasi penjumlahan dan perkalian pada F_D terdefinisi dengan baik.*

BUKTI. Kita akan membuktikan bahwa operasi penjumlahan terdefinisi dengan baik. Bukti bahwa perkalian terdefinisi dengan baik diserahkan sebagai latihan. Misalkan $[a_1, b_1] = [a_2, b_2]$ dan $[c_1, d_1] = [c_2, d_2]$. Kita harus menunjukkan bahwa

$$[a_1d_1 + b_1c_1, b_1d_1] = [a_2d_2 + b_2c_2, b_2d_2]$$

atau, secara ekuivalen, bahwa

$$(a_1d_1 + b_1c_1)(b_2d_2) = (b_1d_1)(a_2d_2 + b_2c_2).$$

Karena $[a_1, b_1] = [a_2, b_2]$ dan $[c_1, d_1] = [c_2, d_2]$, kita mengetahui bahwa $a_1b_2 = b_1a_2$ dan $c_1d_2 = d_1c_2$. Oleh karena itu,

$$(a_1d_1 + b_1c_1)(b_2d_2) = a_1d_1b_2d_2 + b_1c_1b_2d_2$$

$$\begin{aligned}&= a_1b_2d_1d_2 + b_1b_2c_1d_2\\ &= b_1a_2d_1d_2 + b_1b_2d_1c_2\\ &= (b_1d_1)(a_2d_2 + b_2c_2).\end{aligned}$$

■

Lema 18.1.3 *Himpunan kelas ekuivalensi dari S, yaitu F_D, di bawah relasi ekuivalensi $\sim$, bersama dengan operasi penjumlahan dan perkalian yang didefinisikan oleh*

$$\begin{aligned}[a,b] + [c,d] &= [ad + bc, bd]\\ [a,b] \cdot [c,d] &= [ac, bd],\end{aligned}$$

merupakan suatu lapangan.

BUKTI. Identitas aditif dan multiplikatif masing-masing adalah $[0,1]$ dan $[1,1]$. Untuk menunjukkan bahwa $[0,1]$ merupakan identitas aditif, perhatikan bahwa

$$[a,b] + [0,1] = [a1 + b0, b1] = [a,b].$$

Mudah ditunjukkan bahwa $[1,1]$ merupakan identitas multiplikatif. Misalkan $[a,b] \in F_D$ dengan $a \neq 0$. Maka $[b,a]$ juga berada dalam F_D dan $[a,b]\cdot[b,a] = [1,1]$; jadi, $[b,a]$ merupakan invers multiplikatif dari $[a,b]$. Demikian pula, $[-a,b]$ merupakan invers aditif dari $[a,b]$. Verifikasi sifat asosiatif dan komutatif perkalian dalam F_D kita serahkan sebagai latihan. Kita juga menyerahkan kepada pembaca untuk menunjukkan bahwa F_D merupakan grup abelian di bawah penjumlahan.

Tinggal menunjukkan bahwa sifat distributif berlaku dalam F_D; memang,

$$\begin{aligned}[a,b][e,f] + [c,d][e,f] &= [ae, bf] + [ce, df]\\ &= [aedf + bfce, bdf^2]\\ &= [aed + bce, bdf]\\ &= [ade + bce, bdf]\\ &= ([a,b] + [c,d])[e,f]\end{aligned}$$

sehingga lema terbukti. ■

Lapangan F_D dalam Lema 18.1.3 disebut **lapangan pecahan** atau **lapangan hasil bagi** dari daerah integral D.

Teorema 18.1.4 *Misalkan D suatu daerah integral. Maka D dapat disematkan ke dalam lapangan pecahan F_D, dengan setiap elemen dalam F_D dapat dinyatakan sebagai hasil bagi dua elemen dalam D. Lebih lanjut, lapangan pecahan F_D tunggal dalam arti bahwa jika E adalah sebarang lapangan yang memuat D, maka terdapat pemetaan $\psi : F_D \to E$ yang memberikan isomorfisma dengan suatu sublapangan dari E sedemikian sehingga $\psi(a) = a$ untuk semua elemen $a \in D$, dengan a diidentifikasi dengan citranya dalam F_D.*

BUKTI. Pertama-tama kita akan menunjukkan bahwa D dapat disematkan ke dalam lapangan F_D. Definisikan pemetaan $\phi : D \to F_D$ dengan $\phi(a) = [a,1]$. Maka untuk a dan b dalam D,

$$\phi(a+b) = [a+b,1] = [a,1] + [b,1] = \phi(a) + \phi(b)$$

dan

$$\phi(ab) = [ab,1] = [a,1][b,1] = \phi(a)\phi(b);$$

jadi, ϕ merupakan homomorfisma. Untuk menunjukkan bahwa ϕ satu-ke-satu,

andaikan bahwa $\phi(a) = \phi(b)$. Maka $[a,1] = [b,1]$, atau $a = a1 = 1b = b$. Terakhir, setiap elemen F_D dapat dinyatakan sebagai hasil bagi dua elemen dalam D, karena

$$\phi(a)[\phi(b)]^{-1} = [a,1][b,1]^{-1} = [a,1] \cdot [1,b] = [a,b].$$

Sekarang misalkan E suatu lapangan yang memuat D dan definisikan pemetaan $\psi : F_D \to E$ dengan $\psi([a,b]) = ab^{-1}$. Untuk menunjukkan bahwa ψ terdefinisi dengan baik, misalkan $[a_1,b_1] = [a_2,b_2]$. Maka $a_1b_2 = b_1a_2$. Oleh karena itu, $a_1b_1^{-1} = a_2b_2^{-1}$ dan $\psi([a_1,b_1]) = \psi([a_2,b_2])$.

Jika $[a,b]$ dan $[c,d]$ berada dalam F_D, maka

$$\begin{aligned}\psi([a,b]+[c,d]) &= \psi([ad+bc,bd]) \\ &= (ad+bc)(bd)^{-1} \\ &= ab^{-1} + cd^{-1} \\ &= \psi([a,b]) + \psi([c,d])\end{aligned}$$

dan

$$\begin{aligned}\psi([a,b]\cdot[c,d]) &= \psi([ac,bd]) \\ &= (ac)(bd)^{-1} \\ &= ab^{-1}cd^{-1} \\ &= \psi([a,b])\psi([c,d]).\end{aligned}$$

Oleh karena itu, ψ merupakan homomorfisma.

Untuk menyelesaikan bukti teorema, kita perlu menunjukkan bahwa ψ satu-ke-satu. Andaikan bahwa $\psi([a,b]) = ab^{-1} = 0$. Maka $a = 0b = 0$ dan $[a,b] = [0,b]$. Oleh karena itu, kernel ψ adalah elemen nol $[0,b]$ dalam F_D, dan ψ bersifat injektif. ■

Contoh 18.1.5 Karena $\mathbb{Q}$ merupakan lapangan, $\mathbb{Q}[x]$ merupakan daerah integral. Lapangan pecahan dari $\mathbb{Q}[x]$ adalah himpunan semua ekspresi rasional $p(x)/q(x)$, dengan $p(x)$ dan $q(x)$ berupa polinomial di atas bilangan rasional dan $q(x)$ bukan polinomial nol. Lapangan ini akan kita nyatakan dengan $\mathbb{Q}(x)$. ▲

Bukti korolari-korolari berikut dari Teorema 18.1.4 kita serahkan sebagai latihan.

Korolari 18.1.6 *Misalkan F suatu lapangan berkarakteristik nol. Maka F memuat sublapangan yang isomorfik dengan $\mathbb{Q}$.*

Korolari 18.1.7 *Misalkan F suatu lapangan berkarakteristik p. Maka F memuat sublapangan yang isomorfik dengan $\mathbb{Z}_p$.*

18.2 Faktorisasi dalam Daerah Integral

Unsur pembangun bilangan bulat adalah bilangan prima. Jika F merupakan lapangan, maka polinomial tak tereduksi dalam $F[x]$ berperan sangat serupa dengan bilangan prima dalam gelanggang bilangan bulat. Dari suatu daerah integral sebarang, kita sampai pada rangkaian definisi berikut.

Misalkan R suatu gelanggang komutatif dengan identitas, dan misalkan a serta b elemen-elemen dalam R. Kita mengatakan bahwa a **membagi** b, dan menulis $a \mid b$, jika terdapat elemen $c \in R$ sedemikian sehingga $b = ac$. Suatu **unit** dalam R adalah elemen yang mempunyai invers multiplikatif. Dua

elemen a dan b dalam R dikatakan **sekawan** jika terdapat unit u dalam R sedemikian sehingga $a = ub$.

Misalkan D suatu daerah integral. Elemen tak nol $p \in D$ yang bukan unit dikatakan **tak tereduksi** jika setiap kali $p = ab$, salah satu dari a atau b merupakan unit. Lebih lanjut, p disebut **prima** jika setiap kali $p \mid ab$, berlaku $p \mid a$ atau $p \mid b$.

Contoh 18.2.1 Penting diperhatikan bahwa elemen prima dan elemen tak tereduksi tidak selalu berimpit. Misalkan R subgelanggang (dengan identitas) dari $\mathbb{Q}[x, y]$ yang dibangkitkan oleh x^2, y^2, dan xy. Setiap elemen ini tak tereduksi dalam R; tetapi, xy tidak prima, karena xy membagi x^2y^2, tetapi tidak membagi x^2 maupun y^2. ▲

Teorema Dasar Aritmetika menyatakan bahwa setiap bilangan bulat positif $n > 1$ dapat difaktorkan menjadi hasil kali bilangan-bilangan prima $p_1 \cdots p_k$, dengan p_i tidak harus berbeda. Kita juga mengetahui bahwa faktorisasi semacam itu tunggal hingga urutan p_i. Hasil ini dapat dengan mudah kita perluas ke bilangan bulat. Muncul pertanyaan apakah faktorisasi semacam itu mungkin dalam gelanggang lain. Dengan memperumum definisi ini, kita mengatakan bahwa daerah integral D merupakan **domain faktorisasi tunggal**, atau **ufd**, jika D memenuhi kriteria berikut.

1. Misalkan $a \in D$ dengan $a \neq 0$ dan a bukan unit. Maka a dapat ditulis sebagai hasil kali elemen-elemen tak tereduksi dalam D.

2. Misalkan $a = p_1 \cdots p_r = q_1 \cdots q_s$, dengan p_i dan q_i tak tereduksi. Maka $r = s$ dan terdapat $\pi \in S_r$ sedemikian sehingga p_i dan $q_{\pi(j)}$ sekawan untuk $j = 1, \ldots, r$.

Contoh 18.2.2 Berdasarkan Teorema Dasar Aritmetika, bilangan bulat membentuk domain faktorisasi tunggal. ▲

Contoh 18.2.3 Tidak setiap daerah integral merupakan domain faktorisasi tunggal. Subgelanggang $\mathbb{Z}[\sqrt{3}\,i] = \{a + b\sqrt{3}\,i\}$ dari bilangan kompleks merupakan daerah integral (Latihan 16.7.12, Bab 16). Misalkan $z = a + b\sqrt{3}\,i$ dan definisikan $\nu : \mathbb{Z}[\sqrt{3}\,i] \to \mathbb{N} \cup \{0\}$ dengan $\nu(z) = |z|^2 = a^2 + 3b^2$. Jelas bahwa $\nu(z) \geq 0$, dengan kesamaan terjadi ketika $z = 0$. Selain itu, dari pengetahuan kita tentang bilangan kompleks, kita mengetahui bahwa $\nu(zw) = \nu(z)\nu(w)$. Mudah ditunjukkan bahwa jika $\nu(z) = 1$, maka z merupakan unit, dan bahwa satu-satunya unit dalam $\mathbb{Z}[\sqrt{3}\,i]$ adalah 1 dan -1.

Kita mengklaim bahwa 4 mempunyai dua faktorisasi berbeda menjadi elemen-elemen tak tereduksi:

$$4 = 2 \cdot 2 = (1 - \sqrt{3}\,i)(1 + \sqrt{3}\,i).$$

Kita harus menunjukkan bahwa setiap faktor ini merupakan elemen tak tereduksi dalam $\mathbb{Z}[\sqrt{3}\,i]$. Jika 2 tereduksi, maka $2 = zw$ untuk elemen-elemen z, w dalam $\mathbb{Z}[\sqrt{3}\,i]$ dengan $\nu(z) = \nu(w) = 2$. Namun, tidak terdapat elemen z dalam $\mathbb{Z}[\sqrt{3}\,i]$ sedemikian sehingga $\nu(z) = 2$, karena persamaan $a^2 + 3b^2 = 2$ tidak mempunyai solusi bilangan bulat. Oleh karena itu, 2 harus tak tereduksi. Argumen serupa menunjukkan bahwa $1 - \sqrt{3}\,i$ dan $1 + \sqrt{3}\,i$ keduanya tak tereduksi. Karena 2 bukan kelipatan unit dari $1 - \sqrt{3}\,i$ maupun $1 + \sqrt{3}\,i$, 4 mempunyai setidaknya dua faktorisasi berbeda menjadi elemen-elemen tak tereduksi. ▲

18.2.1 Domain Ideal Utama

Misalkan R suatu gelanggang komutatif dengan identitas. Ingat bahwa ideal utama yang dibangkitkan oleh $a \in R$ adalah ideal berbentuk $\langle a \rangle = \{ra : r \in R\}$. Daerah integral yang setiap idealnya merupakan ideal utama disebut **domain ideal utama**, atau **pid**.

Lema 18.2.4 *Misalkan D suatu daerah integral dan misalkan $a, b \in D$. Maka*

1. *$a \mid b$ jika dan hanya jika $\langle b \rangle \subset \langle a \rangle$.*
2. *a dan b sekawan jika dan hanya jika $\langle b \rangle = \langle a \rangle$.*
3. *a merupakan unit dalam D jika dan hanya jika $\langle a \rangle = D$.*

BUKTI. (1) Andaikan $a \mid b$. Maka $b = ax$ untuk suatu $x \in D$. Jadi, untuk setiap r dalam D, $br = (ax)r = a(xr)$ dan $\langle b \rangle \subset \langle a \rangle$. Sebaliknya, andaikan $\langle b \rangle \subset \langle a \rangle$. Maka $b \in \langle a \rangle$. Akibatnya, $b = ax$ untuk suatu $x \in D$. Dengan demikian, $a \mid b$.

(2) Karena a dan b sekawan, terdapat unit u sedemikian sehingga $a = ub$. Oleh karena itu, $b \mid a$ dan $\langle a \rangle \subset \langle b \rangle$. Demikian pula, $\langle b \rangle \subset \langle a \rangle$. Akibatnya, $\langle a \rangle = \langle b \rangle$. Sebaliknya, andaikan $\langle a \rangle = \langle b \rangle$. Menurut bagian (1), $a \mid b$ dan $b \mid a$. Maka $a = bx$ dan $b = ay$ untuk suatu $x, y \in D$. Oleh karena itu, $a = bx = ayx$. Karena D merupakan daerah integral, $xy = 1$; artinya, x dan y merupakan unit serta a dan b sekawan.

(3) Elemen $a \in D$ merupakan unit jika dan hanya jika a sekawan dengan 1. Sementara itu, a sekawan dengan 1 jika dan hanya jika $\langle a \rangle = \langle 1 \rangle = D$. ■

Teorema 18.2.5 *Misalkan D suatu PID dan $\langle p \rangle$ suatu ideal tak nol dalam D. Maka $\langle p \rangle$ merupakan ideal maksimal jika dan hanya jika p tak tereduksi.*

BUKTI. Andaikan $\langle p \rangle$ merupakan ideal maksimal. Jika suatu elemen a dalam D membagi p, maka $\langle p \rangle \subset \langle a \rangle$. Karena $\langle p \rangle$ maksimal, berlaku $D = \langle a \rangle$ atau $\langle p \rangle = \langle a \rangle$. Akibatnya, a dan p sekawan atau a merupakan unit. Oleh karena itu, p tak tereduksi.

Sebaliknya, misalkan p tak tereduksi. Jika $\langle a \rangle$ merupakan ideal dalam D sedemikian sehingga $\langle p \rangle \subset \langle a \rangle \subset D$, maka $a \mid p$. Karena p tak tereduksi, a merupakan unit atau a dan p sekawan. Oleh karena itu, $D = \langle a \rangle$ atau $\langle p \rangle = \langle a \rangle$. Dengan demikian, $\langle p \rangle$ merupakan ideal maksimal. ■

Korolari 18.2.6 *Misalkan D suatu PID. Jika p tak tereduksi, maka p prima.*

BUKTI. Misalkan p tak tereduksi dan andaikan $p \mid ab$. Maka $\langle ab \rangle \subset \langle p \rangle$. Menurut Korolari 16.4.6, karena $\langle p \rangle$ merupakan ideal maksimal, $\langle p \rangle$ juga harus merupakan ideal prima. Dengan demikian, $a \in \langle p \rangle$ atau $b \in \langle p \rangle$. Jadi, $p \mid a$ atau $p \mid b$. ■

Lema 18.2.7 *Misalkan D suatu PID. Misalkan $I_1, I_2, \ldots$ suatu himpunan ideal sedemikian sehingga $I_1 \subset I_2 \subset \cdots$. Maka terdapat bilangan bulat N sedemikian sehingga $I_n = I_N$ untuk semua $n \geq N$.*

BUKTI. Kita mengklaim bahwa $I = \bigcup_{i=1}^{\infty} I_i$ merupakan ideal dari D. Jelas bahwa I tidak kosong, karena $I_1 \subset I$ dan $0 \in I$. Jika $a, b \in I$, maka $a \in I_i$ dan $b \in I_j$ untuk suatu i dan j dalam $\mathbb{N}$. Tanpa mengurangi keumuman, kita dapat mengandaikan bahwa $i \leq j$. Jadi, a dan b keduanya berada dalam I_j, sehingga $a - b$ juga berada dalam I_j. Sekarang misalkan $r \in D$ dan $a \in I$. Sekali lagi, perhatikan bahwa $a \in I_i$ untuk suatu bilangan bulat positif i. Karena I_i merupakan ideal, $ra \in I_i$ dan karenanya harus berada dalam I. Oleh karena itu, kita telah menunjukkan bahwa I merupakan ideal dalam D.

Karena D merupakan domain ideal utama, terdapat elemen $\overline{a} \in D$ yang membangkitkan I. Karena $\overline{a}$ berada dalam I_N untuk suatu $N \in \mathbb{N}$, kita mengetahui bahwa $I_N = I = \langle \overline{a} \rangle$. Akibatnya, $I_n = I_N$ untuk $n \geq N$. ■

Setiap gelanggang komutatif yang memenuhi syarat dalam Lema 18.2.7 dikatakan memenuhi **syarat rantai naik**, atau **ACC**. Gelanggang semacam itu disebut **gelanggang Noetherian**, menurut nama Emmy Noether.

Teorema 18.2.8 *Setiap* PID *merupakan* UFD.

BUKTI.

Eksistensi faktorisasi. Misalkan D suatu PID dan a suatu elemen tak nol dalam D yang bukan unit. Jika a tak tereduksi, bukti selesai. Jika tidak, terdapat faktorisasi $a = a_1 b_1$, dengan a_1 maupun b_1 bukan unit. Jadi, $\langle a \rangle \subset \langle a_1 \rangle$. Menurut Lema 18.2.4, kita mengetahui bahwa $\langle a \rangle \neq \langle a_1 \rangle$; jika tidak, a dan a_1 akan sekawan serta b_1 akan menjadi unit, yang bertentangan dengan pengandaian kita. Sekarang andaikan bahwa $a_1 = a_2 b_2$, dengan a_2 maupun b_2 bukan unit. Dengan argumen yang sama seperti sebelumnya, $\langle a_1 \rangle \subset \langle a_2 \rangle$. Konstruksi ini dapat kita lanjutkan untuk memperoleh rantai naik ideal

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots.$$

Menurut Lema 18.2.7, terdapat bilangan bulat positif N sedemikian sehingga $\langle a_n \rangle = \langle a_N \rangle$ untuk semua $n \geq N$. Akibatnya, a_N harus tak tereduksi. Sekarang kita telah menunjukkan bahwa a merupakan hasil kali dua elemen, dan salah satunya harus tak tereduksi.

Sekarang andaikan bahwa $a = c_1 p_1$, dengan p_1 tak tereduksi. Jika c_1 bukan unit, kita dapat mengulangi argumen sebelumnya untuk menyimpulkan bahwa $\langle a \rangle \subset \langle c_1 \rangle$. Elemen c_1 tak tereduksi atau $c_1 = c_2 p_2$, dengan p_2 tak tereduksi dan c_2 bukan unit. Dengan melanjutkan cara ini, kita memperoleh rantai ideal lain

$$\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset \cdots.$$

Rantai ini harus memenuhi syarat rantai naik; oleh karena itu,

$$a = p_1 p_2 \cdots p_r$$

untuk elemen-elemen tak tereduksi $p_1, \ldots, p_r$.

Ketunggalan faktorisasi. Untuk menunjukkan ketunggalan, misalkan

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

dengan setiap p_i dan setiap q_i tak tereduksi. Tanpa mengurangi keumuman, kita dapat mengandaikan bahwa $r < s$. Karena p_1 membagi $q_1 q_2 \cdots q_s$, menurut Korolari 18.2.6 elemen tersebut harus membagi suatu q_i. Dengan menyusun ulang q_i, kita dapat mengandaikan bahwa $p_1 \mid q_1$; jadi, $q_1 = u_1 p_1$ untuk suatu unit u_1 dalam D. Oleh karena itu,

$$a = p_1 p_2 \cdots p_r = u_1 p_1 q_2 \cdots q_s$$

atau

$$p_2 \cdots p_r = u_1 q_2 \cdots q_s.$$

Dengan melanjutkan cara ini, kita dapat menyusun q_i sedemikian sehingga $p_2 = q_2, p_3 = q_3, \ldots, p_r = q_r$, untuk memperoleh

$$u_1 u_2 \cdots u_r q_{r+1} \cdots q_s = 1.$$

Dalam hal ini $q_{r+1} \cdots q_s$ merupakan unit, yang bertentangan dengan fakta bahwa $q_{r+1}, \ldots, q_s$ tak tereduksi. Oleh karena itu, $r = s$ dan faktorisasi a tunggal. ■

Korolari 18.2.9 *Misalkan F suatu lapangan. Maka $F[x]$ merupakan* UFD.

Contoh 18.2.10 Setiap PID merupakan UFD, tetapi tidak setiap UFD merupakan PID. Dalam Korolari 18.2.24, kita akan membuktikan bahwa $\mathbb{Z}[x]$ merupakan UFD. Akan tetapi, $\mathbb{Z}[x]$ bukan PID. Misalkan $I = \{5f(x) + xg(x) : f(x), g(x) \in \mathbb{Z}[x]\}$. Mudah ditunjukkan bahwa I merupakan ideal dari $\mathbb{Z}[x]$. Andaikan bahwa $I = \langle p(x)\rangle$. Karena $5 \in I$, $5 = f(x)p(x)$. Dalam hal ini $p(x) = p$ harus merupakan konstanta. Karena $x \in I$, $x = pg(x)$; akibatnya, $p = \pm 1$. Namun, dari fakta ini diperoleh $\langle p(x)\rangle = \mathbb{Z}[x]$. Akan tetapi, ini berarti bahwa 3 berada dalam I. Oleh karena itu, kita dapat menulis $3 = 5f(x)+xg(x)$ untuk suatu $f(x)$ dan $g(x)$ dalam $\mathbb{Z}[x]$. Dengan meninjau suku konstan polinomial ini, kita melihat bahwa $3 = 5f(x)$, yang mustahil. ▲

18.2.2 Domain Euklides

Kita telah berulang kali menggunakan algoritma pembagian ketika membuktikan hasil mengenai $\mathbb{Z}$ ataupun $F[x]$, dengan F suatu lapangan. Sekarang kita patut bertanya kapan algoritma pembagian tersedia bagi suatu daerah integral.

Misalkan D suatu daerah integral yang memiliki fungsi $\nu : D \setminus \{0\} \to \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ yang memenuhi syarat-syarat berikut.

1. Jika a dan b merupakan elemen tak nol dalam D, maka $\nu(a) \leq \nu(ab)$.
2. Misalkan $a, b \in D$ dan andaikan bahwa $b \neq 0$. Maka terdapat elemen-elemen $q, r \in D$ sedemikian sehingga $a = bq + r$ dan berlaku $r = 0$ atau $\nu(r) < \nu(b)$.

Maka D disebut **domain Euklides** dan ν disebut **valuasi Euklides**.

Contoh 18.2.11 Nilai mutlak pada $\mathbb{Z}$ merupakan valuasi Euklides. ▲

Contoh 18.2.12 Misalkan F suatu lapangan. Maka derajat polinomial dalam $F[x]$ merupakan valuasi Euklides. ▲

Contoh 18.2.13 Ingat bahwa bilangan bulat Gaussian dalam Contoh 16.2.1 dari Bab 16 didefinisikan oleh

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Biasanya kita mengukur besar bilangan kompleks $a+bi$ dengan nilai mutlaknya, $|a+bi| = \sqrt{a^2 + b^2}$; tetapi, $\sqrt{a^2 + b^2}$ belum tentu bilangan bulat. Untuk valuasi kita, kita ambil $\nu(a + bi) = a^2 + b^2$ agar hasilnya merupakan bilangan bulat.

Kita mengklaim bahwa $\nu(a + bi) = a^2 + b^2$ merupakan valuasi Euklides pada $\mathbb{Z}[i]$. Misalkan $z, w \in \mathbb{Z}[i]$. Maka $\nu(zw) = |zw|^2 = |z|^2|w|^2 = \nu(z)\nu(w)$. Karena $\nu(z) \geq 1$ untuk setiap $z \in \mathbb{Z}[i]$ yang tak nol, $\nu(z) \leq \nu(z)\nu(w)$.

Selanjutnya, kita harus menunjukkan bahwa untuk sebarang $z = a + bi$ dan $w = c + di$ dalam $\mathbb{Z}[i]$ dengan $w \neq 0$, terdapat elemen q dan r dalam $\mathbb{Z}[i]$ sedemikian sehingga $z = qw + r$ dengan $r = 0$ atau $\nu(r) < \nu(w)$. Kita dapat memandang z dan w sebagai elemen-elemen dalam $\mathbb{Q}(i) = \{p + qi : p, q \in \mathbb{Q}\}$, yaitu lapangan pecahan dari $\mathbb{Z}[i]$. Perhatikan bahwa

$$\begin{aligned} zw^{-1} &= (a + bi)\frac{c - di}{c^2 + d^2} \\ &= \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}\,i \\ &= \left(m_1 + \frac{n_1}{c^2 + d^2}\right) + \left(m_2 + \frac{n_2}{c^2 + d^2}\right) i \end{aligned}$$

$$= (m_1 + m_2 i) + \left(\frac{n_1}{c^2 + d^2} + \frac{n_2}{c^2 + d^2} i \right)$$
$$= (m_1 + m_2 i) + (s + ti)$$

dalam $\mathbb{Q}(i)$. Pada langkah-langkah terakhir, kita menulis bagian riil dan imajiner sebagai bilangan bulat ditambah pecahan sejati. Artinya, kita mengambil bilangan bulat terdekat m_i sedemikian sehingga bagian pecahannya memenuhi $|n_i/(a^2 + b^2)| \leq 1/2$. Sebagai contoh, kita menulis

$$\frac{9}{8} = 1 + \frac{1}{8}$$
$$\frac{15}{8} = 2 - \frac{1}{8}.$$

Dengan demikian, s dan t merupakan "bagian pecahan" dari $zw^{-1} = (m_1 + m_2 i) + (s + ti)$. Kita juga mengetahui bahwa $s^2 + t^2 \leq 1/4 + 1/4 = 1/2$. Dengan mengalikan oleh w, kita memperoleh

$$z = zw^{-1}w = w(m_1 + m_2 i) + w(s + ti) = qw + r,$$

dengan $q = m_1 + m_2 i$ dan $r = w(s + ti)$. Karena z dan qw berada dalam $\mathbb{Z}[i]$, r harus berada dalam $\mathbb{Z}[i]$. Terakhir, kita perlu menunjukkan bahwa $r = 0$ atau $\nu(r) < \nu(w)$. Memang,

$$\nu(r) = \nu(w)\nu(s + ti) \leq \frac{1}{2}\nu(w) < \nu(w).$$

▲

Teorema 18.2.14 *Setiap domain Euklides merupakan domain ideal utama.*

BUKTI. Misalkan D suatu domain Euklides dan misalkan ν suatu valuasi Euklides pada D. Andaikan I merupakan ideal tak trivial dalam D dan pilih elemen tak nol $b \in I$ sedemikian sehingga $\nu(b)$ minimal bagi semua $a \in I$. Karena D merupakan domain Euklides, terdapat elemen q dan r dalam D sedemikian sehingga $a = bq + r$ dan berlaku $r = 0$ atau $\nu(r) < \nu(b)$. Namun, $r = a - bq$ berada dalam I karena I merupakan ideal; oleh karena itu, $r = 0$ berdasarkan keminimalan b. Akibatnya, $a = bq$ dan $I = \langle b \rangle$. ■

Korolari 18.2.15 *Setiap domain Euklides merupakan domain faktorisasi tunggal.*

18.2.3 Faktorisasi dalam $D[x]$

Salah satu gelanggang polinomial terpenting adalah $\mathbb{Z}[x]$. Salah satu pertanyaan pertama yang muncul mengenai $\mathbb{Z}[x]$ adalah apakah gelanggang tersebut merupakan UFD. Di sini kita akan membuktikan pernyataan yang lebih umum. Tugas pertama kita adalah memperoleh versi yang lebih umum dari Lema Gauss (Teorema 17.3.4).

Misalkan D suatu domain faktorisasi tunggal dan andaikan bahwa

$$p(x) = a_n x^n + \cdots + a_1 x + a_0$$

dalam $D[x]$. Maka **konten** dari $p(x)$ adalah faktor persekutuan terbesar dari $a_0, \ldots, a_n$. Kita mengatakan bahwa $p(x)$ **primitif** jika $\gcd(a_0, \ldots, a_n) = 1$.

Contoh 18.2.16 Dalam $\mathbb{Z}[x]$, polinomial $p(x) = 5x^4 - 3x^3 + x - 4$ merupakan polinomial primitif karena faktor persekutuan terbesar koefisien-koefisiennya adalah 1; tetapi, polinomial $q(x) = 4x^2 - 6x + 8$ tidak primitif karena konten

$q(x)$ adalah 2. ▲

Teorema 18.2.17 Lema Gauss. *Misalkan D suatu UFD dan misalkan $f(x)$ serta $g(x)$ polinomial primitif dalam $D[x]$. Maka $f(x)g(x)$ primitif.*

BUKTI. Misalkan $f(x) = \sum_{i=0}^{m} a_i x^i$ dan $g(x) = \sum_{i=0}^{n} b_i x^i$. Andaikan p suatu prima yang membagi koefisien-koefisien $f(x)g(x)$. Misalkan r bilangan bulat terkecil sedemikian sehingga $p \nmid a_r$ dan s bilangan bulat terkecil sedemikian sehingga $p \nmid b_s$. Koefisien x^{r+s} dalam $f(x)g(x)$ adalah

$$c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r+s-1} b_1 + a_{r+s} b_0.$$

Karena p membagi $a_0, \ldots, a_{r-1}$ dan $b_0, \ldots, b_{s-1}$, p membagi setiap suku c_{r+s} kecuali suku $a_r b_s$. Namun, karena $p \mid c_{r+s}$, p membagi a_r atau p membagi b_s. Ini mustahil. ■

Lema 18.2.18 *Misalkan D suatu UFD, dan misalkan $p(x)$ serta $q(x)$ berada dalam $D[x]$. Maka konten $p(x)q(x)$ sama dengan hasil kali konten $p(x)$ dan konten $q(x)$.*

BUKTI. Misalkan $p(x) = cp_1(x)$ dan $q(x) = dq_1(x)$, dengan c dan d masing-masing merupakan konten $p(x)$ dan $q(x)$. Maka $p_1(x)$ dan $q_1(x)$ primitif. Sekarang kita dapat menulis $p(x)q(x) = cdp_1(x)q_1(x)$. Karena $p_1(x)q_1(x)$ primitif, konten $p(x)q(x)$ haruslah cd. ■

Lema 18.2.19 *Misalkan D suatu UFD dan F lapangan pecahannya. Andaikan bahwa $p(x) \in D[x]$ dan $p(x) = f(x)g(x)$, dengan $f(x)$ serta $g(x)$ berada dalam $F[x]$. Maka $p(x) = f_1(x)g_1(x)$, dengan $f_1(x)$ serta $g_1(x)$ berada dalam $D[x]$. Lebih lanjut, $\deg f(x) = \deg f_1(x)$ dan $\deg g(x) = \deg g_1(x)$.*

BUKTI. Misalkan a dan b elemen tak nol dari D sedemikian sehingga $af(x), bg(x)$ berada dalam $D[x]$. Kita dapat menemukan $a_1, b_1 \in D$ sedemikian sehingga $af(x) = a_1 f_1(x)$ dan $bg(x) = b_1 g_1(x)$, dengan $f_1(x)$ dan $g_1(x)$ merupakan polinomial primitif dalam $D[x]$. Oleh karena itu, $abp(x) = (a_1 f_1(x))(b_1 g_1(x))$. Karena $f_1(x)$ dan $g_1(x)$ merupakan polinomial primitif, menurut Lema Gauss harus berlaku $ab \mid a_1 b_1$. Dengan demikian terdapat $c \in D$ sedemikian sehingga $p(x) = cf_1(x)g_1(x)$. Jelas bahwa $\deg f(x) = \deg f_1(x)$ dan $\deg g(x) = \deg g_1(x)$. ■

Korolari-korolari berikut merupakan akibat langsung dari Lema 18.2.19.

Korolari 18.2.20 *Misalkan D suatu UFD dan F lapangan pecahannya. Polinomial primitif $p(x)$ dalam $D[x]$ tak tereduksi dalam $F[x]$ jika dan hanya jika polinomial tersebut tak tereduksi dalam $D[x]$.*

Korolari 18.2.21 *Misalkan D suatu UFD dan F lapangan pecahannya. Jika $p(x)$ merupakan polinomial monik dalam $D[x]$ dengan $p(x) = f(x)g(x)$ dalam $F[x]$, maka $p(x) = f_1(x)g_1(x)$, dengan $f_1(x)$ serta $g_1(x)$ berada dalam $D[x]$. Lebih lanjut, $\deg f(x) = \deg f_1(x)$ dan $\deg g(x) = \deg g_1(x)$.*

Teorema 18.2.22 *Jika D merupakan UFD, maka $D[x]$ merupakan UFD.*

BUKTI. Misalkan $p(x)$ suatu polinomial tak nol dalam $D[x]$. Jika $p(x)$ merupakan polinomial konstan, maka polinomial itu harus mempunyai faktorisasi tunggal karena D merupakan UFD. Sekarang andaikan bahwa $p(x)$ merupakan polinomial berderajat positif dalam $D[x]$. Misalkan F lapangan pecahan dari D, dan ambil $p(x) = f_1(x)f_2(x)\cdots f_n(x)$ dari suatu faktorisasi $p(x)$, dengan setiap $f_i(x)$ tak tereduksi. Pilih $a_i \in D$ sedemikian sehingga $a_i f_i(x)$ berada dalam $D[x]$. Terdapat $b_1, \ldots, b_n \in D$ sedemikian sehingga $a_i f_i(x) = b_i g_i(x)$, dengan $g_i(x)$ suatu polinomial primitif dalam $D[x]$. Menurut Korolari 18.2.20,

setiap $g_i(x)$ tak tereduksi dalam $D[x]$. Akibatnya, kita dapat menulis

$$a_1 \cdots a_n p(x) = b_1 \cdots b_n g_1(x) \cdots g_n(x).$$

Misalkan $b = b_1 \cdots b_n$. Karena $g_1(x) \cdots g_n(x)$ primitif, $a_1 \cdots a_n$ membagi b. Oleh karena itu, $p(x) = a g_1(x) \cdots g_n(x)$, dengan $a \in D$. Karena D merupakan UFD, kita dapat memfaktorkan a sebagai $uc_1 \cdots c_k$, dengan u suatu unit dan setiap c_i tak tereduksi dalam D.

Sekarang kita akan menunjukkan ketunggalan faktorisasi ini. Misalkan

$$p(x) = a_1 \cdots a_m f_1(x) \cdots f_n(x) = b_1 \cdots b_r g_1(x) \cdots g_s(x)$$

merupakan dua faktorisasi $p(x)$, dengan semua faktornya tak tereduksi dalam $D[x]$. Menurut Korolari 18.2.20, setiap f_i dan g_i tak tereduksi dalam $F[x]$. Elemen-elemen a_i dan b_i merupakan unit dalam F. Karena $F[x]$ merupakan PID, gelanggang tersebut merupakan UFD; oleh karena itu, $n = s$. Sekarang susun ulang $g_i(x)$ sedemikian sehingga $f_i(x)$ dan $g_i(x)$ sekawan untuk $i = 1, \ldots, n$. Maka terdapat $c_1, \ldots, c_n$ dan $d_1, \ldots, d_n$ dalam D sedemikian sehingga $(c_i/d_i) f_i(x) = g_i(x)$ atau $c_i f_i(x) = d_i g_i(x)$. Polinomial $f_i(x)$ dan $g_i(x)$ primitif; jadi, c_i dan d_i sekawan dalam D. Dengan demikian, $a_1 \cdots a_m = u b_1 \cdots b_r$ dalam D, dengan u suatu unit dalam D. Karena D merupakan domain faktorisasi tunggal, $m = s$. Terakhir, kita dapat menyusun ulang b_i sedemikian sehingga a_i dan b_i sekawan untuk setiap i. Ini menyelesaikan bagian ketunggalan dari bukti. ■

Teorema yang baru saja kita buktikan mempunyai beberapa korolari yang jelas tetapi penting.

Korolari 18.2.23 *Misalkan F suatu lapangan. Maka $F[x]$ merupakan UFD.*

Korolari 18.2.24 *Gelanggang polinomial di atas bilangan bulat, $\mathbb{Z}[x]$, merupakan UFD.*

Korolari 18.2.25 *Misalkan D suatu UFD. Maka $D[x_1, \ldots, x_n]$ merupakan UFD.*

Catatan 18.2.26 Penting diperhatikan bahwa setiap domain Euklides merupakan PID dan setiap PID merupakan UFD. Akan tetapi, kebalikan setiap pernyataan tersebut tidak berlaku. Terdapat domain ideal utama yang bukan domain Euklides, dan terdapat domain faktorisasi tunggal yang bukan domain ideal utama ($\mathbb{Z}[x]$).

Catatan Sejarah

Karl Friedrich Gauss, lahir di Brunswick, Jerman, pada 30 April 1777, dianggap sebagai salah satu matematikawan terbesar sepanjang masa. Gauss benar-benar anak ajaib. Pada usia tiga tahun ia mampu menemukan kesalahan dalam pembukuan usaha ayahnya. Gauss masuk perguruan tinggi pada usia 15 tahun. Sebelum berusia 20 tahun, Gauss mampu mengonstruksi poligon beraturan bersisi 17 dengan penggaris dan jangka. Ini merupakan konstruksi baru pertama untuk poligon beraturan bersisi n sejak zaman Yunani kuno. Gauss berhasil menunjukkan bahwa jika $N = 2^{2^n} + 1$ prima, maka poligon beraturan bersisi N dapat dikonstruksi.

Gauss memperoleh gelar Ph.D. pada tahun 1799 di bawah bimbingan Pfaff di Universitas Helmstedt. Dalam disertasinya, ia memberikan bukti lengkap pertama Teorema Dasar Aljabar, yang menyatakan bahwa setiap polinomial berkoefisien riil dapat difaktorkan menjadi faktor-faktor linear di atas bilangan kompleks. Penerimaan terhadap bilangan kompleks didorong oleh Gauss, yang

merupakan orang pertama yang menggunakan notasi i untuk $\sqrt{-1}$.
Gauss kemudian mengalihkan perhatiannya pada teori bilangan; pada tahun 1801, ia menerbitkan bukunya yang terkenal tentang teori bilangan, *Disquisitiones Arithmeticae*. Sepanjang hidupnya, Gauss terpikat oleh cabang matematika ini. Ia pernah menulis, "Matematika adalah ratu ilmu pengetahuan, dan teori bilangan adalah ratu matematika."
Pada tahun 1807, Gauss diangkat sebagai direktur Observatorium Universitas Göttingen, jabatan yang dipegangnya hingga meninggal. Jabatan ini mengharuskannya mempelajari penerapan matematika dalam ilmu pengetahuan. Ia berhasil memberikan sumbangsih pada bidang-bidang seperti astronomi, mekanika, optika, geodesi, dan magnetisme. Bersama Wilhelm Weber, ia turut menciptakan telegraf listrik praktis pertama beberapa tahun sebelum Samuel F. B. Morse menciptakan versi yang lebih baik.
Gauss jelas merupakan matematikawan paling terkemuka di dunia pada awal abad kesembilan belas. Statusnya secara alami membuat penemuan-penemuannya diperiksa dengan sangat cermat. Kepribadian Gauss yang dingin dan menjaga jarak sering kali membuatnya mengabaikan karya orang-orang sezamannya, sehingga ia mempunyai banyak musuh. Ia tidak terlalu menyukai mengajar, dan matematikawan muda yang mendatanginya untuk mencari dukungan sering kali ditolak. Meskipun demikian, ia mempunyai banyak mahasiswa yang luar biasa, termasuk Eisenstein, Riemann, Kummer, Dirichlet, dan Dedekind. Gauss juga memberikan banyak dukungan kepada Sophie Germain (1776–1831), yang mengatasi berbagai rintangan yang dihadapi perempuan pada masanya untuk menjadi matematikawan yang sangat terkemuka. Gauss meninggal pada usia 78 tahun di Göttingen pada 23 Februari 1855.

18.3 Pertanyaan Bacaan

1. Daerah integral merupakan abstraksi dari dua gelanggang dasar apa yang telah kita pelajari?

2. Apa saja jenis daerah integral yang didefinisikan dalam bagian ini?

3. Lapangan pecahan suatu gelanggang mengabstraksikan gagasan apa dari matematika dasar?

4. Dalam bab sebelumnya terdapat teorema tentang polinomial tak tereduksi yang membangkitkan ideal maksimal. Teorema mana dalam bab ini yang memperumum hasil tersebut?

5. Uraikan sebuah contoh yang merupakan UFD, tetapi bukan PID.

18.4 Latihan

1. Misalkan $z = a + b\sqrt{3}\,i$ berada dalam $\mathbb{Z}[\sqrt{3}\,i]$. Jika $a^2 + 3b^2 = 1$, tunjukkan bahwa z harus merupakan unit. Tunjukkan bahwa satu-satunya unit dalam $\mathbb{Z}[\sqrt{3}\,i]$ adalah 1 dan -1.

Petunjuk. Perhatikan bahwa $z^{-1} = 1/(a + b\sqrt{3}\,i) = (a - b\sqrt{3}\,i)/(a^2 + 3b^2)$ berada dalam $\mathbb{Z}[\sqrt{3}\,i]$ jika dan hanya jika $a^2 + 3b^2 = 1$. Satu-satunya solusi bilangan bulat untuk persamaan tersebut adalah $a = \pm 1, b = 0$.

2. Bilangan bulat Gaussian, $\mathbb{Z}[i]$, membentuk UFD. Faktorkan setiap elemen berikut dalam $\mathbb{Z}[i]$ menjadi hasil kali elemen-elemen tak tereduksi.

(a) 5

(b) $1 + 3i$

(c) $6 + 8i$

(d) 2

Petunjuk. (a) $5 = -i(1+2i)(2+i)$; (c) $6+8i = -i(1+i)^2(2+i)^2$.

3. Misalkan D suatu daerah integral.

(a) Buktikan bahwa F_D merupakan grup abelian di bawah operasi penjumlahan.

(b) Tunjukkan bahwa operasi perkalian terdefinisi dengan baik dalam lapangan pecahan, F_D.

(c) Verifikasikan sifat asosiatif dan komutatif perkalian dalam F_D.

4. Buktikan atau bantah: Setiap subgelanggang dari lapangan F yang memuat 1 merupakan daerah integral.

Petunjuk. Benar.

5. Buktikan atau bantah: Jika D merupakan daerah integral, maka setiap elemen prima dalam D juga tak tereduksi dalam D.

6. Misalkan F suatu lapangan berkarakteristik nol. Buktikan bahwa F memuat sublapangan yang isomorfik dengan $\mathbb{Q}$.

7. Misalkan F suatu lapangan.

(a) Buktikan bahwa lapangan pecahan dari $F[x]$, yang dinyatakan dengan $F(x)$, isomorfik dengan himpunan semua ekspresi rasional $p(x)/q(x)$, dengan $q(x)$ bukan polinomial nol.

(b) Misalkan $p(x_1, \ldots, x_n)$ dan $q(x_1, \ldots, x_n)$ merupakan polinomial dalam $F[x_1, \ldots, x_n]$. Tunjukkan bahwa himpunan semua ekspresi rasional $p(x_1, \ldots, x_n)/q(x_1, \ldots, x_n)$ isomorfik dengan lapangan pecahan dari $F[x_1, \ldots, x_n]$. Kita menyatakan lapangan pecahan dari $F[x_1, \ldots, x_n]$ dengan $F(x_1, \ldots, x_n)$.

8. Misalkan p prima dan nyatakan lapangan pecahan dari $\mathbb{Z}_p[x]$ dengan $\mathbb{Z}_p(x)$. Buktikan bahwa $\mathbb{Z}_p(x)$ merupakan lapangan tak hingga berkarakteristik p.

9. Buktikan bahwa lapangan pecahan dari bilangan bulat Gaussian, $\mathbb{Z}[i]$, adalah

$$\mathbb{Q}(i) = \{p + qi : p, q \in \mathbb{Q}\}.$$

Petunjuk. Misalkan $z = a + bi$ dan $w = c + di \neq 0$ berada dalam $\mathbb{Z}[i]$. Buktikan bahwa $z/w \in \mathbb{Q}(i)$.

10. Lapangan F disebut **lapangan prima** jika tidak mempunyai sublapangan sejati. Jika E merupakan sublapangan dari F dan E merupakan lapangan prima, maka E merupakan **sublapangan prima** dari F.

(a) Buktikan bahwa setiap lapangan memuat sublapangan prima yang tunggal.

(b) Jika F merupakan lapangan berkarakteristik nol, buktikan bahwa sublapangan prima dari F isomorfik dengan lapangan bilangan rasional, $\mathbb{Q}$.

(c) Jika F merupakan lapangan berkarakteristik p, buktikan bahwa sublapangan prima dari F isomorfik dengan $\mathbb{Z}_p$.

11. Misalkan $\mathbb{Z}[\sqrt{2}\,] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.

(a) Buktikan bahwa $\mathbb{Z}[\sqrt{2}\,]$ merupakan daerah integral.

(b) Tentukan semua unit dalam $\mathbb{Z}[\sqrt{2}\,]$.

(c) Tentukan lapangan pecahan dari $\mathbb{Z}[\sqrt{2}\,]$.

(d) Buktikan bahwa $\mathbb{Z}[\sqrt{2}i]$ merupakan domain Euklides di bawah valuasi Euklides $\nu(a + b\sqrt{2}\,i) = a^2 + 2b^2$.

12. Misalkan D suatu UFD. Elemen $d \in D$ merupakan **faktor persekutuan terbesar dari** a **dan** b **dalam** D jika $d \mid a$ dan $d \mid b$, serta d dapat dibagi oleh setiap elemen lain yang membagi a dan b.

(a) Jika D merupakan PID dan a serta b keduanya merupakan elemen tak nol dari D, buktikan bahwa terdapat faktor persekutuan terbesar dari a dan b yang tunggal hingga kesekawanan. Artinya, jika d dan d' keduanya merupakan faktor persekutuan terbesar dari a dan b, maka d dan d' sekawan. Kita menulis $\gcd(a, b)$ untuk faktor persekutuan terbesar dari a dan b.

(b) Misalkan D suatu PID serta a dan b elemen tak nol dari D. Buktikan bahwa terdapat elemen s dan t dalam D sedemikian sehingga $\gcd(a, b) = as + bt$.

13. Misalkan D suatu daerah integral. Definisikan suatu relasi pada D dengan $a \sim b$ jika a dan b sekawan dalam D. Buktikan bahwa $\sim$ merupakan relasi ekuivalensi pada D.

14. Misalkan D suatu domain Euklides dengan valuasi Euklides ν. Jika u merupakan unit dalam D, tunjukkan bahwa $\nu(u) = \nu(1)$.

15. Misalkan D suatu domain Euklides dengan valuasi Euklides ν. Jika a dan b sekawan dalam D, buktikan bahwa $\nu(a) = \nu(b)$.

Petunjuk. Misalkan $a = ub$ dengan u suatu unit. Maka $\nu(b) \leq \nu(ub) \leq \nu(a)$. Demikian pula, $\nu(a) \leq \nu(b)$.

16. Tunjukkan bahwa $\mathbb{Z}[\sqrt{5}\,i]$ bukan domain faktorisasi tunggal.

Petunjuk. Tunjukkan bahwa 21 dapat difaktorkan dengan dua cara berbeda.

17. Buktikan atau bantah: Setiap subdomain dari UFD juga merupakan UFD.

18. Suatu ideal dari gelanggang komutatif R dikatakan **dibangkitkan secara hingga** jika terdapat elemen-elemen $a_1, \ldots, a_n$ dalam R sedemikian sehingga setiap elemen r dalam ideal tersebut dapat ditulis sebagai $a_1r_1 + \cdots + a_nr_n$ untuk suatu $r_1, \ldots, r_n$ dalam R. Buktikan bahwa R memenuhi syarat rantai naik jika dan hanya jika setiap ideal dari R dibangkitkan secara hingga.

19. Misalkan D suatu daerah integral dengan rantai turun ideal $I_1 \supset I_2 \supset I_3 \supset \cdots$. Andaikan terdapat N sedemikian sehingga $I_k = I_N$ untuk semua $k \geq N$. Gelanggang yang memenuhi syarat ini dikatakan memenuhi **syarat rantai turun**, atau **DCC**. Gelanggang yang memenuhi DCC disebut **gelanggang Artinian**, menurut nama Emil Artin. Tunjukkan bahwa jika D memenuhi syarat rantai turun, maka domain tersebut harus memenuhi syarat rantai naik.

20. Misalkan R suatu gelanggang komutatif dengan identitas. Kita mendefinisikan **himpunan bagian multiplikatif** dari R sebagai himpunan bagian S sedemikian sehingga $1 \in S$ dan $ab \in S$ jika $a, b \in S$.

(a) Definisikan relasi $\sim$ pada $R \times S$ dengan $(a, s) \sim (a', s')$ jika terdapat $s^* \in S$ sedemikian sehingga $s^*(s'a - sa') = 0$. Tunjukkan bahwa $\sim$ merupakan relasi ekuivalensi pada $R \times S$.

(b) Misalkan a/s menyatakan kelas ekuivalensi dari $(a, s) \in R \times S$ dan

misalkan $S^{-1}R$ himpunan semua kelas ekuivalensi terhadap $\sim$. Definisikan operasi penjumlahan dan perkalian pada $S^{-1}R$ dengan

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$
$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st},$$

secara berturut-turut. Buktikan bahwa operasi-operasi ini terdefinisi dengan baik pada $S^{-1}R$ dan bahwa $S^{-1}R$ merupakan gelanggang dengan identitas di bawah operasi-operasi tersebut. Gelanggang $S^{-1}R$ disebut **gelanggang hasil bagi** dari R terhadap S.

(c) Tunjukkan bahwa pemetaan $\psi : R \to S^{-1}R$ yang didefinisikan oleh $\psi(a) = a/1$ merupakan homomorfisma gelanggang.

(d) Jika R tidak mempunyai pembagi nol dan $0 \notin S$, tunjukkan bahwa ψ satu-ke-satu.

(e) Buktikan bahwa P merupakan ideal prima dari R jika dan hanya jika $S = R \setminus P$ merupakan himpunan bagian multiplikatif dari R.

(f) Jika P merupakan ideal prima dari R dan $S = R \setminus P$, tunjukkan bahwa gelanggang hasil bagi $S^{-1}R$ mempunyai ideal maksimal yang tunggal. Setiap gelanggang yang mempunyai ideal maksimal tunggal disebut **gelanggang lokal**.

18.5 Referensi dan Bacaan yang Disarankan

[1] Atiyah, M. F. and MacDonald, I. G. *Introduction to Commutative Algebra.* Westview Press, Boulder, CO, 1994.

[2] Zariski, O. and Samuel, P. *Commutative Algebra*, vols. I and II. Springer, New York, 1975, 1960.

19

Latis dan Aljabar Boolean

Aksioma gelanggang memberi struktur pada operasi penjumlahan dan perkalian dalam suatu himpunan. Namun, kita dapat membangun struktur aljabar yang dikenal sebagai latis dan aljabar Boolean, yang memperumum jenis operasi lainnya. Sebagai contoh, operasi penting pada himpunan adalah inklusi, gabungan, dan irisan. Latis merupakan perumuman relasi urutan pada ruang aljabar, seperti inklusi himpunan dalam teori himpunan dan pertidaksamaan dalam sistem bilangan yang telah dikenal, yaitu $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, dan $\mathbb{R}$. Aljabar Boolean memperumum operasi irisan dan gabungan. Latis dan aljabar Boolean diterapkan dalam logika, teori rangkaian, dan peluang.

19.1 Latis

19.1.1 Himpunan Terurut Parsial

Kita memulai kajian latis dan aljabar Boolean dengan memperumum gagasan pertidaksamaan. Ingat bahwa **relasi** pada himpunan X merupakan himpunan bagian dari $X \times X$. Relasi P pada X disebut **urutan parsial** pada X jika memenuhi aksioma-aksioma berikut.

1. Relasi tersebut **refleksif**: $(a, a) \in P$ untuk setiap $a \in X$.
2. Relasi tersebut **antisimetris**: jika $(a, b) \in P$ dan $(b, a) \in P$, maka $a = b$.
3. Relasi tersebut **transitif**: jika $(a, b) \in P$ dan $(b, c) \in P$, maka $(a, c) \in P$.

Biasanya kita menulis $a \preceq b$ untuk menyatakan $(a, b) \in P$, kecuali jika suatu lambang secara alami berkaitan dengan urutan parsial tertentu, seperti $a \leq b$ untuk bilangan bulat a dan b, atau $A \subset B$ untuk himpunan A dan B. Himpunan X bersama urutan parsial $\preceq$ disebut **himpunan terurut parsial**, atau **poset**.

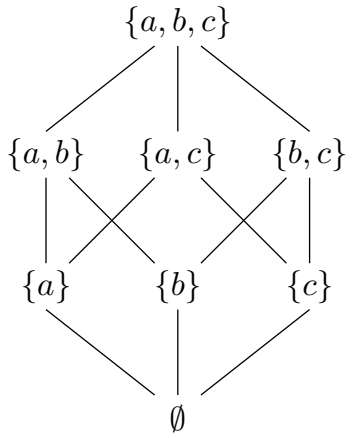
Contoh 19.1.1 Himpunan bilangan bulat (atau bilangan rasional maupun real) merupakan poset, dengan $a \leq b$ memiliki makna lazim bagi dua bilangan bulat a dan b dalam $\mathbb{Z}$. ▲

Contoh 19.1.2 Misalkan X sebarang himpunan. Kita mendefinisikan **himpunan kuasa** dari X sebagai himpunan semua himpunan bagian dari X. Himpunan kuasa dari X dinotasikan dengan $\mathcal{P}(X)$. Sebagai contoh, misalkan $X = \{a, b, c\}$. Maka $\mathcal{P}(X)$ merupakan himpunan semua himpunan bagian dari

$\{a, b, c\}$:

$$\begin{array}{llll} \emptyset & \{a\} & \{b\} & \{c\} \\ \{a, b\} & \{a, c\} & \{b, c\} & \{a, b, c\}. \end{array}$$

Pada himpunan kuasa dari sebarang himpunan X, inklusi himpunan, $\subset$, merupakan urutan parsial. Kita dapat merepresentasikan urutan pada $\{a, b, c\}$ secara skematis dengan diagram seperti pada Gambar 19.1.3. ▲

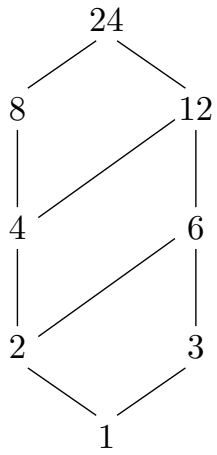


Gambar 19.1.3 Urutan parsial pada $\mathcal{P}(\{a, b, c\})$

Contoh 19.1.4 Misalkan G suatu grup. Himpunan subgrup dari G merupakan poset, dengan inklusi himpunan sebagai urutan parsialnya. ▲

Contoh 19.1.5 Pada suatu himpunan tertentu dapat terdapat lebih dari satu urutan parsial. Kita dapat membentuk urutan parsial pada $\mathbb{N}$ dengan menetapkan $a \preceq b$ jika $a \mid b$. Relasi ini jelas refleksif karena $a \mid a$ untuk setiap $a \in \mathbb{N}$. Jika $m \mid n$ dan $n \mid m$, maka $m = n$; jadi, relasi tersebut juga antisimetris. Relasi ini transitif, sebab jika $m \mid n$ dan $n \mid p$, maka $m \mid p$. ▲

Contoh 19.1.6 Misalkan $X = \{1, 2, 3, 4, 6, 8, 12, 24\}$ adalah himpunan pembagi 24 dengan urutan parsial yang didefinisikan dalam Contoh 19.1.5. Gambar 19.1.7 memperlihatkan urutan parsial pada X. ▲



Gambar 19.1.7 Urutan parsial pada pembagi 24

Misalkan Y himpunan bagian dari poset X. Elemen u dalam X disebut **batas atas** dari Y jika $a \preceq u$ untuk setiap elemen $a \in Y$. Jika u merupakan

batas atas dari Y sedemikian sehingga $u \preceq v$ untuk setiap batas atas lain v dari Y, maka u disebut **batas atas terkecil** atau **supremum** dari Y. Elemen l dalam X disebut **batas bawah** dari Y jika $l \preceq a$ untuk setiap $a \in Y$. Jika l merupakan batas bawah dari Y sedemikian sehingga $k \preceq l$ untuk setiap batas bawah lain k dari Y, maka l disebut **batas bawah terbesar** atau **infimum** dari Y.

Contoh 19.1.8 Misalkan $Y = \{2, 3, 4, 6\}$ termuat dalam himpunan X pada Contoh 19.1.6. Maka Y memiliki batas atas 12 dan 24, dengan 12 sebagai batas atas terkecil. Satu-satunya batas bawah adalah 1; jadi, elemen ini harus menjadi batas bawah terbesar. ▲

Ternyata, batas atas terkecil dan batas bawah terbesar bersifat tunggal jika ada.

Teorema 19.1.9 *Misalkan Y himpunan bagian tak kosong dari poset X. Jika Y memiliki batas atas terkecil, maka Y memiliki batas atas terkecil yang tunggal. Jika Y memiliki batas bawah terbesar, maka Y memiliki batas bawah terbesar yang tunggal.*

BUKTI. Misalkan u_1 dan u_2 batas atas terkecil dari Y. Berdasarkan definisi batas atas terkecil, $u_1 \preceq u$ untuk setiap batas atas u dari Y. Secara khusus, $u_1 \preceq u_2$. Serupa dengan itu, $u_2 \preceq u_1$. Oleh karena itu, $u_1 = u_2$ berdasarkan antisimetri. Argumen serupa menunjukkan bahwa batas bawah terbesar bersifat tunggal. ■

Pada banyak poset, operasi biner dapat didefinisikan menggunakan batas bawah terbesar dan batas atas terkecil dari dua elemen. **Latis** adalah poset L sedemikian sehingga setiap pasangan elemen dalam L memiliki batas atas terkecil dan batas bawah terbesar. Batas atas terkecil dari $a, b \in L$ disebut **gabung** dari a dan b, serta dinotasikan dengan $a \vee b$. Batas bawah terbesar dari $a, b \in L$ disebut **temu** dari a dan b, serta dinotasikan dengan $a \wedge b$.

Contoh 19.1.10 Misalkan X suatu himpunan. Maka himpunan kuasa dari X, yaitu $\mathcal{P}(X)$, merupakan latis. Untuk dua himpunan A dan B dalam $\mathcal{P}(X)$, batas atas terkecil dari A dan B adalah $A \cup B$. Tentu saja, $A \cup B$ merupakan batas atas dari A dan B, sebab $A \subset A \cup B$ dan $B \subset A \cup B$. Jika C adalah himpunan lain yang memuat A maupun B, maka C harus memuat $A \cup B$; jadi, $A \cup B$ merupakan batas atas terkecil dari A dan B. Serupa dengan itu, batas bawah terbesar dari A dan B adalah $A \cap B$. ▲

Contoh 19.1.11 Misalkan G suatu grup dan andaikan X adalah himpunan subgrup dari G. Maka X merupakan poset yang diurutkan oleh inklusi himpunan, yaitu $\subset$. Himpunan subgrup dari G juga merupakan latis. Jika H dan K subgrup dari G, batas bawah terbesar dari H dan K adalah $H \cap K$. Himpunan $H \cup K$ belum tentu merupakan subgrup dari G. Sebagai latihan, tunjukkan bahwa batas atas terkecil dari H dan K adalah subgrup yang dibangkitkan oleh $H \cup K$. ▲

Dalam teori himpunan terdapat kondisi dualitas tertentu. Sebagai contoh, berdasarkan hukum De Morgan, setiap pernyataan tentang himpunan yang berlaku bagi $(A \cup B)'$ juga harus berlaku bagi $A' \cap B'$. Kita juga memiliki prinsip dualitas untuk latis.

Aksioma 19.1.12 Prinsip Dualitas. *Setiap pernyataan yang berlaku bagi semua latis tetap berlaku jika $\preceq$ diganti dengan $\succeq$, serta $\vee$ dan $\wedge$ dipertukarkan di seluruh pernyataan.*

Teorema berikut menyatakan bahwa latis merupakan struktur aljabar dengan dua operasi biner yang memenuhi aksioma tertentu.

Teorema 19.1.13 *Jika L suatu latis, maka operasi biner $\vee$ dan $\wedge$ memenuhi sifat-sifat berikut untuk $a, b, c \in L$.*

1. *Hukum komutatif: $a \vee b = b \vee a$ dan $a \wedge b = b \wedge a$.*
2. *Hukum asosiatif: $a \vee (b \vee c) = (a \vee b) \vee c$ dan $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.*
3. *Hukum idempoten: $a \vee a = a$ dan $a \wedge a = a$.*
4. *Hukum absorpsi: $a \vee (a \wedge b) = a$ dan $a \wedge (a \vee b) = a$.*

Bukti. Berdasarkan Prinsip Dualitas, kita hanya perlu membuktikan pernyataan pertama pada setiap bagian.

(1) Berdasarkan definisi, $a \vee b$ merupakan batas atas terkecil dari $\{a, b\}$, dan $b \vee a$ merupakan batas atas terkecil dari $\{b, a\}$; padahal, $\{a, b\} = \{b, a\}$.

(2) Kita akan menunjukkan bahwa $a \vee (b \vee c)$ dan $(a \vee b) \vee c$ keduanya merupakan batas atas terkecil dari $\{a, b, c\}$. Misalkan $d = a \vee b$. Maka $c \preceq d \vee c = (a \vee b) \vee c$. Kita juga mengetahui bahwa

$$a \preceq a \vee b = d \preceq d \vee c = (a \vee b) \vee c.$$

Argumen serupa menunjukkan bahwa $b \preceq (a \vee b) \vee c$. Oleh karena itu, $(a \vee b) \vee c$ merupakan batas atas dari $\{a, b, c\}$. Sekarang kita perlu menunjukkan bahwa $(a \vee b) \vee c$ merupakan batas atas terkecil dari $\{a, b, c\}$. Misalkan u batas atas lain dari $\{a, b, c\}$. Maka $a \preceq u$ dan $b \preceq u$; jadi, $d = a \vee b \preceq u$. Karena $c \preceq u$, diperoleh $(a \vee b) \vee c = d \vee c \preceq u$. Oleh karena itu, $(a \vee b) \vee c$ harus menjadi batas atas terkecil dari $\{a, b, c\}$. Argumen yang menunjukkan bahwa $a \vee (b \vee c)$ merupakan batas atas terkecil dari $\{a, b, c\}$ sama saja. Akibatnya, $a \vee (b \vee c) = (a \vee b) \vee c$.

(3) Gabung dari a dan a merupakan batas atas terkecil dari $\{a\}$; jadi, $a \vee a = a$.

(4) Misalkan $d = a \wedge b$. Maka $a \preceq a \vee d$. Di sisi lain, $d = a \wedge b \preceq a$, sehingga $a \vee d \preceq a$. Oleh karena itu, $a \vee (a \wedge b) = a$. ■

Diberikan sebarang himpunan L dengan operasi $\vee$ dan $\wedge$ yang memenuhi kondisi teorema sebelumnya, wajar untuk bertanya apakah himpunan ini berasal dari suatu latis. Teorema berikut menyatakan bahwa hal tersebut selalu berlaku.

Teorema 19.1.14 *Misalkan L himpunan tak kosong dengan dua operasi biner $\vee$ dan $\wedge$ yang memenuhi hukum komutatif, asosiatif, idempoten, dan absorpsi. Kita dapat mendefinisikan urutan parsial pada L dengan $a \preceq b$ jika $a \vee b = b$. Lebih lanjut, L merupakan latis terhadap $\preceq$ jika untuk setiap $a, b \in L$, kita mendefinisikan batas atas terkecil dan batas bawah terbesar dari a dan b masing-masing sebagai $a \vee b$ dan $a \wedge b$.*

Bukti. Pertama-tama kita menunjukkan bahwa L merupakan poset di bawah $\preceq$. Karena $a \vee a = a$, $a \preceq a$ dan $\preceq$ refleksif. Untuk menunjukkan bahwa $\preceq$ antisimetris, misalkan $a \preceq b$ dan $b \preceq a$. Maka $a \vee b = b$ dan $b \vee a = a$. Berdasarkan hukum komutatif, $b = a \vee b = b \vee a = a$. Terakhir, kita harus menunjukkan bahwa $\preceq$ transitif. Misalkan $a \preceq b$ dan $b \preceq c$. Maka $a \vee b = b$ dan $b \vee c = c$. Jadi,

$$a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c,$$

atau $a \preceq c$.

Untuk menunjukkan bahwa L merupakan latis, kita harus membuktikan bahwa $a \vee b$ dan $a \wedge b$ masing-masing merupakan batas atas terkecil dan batas bawah terbesar dari a serta b. Karena $a = (a \vee b) \wedge a = a \wedge (a \vee b)$, diperoleh

$a \preceq a \vee b$. Serupa dengan itu, $b \preceq a \vee b$. Oleh karena itu, $a \vee b$ merupakan batas atas dari a dan b. Misalkan u sebarang batas atas lain dari a maupun b. Maka $a \preceq u$ dan $b \preceq u$. Namun, $a \vee b \preceq u$ karena

$$(a \vee b) \vee u = a \vee (b \vee u) = a \vee u = u.$$

Pembuktian bahwa $a \wedge b$ merupakan batas bawah terbesar dari a dan b diserahkan sebagai latihan. ■

19.2 Aljabar Boolean

Mari kita telaah lebih saksama contoh berupa himpunan kuasa $\mathcal{P}(X)$ dari suatu himpunan X. Himpunan kuasa merupakan latis yang terurut oleh inklusi. Berdasarkan definisi himpunan kuasa, unsur terbesar dalam $\mathcal{P}(X)$ adalah X sendiri dan unsur terkecilnya adalah $\emptyset$, yaitu himpunan kosong. Untuk sebarang himpunan A dalam $\mathcal{P}(X)$, kita mengetahui bahwa $A \cap X = A$ dan $A \cup \emptyset = A$. Hal ini mengarahkan kita pada definisi berikut untuk latis. Suatu unsur I dalam poset X disebut **unsur terbesar** jika $a \preceq I$ untuk semua $a \in X$. Suatu unsur O disebut **unsur terkecil** dari X jika $O \preceq a$ untuk semua $a \in X$.

Misalkan A berada dalam $\mathcal{P}(X)$. Ingat bahwa komplemen dari A adalah

$$A' = X \setminus A = \{x : x \in X \text{ dan } x \notin A\}.$$

Kita mengetahui bahwa $A \cup A' = X$ dan $A \cap A' = \emptyset$. Contoh ini dapat kita perumum untuk latis. Suatu latis L dengan unsur terbesar I dan unsur terkecil O disebut **berkomplemen** jika untuk setiap $a \in L$, terdapat a' sedemikian sehingga $a \vee a' = I$ dan $a \wedge a' = O$.

Dalam suatu latis L, operasi biner $\vee$ dan $\wedge$ memenuhi hukum komutatif dan asosiatif; namun, keduanya tidak selalu memenuhi hukum distributif

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c);$$

Akan tetapi, dalam $\mathcal{P}(X)$, hukum distributif terpenuhi karena

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

untuk $A, B, C \in \mathcal{P}(X)$. Kita menyebut suatu latis L **distributif** jika hukum distributif berikut berlaku:

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

untuk semua $a, b, c \in L$.

Teorema 19.2.1 *Suatu latis L bersifat distributif jika dan hanya jika*

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

untuk semua $a, b, c \in L$.

Bukti. Misalkan L merupakan latis distributif.

$$\begin{aligned} a \vee (b \wedge c) &= [a \vee (a \wedge c)] \vee (b \wedge c) \\ &= a \vee [(a \wedge c) \vee (b \wedge c)] \\ &= a \vee [(c \wedge a) \vee (c \wedge b)] \\ &= a \vee [c \wedge (a \vee b)] \\ &= a \vee [(a \vee b) \wedge c] \end{aligned}$$

$$\begin{aligned} &= [(a \vee b) \wedge a] \vee [(a \vee b) \wedge c] \\ &= (a \vee b) \wedge (a \vee c). \end{aligned}$$

Arah sebaliknya langsung mengikuti Prinsip Dualitas. ■

Aljabar Boolean adalah latis B dengan unsur terbesar I dan unsur terkecil O sedemikian sehingga B bersifat distributif sekaligus berkomplemen. Himpunan kuasa dari X, yaitu $\mathcal{P}(X)$, menjadi prototipe kita untuk aljabar Boolean. Ternyata, himpunan kuasa juga merupakan salah satu aljabar Boolean yang paling penting. Teorema berikut memungkinkan kita mencirikan aljabar Boolean melalui operasi biner $\vee$ dan $\wedge$ tanpa perlu menyebutkan bahwa aljabar Boolean merupakan poset.

Teorema 19.2.2 *Suatu himpunan B merupakan aljabar Boolean jika dan hanya jika terdapat operasi biner $\vee$ dan $\wedge$ pada B yang memenuhi aksioma-aksioma berikut.*

1. $a \vee b = b \vee a$ *dan* $a \wedge b = b \wedge a$ *untuk* $a, b \in B$.
2. $a \vee (b \vee c) = (a \vee b) \vee c$ *dan* $a \wedge (b \wedge c) = (a \wedge b) \wedge c$ *untuk* $a, b, c \in B$.
3. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ *dan* $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ *untuk* $a, b, c \in B$.
4. *Terdapat unsur* I *dan* O *sedemikian sehingga* $a \vee O = a$ *dan* $a \wedge I = a$ *untuk semua* $a \in B$.
5. *Untuk setiap* $a \in B$, *terdapat* $a' \in B$ *sedemikian sehingga* $a \vee a' = I$ *dan* $a \wedge a' = O$.

Bukti. Misalkan B suatu himpunan yang memenuhi (1)–(5) dalam teorema. Salah satu hukum idempoten terpenuhi karena

$$\begin{aligned} a &= a \vee O \\ &= a \vee (a \wedge a') \\ &= (a \vee a) \wedge (a \vee a') \\ &= (a \vee a) \wedge I \\ &= a \vee a. \end{aligned}$$

Perhatikan bahwa

$$I \vee b = (b \vee b') \vee b = (b' \vee b) \vee b = b' \vee (b \vee b) = b' \vee b = I.$$

Akibatnya, hukum pertama dari kedua hukum absorpsi berlaku, sebab

$$\begin{aligned} a \vee (a \wedge b) &= (a \wedge I) \vee (a \wedge b) \\ &= a \wedge (I \vee b) \\ &= a \wedge I \\ &= a. \end{aligned}$$

Hukum idempoten dan hukum absorpsi lainnya dibuktikan dengan cara serupa. Karena B juga memenuhi (1)–(3), syarat-syarat dalam Teorema 19.1.14 terpenuhi; oleh karena itu, B harus merupakan latis. Syarat (4) memberi tahu kita bahwa B merupakan latis distributif.

Untuk $a \in B$, berlaku $O \vee a = a$; dengan demikian, $O \preceq a$ dan O merupakan unsur terkecil dalam B. Untuk menunjukkan bahwa I merupakan unsur terbesar dalam B, terlebih dahulu kita akan menunjukkan bahwa $a \vee b = b$

ekuivalen dengan $a \wedge b = a$. Karena $a \vee I = a$ untuk semua $a \in B$, dengan menggunakan hukum absorpsi kita dapat menentukan bahwa

$$a \vee I = (a \wedge I) \vee I = I \vee (I \wedge a) = I$$

atau $a \preceq I$ untuk semua a dalam B. Akhirnya, karena berdasarkan (5) kita mengetahui bahwa B berkomplemen, B harus merupakan aljabar Boolean.

Sebaliknya, misalkan B merupakan aljabar Boolean. Misalkan I dan O masing-masing merupakan unsur terbesar dan terkecil dalam B. Jika kita mendefinisikan $a \vee b$ dan $a \wedge b$ sebagai batas atas terkecil dan batas bawah terbesar dari $\{a, b\}$, maka B merupakan aljabar Boolean berdasarkan Teorema 19.1.14, Teorema 19.2.1, dan hipotesis kita. ■

Banyak identitas lain berlaku dalam aljabar Boolean. Beberapa di antaranya dicantumkan dalam teorema berikut.

Teorema 19.2.3 *Misalkan B suatu aljabar Boolean. Maka*

1. *$a \vee I = I$ dan $a \wedge O = O$ untuk semua $a \in B$.*
2. *Jika $a \vee b = a \vee c$ dan $a \wedge b = a \wedge c$ untuk $a, b, c \in B$, maka $b = c$.*
3. *Jika $a \vee b = I$ dan $a \wedge b = O$, maka $b = a'$.*
4. *$(a')' = a$ untuk semua $a \in B$.*
5. *$I' = O$ dan $O' = I$.*
6. *$(a \vee b)' = a' \wedge b'$ dan $(a \wedge b)' = a' \vee b'$ (Hukum De Morgan).*

Bukti. Kita hanya akan membuktikan (2). Identitas-identitas lainnya diserahkan sebagai latihan. Untuk $a \vee b = a \vee c$ dan $a \wedge b = a \wedge c$, kita memperoleh

$$\begin{aligned}
b &= b \vee (b \wedge a) \\
&= b \vee (a \wedge b) \\
&= b \vee (a \wedge c) \\
&= (b \vee a) \wedge (b \vee c) \\
&= (a \vee b) \wedge (b \vee c) \\
&= (a \vee c) \wedge (b \vee c) \\
&= (c \vee a) \wedge (c \vee b) \\
&= c \vee (a \wedge b) \\
&= c \vee (a \wedge c) \\
&= c \vee (c \wedge a) \\
&= c.
\end{aligned}$$

■

19.2.1 Aljabar Boolean Hingga

Suatu aljabar Boolean disebut **aljabar Boolean hingga** jika sebagai himpunan ia memuat sejumlah hingga unsur. Aljabar Boolean hingga sangat menyenangkan untuk dipelajari karena kita dapat mengklasifikasikannya hingga isomorfisma.

Misalkan B dan C merupakan aljabar Boolean. Suatu pemetaan bijektif $\phi : B \to C$ disebut **isomorfisma** aljabar Boolean jika

$$\phi(a \vee b) = \phi(a) \vee \phi(b)$$

$$\phi(a \wedge b) = \phi(a) \wedge \phi(b)$$

untuk semua a dan b dalam B.

Kita akan menunjukkan bahwa setiap aljabar Boolean hingga isomorfik dengan aljabar Boolean yang diperoleh dengan mengambil himpunan kuasa dari suatu himpunan hingga X. Sebelum membuktikan hasil ini, kita memerlukan beberapa lema dan definisi. Misalkan B suatu aljabar Boolean hingga. Suatu unsur $a \in B$ disebut **atom** dari B jika $a \neq O$ dan $a \wedge b = a$ untuk semua $b \in B$ dengan $b \neq O$. Secara ekuivalen, a merupakan atom dari B jika tidak terdapat $b \in B$ dengan $b \neq O$ yang berbeda dari a sedemikian sehingga $O \preceq b \preceq a$.

Lema 19.2.4 *Misalkan B suatu aljabar Boolean hingga. Jika b merupakan unsur dari B dengan $b \neq O$, maka terdapat atom a dalam B sedemikian sehingga $a \preceq b$.*

Bukti. Jika b merupakan atom, ambil $a = b$. Jika tidak, pilih unsur b_1, yang tidak sama dengan O maupun b, sedemikian sehingga $b_1 \preceq b$. Pilihan ini dijamin mungkin karena b bukan atom. Jika b_1 merupakan atom, pembuktian selesai. Jika tidak, pilih b_2, yang tidak sama dengan O maupun b_1, sedemikian sehingga $b_2 \preceq b_1$. Sekali lagi, jika b_2 merupakan atom, ambil $a = b_2$. Dengan melanjutkan proses ini, kita memperoleh suatu rantai

$$O \preceq \cdots \preceq b_3 \preceq b_2 \preceq b_1 \preceq b.$$

Karena B merupakan aljabar Boolean hingga, rantai ini harus berhingga. Artinya, untuk suatu k, b_k merupakan atom. Ambil $a = b_k$. ■

Lema 19.2.5 *Misalkan a dan b merupakan atom dalam suatu aljabar Boolean hingga B dengan $a \neq b$. Maka $a \wedge b = O$.*

Bukti. Karena $a \wedge b$ merupakan batas bawah terbesar dari a dan b, kita mengetahui bahwa $a \wedge b \preceq a$. Oleh karena itu, $a \wedge b = a$ atau $a \wedge b = O$. Akan tetapi, jika $a \wedge b = a$, maka $a \preceq b$ atau $a = O$. Kedua kemungkinan tersebut menimbulkan kontradiksi karena a dan b sama-sama atom; dengan demikian, $a \wedge b = O$. ■

Lema 19.2.6 *Misalkan B suatu aljabar Boolean dan $a, b \in B$. Pernyataan-pernyataan berikut ekuivalen.*

1. $a \preceq b$.
2. $a \wedge b' = O$.
3. $a' \vee b = I$.

Bukti. (1) $\Rightarrow$ (2). Jika $a \preceq b$, maka $a \vee b = b$. Oleh karena itu,

$$\begin{aligned} a \wedge b' &= a \wedge (a \vee b)' \\ &= a \wedge (a' \wedge b') \\ &= (a \wedge a') \wedge b' \\ &= O \wedge b' \\ &= O. \end{aligned}$$

(2) $\Rightarrow$ (3). Jika $a \wedge b' = O$, maka $a' \vee b = (a \wedge b')' = O' = I$.
(3) $\Rightarrow$ (1). Jika $a' \vee b = I$, maka

$$\begin{aligned} a &= a \wedge (a' \vee b) \\ &= (a \wedge a') \vee (a \wedge b) \\ &= O \vee (a \wedge b) \end{aligned}$$

$$= a \wedge b.$$

Jadi, $a \preceq b$. ■

Lema 19.2.7 *Misalkan B suatu aljabar Boolean dan b serta c merupakan unsur dalam B sedemikian sehingga $b \not\preceq c$. Maka terdapat atom $a \in B$ sedemikian sehingga $a \preceq b$ dan $a \not\preceq c$.*

BUKTI. Berdasarkan Lema 19.2.6, $b \wedge c' \neq O$. Oleh karena itu, terdapat atom a sedemikian sehingga $a \preceq b \wedge c'$. Akibatnya, $a \preceq b$ dan $a \not\preceq c$. ■

Lema 19.2.8 *Misalkan $b \in B$ dan $a_1, \ldots, a_n$ merupakan atom-atom dari B sedemikian sehingga $a_i \preceq b$. Maka $b = a_1 \vee \cdots \vee a_n$. Selanjutnya, jika $a, a_1, \ldots, a_n$ merupakan atom-atom dari B sedemikian sehingga $a \preceq b$, $a_i \preceq b$, dan $b = a \vee a_1 \vee \cdots \vee a_n$, maka $a = a_i$ untuk suatu $i = 1, \ldots, n$.*

BUKTI. Ambil $b_1 = a_1 \vee \cdots \vee a_n$. Karena $a_i \preceq b$ untuk setiap i, kita mengetahui bahwa $b_1 \preceq b$. Jika kita dapat menunjukkan bahwa $b \preceq b_1$, maka lema ini benar berdasarkan antisimetrisitas. Andaikan $b \not\preceq b_1$. Maka terdapat atom a sedemikian sehingga $a \preceq b$ dan $a \not\preceq b_1$. Karena a merupakan atom dan $a \preceq b$, kita dapat menyimpulkan bahwa $a = a_i$ untuk suatu a_i. Namun, hal ini mustahil karena $a \preceq b_1$. Oleh karena itu, $b \preceq b_1$.

Sekarang misalkan $b = a_1 \vee \cdots \vee a_n$. Jika a merupakan atom yang lebih kecil dari b,

$$a = a \wedge b = a \wedge (a_1 \vee \cdots \vee a_n) = (a \wedge a_1) \vee \cdots \vee (a \wedge a_n).$$

Akan tetapi, setiap suku bernilai O atau a, dengan $a \wedge a_i$ muncul hanya untuk satu a_i. Jadi, berdasarkan Lema 19.2.5, $a = a_i$ untuk suatu i. ■

Teorema 19.2.9 *Misalkan B suatu aljabar Boolean hingga. Maka terdapat himpunan X sedemikian sehingga B isomorfik dengan $\mathcal{P}(X)$.*

BUKTI. Kita akan menunjukkan bahwa B isomorfik dengan $\mathcal{P}(X)$, dengan X sebagai himpunan atom-atom dari B. Misalkan $a \in B$. Berdasarkan Lema 19.2.8, kita dapat menuliskan a secara tunggal sebagai $a = a_1 \vee \cdots \vee a_n$ untuk $a_1, \ldots, a_n \in X$. Akibatnya, kita dapat mendefinisikan pemetaan $\phi : B \to \mathcal{P}(X)$ melalui

$$\phi(a) = \phi(a_1 \vee \cdots \vee a_n) = \{a_1, \ldots, a_n\}.$$

Jelas bahwa ϕ surjektif.

Sekarang misalkan $a = a_1 \vee \cdots \vee a_n$ dan $b = b_1 \vee \cdots \vee b_m$ merupakan unsur-unsur dalam B, dengan setiap a_i dan setiap b_i merupakan atom. Jika $\phi(a) = \phi(b)$, maka $\{a_1, \ldots, a_n\} = \{b_1, \ldots, b_m\}$ dan $a = b$. Akibatnya, ϕ injektif.

Gabung dari a dan b dipertahankan oleh ϕ karena

$$\begin{aligned}
\phi(a \vee b) &= \phi(a_1 \vee \cdots \vee a_n \vee b_1 \vee \cdots \vee b_m) \\
&= \{a_1, \ldots, a_n, b_1, \ldots, b_m\} \\
&= \{a_1, \ldots, a_n\} \cup \{b_1, \ldots, b_m\} \\
&= \phi(a_1 \vee \cdots \vee a_n) \cup \phi(b_1 \wedge \cdots \vee b_m) \\
&= \phi(a) \cup \phi(b).
\end{aligned}$$

Serupa dengan itu, $\phi(a \wedge b) = \phi(a) \cap \phi(b)$. ■

Pembuktian korolari berikut diserahkan sebagai latihan.

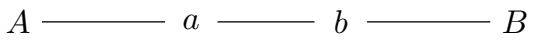
Korolari 19.2.10 *Orde setiap aljabar Boolean hingga harus berbentuk* 2^n *untuk suatu bilangan bulat positif* n.

19.3 Aljabar Rangkaian Listrik

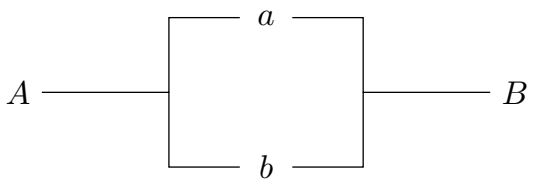
Kegunaan aljabar Boolean semakin tampak selama beberapa dasawarsa terakhir seiring perkembangan komputer modern. Desain rangkaian cip komputer dapat dinyatakan dalam aljabar Boolean. Dalam bagian ini kita akan mengembangkan aljabar Boolean untuk rangkaian listrik dan sakelar; namun, hasil-hasil ini dapat dengan mudah diperumum ke desain rangkaian terpadu komputer.

Sakelar adalah perangkat yang ditempatkan pada suatu titik dalam rangkaian listrik dan mengendalikan aliran arus melalui rangkaian tersebut. Setiap sakelar memiliki dua keadaan yang mungkin: sakelar dapat **terbuka** sehingga tidak mengizinkan arus melewati rangkaian, atau dapat **tertutup** sehingga mengizinkan arus mengalir. Kedua keadaan ini saling eksklusif. Kita mensyaratkan bahwa setiap sakelar berada dalam salah satu keadaan tersebut—sakelar tidak dapat terbuka dan tertutup pada saat yang sama. Selain itu, jika suatu sakelar selalu berada dalam keadaan yang sama dengan sakelar lain, kita menyatakan keduanya dengan huruf yang sama; artinya, dua sakelar yang sama-sama diberi label a akan selalu terbuka pada saat yang sama dan tertutup pada saat yang sama.

Dari dua sakelar, kita dapat menyusun dua jenis dasar rangkaian. Dua sakelar a dan b tersusun **seri** jika keduanya membentuk rangkaian seperti yang diilustrasikan dalam Gambar 19.3.1. Dalam rangkaian seri, arus dapat mengalir di antara terminal A dan B hanya jika kedua sakelar a dan b tertutup. Kombinasi sakelar ini kita nyatakan dengan $a \wedge b$. Dua sakelar a dan b tersusun **paralel** jika keduanya membentuk rangkaian seperti yang tampak dalam Gambar 19.3.2. Dalam rangkaian paralel, arus dapat mengalir di antara A dan B jika salah satu sakelar tertutup. Kombinasi paralel rangkaian a dan b kita nyatakan dengan $a \vee b$.



Gambar 19.3.1 $a \wedge b$

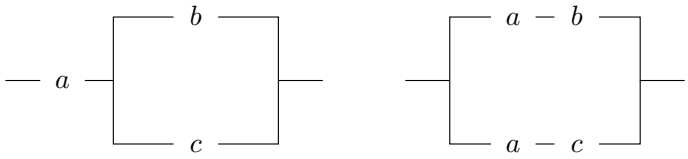


Gambar 19.3.2 $a \vee b$

Kita dapat membangun rangkaian listrik yang lebih rumit dari rangkaian seri dan paralel dengan mengganti sebarang sakelar dalam rangkaian dengan salah satu dari dua jenis dasar rangkaian tersebut. Rangkaian yang dibangun dengan cara ini disebut **rangkaian seri-paralel**.

Dua rangkaian kita anggap ekuivalen jika keduanya bekerja dengan cara yang sama. Artinya, jika sakelar-sakelar dalam rangkaian yang ekuivalen kita atur dengan tepat sama, kita akan memperoleh hasil yang sama. Sebagai contoh, dalam rangkaian seri, $a \wedge b$ sama persis dengan $b \wedge a$. Perhatikan bahwa hal ini tepat merupakan hukum komutatif untuk aljabar Boolean. Bahkan, himpunan semua rangkaian seri-paralel membentuk aljabar Boolean di bawah

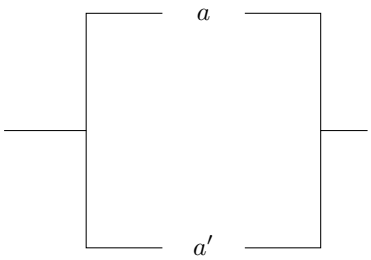
operasi $\vee$ dan $\wedge$. Kita dapat menggunakan diagram untuk memverifikasi berbagai aksioma aljabar Boolean. Hukum distributif, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, diilustrasikan dalam Gambar 19.3.3. Jika a merupakan sakelar, maka a' adalah sakelar yang selalu terbuka ketika a tertutup dan selalu tertutup ketika a terbuka. Rangkaian yang selalu tertutup merupakan I dalam aljabar kita; rangkaian yang selalu terbuka merupakan O. Hukum $a \wedge a' = O$ dan $a \vee a' = I$ masing-masing ditunjukkan dalam Gambar 19.3.4 dan Gambar 19.3.5.



Gambar 19.3.3 $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$



Gambar 19.3.4 $a \wedge a' = O$



Gambar 19.3.5 $a \vee a' = I$

Contoh 19.3.6 Setiap ekspresi Boolean merepresentasikan suatu rangkaian pensakelaran. Sebagai contoh, dari ekspresi $(a \vee b) \wedge (a \vee b') \wedge (a \vee b)$, kita dapat menyusun rangkaian dalam Gambar 19.3.9. ▲

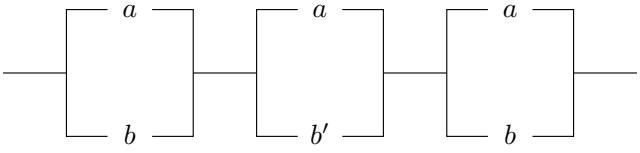
Teorema 19.3.7 *Himpunan semua rangkaian merupakan aljabar Boolean.*

Pembuktian teorema ini untuk aksioma aljabar Boolean yang belum diverifikasi diserahkan sebagai latihan. Sekarang kita dapat menerapkan teknik aljabar Boolean pada teori pensakelaran.

Contoh 19.3.8 Jika diberikan suatu rangkaian kompleks, kita sekarang dapat menerapkan teknik aljabar Boolean untuk menyederhanakannya. Perhatikan rangkaian dalam Gambar 19.3.9. Karena

$$\begin{aligned}(a \vee b) \wedge (a \vee b') \wedge (a \vee b) &= (a \vee b) \wedge (a \vee b) \wedge (a \vee b') \\ &= (a \vee b) \wedge (a \vee b') \\ &= a \vee (b \wedge b') \\ &= a \vee O \\ &= a,\end{aligned}$$

kita dapat mengganti rangkaian yang lebih rumit tersebut dengan rangkaian yang hanya memuat sakelar a dan memperoleh fungsi yang sama. ▲



Gambar 19.3.9 $(a \vee b) \wedge (a \vee b') \wedge (a \vee b)$

Catatan Sejarah

George Boole (1815–1864) adalah orang pertama yang mempelajari latis. Pada 1847, ia menerbitkan *The Investigation of the Laws of Thought*, sebuah buku yang menggunakan latis untuk memformalkan logika dan kalkulus proposisi. Boole berpendapat bahwa matematika adalah kajian tentang bentuk, bukan isi; artinya, ia tidak terlalu mempersoalkan apa yang dihitungnya, melainkan bagaimana ia menghitungnya. Karya Boole diteruskan oleh sahabatnya, Augustus De Morgan (1806–1871). De Morgan mengamati bahwa prinsip dualitas sering berlaku dalam teori himpunan, sebagaimana diilustrasikan oleh hukum De Morgan untuk teori himpunan. Seperti Boole, ia berpendapat bahwa matematika adalah kajian tentang simbol dan operasi abstrak.

Teori himpunan dan logika dikembangkan lebih lanjut oleh matematikawan seperti Alfred North Whitehead (1861–1947), Bertrand Russell (1872–1970), dan David Hilbert (1862–1943). Dalam *Principia Mathematica*, Whitehead dan Russell berupaya menunjukkan hubungan antara matematika dan logika dengan menurunkan sistem bilangan asli dari kaidah logika formal. Jika bilangan asli dapat ditentukan dari logika itu sendiri, sebagian besar matematika yang ada pun dapat ditentukan dengan cara yang sama. Hilbert berupaya membangun matematika dengan menggunakan logika simbolik sedemikian rupa sehingga konsistensi matematika dapat dibuktikan. Pendekatannya menerima pukulan telak dari Kurt Gödel (1906–1978), yang membuktikan bahwa akan selalu terdapat masalah yang "tak terputuskan" dalam setiap sistem aksiomatik yang cukup kaya; artinya, dalam setiap sistem matematika yang cukup bermakna, akan selalu terdapat pernyataan yang tidak pernah dapat dibuktikan benar maupun salah.

Sebagaimana sering terjadi, penelitian dasar dalam matematika murni ini kemudian menjadi sangat diperlukan dalam beragam penerapan. Aljabar Boolean dan logika telah menjadi unsur penting dalam desain rangkaian terpadu berskala besar yang terdapat pada cip komputer masa kini. Para sosiolog menggunakan latis dan aljabar Boolean untuk memodelkan hierarki sosial; para biolog menggunakannya untuk mendeskripsikan biosistem.

19.4 Pertanyaan Bacaan

1. Jelaskan secara ringkas apa itu poset. Jangan sekadar mendaftarkan sifat-sifat yang mendefinisikannya, tetapi berikan deskripsi yang dapat dipahami oleh mahasiswa aljabar lain yang belum pernah menjumpai poset. Sebagai contoh, sebagian jawaban Anda dapat menyebutkan jenis topik aljabar umum yang diperumum oleh poset, dan jawaban Anda hendaknya tidak banyak menggunakan simbol.

2. Apa perbedaan latis dengan poset? Jawablah dengan semangat yang sama seperti pertanyaan sebelumnya.

3. Apa perbedaan aljabar Boolean dengan latis? Sekali lagi, jawablah dengan semangat yang sama seperti dua pertanyaan sebelumnya.

4. Berikan dua alasan (yang mungkin saling berkaitan) mengapa pembahasan aljabar Boolean hingga dapat berpusat pada contoh himpunan kuasa dari suatu himpunan hingga.

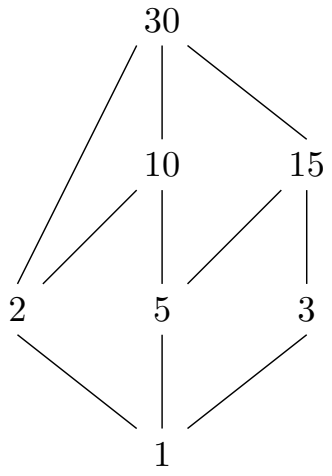
5. Jelaskan salah satu inovasi besar pada pertengahan abad kedua puluh yang dimungkinkan oleh aljabar Boolean.

19.5 Latihan

1. Gambarlah diagram latis untuk himpunan kuasa dari $X = \{a, b, c, d\}$ dengan relasi inklusi himpunan, $\subset$.

2. Gambarlah diagram untuk himpunan bilangan bulat positif yang merupakan pembagi dari 30. Apakah poset ini merupakan aljabar Boolean?

Petunjuk.



3. Gambarlah diagram latis subgrup dari $\mathbb{Z}_{12}$.

4. Misalkan B himpunan bilangan bulat positif yang merupakan pembagi dari 210. Definisikan suatu urutan pada B dengan $a \preceq b$ jika $a \mid b$. Buktikan bahwa B merupakan aljabar Boolean. Carilah himpunan X sedemikian sehingga B isomorfik dengan $\mathcal{P}(X)$.

Petunjuk. Apa saja atom dari B?

5. Buktikan atau berikan sangkalan: $\mathbb{Z}$ merupakan poset di bawah relasi $a \preceq b$ jika $a \mid b$.

Petunjuk. Salah.

6. Gambarlah rangkaian pensakelaran untuk setiap ekspresi Boolean berikut.

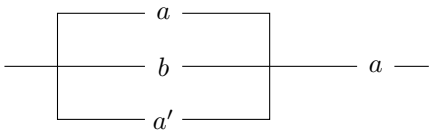
(a) $(a \vee b \vee a') \wedge a$

(b) $(a \vee b)' \wedge (a \vee b)$

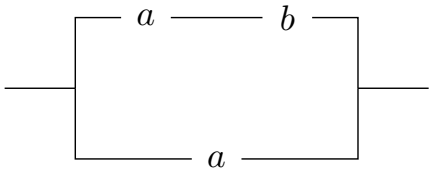
(c) $a \vee (a \wedge b)$

(d) $(c \vee a \vee b) \wedge c' \wedge (a \vee b)'$

Petunjuk. (a) $(a \vee b \vee a') \wedge a$

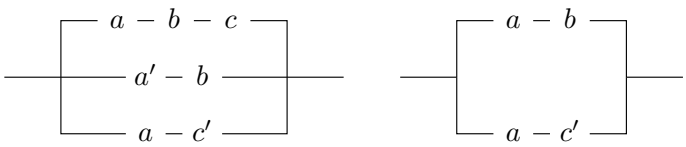


(c) $a \vee (a \wedge b)$



7. Gambarlah rangkaian yang akan tertutup tepat ketika hanya satu dari tiga sakelar a, b, dan c tertutup.

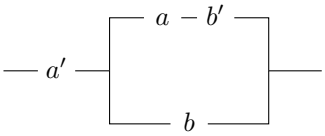
8. Buktikan atau berikan sangkalan bahwa kedua rangkaian yang ditampilkan bersifat ekuivalen.

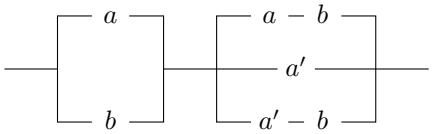


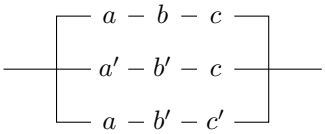
Petunjuk. Tidak ekuivalen.

9. Misalkan X suatu himpunan hingga yang memuat n unsur. Buktikan bahwa $|\mathcal{P}(X)| = 2^n$. Simpulkan bahwa orde setiap aljabar Boolean hingga harus berbentuk 2^n untuk suatu $n \in \mathbb{N}$.

10. Untuk setiap rangkaian berikut, tuliskan suatu ekspresi Boolean. Jika rangkaian tersebut dapat diganti dengan rangkaian yang memiliki lebih sedikit sakelar, berikan ekspresi Boolean dan gambarlah diagram rangkaian yang baru.







Petunjuk. (a) $a' \wedge [(a \wedge b') \vee b] = a \wedge (a \vee b)$.

11. Buktikan atau berikan sangkalan: himpunan semua bilangan bulat tak nol merupakan latis, dengan $a \preceq b$ didefinisikan oleh $a \mid b$.

12. Misalkan L suatu himpunan tak kosong dengan dua operasi biner $\vee$ dan $\wedge$ yang memenuhi hukum komutatif, asosiatif, idempoten, dan absorpsi. Kita dapat mendefinisikan urutan parsial pada L, sebagaimana dalam Teorema 19.1.14, dengan $a \preceq b$ jika $a \vee b = b$. Buktikan bahwa batas bawah terbesar dari a dan b adalah $a \wedge b$.

13. Misalkan G suatu grup dan X himpunan subgrup dari G yang diurutkan oleh inklusi himpunan. Jika H dan K merupakan subgrup dari G, tunjukkan bahwa batas atas terkecil dari H dan K adalah subgrup yang dibangkitkan oleh $H \cup K$.

14. Misalkan R suatu gelanggang dan X himpunan ideal dari R. Tunjukkan bahwa X merupakan poset yang diurutkan oleh inklusi himpunan, $\subset$. Definisikan temu dari dua ideal I dan J dalam X sebagai $I \cap J$ dan gabung dari I dan J sebagai $I + J$. Buktikan bahwa himpunan ideal dari

R merupakan latis di bawah operasi-operasi ini.

Petunjuk. Misalkan I, J merupakan ideal dalam R. Kita perlu menunjukkan bahwa $I + J = \{r + s : r \in I \text{ dan } s \in J\}$ merupakan ideal terkecil dalam R yang memuat I dan J. Jika $r_1, r_2 \in I$ dan $s_1, s_2 \in J$, maka $(r_1 + s_1) + (r_2 + s_2) = (r_1 + r_2) + (s_1 + s_2)$ berada dalam $I + J$. Untuk $a \in R$, $a(r_1 + s_1) = ar_1 + as_1 \in I + J$; dengan demikian, $I + J$ merupakan ideal dalam R.

15. Misalkan B suatu aljabar Boolean. Buktikan setiap identitas berikut.

(a) $a \vee I = I$ dan $a \wedge O = O$ untuk semua $a \in B$.

(b) Jika $a \vee b = I$ dan $a \wedge b = O$, maka $b = a'$.

(c) $(a')' = a$ untuk semua $a \in B$.

(d) $I' = O$ dan $O' = I$.

(e) $(a \vee b)' = a' \wedge b'$ dan $(a \wedge b)' = a' \vee b'$ (hukum De Morgan).

16. Dengan menggambar diagram yang sesuai, lengkapilah pembuktian Teorema 19.3.7 untuk menunjukkan bahwa fungsi pensakelaran membentuk aljabar Boolean.

17. Misalkan B suatu aljabar Boolean. Definisikan operasi biner $+$ dan $\cdot$ pada B melalui

$$a + b = (a \wedge b') \vee (a' \wedge b)$$
$$a \cdot b = a \wedge b.$$

Buktikan bahwa B merupakan gelanggang komutatif di bawah operasi-operasi ini dan memenuhi $a^2 = a$ untuk semua $a \in B$.

18. Misalkan X suatu poset sedemikian sehingga untuk setiap a dan b dalam X, berlaku $a \preceq b$ atau $b \preceq a$. Maka X disebut **himpunan terurut total**.

(a) Apakah $a \mid b$ merupakan urutan total pada $\mathbb{N}$?

(b) Buktikan bahwa $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, dan $\mathbb{R}$ merupakan himpunan terurut total di bawah urutan biasa $\leq$.

Petunjuk. (a) Tidak.

19. Misalkan X dan Y merupakan poset. Suatu pemetaan $\phi : X \to Y$ disebut **mempertahankan urutan** jika $a \preceq b$ mengakibatkan $\phi(a) \preceq \phi(b)$. Misalkan L dan M merupakan latis. Suatu pemetaan $\psi : L \to M$ disebut **homomorfisma latis** jika $\psi(a \vee b) = \psi(a) \vee \psi(b)$ dan $\psi(a \wedge b) = \psi(a) \wedge \psi(b)$. Tunjukkan bahwa setiap homomorfisma latis mempertahankan urutan, tetapi tidak setiap homomorfisma yang mempertahankan urutan merupakan homomorfisma latis.

20. Misalkan B suatu aljabar Boolean. Buktikan bahwa $a = b$ jika dan hanya jika $(a \wedge b') \vee (a' \wedge b) = O$ untuk $a, b \in B$.

Petunjuk. $(\Rightarrow)$. $a = b \Rightarrow (a \wedge b') \vee (a' \wedge b) = (a \wedge a') \vee (a' \wedge a) = O \vee O = O$. $(\Leftarrow)$. $(a \wedge b') \vee (a' \wedge b) = O \Rightarrow a \vee b = (a \vee a) \vee b = a \vee (a \vee b) = a \vee [I \wedge (a \vee b)] = a \vee [(a \vee a') \wedge (a \vee b)] = [a \vee (a \wedge b')] \vee [a \vee (a' \wedge b)] = a \vee [(a \wedge b') \vee (a' \wedge b)] = a \vee 0 = a$. Argumen yang simetris menunjukkan bahwa $a \vee b = b$.

21. Misalkan B suatu aljabar Boolean. Buktikan bahwa $a = O$ jika dan hanya jika $(a \wedge b') \vee (a' \wedge b) = b$ untuk semua $b \in B$.

22. Misalkan L dan M merupakan latis. Definisikan suatu relasi urutan pada $L \times M$ dengan $(a, b) \preceq (c, d)$ jika $a \preceq c$ dan $b \preceq d$. Tunjukkan bahwa $L \times M$ merupakan latis di bawah urutan parsial ini.

19.6 Latihan Pemrograman

1. Suatu **fungsi Boolean** atau **fungsi pensakelaran pada** n **variabel** adalah pemetaan $f : \{O, I\}^n \to \{0, I\}$. Polinomial Boolean merupakan jenis khusus fungsi Boolean: yaitu sebarang ekspresi Boolean yang dibentuk dari kombinasi hingga variabel $x_1, \ldots, x_n$ bersama O dan I, dengan menggunakan operasi $\vee$, $\wedge$, dan $'$. Nilai fungsi-fungsi tersebut didefinisikan dalam Tabel 19.6.1. Tulislah program untuk mengevaluasi polinomial Boolean.

Tabel 19.6.1 Polinomial Boolean

x	y	x'	$x \vee y$	$x \wedge y$
0	0	1	0	0
0	1	1	1	0
1	0	0	1	0
1	1	0	1	1

19.7 Referensi dan Bacaan yang Disarankan

[1] Donnellan, T. *Lattice Theory.* Pergamon Press, Oxford, 1968.

[2] Halmos, P. R. "The Basic Concepts of Algebraic Logic," *American Mathematical Monthly* 53 (1956), 363–87.

[3] Hohn, F. "Some Mathematical Aspects of Switching," *American Mathematical Monthly* 62 (1955), 75–90.

[4] Hohn, F. *Applied Boolean Algebra.* 2nd ed. Macmillan, New York, 1966.

[5] Lidl, R. and Pilz, G. *Applied Abstract Algebra.* 2nd ed. Springer, New York, 1998.

[6] Whitesitt, J. *Boolean Algebra and Its Applications.* Dover, Mineola, NY, 2010.

20

Ruang Vektor

Dalam suatu sistem fisik, sebuah besaran sering kali dapat dideskripsikan dengan satu bilangan. Sebagai contoh, kita hanya perlu mengetahui satu bilangan untuk mendeskripsikan suhu, massa, atau volume. Namun, untuk beberapa besaran, seperti lokasi, kita memerlukan beberapa bilangan. Untuk menyatakan lokasi suatu titik dalam ruang, kita memerlukan koordinat x, y, dan z. Distribusi suhu pada suatu benda padat memerlukan empat bilangan: tiga untuk mengidentifikasi setiap titik di dalam benda tersebut dan satu lagi untuk mendeskripsikan suhu pada titik itu. Sering kali, tupel-n bilangan, atau vektor, juga memiliki sifat-sifat aljabar tertentu, seperti penjumlahan atau perkalian skalar.

Dalam bab ini, kita akan mempelajari struktur matematika yang disebut ruang vektor. Seperti halnya grup dan gelanggang, kita ingin memberikan daftar sederhana aksioma yang harus dipenuhi agar suatu himpunan vektor menjadi struktur yang layak dipelajari.

20.1 Definisi dan Contoh

Ruang vektor V atas suatu lapangan F adalah grup abelian yang dilengkapi **hasil kali skalar** $\alpha \cdot v$ atau αv, yang didefinisikan untuk setiap $\alpha \in F$ dan setiap $v \in V$, serta memenuhi aksioma-aksioma berikut.

- $\alpha(\beta v) = (\alpha\beta)v$;
- $(\alpha + \beta)v = \alpha v + \beta v$;
- $\alpha(u + v) = \alpha u + \alpha v$;
- $1v = v$;

dengan $\alpha, \beta \in F$ dan $u, v \in V$.

Elemen-elemen V disebut **vektor**; elemen-elemen F disebut **skalar**. Penting untuk diperhatikan bahwa dalam kebanyakan kasus, dua vektor tidak dapat dikalikan. Secara umum, kita hanya dapat mengalikan suatu vektor dengan suatu skalar. Untuk membedakan nol skalar dari vektor nol, kita akan menuliskannya masing-masing sebagai 0 dan $\mathbf{0}$.

Mari kita telaah beberapa contoh ruang vektor. Sebagian di antaranya akan terasa cukup akrab; sebagian lainnya mungkin tidak.

Contoh 20.1.1 Tupel-n bilangan real, yang dinotasikan dengan $\mathbb{R}^n$, membentuk ruang vektor atas $\mathbb{R}$. Diberikan vektor $u = (u_1, \ldots, u_n)$ dan $v =$

$(v_1, \ldots, v_n)$ dalam $\mathbb{R}^n$ dan α dalam $\mathbb{R}$, kita dapat mendefinisikan penjumlahan vektor dengan

$$u + v = (u_1, \ldots, u_n) + (v_1, \ldots, v_n) = (u_1 + v_1, \ldots, u_n + v_n)$$

dan perkalian skalar dengan

$$\alpha u = \alpha(u_1, \ldots, u_n) = (\alpha u_1, \ldots, \alpha u_n).$$

▲

Contoh 20.1.2 Jika F adalah lapangan, maka $F[x]$ merupakan ruang vektor atas F. Vektor-vektor dalam $F[x]$ tidak lain adalah polinomial, dan penjumlahan vektor tidak lain adalah penjumlahan polinomial. Jika $\alpha \in F$ dan $p(x) \in F[x]$, maka perkalian skalar didefinisikan sebagai $\alpha p(x)$. ▲

Contoh 20.1.3 Himpunan semua fungsi kontinu bernilai real pada interval tertutup $[a, b]$ merupakan ruang vektor atas $\mathbb{R}$. Jika $f(x)$ dan $g(x)$ kontinu pada $[a, b]$, maka $(f + g)(x)$ didefinisikan sebagai $f(x) + g(x)$. Perkalian skalar didefinisikan oleh $(\alpha f)(x) = \alpha f(x)$ untuk $\alpha \in \mathbb{R}$. Sebagai contoh, jika $f(x) = \sin x$ dan $g(x) = x^2$, maka $(2f + 5g)(x) = 2 \sin x + 5x^2$. ▲

Contoh 20.1.4 Misalkan $V = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Maka V merupakan ruang vektor atas $\mathbb{Q}$. Jika $u = a + b\sqrt{2}$ dan $v = c + d\sqrt{2}$, maka $u + v = (a + c) + (b + d)\sqrt{2}$ kembali berada dalam V. Selain itu, untuk $\alpha \in \mathbb{Q}$, αv berada dalam V. Verifikasi bahwa semua aksioma ruang vektor berlaku untuk V diserahkan sebagai latihan. ▲

Proposisi 20.1.5 *Misalkan V adalah ruang vektor atas F. Maka setiap pernyataan berikut benar.*

1. $0v = \mathbf{0}$ *untuk setiap* $v \in V$.
2. $\alpha\mathbf{0} = \mathbf{0}$ *untuk setiap* $\alpha \in F$.
3. *Jika* $\alpha v = \mathbf{0}$, *maka* $\alpha = 0$ *atau* $v = \mathbf{0}$.
4. $(-1)v = -v$ *untuk setiap* $v \in V$.
5. $-(\alpha v) = (-\alpha)v = \alpha(-v)$ *untuk setiap* $\alpha \in F$ *dan setiap* $v \in V$.

Bukti. Untuk membuktikan (1), perhatikan bahwa

$$0v = (0 + 0)v = 0v + 0v;$$

akibatnya, $\mathbf{0} + 0v = 0v + 0v$. Karena V merupakan grup abelian, $\mathbf{0} = 0v$.

Pembuktian (2) hampir identik dengan pembuktian (1). Untuk (3), pernyataan tersebut langsung benar jika $\alpha = 0$. Andaikan $\alpha \neq 0$. Dengan mengalikan kedua ruas $\alpha v = \mathbf{0}$ dengan $1/\alpha$, kita memperoleh $v = \mathbf{0}$.

Untuk menunjukkan (4), perhatikan bahwa

$$v + (-1)v = 1v + (-1)v = (1 - 1)v = 0v = \mathbf{0},$$

sehingga $-v = (-1)v$. Pembuktian (5) diserahkan sebagai latihan. ■

20.2 Subruang

Sebagaimana grup memiliki subgrup dan gelanggang memiliki subgelanggang, ruang vektor juga memiliki substruktur. Misalkan V adalah ruang vektor atas

suatu lapangan F dan W suatu himpunan bagian dari V. Maka W merupakan **subruang** dari V jika tertutup terhadap penjumlahan vektor dan perkalian skalar; yaitu, jika $u, v \in W$ dan $\alpha \in F$, maka $u+v$ dan αv selalu berada dalam W.

Contoh 20.2.1 Misalkan W adalah subruang dari $\mathbb{R}^3$ yang didefinisikan oleh $W = \{(x_1, 2x_1 + x_2, x_1 - x_2) : x_1, x_2 \in \mathbb{R}\}$. Kita menyatakan bahwa W merupakan subruang dari $\mathbb{R}^3$. Karena

$$\begin{aligned}\alpha(x_1, 2x_1 + x_2, x_1 - x_2) &= (\alpha x_1, \alpha(2x_1 + x_2), \alpha(x_1 - x_2)) \\ &= (\alpha x_1, 2(\alpha x_1) + \alpha x_2, \alpha x_1 - \alpha x_2),\end{aligned}$$

W tertutup terhadap perkalian skalar. Untuk menunjukkan bahwa W tertutup terhadap penjumlahan vektor, misalkan $u = (x_1, 2x_1 + x_2, x_1 - x_2)$ dan $v = (y_1, 2y_1 + y_2, y_1 - y_2)$ adalah vektor-vektor dalam W. Maka

$$u + v = (x_1 + y_1, 2(x_1 + y_1) + (x_2 + y_2), (x_1 + y_1) - (x_2 + y_2)).$$

▲

Contoh 20.2.2 Misalkan W adalah himpunan bagian polinomial dalam $F[x]$ yang tidak memiliki suku berpangkat ganjil. Jika $p(x)$ dan $q(x)$ tidak memiliki suku berpangkat ganjil, maka $p(x) + q(x)$ juga tidak memilikinya. Selain itu, $\alpha p(x) \in W$ untuk $\alpha \in F$ dan $p(x) \in W$. ▲

Misalkan V adalah sebarang ruang vektor atas suatu lapangan F dan andaikan $v_1, v_2, \ldots, v_n$ adalah vektor-vektor dalam V dan $\alpha_1, \alpha_2, \ldots, \alpha_n$ adalah skalar-skalar dalam F. Setiap vektor w dalam V yang berbentuk

$$w = \sum_{i=1}^{n} \alpha_i v_i = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$$

disebut **kombinasi linear** dari vektor-vektor $v_1, v_2, \ldots, v_n$. **Himpunan perentang** dari vektor-vektor $v_1, v_2, \ldots, v_n$ adalah himpunan vektor yang diperoleh dari semua kombinasi linear yang mungkin dari $v_1, v_2, \ldots, v_n$. Jika W adalah himpunan perentang dari $v_1, v_2, \ldots, v_n$, kita mengatakan bahwa W **direntang** oleh $v_1, v_2, \ldots, v_n$.

Proposisi 20.2.3 *Misalkan $S = \{v_1, v_2, \ldots, v_n\}$ adalah himpunan vektor dalam suatu ruang vektor V. Maka rentang S merupakan subruang dari V.*

Bukti. Misalkan u dan v berada dalam S. Kita dapat menuliskan kedua vektor tersebut sebagai kombinasi linear dari v_i:

$$\begin{aligned}u &= \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n \\ v &= \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n.\end{aligned}$$

Maka

$$u + v = (\alpha_1 + \beta_1)v_1 + (\alpha_2 + \beta_2)v_2 + \cdots + (\alpha_n + \beta_n)v_n$$

merupakan kombinasi linear dari v_i. Untuk $\alpha \in F$,

$$\alpha u = (\alpha\alpha_1)v_1 + (\alpha\alpha_2)v_2 + \cdots + (\alpha\alpha_n)v_n$$

berada dalam rentang S. ■

20.3 Kebebasan Linear

Misalkan $S = \{v_1, v_2, \ldots, v_n\}$ adalah himpunan vektor dalam suatu ruang vektor V. Jika terdapat skalar $\alpha_1, \alpha_2 \ldots \alpha_n \in F$ sedemikian sehingga α_i tidak semuanya nol dan

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \mathbf{0},$$

maka S dikatakan **bergantung linear**. Jika himpunan S tidak bergantung linear, himpunan tersebut dikatakan **bebas linear**. Secara lebih khusus, S merupakan himpunan bebas linear jika

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \mathbf{0}$$

mengakibatkan

$$\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0$$

untuk setiap himpunan skalar $\{\alpha_1, \alpha_2 \ldots \alpha_n\}$.

Proposisi 20.3.1 *Misalkan $\{v_1, v_2, \ldots, v_n\}$ adalah himpunan vektor bebas linear dalam suatu ruang vektor. Andaikan*

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n.$$

Maka $\alpha_1 = \beta_1, \alpha_2 = \beta_2, \ldots, \alpha_n = \beta_n$.

Bukti. Jika

$$v = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \beta_1 v_1 + \beta_2 v_2 + \cdots + \beta_n v_n,$$

maka

$$(\alpha_1 - \beta_1)v_1 + (\alpha_2 - \beta_2)v_2 + \cdots + (\alpha_n - \beta_n)v_n = \mathbf{0}.$$

Karena $v_1, \ldots, v_n$ bebas linear, $\alpha_i - \beta_i = 0$ untuk $i = 1, \ldots, n$. ■

Definisi kebergantungan linear menjadi lebih mudah dipahami jika kita meninjau proposisi berikut.

Proposisi 20.3.2 *Himpunan vektor $\{v_1, v_2, \ldots, v_n\}$ dalam suatu ruang vektor V bergantung linear jika dan hanya jika salah satu v_i merupakan kombinasi linear dari vektor-vektor lainnya.*

Bukti. Andaikan $\{v_1, v_2, \ldots, v_n\}$ adalah himpunan vektor yang bergantung linear. Maka terdapat skalar $\alpha_1, \ldots, \alpha_n$ sedemikian sehingga

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = \mathbf{0},$$

dengan sekurang-kurangnya satu α_i tidak sama dengan nol. Andaikan $\alpha_k \neq 0$. Maka

$$v_k = -\frac{\alpha_1}{\alpha_k} v_1 - \cdots - \frac{\alpha_{k-1}}{\alpha_k} v_{k-1} - \frac{\alpha_{k+1}}{\alpha_k} v_{k+1} - \cdots - \frac{\alpha_n}{\alpha_k} v_n.$$

Sebaliknya, andaikan

$$v_k = \beta_1 v_1 + \cdots + \beta_{k-1} v_{k-1} + \beta_{k+1} v_{k+1} + \cdots + \beta_n v_n.$$

Maka

$$\beta_1 v_1 + \cdots + \beta_{k-1} v_{k-1} - v_k + \beta_{k+1} v_{k+1} + \cdots + \beta_n v_n = \mathbf{0}.$$

■

Proposisi berikut merupakan akibat dari fakta bahwa setiap sistem persamaan linear homogen yang memiliki lebih banyak peubah daripada persamaan

akan mempunyai solusi taktrivial. Rincian pembuktiannya diserahkan sebagai latihan akhir bab.

Proposisi 20.3.3 *Andaikan ruang vektor V direntang oleh n vektor. Jika $m > n$, maka setiap himpunan yang terdiri atas m vektor dalam V pasti bergantung linear.*

Himpunan vektor $\{e_1, e_2, \ldots, e_n\}$ dalam suatu ruang vektor V disebut **basis** bagi V jika $\{e_1, e_2, \ldots, e_n\}$ merupakan himpunan bebas linear yang merentang V.

Contoh 20.3.4 Vektor $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$, dan $e_3 = (0, 0, 1)$ membentuk basis bagi $\mathbb{R}^3$. Himpunan tersebut jelas merentang $\mathbb{R}^3$, karena setiap vektor sebarang (x_1, x_2, x_3) dalam $\mathbb{R}^3$ dapat dituliskan sebagai $x_1e_1 + x_2e_2 + x_3e_3$. Selain itu, tidak satu pun dari vektor e_1, e_2, e_3 dapat dituliskan sebagai kombinasi linear dari dua vektor lainnya; oleh karena itu, vektor-vektor tersebut bebas linear. Vektor e_1, e_2, e_3 bukan satu-satunya basis bagi $\mathbb{R}^3$: himpunan $\{(3, 2, 1), (3, 2, 0), (1, 1, 1)\}$ juga merupakan basis bagi $\mathbb{R}^3$. ▲

Contoh 20.3.5 Misalkan $\mathbb{Q}(\sqrt{2}\,) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Himpunan $\{1, \sqrt{2}\,\}$ dan $\{1 + \sqrt{2}, 1 - \sqrt{2}\,\}$ keduanya merupakan basis bagi $\mathbb{Q}(\sqrt{2}\,)$. ▲

Dari dua contoh terakhir, seharusnya jelas bahwa suatu ruang vektor memiliki beberapa basis. Bahkan, kedua contoh tersebut masing-masing memiliki tak hingga banyak basis. *Secara umum, suatu ruang vektor tidak memiliki basis tunggal.* Namun, setiap basis $\mathbb{R}^3$ terdiri atas tepat tiga vektor, dan setiap basis $\mathbb{Q}(\sqrt{2}\,)$ terdiri atas tepat dua vektor. Hal ini merupakan akibat dari proposisi berikut.

Proposisi 20.3.6 *Misalkan $\{e_1, e_2, \ldots, e_m\}$ dan $\{f_1, f_2, \ldots, f_n\}$ adalah dua basis bagi suatu ruang vektor V. Maka $m = n$.*

Bukti. Karena $\{e_1, e_2, \ldots, e_m\}$ merupakan basis, himpunan tersebut bebas linear. Berdasarkan Proposisi 20.3.3, $n \leq m$. Demikian pula, $\{f_1, f_2, \ldots, f_n\}$ merupakan himpunan bebas linear, dan proposisi terakhir mengakibatkan $m \leq n$. Akibatnya, $m = n$. ■

Jika $\{e_1, e_2, \ldots, e_n\}$ merupakan basis bagi suatu ruang vektor V, kita mengatakan bahwa **dimensi** V adalah n dan menuliskan $\dim V = n$. Pembuktian teorema berikut diserahkan sebagai latihan.

Teorema 20.3.7 *Misalkan V adalah ruang vektor berdimensi n.*

1. *Jika $S = \{v_1, \ldots, v_n\}$ adalah himpunan vektor bebas linear dalam V, maka S merupakan basis bagi V.*
2. *Jika $S = \{v_1, \ldots, v_n\}$ merentang V, maka S merupakan basis bagi V.*
3. *Jika $S = \{v_1, \ldots, v_k\}$ adalah himpunan vektor bebas linear dalam V dengan $k < n$, maka terdapat vektor $v_{k+1}, \ldots, v_n$ sedemikian sehingga*

$$\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$$

merupakan basis bagi V.

20.4 Pertanyaan Bacaan

1. Mengapa aksioma ruang vektor tampaknya hanya memiliki empat syarat, bukan sepuluh syarat yang mungkin pernah Anda lihat ketika pertama kali mempelajari definisi aksiomatik?

2. Himpunan $V = \mathbb{Q}(\sqrt{11}) = \{a + b\sqrt{11} \mid a, b \in \mathbb{Q}\}$ merupakan ruang vektor. Definisikan dengan cermat operasi-operasi pada himpunan ini yang membuat hal tersebut mungkin. Deskripsikan subruang yang direntang oleh $S = \{\mathbf{u}\}$, dengan $\mathbf{u} = 3 + \frac{2}{7}\sqrt{11} \in V$.

3. Tulislah sebuah paragraf panjang, atau esai singkat, mengenai pentingnya kebebasan linear dalam aljabar linear.

4. Tulislah sebuah paragraf panjang, atau esai singkat, mengenai pentingnya himpunan perentang dalam aljabar linear.

5. "Aljabar linear sepenuhnya membahas kombinasi linear." Jelaskan mengapa Anda mungkin mengatakan demikian.

20.5 Latihan

1. Jika F adalah lapangan, tunjukkan bahwa $F[x]$ merupakan ruang vektor atas F, dengan vektor-vektor dalam $F[x]$ berupa polinomial. Penjumlahan vektor adalah penjumlahan polinomial, dan perkalian skalar didefinisikan oleh $\alpha p(x)$ untuk $\alpha \in F$.

2. Buktikan bahwa $\mathbb{Q}(\sqrt{2}\,)$ merupakan ruang vektor.

3. Misalkan $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,)$ adalah lapangan yang dibangkitkan oleh elemen-elemen berbentuk $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, dengan a, b, c, d berada dalam $\mathbb{Q}$. Buktikan bahwa $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,)$ merupakan ruang vektor berdimensi 4 atas $\mathbb{Q}$. Temukan basis bagi $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,)$.

Petunjuk. $\mathbb{Q}(\sqrt{2}, \sqrt{3}\,)$ memiliki basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\,\}$ atas $\mathbb{Q}$.

4. Buktikan bahwa bilangan kompleks merupakan ruang vektor berdimensi 2 atas $\mathbb{R}$.

5. Buktikan bahwa himpunan P_n yang terdiri atas semua polinomial berderajat kurang dari n membentuk subruang dari ruang vektor $F[x]$. Temukan basis bagi P_n dan hitung dimensi P_n.

Petunjuk. Himpunan $\{1, x, x^2, \ldots, x^{n-1}\}$ merupakan basis bagi P_n.

6. Misalkan F adalah lapangan dan nyatakan himpunan tupel-n atas F dengan F^n. Diberikan vektor $u = (u_1, \ldots, u_n)$ dan $v = (v_1, \ldots, v_n)$ dalam F^n dan α dalam F, definisikan penjumlahan vektor dengan

$$u + v = (u_1, \ldots, u_n) + (v_1, \ldots, v_n) = (u_1 + v_1, \ldots, u_n + v_n)$$

dan perkalian skalar dengan

$$\alpha u = \alpha(u_1, \ldots, u_n) = (\alpha u_1, \ldots, \alpha u_n).$$

Buktikan bahwa F^n merupakan ruang vektor berdimensi n terhadap operasi-operasi tersebut.

7. Manakah di antara himpunan berikut yang merupakan subruang dari $\mathbb{R}^3$? Jika himpunan tersebut memang merupakan subruang, temukan basis bagi subruang itu dan hitung dimensinya.

(a) $\{(x_1, x_2, x_3) : 3x_1 - 2x_2 + x_3 = 0\}$

(b) $\{(x_1, x_2, x_3) : 3x_1 + 4x_3 = 0, 2x_1 - x_2 + x_3 = 0\}$

(c) $\{(x_1, x_2, x_3) : x_1 - 2x_2 + 2x_3 = 2\}$

(d) $\{(x_1, x_2, x_3) : 3x_1 - 2x_2^2 = 0\}$

Petunjuk. (a) Subruang berdimensi 2 dengan basis $\{(1, 0, -3), (0, 1, 2)\}$; (d) bukan subruang

8. Tunjukkan bahwa himpunan semua solusi yang mungkin $(x, y, z) \in \mathbb{R}^3$ dari persamaan

$$Ax + By + Cz = 0$$
$$Dx + Ey + Cz = 0$$

membentuk subruang dari $\mathbb{R}^3$.

9. Misalkan W adalah himpunan bagian fungsi kontinu pada $[0, 1]$ sedemikian sehingga $f(0) = 0$. Buktikan bahwa W merupakan subruang dari $C[0, 1]$.

10. Misalkan V adalah ruang vektor atas F. Buktikan bahwa $-(\alpha v) = (-\alpha)v = \alpha(-v)$ untuk setiap $\alpha \in F$ dan setiap $v \in V$.

Petunjuk. Karena $0 = \alpha 0 = \alpha(-v+v) = \alpha(-v)+\alpha v$, diperoleh $-\alpha v = \alpha(-v)$.

11. Misalkan V adalah ruang vektor berdimensi n. Buktikan setiap pernyataan berikut.

(a) Jika $S = \{v_1, \ldots, v_n\}$ adalah himpunan vektor bebas linear dalam V, maka S merupakan basis bagi V.

(b) Jika $S = \{v_1, \ldots, v_n\}$ merentang V, maka S merupakan basis bagi V.

(c) Jika $S = \{v_1, \ldots, v_k\}$ adalah himpunan vektor bebas linear dalam V dengan $k < n$, maka terdapat vektor $v_{k+1}, \ldots, v_n$ sedemikian sehingga

$$\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$$

merupakan basis bagi V.

12. Buktikan bahwa setiap himpunan vektor yang memuat $\mathbf{0}$ bergantung linear.

Petunjuk. Misalkan $v_0 = 0, v_1, \ldots, v_n \in V$ dan $\alpha_0 \neq 0, \alpha_1, \ldots, \alpha_n \in F$. Maka $\alpha_0 v_0 + \cdots + \alpha_n v_n = 0$.

13. Misalkan V adalah ruang vektor. Tunjukkan bahwa $\{\mathbf{0}\}$ merupakan subruang berdimensi nol dari V.

14. Jika suatu ruang vektor V direntang oleh n vektor, tunjukkan bahwa setiap himpunan yang terdiri atas m vektor dalam V pasti bergantung linear untuk $m > n$.

15. Transformasi Linear. Misalkan V dan W adalah ruang vektor atas suatu lapangan F, yang masing-masing berdimensi m dan n. Jika $T : V \to W$ adalah pemetaan yang memenuhi

$$T(u + v) = T(u) + T(v)$$
$$T(\alpha v) = \alpha T(v)$$

untuk setiap $\alpha \in F$ dan setiap $u, v \in V$, maka T disebut **transformasi linear** dari V ke W.

(a) Buktikan bahwa **kernel** T, $\ker(T) = \{v \in V : T(v) = \mathbf{0}\}$, merupakan subruang dari V. Kernel T kadang-kadang disebut **ruang nol** T.

(b) Buktikan bahwa **citra** atau **ruang citra** T, $R(V) = \{w \in W : T(v) = w \text{ untuk suatu } v \in V\}$, merupakan subruang dari W.

(c) Tunjukkan bahwa $T : V \to W$ injektif jika dan hanya jika $\ker(T) = \{\mathbf{0}\}$.

(d) Misalkan $\{v_1, \ldots, v_k\}$ adalah basis bagi ruang nol T. Kita dapat memperluas basis ini menjadi basis $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_m\}$ bagi V. Mengapa? Buktikan bahwa $\{T(v_{k+1}), \ldots, T(v_m)\}$ merupakan basis bagi citra T. Simpulkan bahwa citra T berdimensi $m - k$.

(e) Misalkan $\dim V = \dim W$. Tunjukkan bahwa transformasi linear $T : V \to W$ injektif jika dan hanya jika surjektif.

Petunjuk. (a) Misalkan $u, v \in \ker(T)$ dan $\alpha \in F$. Maka

$$T(u + v) = T(u) + T(v) = 0$$
$$T(\alpha v) = \alpha T(v) = \alpha 0 = 0.$$

Oleh karena itu, $u+v, \alpha v \in \ker(T)$, dan $\ker(T)$ merupakan subruang dari V.

(c) Pernyataan $T(u) = T(v)$ ekuivalen dengan $T(u - v) = T(u) - T(v) = 0$, yang benar jika dan hanya jika $u - v = 0$ atau $u = v$.

16. Misalkan V dan W adalah ruang vektor berdimensi hingga n atas suatu lapangan F. Andaikan $T : V \to W$ adalah isomorfisma ruang vektor. Jika $\{v_1, \ldots, v_n\}$ merupakan basis bagi V, tunjukkan bahwa $\{T(v_1), \ldots, T(v_n)\}$ merupakan basis bagi W. Simpulkan bahwa setiap ruang vektor atas suatu lapangan F yang berdimensi n isomorfik dengan F^n.

17. Jumlah Langsung. Misalkan U dan V adalah subruang dari suatu ruang vektor W. Jumlah U dan V, yang dinotasikan dengan $U + V$, didefinisikan sebagai himpunan semua vektor berbentuk $u + v$, dengan $u \in U$ dan $v \in V$.

(a) Buktikan bahwa $U + V$ dan $U \cap V$ merupakan subruang dari W.

(b) Jika $U+V = W$ dan $U \cap V = \mathbf{0}$, maka W disebut **jumlah langsung.** Dalam hal ini, kita menuliskan $W = U \oplus V$. Tunjukkan bahwa setiap elemen $w \in W$ dapat dituliskan secara tunggal sebagai $w = u + v$, dengan $u \in U$ dan $v \in V$.

(c) Misalkan U adalah subruang berdimensi k dari suatu ruang vektor W berdimensi n. Buktikan bahwa terdapat subruang V berdimensi $n-k$ sedemikian sehingga $W = U \oplus V$. Apakah subruang V tunggal?

(d) Jika U dan V adalah subruang sebarang dari suatu ruang vektor W, tunjukkan bahwa

$$\dim(U + V) = \dim U + \dim V - \dim(U \cap V).$$

Petunjuk. (a) Misalkan $u, u' \in U$ dan $v, v' \in V$. Maka

$$(u+v)+(u'+v') = (u+u')+(v+v') \in U+V$$
$$\alpha(u+v) = \alpha u + \alpha v \in U+V.$$

18. Ruang Dual. Misalkan V dan W adalah ruang vektor berdimensi hingga atas suatu lapangan F.

(a) Tunjukkan bahwa himpunan semua transformasi linear dari V ke W, yang dinotasikan dengan $\text{Hom}(V, W)$, merupakan ruang vektor atas F, dengan penjumlahan vektor yang didefinisikan sebagai berikut:

$$(S+T)(v) = S(v) + T(v)$$
$$(\alpha S)(v) = \alpha S(v),$$

dengan $S, T \in \text{Hom}(V, W)$, $\alpha \in F$, dan $v \in V$.

(b) Misalkan V adalah ruang vektor atas F. Definisikan **ruang dual** dari V sebagai $V^* = \text{Hom}(V, F)$. Elemen-elemen dalam ruang dual V disebut **fungsional linear.** Misalkan $v_1, \ldots, v_n$ adalah basis terurut bagi V. Jika $v = \alpha_1 v_1 + \cdots + \alpha_n v_n$ adalah sebarang vektor dalam V, definisikan fungsional linear $\phi_i : V \to F$ dengan $\phi_i(v) = \alpha_i$. Tunjukkan bahwa ϕ_i membentuk basis bagi V^*. Basis ini disebut **basis dual** dari $v_1, \ldots, v_n$ (atau cukup basis dual jika konteksnya sudah jelas).

(c) Tinjau basis $\{(3, 1), (2, -2)\}$ bagi $\mathbb{R}^2$. Apakah basis dual bagi $(\mathbb{R}^2)^*$?

(d) Misalkan V adalah ruang vektor berdimensi n atas suatu lapangan F dan misalkan V^{**} adalah ruang dual dari V^*. Tunjukkan bahwa setiap elemen $v \in V$ menghasilkan suatu elemen λ_v dalam V^{**} dan bahwa pemetaan $v \mapsto \lambda_v$ merupakan isomorfisma antara V dan V^{**}.

20.6 Referensi dan Bacaan yang Disarankan

[1] Beezer, R. *A First Course in Linear Algebra* . Available online at linear.ups.edu. 2004–2014.

[2] Bretscher, O. *Linear Algebra with Applications*. 4th ed. Pearson, Upper Saddle River, NJ, 2009.

[3] Curtis, C. W. *Linear Algebra: An Introductory Approach*. 4th ed. Springer, New York, 1984.

[4] Hoffman, K. and Kunze, R. *Linear Algebra*. 2nd ed. Prentice-Hall, Englewood Cliffs, NJ, 1971.

[5] Johnson, L. W., Riess, R. D., and Arnold, J. T. *Introduction to Linear Algebra*. 6th ed. Pearson, Upper Saddle River, NJ, 2011.

[6] Leon, S. J. *Linear Algebra with Applications*. 8th ed. Pearson, Upper Saddle River, NJ, 2010.

21

Lapangan

Wajar untuk menanyakan apakah suatu lapangan F termuat dalam lapangan yang lebih besar. Kita dapat memikirkan bilangan rasional, yang berada di dalam bilangan real, sedangkan bilangan real sendiri berada di dalam bilangan kompleks. Kita juga dapat mempelajari lapangan-lapangan di antara $\mathbb{Q}$ dan $\mathbb{R}$ serta menyelidiki sifat lapangan-lapangan tersebut.

Secara lebih khusus, jika diberikan lapangan F dan polinomial $p(x) \in F[x]$, kita dapat menanyakan apakah dapat ditemukan lapangan E yang memuat F sedemikian sehingga $p(x)$ terfaktor menjadi faktor-faktor linear atas $E[x]$. Sebagai contoh, jika kita meninjau polinomial

$$p(x) = x^4 - 5x^2 + 6$$

di $\mathbb{Q}[x]$, maka $p(x)$ terfaktor sebagai $(x^2 - 2)(x^2 - 3)$. Akan tetapi, kedua faktor ini tak tereduksi di $\mathbb{Q}[x]$. Jika kita ingin menemukan suatu nol dari $p(x)$, kita harus beralih ke lapangan yang lebih besar. Lapangan bilangan real tentu memenuhi kebutuhan ini, karena

$$p(x) = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3}).$$

Kita dapat menemukan lapangan yang lebih kecil tempat $p(x)$ memiliki nol, yaitu

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

Kita ingin dapat menghitung dan mempelajari lapangan semacam itu untuk sembarang polinomial atas suatu lapangan F.

21.1 Perluasan Lapangan

Lapangan E merupakan **perluasan lapangan** dari lapangan F jika F merupakan sublapangan dari E. Lapangan F disebut **lapangan dasar**. Kita menulis $F \subset E$.

Contoh 21.1.1 Sebagai contoh, misalkan

$$F = \mathbb{Q}(\sqrt{2}\,) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

dan misalkan $E = \mathbb{Q}(\sqrt{2} + \sqrt{3}\,)$ adalah lapangan terkecil yang memuat $\mathbb{Q}$ dan $\sqrt{2} + \sqrt{3}$. Baik E maupun F merupakan perluasan lapangan dari bilangan rasional. Kita mengklaim bahwa E merupakan perluasan lapangan dari F. Untuk melihatnya, kita hanya perlu menunjukkan bahwa $\sqrt{2}$ berada di E. Karena $\sqrt{2} + \sqrt{3}$ berada di E, $1/(\sqrt{2} + \sqrt{3}\,) = \sqrt{3} - \sqrt{2}$ juga harus berada

di E. Dengan mengambil kombinasi linear dari $\sqrt{2}+\sqrt{3}$ dan $\sqrt{3}-\sqrt{2}$, kita menemukan bahwa $\sqrt{2}$ dan $\sqrt{3}$ keduanya harus berada di E. ▲

Contoh 21.1.2 Misalkan $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Karena 0 maupun 1 bukan akar polinomial ini, kita mengetahui bahwa $p(x)$ tak tereduksi atas $\mathbb{Z}_2$. Kita akan membangun perluasan lapangan dari $\mathbb{Z}_2$ yang memuat elemen α sedemikian sehingga $p(\alpha) = 0$. Berdasarkan Teorema 17.3.12, ideal $\langle p(x)\rangle$ yang dibangkitkan oleh $p(x)$ bersifat maksimal; jadi, $\mathbb{Z}_2[x]/\langle p(x)\rangle$ merupakan lapangan. Misalkan $f(x) + \langle p(x)\rangle$ sembarang elemen dari $\mathbb{Z}_2[x]/\langle p(x)\rangle$. Berdasarkan algoritma pembagian,

$$f(x) = (x^2 + x + 1)q(x) + r(x),$$

dengan derajat $r(x)$ kurang dari derajat $x^2 + x + 1$. Oleh karena itu,

$$f(x) + \langle x^2 + x + 1\rangle = r(x) + \langle x^2 + x + 1\rangle.$$

Jadi, satu-satunya kemungkinan bagi $r(x)$ adalah 0, 1, x, dan $1+x$. Akibatnya, $E = \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ merupakan lapangan dengan empat elemen dan harus menjadi perluasan lapangan dari $\mathbb{Z}_2$, yang memuat nol α dari $p(x)$. Lapangan $\mathbb{Z}_2(\alpha)$ terdiri atas elemen-elemen

$$\begin{aligned} 0 + 0\alpha &= 0 \\ 1 + 0\alpha &= 1 \\ 0 + 1\alpha &= \alpha \\ 1 + 1\alpha &= 1 + \alpha. \end{aligned}$$

Perhatikan bahwa $\alpha^2 + \alpha + 1 = 0$; jadi, jika kita menghitung $(1 + \alpha)^2$,

$$(1 + \alpha)(1 + \alpha) = 1 + \alpha + \alpha + (\alpha)^2 = \alpha.$$

Perhitungan lain dilakukan dengan cara serupa. Kita merangkum perhitungan ini dalam tabel-tabel berikut, yang menunjukkan cara menjumlahkan dan mengalikan elemen-elemen di E. ▲

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

Gambar 21.1.3 Tabel Penjumlahan untuk $\mathbb{Z}_2(\alpha)$

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Gambar 21.1.4 Tabel Perkalian untuk $\mathbb{Z}_2(\alpha)$

Teorema berikut, yang berasal dari Kronecker, begitu penting dan mendasar bagi pemahaman kita tentang lapangan sehingga sering dikenal sebagai Teorema Fundamental Teori Lapangan.

Teorema 21.1.5 *Misalkan F suatu lapangan dan $p(x)$ polinomial takkonstan di $F[x]$. Maka terdapat perluasan lapangan E dari F dan elemen $\alpha \in E$ sedemikian sehingga $p(\alpha) = 0$.*

BUKTI. Untuk membuktikan teorema ini, kita akan menggunakan metode yang dipakai untuk membangun Contoh 21.1.2. Jelas bahwa kita dapat mengasumsikan $p(x)$ merupakan polinomial tak tereduksi. Kita ingin menemukan perluasan lapangan E dari F yang memuat elemen α sedemikian sehingga $p(\alpha) = 0$. Ideal $\langle p(x)\rangle$ yang dibangkitkan oleh $p(x)$ merupakan ideal maksimal di $F[x]$ berdasarkan Teorema 17.3.12; jadi, $F[x]/\langle p(x)\rangle$ merupakan lapangan. Kita mengklaim bahwa $E = F[x]/\langle p(x)\rangle$ adalah lapangan yang diinginkan.

Pertama-tama kita menunjukkan bahwa E merupakan perluasan lapangan dari F. Kita dapat mendefinisikan homomorfisma gelanggang komutatif melalui pemetaan $\psi : F \to F[x]/\langle p(x)\rangle$, dengan $\psi(a) = a + \langle p(x)\rangle$ untuk $a \in F$. Mudah diperiksa bahwa ψ memang merupakan homomorfisma gelanggang. Perhatikan bahwa

$$\psi(a) + \psi(b) = (a + \langle p(x)\rangle) + (b + \langle p(x)\rangle) = (a + b) + \langle p(x)\rangle = \psi(a + b)$$

dan

$$\psi(a)\psi(b) = (a + \langle p(x)\rangle)(b + \langle p(x)\rangle) = ab + \langle p(x)\rangle = \psi(ab).$$

Untuk membuktikan bahwa ψ satu-ke-satu, asumsikan bahwa

$$a + \langle p(x)\rangle = \psi(a) = \psi(b) = b + \langle p(x)\rangle.$$

Maka $a - b$ merupakan kelipatan $p(x)$, karena berada dalam ideal $\langle p(x)\rangle$. Karena $p(x)$ polinomial takkonstan, satu-satunya kemungkinan adalah $a - b = 0$. Akibatnya, $a = b$ dan ψ injektif. Karena ψ satu-ke-satu, kita dapat mengidentifikasi F dengan sublapangan $\{a + \langle p(x)\rangle : a \in F\}$ dari E dan memandang E sebagai perluasan lapangan dari F.

Tinggal membuktikan bahwa $p(x)$ memiliki nol $\alpha \in E$. Tetapkan $\alpha = x + \langle p(x)\rangle$. Maka α berada di E. Jika $p(x) = a_0 + a_1x + \cdots + a_nx^n$, maka

$$\begin{aligned} p(\alpha) &= a_0 + a_1(x + \langle p(x)\rangle) + \cdots + a_n(x + \langle p(x)\rangle)^n \\ &= a_0 + (a_1x + \langle p(x)\rangle) + \cdots + (a_nx^n + \langle p(x)\rangle) \\ &= a_0 + a_1x + \cdots + a_nx^n + \langle p(x)\rangle \\ &= 0 + \langle p(x)\rangle. \end{aligned}$$

Oleh karena itu, kita telah menemukan elemen $\alpha \in E = F[x]/\langle p(x)\rangle$ sedemikian sehingga α merupakan nol dari $p(x)$. ■

Contoh 21.1.6 Misalkan $p(x) = x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$. Maka $p(x)$ memiliki faktor-faktor tak tereduksi $x^2 + x + 1$ dan $x^3 + x + 1$. Untuk memperoleh perluasan lapangan E dari $\mathbb{Z}_2$ sedemikian sehingga $p(x)$ memiliki akar di E, kita dapat mengambil E sebagai $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ atau $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$. Kita serahkan sebagai latihan untuk menunjukkan bahwa $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ merupakan lapangan dengan $2^3 = 8$ elemen. ▲

21.1.1 Unsur Aljabar

Suatu elemen α dalam perluasan lapangan E atas F disebut **aljabar** atas F jika $f(\alpha) = 0$ untuk suatu polinomial taknol $f(x) \in F[x]$. Elemen di E yang tidak aljabar atas F disebut **transenden** atas F. Perluasan lapangan E dari lapangan F disebut **perluasan aljabar** dari F jika setiap elemen di E aljabar

atas F. Jika E merupakan perluasan lapangan dari F dan $\alpha_1, \ldots, \alpha_n$ termuat di E, kita menyatakan lapangan terkecil yang memuat F dan $\alpha_1, \ldots, \alpha_n$ dengan $F(\alpha_1, \ldots, \alpha_n)$. Jika $E = F(\alpha)$ untuk suatu $\alpha \in E$, maka E merupakan **perluasan sederhana** dari F.

Contoh 21.1.7 $\sqrt{2}$ dan i keduanya aljabar atas $\mathbb{Q}$ karena masing-masing merupakan nol dari polinomial x^2-2 dan x^2+1. Jelas bahwa π dan e aljabar atas bilangan real; akan tetapi, fakta bahwa keduanya transenden atas $\mathbb{Q}$ tidaklah sepele. Bilangan-bilangan di $\mathbb{R}$ yang aljabar atas $\mathbb{Q}$ sebenarnya cukup langka. Hampir semua bilangan real transenden atas $\mathbb{Q}$.[1](Dalam banyak kasus kita tidak mengetahui apakah suatu bilangan tertentu transenden; sebagai contoh, masih belum diketahui apakah $\pi + e$ transenden atau aljabar.) ▲

Bilangan kompleks yang aljabar atas $\mathbb{Q}$ disebut **bilangan aljabar**. **Bilangan transenden** adalah elemen dari $\mathbb{C}$ yang transenden atas $\mathbb{Q}$.

Contoh 21.1.8 Kita akan menunjukkan bahwa $\sqrt{2+\sqrt{3}}$ aljabar atas $\mathbb{Q}$. Jika $\alpha = \sqrt{2+\sqrt{3}}$, maka $\alpha^2 = 2+\sqrt{3}$. Jadi, $\alpha^2-2 = \sqrt{3}$ dan $(\alpha^2-2)^2 = 3$. Karena $\alpha^4-4\alpha^2+1 = 0$, haruslah α merupakan nol dari polinomial $x^4-4x^2+1 \in \mathbb{Q}[x]$. ▲

Sangat mudah memberikan contoh perluasan lapangan E atas lapangan F, dengan E memuat elemen yang transenden atas F. Teorema berikut mencirikan perluasan transenden.

Teorema 21.1.9 *Misalkan E perluasan lapangan dari F dan $\alpha \in E$. Maka α transenden atas F jika dan hanya jika $F(\alpha)$ isomorfik dengan $F(x)$, yaitu lapangan pecahan dari $F[x]$.*

Bukti. Misalkan $\phi_\alpha : F[x] \to E$ homomorfisma evaluasi untuk α. Maka α transenden atas F jika dan hanya jika $\phi_\alpha(p(x)) = p(\alpha) \neq 0$ untuk semua polinomial takkonstan $p(x) \in F[x]$. Hal ini benar jika dan hanya jika $\ker \phi_\alpha = \{0\}$; yakni, tepat ketika ϕ_α satu-ke-satu. Jadi, E harus memuat salinan $F[x]$. Lapangan terkecil yang memuat $F[x]$ adalah lapangan pecahan $F(x)$. Berdasarkan Teorema 18.1.4, E harus memuat salinan lapangan ini. ■

Kita menghadapi situasi yang lebih menarik dalam kasus perluasan aljabar.

Teorema 21.1.10 *Misalkan E perluasan lapangan dari lapangan F dan $\alpha \in E$, dengan α aljabar atas F. Maka terdapat polinomial monik tak tereduksi yang tunggal, $p(x) \in F[x]$, dengan derajat terkecil sedemikian sehingga $p(\alpha) = 0$. Jika $f(x)$ polinomial lain di $F[x]$ sedemikian sehingga $f(\alpha) = 0$, maka $p(x)$ membagi $f(x)$.*

Bukti. Misalkan $\phi_\alpha : F[x] \to E$ homomorfisma evaluasi. Kernel ϕ_α merupakan ideal utama yang dibangkitkan oleh suatu $p(x) \in F[x]$ dengan $\deg p(x) \geq 1$. Kita mengetahui bahwa polinomial semacam itu ada, karena $F[x]$ merupakan domain ideal utama dan α aljabar. Ideal $\langle p(x) \rangle$ tepat terdiri atas elemen-elemen $F[x]$ yang memiliki α sebagai nol. Jika $f(\alpha) = 0$ dan $f(x)$ bukan polinomial nol, maka $f(x) \in \langle p(x) \rangle$ dan $p(x)$ membagi $f(x)$. Jadi, $p(x)$ merupakan polinomial berderajat minimum yang memiliki α sebagai nol. Setiap polinomial lain berderajat sama yang memiliki α sebagai nol harus berbentuk $\beta p(x)$ untuk suatu $\beta \in F$.

Sekarang misalkan $p(x) = r(x)s(x)$ merupakan faktorisasi $p(x)$ menjadi polinomial-polinomial berderajat lebih rendah. Karena $p(\alpha) = 0$, $r(\alpha)s(\alpha) = 0$; akibatnya, $r(\alpha) = 0$ atau $s(\alpha) = 0$, yang bertentangan dengan fakta bahwa p berderajat minimum. Oleh karena itu, $p(x)$ harus tak tereduksi. ■

[1]Probabilitas bahwa bilangan real yang dipilih secara acak dari interval $[0, 1]$ bersifat transenden atas bilangan rasional adalah satu.

Misalkan E perluasan lapangan dari F dan $\alpha \in E$ aljabar atas F. Polinomial monik tunggal $p(x)$ dalam teorema terakhir disebut **polinomial minimal** dari α atas F. Derajat $p(x)$ disebut **derajat α atas F**.

Contoh 21.1.11 Misalkan $f(x) = x^2 - 2$ dan $g(x) = x^4 - 4x^2 + 1$. Polinomial-polinomial ini masing-masing merupakan polinomial minimal dari $\sqrt{2}$ dan $\sqrt{2+\sqrt{3}}$. ▲

Proposisi 21.1.12 *Misalkan E perluasan lapangan dari F dan $\alpha \in E$ aljabar atas F. Maka $F(\alpha) \cong F[x]/\langle p(x)\rangle$, dengan $p(x)$ polinomial minimal dari α atas F.*

BUKTI. Misalkan $\phi_\alpha : F[x] \to E$ homomorfisma evaluasi. Kernel pemetaan ini adalah $\langle p(x)\rangle$, dengan $p(x)$ polinomial minimal dari α. Berdasarkan Teorema Isomorfisma Pertama untuk gelanggang, citra ϕ_α di E isomorfik dengan $F(\alpha)$ karena memuat F dan α. ■

Teorema 21.1.13 *Misalkan $E = F(\alpha)$ perluasan sederhana dari F, dengan $\alpha \in E$ aljabar atas F. Misalkan derajat α atas F adalah n. Maka setiap elemen $\beta \in E$ dapat dinyatakan secara tunggal dalam bentuk*

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

untuk $b_i \in F$.

BUKTI. Karena $\phi_\alpha(F[x]) \cong F(\alpha)$, setiap elemen di $E = F(\alpha)$ harus berbentuk $\phi_\alpha(f(x)) = f(\alpha)$, dengan $f(\alpha)$ polinomial dalam α yang koefisiennya berada di F. Misalkan

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

adalah polinomial minimal dari α. Maka $p(\alpha) = 0$; jadi,

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_0.$$

Demikian pula,

$$\begin{aligned}\alpha^{n+1} &= \alpha\alpha^n \\ &= -a_{n-1}\alpha^n - a_{n-2}\alpha^{n-1} - \cdots - a_0\alpha \\ &= -a_{n-1}(-a_{n-1}\alpha^{n-1} - \cdots - a_0) - a_{n-2}\alpha^{n-1} - \cdots - a_0\alpha.\end{aligned}$$

Dengan melanjutkan cara ini, kita dapat menyatakan setiap monomial α^m, $m \geq n$, sebagai kombinasi linear pangkat-pangkat α yang kurang dari n. Jadi, setiap $\beta \in F(\alpha)$ dapat ditulis sebagai

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}.$$

Untuk menunjukkan ketunggalan, misalkan

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

untuk b_i dan c_i di F. Maka

$$g(x) = (b_0 - c_0) + (b_1 - c_1)x + \cdots + (b_{n-1} - c_{n-1})x^{n-1}$$

berada di $F[x]$ dan $g(\alpha) = 0$. Karena derajat $g(x)$ kurang dari derajat $p(x)$, yaitu polinomial tak tereduksi dari α, $g(x)$ harus merupakan polinomial nol. Akibatnya,

$$b_0 - c_0 = b_1 - c_1 = \cdots = b_{n-1} - c_{n-1} = 0,$$

atau $b_i = c_i$ untuk $i = 0, 1, \ldots, n-1$. Oleh karena itu, kita telah menunjukkan ketunggalan. ■

Contoh 21.1.14 Karena x^2+1 tak tereduksi atas $\mathbb{R}$, $\langle x^2+1\rangle$ merupakan ideal maksimal di $\mathbb{R}[x]$. Jadi, $E = \mathbb{R}[x]/\langle x^2+1\rangle$ merupakan perluasan lapangan dari $\mathbb{R}$ yang memuat suatu akar dari x^2+1. Misalkan $\alpha = x + \langle x^2+1\rangle$. Kita dapat mengidentifikasi E dengan bilangan kompleks. Berdasarkan Proposisi 21.1.12, E isomorfik dengan $\mathbb{R}(\alpha) = \{a + b\alpha : a, b \in \mathbb{R}\}$. Kita mengetahui bahwa $\alpha^2 = -1$ di E, karena

$$\begin{aligned}\alpha^2 + 1 &= (x + \langle x^2+1\rangle)^2 + (1 + \langle x^2+1\rangle)\\ &= (x^2+1) + \langle x^2+1\rangle\\ &= 0.\end{aligned}$$

Jadi, kita memiliki isomorfisma antara $\mathbb{R}(\alpha)$ dan $\mathbb{C}$ yang didefinisikan oleh pemetaan yang membawa $a + b\alpha$ ke $a + bi$. ▲

Misalkan E perluasan lapangan dari lapangan F. Jika kita memandang E sebagai ruang vektor atas F, kita dapat menerapkan perangkat aljabar linear pada masalah-masalah yang akan dijumpai dalam kajian lapangan. Elemen-elemen dalam lapangan E adalah vektor; elemen-elemen dalam lapangan F adalah skalar. Kita dapat memandang penjumlahan di E sebagai penjumlahan vektor. Ketika kita mengalikan suatu elemen di E dengan elemen dari F, kita mengalikan vektor dengan skalar. Pandangan terhadap perluasan lapangan ini sangat bermanfaat jika perluasan lapangan E dari F merupakan ruang vektor berdimensi hingga atas F, dan Teorema 21.1.13 menyatakan bahwa $E = F(\alpha)$ merupakan ruang vektor berdimensi hingga atas F dengan basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.

Jika perluasan lapangan E dari lapangan F merupakan ruang vektor berdimensi hingga atas F dengan dimensi n, kita mengatakan bahwa E merupakan **perluasan hingga berderajat** n **atas** F. Kita menulis

$$[E : F] = n.$$

untuk menyatakan dimensi E atas F.

Teorema 21.1.15 *Setiap perluasan hingga E dari lapangan F merupakan perluasan aljabar.*

Bukti. Misalkan $\alpha \in E$. Karena $[E : F] = n$, elemen-elemen

$$1, \alpha, \ldots, \alpha^n$$

tidak mungkin bebas linear. Jadi, terdapat $a_i \in F$, yang tidak semuanya nol, sedemikian sehingga

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Oleh karena itu,

$$p(x) = a_n x^n + \cdots + a_0 \in F[x]$$

merupakan polinomial taknol dengan $p(\alpha) = 0$. ■

Catatan 21.1.16 Teorema 21.1.15 menyatakan bahwa setiap perluasan hingga dari lapangan F merupakan perluasan aljabar. Akan tetapi, konversnya salah. Kita serahkan sebagai latihan untuk menunjukkan bahwa himpunan semua elemen di $\mathbb{R}$ yang aljabar atas $\mathbb{Q}$ membentuk perluasan lapangan takhingga dari $\mathbb{Q}$.

Teorema berikutnya adalah teorema pencacahan, yang serupa dengan Teorema Lagrange dalam teori grup. Teorema 21.1.17 akan terbukti menjadi alat

yang sangat berguna dalam penyelidikan kita mengenai perluasan lapangan hingga.

Teorema 21.1.17 *Jika E merupakan perluasan hingga dari F dan K merupakan perluasan hingga dari E, maka K merupakan perluasan hingga dari F dan*

$$[K : F] = [K : E][E : F].$$

BUKTI. Misalkan $\{\alpha_1, \ldots, \alpha_n\}$ suatu basis untuk E sebagai ruang vektor atas F dan $\{\beta_1, \ldots, \beta_m\}$ suatu basis untuk K sebagai ruang vektor atas E. Kita mengklaim bahwa $\{\alpha_i\beta_j\}$ merupakan basis untuk K atas F. Pertama-tama kita akan menunjukkan bahwa vektor-vektor ini merentang K. Misalkan $u \in K$. Maka $u = \sum_{j=1}^{m} b_j\beta_j$ dan $b_j = \sum_{i=1}^{n} a_{ij}\alpha_i$, dengan $b_j \in E$ dan $a_{ij} \in F$. Maka

$$u = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij}\alpha_i \right) \beta_j = \sum_{i,j} a_{ij}(\alpha_i\beta_j).$$

Jadi, mn vektor $\alpha_i\beta_j$ harus merentang K atas F.

Kita harus menunjukkan bahwa $\{\alpha_i\beta_j\}$ bebas linear. Ingat bahwa suatu himpunan vektor $v_1, v_2, \ldots, v_n$ dalam ruang vektor V bebas linear jika

$$c_1v_1 + c_2v_2 + \cdots + c_nv_n = 0$$

mengakibatkan

$$c_1 = c_2 = \cdots = c_n = 0.$$

Misalkan

$$u = \sum_{i,j} c_{ij}(\alpha_i\beta_j) = 0$$

untuk $c_{ij} \in F$. Kita perlu membuktikan bahwa semua c_{ij} bernilai nol. Kita dapat menulis ulang u sebagai

$$\sum_{j=1}^{m} \left(\sum_{i=1}^{n} c_{ij}\alpha_i \right) \beta_j = 0,$$

dengan $\sum_i c_{ij}\alpha_i \in E$. Karena setiap β_j bebas linear atas E, haruslah

$$\sum_{i=1}^{n} c_{ij}\alpha_i = 0$$

untuk semua j. Akan tetapi, setiap α_j juga bebas linear atas F. Oleh karena itu, $c_{ij} = 0$ untuk semua i dan j, yang menyelesaikan pembuktian. ■

Korolari berikut mudah dibuktikan dengan induksi matematika.

Korolari 21.1.18 *Jika F_i merupakan lapangan untuk $i = 1, \ldots, k$ dan F_{i+1} merupakan perluasan hingga dari F_i, maka F_k merupakan perluasan hingga dari F_1 dan*

$$[F_k : F_1] = [F_k : F_{k-1}] \cdots [F_2 : F_1].$$

Korolari 21.1.19 *Misalkan E perluasan lapangan dari F. Jika $\alpha \in E$ aljabar atas F dengan polinomial minimal $p(x)$ dan $\beta \in F(\alpha)$ dengan polinomial minimal $q(x)$, maka* $\deg q(x)$ *membagi* $\deg p(x)$.

BUKTI. Kita mengetahui bahwa $\deg p(x) = [F(\alpha) : F]$ dan $\deg q(x) = [F(\beta) : F]$. Karena $F \subset F(\beta) \subset F(\alpha)$,

$$[F(\alpha) : F] = [F(\alpha) : F(\beta)][F(\beta) : F].$$

■

Contoh 21.1.20 Mari kita tentukan perluasan lapangan dari $\mathbb{Q}$ yang memuat $\sqrt{3}+\sqrt{5}$. Mudah ditentukan bahwa polinomial minimal dari $\sqrt{3}+\sqrt{5}$ adalah x^4-16x^2+4. Dengan demikian,

$$[\mathbb{Q}(\sqrt{3}+\sqrt{5}\,):\mathbb{Q}]=4.$$

Kita mengetahui bahwa $\{1,\sqrt{3}\,\}$ merupakan basis untuk $\mathbb{Q}(\sqrt{3}\,)$ atas $\mathbb{Q}$. Jadi, $\sqrt{3}+\sqrt{5}$ tidak mungkin berada di $\mathbb{Q}(\sqrt{3}\,)$. Dengan demikian, $\sqrt{5}$ juga tidak mungkin berada di $\mathbb{Q}(\sqrt{3}\,)$. Oleh karena itu, $\{1,\sqrt{5}\,\}$ merupakan basis untuk $\mathbb{Q}(\sqrt{3},\sqrt{5}\,)=(\mathbb{Q}(\sqrt{3}\,))(\sqrt{5}\,)$ atas $\mathbb{Q}(\sqrt{3}\,)$ dan $\{1,\sqrt{3},\sqrt{5},\sqrt{3}\sqrt{5}=\sqrt{15}\,\}$ merupakan basis untuk $\mathbb{Q}(\sqrt{3},\sqrt{5}\,)=\mathbb{Q}(\sqrt{3}+\sqrt{5}\,)$ atas $\mathbb{Q}$. Contoh ini menunjukkan bahwa mungkin saja suatu perluasan $F(\alpha_1,\ldots,\alpha_n)$ sebenarnya merupakan perluasan sederhana dari F meskipun $n>1$. ▲

Contoh 21.1.21 Mari kita hitung basis untuk $\mathbb{Q}(\sqrt[3]{5},\sqrt{5}\,i)$, dengan $\sqrt{5}$ akar kuadrat positif dari 5 dan $\sqrt[3]{5}$ akar pangkat tiga real dari 5. Kita mengetahui bahwa $\sqrt{5}\,i\notin\mathbb{Q}(\sqrt[3]{5}\,)$, sehingga

$$[\mathbb{Q}(\sqrt[3]{5},\sqrt{5}\,i):\mathbb{Q}(\sqrt[3]{5}\,)]=2.$$

Mudah ditentukan bahwa $\{1,\sqrt{5}i\,\}$ merupakan basis untuk $\mathbb{Q}(\sqrt[3]{5},\sqrt{5}\,i)$ atas $\mathbb{Q}(\sqrt[3]{5}\,)$. Kita juga mengetahui bahwa $\{1,\sqrt[3]{5},(\sqrt[3]{5}\,)^2\}$ merupakan basis untuk $\mathbb{Q}(\sqrt[3]{5}\,)$ atas $\mathbb{Q}$. Jadi, suatu basis untuk $\mathbb{Q}(\sqrt[3]{5},\sqrt{5}\,i)$ atas $\mathbb{Q}$ adalah

$$\{1,\sqrt{5}\,i,\sqrt[3]{5},(\sqrt[3]{5}\,)^2,(\sqrt[6]{5}\,)^5i,(\sqrt[6]{5}\,)^7i=5\sqrt[6]{5}\,i \text{ atau } \sqrt[6]{5}\,i\}.$$

Perhatikan bahwa $\sqrt[6]{5}\,i$ merupakan nol dari x^6+5. Kita dapat menunjukkan bahwa polinomial ini tak tereduksi atas $\mathbb{Q}$ dengan menggunakan Kriteria Eisenstein, dengan mengambil $p=5$. Akibatnya,

$$\mathbb{Q}\subset\mathbb{Q}(\sqrt[6]{5}\,i)\subset\mathbb{Q}(\sqrt[3]{5},\sqrt{5}\,i).$$

Akan tetapi, haruslah $\mathbb{Q}(\sqrt[6]{5}\,i)=\mathbb{Q}(\sqrt[3]{5},\sqrt{5}\,i)$, karena derajat kedua perluasan ini adalah 6. ▲

Teorema 21.1.22 *Misalkan E perluasan lapangan dari F. Maka pernyataan-pernyataan berikut ekuivalen.*

1. *E merupakan perluasan hingga dari F.*
2. *Terdapat sejumlah hingga elemen aljabar $\alpha_1,\ldots,\alpha_n\in E$ sedemikian sehingga $E=F(\alpha_1,\ldots,\alpha_n)$.*
3. *Terdapat barisan lapangan*

$$E=F(\alpha_1,\ldots,\alpha_n)\supset F(\alpha_1,\ldots,\alpha_{n-1})\supset\cdots\supset F(\alpha_1)\supset F,$$

dengan setiap lapangan $F(\alpha_1,\ldots,\alpha_i)$ aljabar atas $F(\alpha_1,\ldots,\alpha_{i-1})$.

BUKTI. (1) ⇒ (2). Misalkan E perluasan aljabar hingga dari F. Maka E merupakan ruang vektor berdimensi hingga atas F dan terdapat basis yang terdiri atas elemen-elemen $\alpha_1,\ldots,\alpha_n$ di E sedemikian sehingga $E=F(\alpha_1,\ldots,\alpha_n)$. Setiap α_i aljabar atas F berdasarkan Teorema 21.1.15.

(2) ⇒ (3). Misalkan $E=F(\alpha_1,\ldots,\alpha_n)$, dengan setiap α_i aljabar atas F. Maka

$$E=F(\alpha_1,\ldots,\alpha_n)\supset F(\alpha_1,\ldots,\alpha_{n-1})\supset\cdots\supset F(\alpha_1)\supset F,$$

dengan setiap lapangan $F(\alpha_1, \ldots, \alpha_i)$ aljabar atas $F(\alpha_1, \ldots, \alpha_{i-1})$.

(3) $\Rightarrow$ (1). Misalkan

$$E = F(\alpha_1, \ldots, \alpha_n) \supset F(\alpha_1, \ldots, \alpha_{n-1}) \supset \cdots \supset F(\alpha_1) \supset F,$$

dengan setiap lapangan $F(\alpha_1, \ldots, \alpha_i)$ aljabar atas $F(\alpha_1, \ldots, \alpha_{i-1})$. Karena

$$F(\alpha_1, \ldots, \alpha_i) = F(\alpha_1, \ldots, \alpha_{i-1})(\alpha_i)$$

merupakan perluasan sederhana dan α_i aljabar atas $F(\alpha_1, \ldots, \alpha_{i-1})$, maka

$$[F(\alpha_1, \ldots, \alpha_i) : F(\alpha_1, \ldots, \alpha_{i-1})]$$

bernilai hingga untuk setiap i. Oleh karena itu, $[E : F]$ bernilai hingga. ■

21.1.2 Penutupan Aljabar

Untuk suatu lapangan F, timbul pertanyaan apakah kita dapat menemukan lapangan E sedemikian sehingga setiap polinomial $p(x)$ memiliki akar di E. Hal ini membawa kita pada teorema berikut.

Teorema 21.1.23 *Misalkan E perluasan lapangan dari F. Himpunan elemen di E yang aljabar atas F membentuk suatu lapangan.*

BUKTI. Misalkan $\alpha, \beta \in E$ aljabar atas F. Maka $F(\alpha, \beta)$ merupakan perluasan hingga dari F. Karena setiap elemen dari $F(\alpha, \beta)$ aljabar atas F, $\alpha \pm \beta$, $\alpha\beta$, dan α/β ($\beta \neq 0$) semuanya aljabar atas F. Akibatnya, himpunan elemen di E yang aljabar atas F membentuk suatu lapangan. ■

Korolari 21.1.24 *Himpunan semua bilangan aljabar membentuk suatu lapangan; yakni, himpunan semua bilangan kompleks yang aljabar atas $\mathbb{Q}$ membentuk suatu lapangan.*

Misalkan E perluasan lapangan dari lapangan F. Kita mendefinisikan **penutupan aljabar** dari lapangan F dalam E sebagai lapangan yang terdiri atas semua elemen di E yang aljabar atas F. Lapangan F disebut **tertutup secara aljabar** jika setiap polinomial takkonstan di $F[x]$ memiliki akar di F.

Teorema 21.1.25 *Lapangan F tertutup secara aljabar jika dan hanya jika setiap polinomial takkonstan di $F[x]$ terfaktor menjadi faktor-faktor linear atas $F[x]$.*

BUKTI. Misalkan F lapangan yang tertutup secara aljabar. Jika $p(x) \in F[x]$ polinomial takkonstan, maka $p(x)$ memiliki nol di F, katakanlah α. Oleh karena itu, $x - \alpha$ harus merupakan faktor dari $p(x)$, sehingga $p(x) = (x - \alpha)q_1(x)$, dengan $\deg q_1(x) = \deg p(x) - 1$. Lanjutkan proses ini pada $q_1(x)$ untuk memperoleh faktorisasi

$$p(x) = (x - \alpha)(x - \beta)q_2(x),$$

dengan $\deg q_2(x) = \deg p(x) - 2$. Proses ini akhirnya harus berhenti karena derajat $p(x)$ hingga.

Sebaliknya, misalkan setiap polinomial takkonstan $p(x)$ di $F[x]$ terfaktor menjadi faktor-faktor linear. Misalkan $ax - b$ salah satu faktor tersebut. Maka $p(b/a) = 0$. Akibatnya, F tertutup secara aljabar. ■

Korolari 21.1.26 *Lapangan F yang tertutup secara aljabar tidak memiliki perluasan aljabar sejati E.*

BUKTI. Misalkan E perluasan aljabar dari F; maka $F \subset E$. Untuk $\alpha \in E$, polinomial minimal dari α adalah $x - \alpha$. Oleh karena itu, $\alpha \in F$ dan $F = E$. ■

Teorema 21.1.27 *Setiap lapangan F memiliki penutupan aljabar yang tunggal.*

Fakta bahwa setiap lapangan memiliki penutupan aljabar yang tunggal tidaklah sepele. Buktinya tidak terlalu sulit, tetapi memerlukan teori himpunan yang cukup canggih. Untuk bukti hasil ini, kami merujuk pembaca ke [3], [4], atau [8].

Sekarang kita menyatakan Teorema Fundamental Aljabar, yang pertama kali dibuktikan Gauss pada usia 22 tahun dalam tesis doktornya. Teorema ini menyatakan bahwa setiap polinomial dengan koefisien bilangan kompleks memiliki akar dalam bilangan kompleks. Bukti teorema ini akan diberikan dalam Bab 23.

Teorema 21.1.28 Teorema Fundamental Aljabar. *Lapangan bilangan kompleks tertutup secara aljabar.*

21.2 Lapangan Pemisah

Misalkan F suatu lapangan dan $p(x)$ polinomial takkonstan di $F[x]$. Kita telah mengetahui bahwa kita dapat menemukan perluasan lapangan dari F yang memuat suatu akar dari $p(x)$. Akan tetapi, kita ingin mengetahui apakah terdapat perluasan E dari F yang memuat semua akar $p(x)$. Dengan kata lain, dapatkah kita menemukan perluasan lapangan dari F sedemikian sehingga $p(x)$ terfaktor menjadi hasil kali polinomial-polinomial linear? Apa perluasan "terkecil" yang memuat semua akar $p(x)$?

Misalkan F suatu lapangan dan $p(x) = a_0 + a_1x + \cdots + a_nx^n$ polinomial takkonstan di $F[x]$. Perluasan lapangan E dari F disebut **lapangan pemisah** dari $p(x)$ jika terdapat elemen-elemen $\alpha_1, \ldots, \alpha_n$ di E sedemikian sehingga $E = F(\alpha_1, \ldots, \alpha_n)$ dan

$$p(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n).$$

Polinomial $p(x) \in F[x]$ disebut **terpisah** di E jika merupakan hasil kali faktor-faktor linear di $E[x]$.

Contoh 21.2.1 Misalkan $p(x) = x^4 + 2x^2 - 8$ berada di $\mathbb{Q}[x]$. Maka $p(x)$ memiliki faktor-faktor tak tereduksi x^2-2 dan x^2+4. Oleh karena itu, lapangan $\mathbb{Q}(\sqrt{2}, i)$ merupakan lapangan pemisah untuk $p(x)$. ▲

Contoh 21.2.2 Misalkan $p(x) = x^3 - 3$ berada di $\mathbb{Q}[x]$. Maka $p(x)$ memiliki akar di lapangan $\mathbb{Q}(\sqrt[3]{3})$. Akan tetapi, lapangan ini bukan lapangan pemisah untuk $p(x)$ karena akar-akar pangkat tiga kompleks dari 3,

$$\frac{-\sqrt[3]{3} \pm (\sqrt[6]{3})^5 i}{2},$$

tidak berada di $\mathbb{Q}(\sqrt[3]{3})$. ▲

Teorema 21.2.3 *Misalkan $p(x) \in F[x]$ polinomial takkonstan. Maka terdapat lapangan pemisah E untuk $p(x)$.*

BUKTI. Kita akan menggunakan induksi matematika pada derajat $p(x)$. Jika $\deg p(x) = 1$, maka $p(x)$ merupakan polinomial linear dan $E = F$. Asumsikan teorema benar untuk semua polinomial berderajat k dengan $1 \leq k < n$ dan misalkan $\deg p(x) = n$. Kita dapat mengasumsikan bahwa $p(x)$ tak tereduksi; jika tidak, berdasarkan hipotesis induksi pembuktian selesai. Berdasarkan

Teorema 21.1.5, terdapat lapangan K sedemikian sehingga $p(x)$ memiliki nol α_1 di K. Jadi, $p(x) = (x-\alpha_1)q(x)$, dengan $q(x) \in K[x]$. Karena $\deg q(x) = n-1$, berdasarkan hipotesis induksi terdapat lapangan pemisah $E \supset K$ dari $q(x)$ yang memuat nol-nol $\alpha_2, \ldots, \alpha_n$ dari $p(x)$. Akibatnya,

$$E = K(\alpha_2, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_n)$$

merupakan lapangan pemisah dari $p(x)$. ■

Kini timbul pertanyaan mengenai ketunggalan lapangan pemisah. Jawaban atas pertanyaan ini adalah ya. Untuk dua lapangan pemisah K dan L dari polinomial $p(x) \in F[x]$, terdapat isomorfisma lapangan $\phi : K \to L$ yang mempertahankan F. Untuk membuktikan hasil ini, pertama-tama kita harus membuktikan suatu lema.

Lema 21.2.4 *Misalkan $\phi : E \to F$ suatu isomorfisma lapangan. Misalkan K perluasan lapangan dari E dan $\alpha \in K$ aljabar atas E dengan polinomial minimal $p(x)$. Misalkan L perluasan lapangan dari F sedemikian sehingga β merupakan akar dari polinomial di $F[x]$ yang diperoleh dari $p(x)$ melalui citra ϕ. Maka ϕ meluas menjadi isomorfisma tunggal $\overline{\phi} : E(\alpha) \to F(\beta)$ sedemikian sehingga $\overline{\phi}(\alpha) = \beta$ dan $\overline{\phi}$ sama dengan ϕ pada E.*

Bukti. Jika $p(x)$ berderajat n, maka berdasarkan Teorema 21.1.13 kita dapat menulis setiap elemen di $E(\alpha)$ sebagai kombinasi linear dari $1, \alpha, \ldots, \alpha^{n-1}$. Oleh karena itu, isomorfisma yang kita cari harus berupa

$$\overline{\phi}(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) = \phi(a_0) + \phi(a_1)\beta + \cdots + \phi(a_{n-1})\beta^{n-1},$$

dengan

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$$

merupakan elemen di $E(\alpha)$. Fakta bahwa $\overline{\phi}$ merupakan isomorfisma dapat diperiksa melalui perhitungan langsung; akan tetapi, lebih mudah untuk mengamati bahwa $\overline{\phi}$ merupakan komposisi pemetaan-pemetaan yang telah kita ketahui sebagai isomorfisma.

Kita dapat memperluas ϕ menjadi isomorfisma dari $E[x]$ ke $F[x]$, yang juga akan kita nyatakan dengan ϕ, dengan menetapkan

$$\phi(a_0 + a_1x + \cdots + a_nx^n) = \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n.$$

Perluasan ini sama dengan isomorfisma asal $\phi : E \to F$, karena polinomial konstan dipetakan ke polinomial konstan. Berdasarkan asumsi, $\phi(p(x)) = q(x)$; jadi, ϕ memetakan $\langle p(x)\rangle$ ke $\langle q(x)\rangle$ secara onto. Akibatnya, kita memiliki isomorfisma $\psi : E[x]/\langle p(x)\rangle \to F[x]/\langle q(x)\rangle$. Berdasarkan Proposisi 21.1.12, kita memiliki isomorfisma $\sigma : E[x]/\langle p(x)\rangle \to E(\alpha)$ dan $\tau : F[x]/\langle q(x)\rangle \to F(\beta)$, yang masing-masing didefinisikan melalui evaluasi di α dan β. Oleh karena itu, $\overline{\phi} = \tau\psi\sigma^{-1}$ adalah isomorfisma yang diperlukan (lihat Gambar 21.2.5).

$$\begin{array}{ccc} E[x]/\langle p(x)\rangle & \xrightarrow{\psi} & F[x]/\langle q(x)\rangle \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \tau} \\ E(\alpha) & \xrightarrow{\overline{\phi}} & F(\beta) \\ \downarrow & & \downarrow \\ E & \xrightarrow{\phi} & F \end{array}$$

Gambar 21.2.5 Diagram komutatif untuk Lema 21.2.4

Bukti ketunggalan kita serahkan sebagai latihan. ■

Teorema 21.2.6 *Misalkan $\phi : E \to F$ suatu isomorfisma lapangan, $p(x)$ polinomial takkonstan di $E[x]$, dan $q(x)$ polinomial yang bersesuaian di $F[x]$ di bawah isomorfisma tersebut. Jika K merupakan lapangan pemisah dari $p(x)$ dan L merupakan lapangan pemisah dari $q(x)$, maka ϕ meluas menjadi isomorfisma $\psi : K \to L$.*

BUKTI. Kita akan menggunakan induksi matematika pada derajat $p(x)$. Kita dapat mengasumsikan bahwa $p(x)$ tak tereduksi atas E. Oleh karena itu, $q(x)$ juga tak tereduksi atas F. Jika $\deg p(x) = 1$, berdasarkan definisi lapangan pemisah, $K = E$ dan $L = F$, sehingga tidak ada yang perlu dibuktikan.

Asumsikan teorema berlaku untuk semua polinomial berderajat kurang dari n. Karena K merupakan lapangan pemisah dari $p(x)$, semua akar $p(x)$ berada di K. Pilih salah satu akar ini, katakanlah α, sedemikian sehingga $E \subset E(\alpha) \subset K$. Demikian pula, kita dapat menemukan akar β dari $q(x)$ di L sedemikian sehingga $F \subset F(\beta) \subset L$. Berdasarkan Lema 21.2.4, terdapat isomorfisma $\overline{\phi} : E(\alpha) \to F(\beta)$ sedemikian sehingga $\overline{\phi}(\alpha) = \beta$ dan $\overline{\phi}$ sama dengan ϕ pada E (lihat Gambar 21.2.7).

$$\begin{array}{ccc} K & \xrightarrow{\psi} & L \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \tau} \\ E(\alpha) & \xrightarrow{\overline{\phi}} & F(\beta) \\ \downarrow & & \downarrow \\ E & \xrightarrow{\phi} & F \end{array}$$

Gambar 21.2.7 Diagram komutatif untuk Teorema 21.2.6

Sekarang tulis $p(x) = (x - \alpha)f(x)$ dan $q(x) = (x - \beta)g(x)$, dengan derajat $f(x)$ dan $g(x)$ masing-masing kurang dari derajat $p(x)$ dan $q(x)$. Perluasan lapangan K merupakan lapangan pemisah untuk $f(x)$ atas $E(\alpha)$, dan L merupakan lapangan pemisah untuk $g(x)$ atas $F(\beta)$. Berdasarkan hipotesis induksi, terdapat isomorfisma $\psi : K \to L$ sedemikian sehingga ψ sama dengan $\overline{\phi}$ pada $E(\alpha)$. Jadi, terdapat isomorfisma $\psi : K \to L$ sedemikian sehingga ψ sama dengan ϕ pada E. ■

Korolari 21.2.8 *Misalkan $p(x)$ suatu polinomial di $F[x]$. Maka terdapat lapangan pemisah K dari $p(x)$ yang tunggal hingga isomorfisma.*

21.3 Konstruksi Geometris

Di Yunani kuno, diajukan tiga masalah klasik. Masalah-masalah ini bersifat geometris dan melibatkan konstruksi penggaris lurus dan jangka dari materi yang kini termasuk geometri sekolah menengah; yaitu, kita hanya diizinkan menggunakan penggaris lurus dan jangka untuk menyelesaikannya. Masalah-masalah tersebut dapat dinyatakan sebagai berikut.

1. Untuk sembarang sudut yang diberikan, dapatkah sudut tersebut ditriseksi menjadi tiga sudut bagian yang sama hanya dengan penggaris lurus dan jangka?

2. Untuk sembarang lingkaran yang diberikan, dapatkah dibangun persegi dengan luas yang sama hanya dengan penggaris lurus dan jangka?

3. Untuk suatu kubus yang diberikan, dapatkah dibangun rusuk kubus lain yang volumenya dua kali volume kubus semula? Sekali lagi, kita hanya diizinkan menggunakan penggaris lurus dan jangka untuk konstruksi tersebut.

Setelah membingungkan para matematikawan selama lebih dari dua ribu tahun, setiap konstruksi ini akhirnya terbukti mustahil. Kita akan menggunakan teori lapangan untuk memberikan bukti bahwa penyelesaiannya tidak ada. Sungguh luar biasa bahwa jawaban yang lama dicari bagi ketiga masalah geometri ini berasal dari aljabar abstrak.

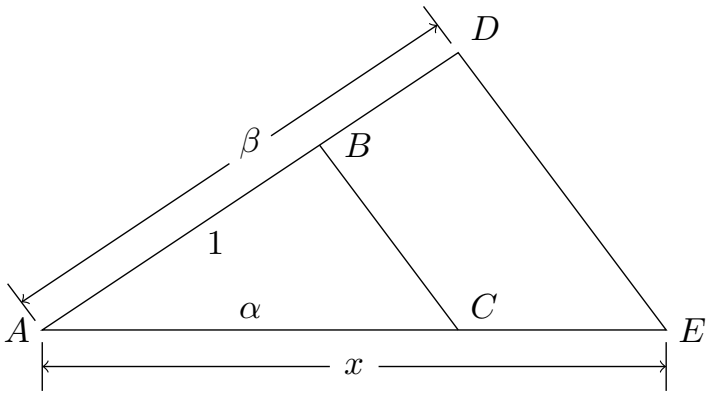
Pertama-tama, mari kita tentukan secara lebih khusus apa yang dimaksud dengan penggaris lurus dan jangka, serta menelaah sifat masalah-masalah ini secara lebih mendalam. Sebagai permulaan, *penggaris lurus bukanlah penggaris ukur*. Kita tidak dapat mengukur sembarang panjang dengan penggaris lurus. Alat ini hanya digunakan untuk menggambar garis melalui dua titik. Pernyataan bahwa triseksi sembarang sudut mustahil berarti terdapat sedikitnya satu sudut yang mustahil ditriseksi dengan konstruksi penggaris lurus dan jangka. Dalam kasus-kasus khusus, suatu sudut tentu dapat ditriseksi. Kita dapat mengonstruksi sudut 30°; jadi, sudut 90° dapat ditriseksi. Akan tetapi, kita akan menunjukkan bahwa sudut 20° mustahil dikonstruksi. Oleh karena itu, kita tidak dapat mentriseksi sudut 60°.

21.3.1 Bilangan yang Dapat Dikonstruksi

Bilangan real α disebut **dapat dikonstruksi** jika kita dapat mengonstruksi ruas garis sepanjang $|\alpha|$ dalam sejumlah hingga langkah dari ruas garis satuan dengan menggunakan penggaris lurus dan jangka.

Teorema 21.3.1 *Himpunan semua bilangan real yang dapat dikonstruksi membentuk sublapangan F dari lapangan bilangan real.*

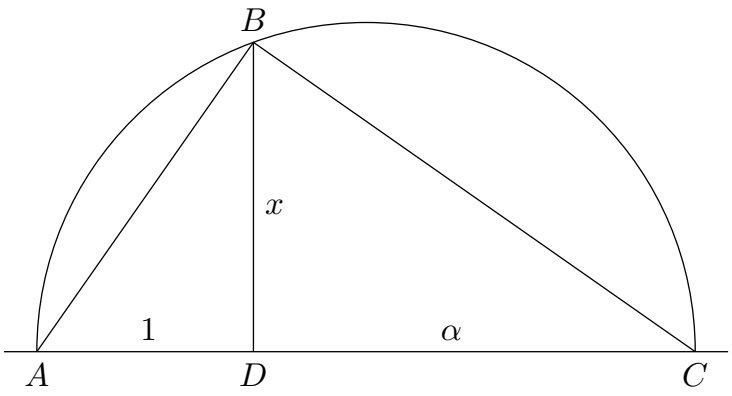
Bukti. Misalkan α dan β bilangan yang dapat dikonstruksi. Kita harus menunjukkan bahwa $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, dan α/β ($\beta \neq 0$) juga merupakan bilangan yang dapat dikonstruksi. Kita dapat mengasumsikan α dan β keduanya positif dengan $\alpha > \beta$. Cara mengonstruksi $\alpha + \beta$ dan $\alpha - \beta$ cukup jelas. Untuk memperoleh ruas garis sepanjang $\alpha\beta$, kita asumsikan $\beta > 1$ dan mengonstruksi segitiga dalam Gambar 21.3.2 sedemikian sehingga segitiga $\triangle ABC$ dan $\triangle ADE$ sebangun. Karena $\alpha/1 = x/\beta$, ruas garis x memiliki panjang $\alpha\beta$. Konstruksi serupa dapat dibuat jika $\beta < 1$. Kita serahkan sebagai latihan untuk menunjukkan bahwa segitiga yang sama dapat digunakan untuk mengonstruksi α/β untuk $\beta \neq 0$. ■



Gambar 21.3.2 Konstruksi hasil kali

Lema 21.3.3 *Jika α merupakan bilangan yang dapat dikonstruksi, maka $\sqrt{\alpha}$ merupakan bilangan yang dapat dikonstruksi.*

BUKTI. Dalam Gambar 21.3.4, segitiga $\triangle ABD$, $\triangle BCD$, dan $\triangle ABC$ sebangun; jadi, $1/x = x/\alpha$, atau $x^2 = \alpha$. ■



Gambar 21.3.4 Konstruksi akar

Berdasarkan Teorema 21.3.1, kita dapat menempatkan pada bidang setiap titik $P = (p, q)$ yang memiliki koordinat rasional p dan q. Kita perlu mengetahui titik-titik lain yang dapat dikonstruksi dengan jangka dan penggaris lurus dari titik-titik berkoordinat rasional.

Lema 21.3.5 *Misalkan F suatu sublapangan dari $\mathbb{R}$.*

1. *Jika suatu garis memuat dua titik di F, maka garis itu memiliki persamaan $ax + by + c = 0$, dengan a, b, dan c berada di F.*

2. *Jika suatu lingkaran berpusat di titik dengan koordinat di F dan berjari-jari yang juga berada di F, maka lingkaran itu memiliki persamaan $x^2 + y^2 + dx + ey + f = 0$, dengan d, e, dan f berada di F.*

BUKTI. Misalkan (x_1, y_1) dan (x_2, y_2) titik-titik pada suatu garis yang koordinatnya berada di F. Jika $x_1 = x_2$, maka persamaan garis melalui kedua titik tersebut adalah $x - x_1 = 0$, yang berbentuk $ax + by + c = 0$. Jika $x_1 \neq x_2$, maka persamaan garis melalui kedua titik diberikan oleh

$$y - y_1 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x - x_1),$$

yang juga dapat dinyatakan dalam bentuk yang sesuai.

Untuk membuktikan bagian kedua lema, misalkan (x_1, y_1) pusat lingkaran berjari-jari r. Maka lingkaran itu memiliki persamaan

$$(x - x_1)^2 + (y - y_1)^2 - r^2 = 0.$$

Persamaan ini mudah dinyatakan dalam bentuk yang sesuai. ■

Dengan memulai dari lapangan bilangan yang dapat dikonstruksi F, kita memiliki tiga cara yang mungkin untuk mengonstruksi titik-titik tambahan di $\mathbb{R}$ dengan jangka dan penggaris lurus.

1. Untuk menemukan titik-titik baru yang mungkin di $\mathbb{R}$, kita dapat mengambil perpotongan dua garis, yang masing-masing melalui dua titik yang diketahui dengan koordinat di F.

2. Perpotongan garis yang melalui dua titik berkoordinat di F dengan ling-

karan yang pusatnya berkoordinat di F dan panjang jari-jarinya berada di F akan menghasilkan titik-titik baru di $\mathbb{R}$.

3. Kita dapat memperoleh titik-titik baru di $\mathbb{R}$ dengan memperpotongkan dua lingkaran yang pusatnya berkoordinat di F dan panjang jari-jarinya berada di F.

Kasus pertama tidak menghasilkan titik baru di $\mathbb{R}$, karena penyelesaian dua persamaan berbentuk $ax+by+c=0$ dengan koefisien di F akan selalu berada di F. Kasus ketiga dapat direduksi menjadi kasus kedua. Misalkan

$$x^2+y^2+d_1x+e_1y+f_1=0$$
$$x^2+y^2+d_2x+e_2y+f_2=0$$

adalah persamaan dua lingkaran, dengan d_i, e_i, dan f_i berada di F untuk $i=1,2$. Kedua lingkaran ini memiliki titik potong yang sama dengan lingkaran

$$x^2+y^2+d_1x+e_1x+f_1=0$$

dan garis

$$(d_1-d_2)x+b(e_2-e_1)y+(f_2-f_1)=0.$$

Persamaan terakhir adalah persamaan tali busur yang melalui titik-titik potong kedua lingkaran. Jadi, perpotongan dua lingkaran dapat direduksi menjadi kasus perpotongan garis dengan lingkaran.

Dengan meninjau kasus perpotongan garis dan lingkaran, kita harus menentukan sifat penyelesaian persamaan-persamaan

$$ax+by+c=0$$
$$x^2+y^2+dx+ey+f=0.$$

Jika kita mengeliminasi y dari persamaan-persamaan ini, kita memperoleh persamaan berbentuk $Ax^2+Bx+C=0$, dengan A, B, dan C berada di F. Koordinat x dari titik-titik potong diberikan oleh

$$x=\frac{-B\pm\sqrt{B^2-4AC}}{2A}$$

dan berada di $F(\sqrt{\alpha}\,)$, dengan $\alpha=B^2-4AC>0$. Kita telah membuktikan lema berikut.

Lema 21.3.6 *Misalkan F lapangan bilangan yang dapat dikonstruksi. Maka titik-titik yang ditentukan oleh perpotongan garis dan lingkaran di F terletak dalam lapangan $F(\sqrt{\alpha}\,)$ untuk suatu α di F.*

Teorema 21.3.7 *Bilangan real α dapat dikonstruksi jika dan hanya jika terdapat barisan lapangan*

$$\mathbb{Q}=F_0\subset F_1\subset\cdots\subset F_k$$

sedemikian sehingga $F_i=F_{i-1}(\sqrt{\alpha_i}\,)$ dengan $\alpha_i\in F_{i-1}$ dan $\alpha\in F_k$. Secara khusus, terdapat bilangan bulat $k>0$ sedemikian sehingga $[\mathbb{Q}(\alpha):\mathbb{Q}]=2^k$.

Bukti. Keberadaan setiap F_i dan α_i merupakan konsekuensi langsung dari Lema 21.3.6 dan fakta bahwa

$$[F_k:\mathbb{Q}]=[F_k:F_{k-1}][F_{k-1}:F_{k-2}]\cdots[F_1:\mathbb{Q}]=2^k.$$

■

Korolari 21.3.8 *Lapangan semua bilangan yang dapat dikonstruksi merupakan perluasan aljabar dari* $\mathbb{Q}$.

Seperti terlihat dari lapangan bilangan yang dapat dikonstruksi, tidak setiap perluasan aljabar dari suatu lapangan merupakan perluasan hingga.

21.3.2 Menggandakan Kubus dan Menguadratkan Lingkaran

Kini kita siap menyelidiki masalah klasik menggandakan kubus dan menguadratkan lingkaran. Kita dapat menggunakan lapangan bilangan yang dapat dikonstruksi untuk menunjukkan dengan tepat kapan suatu konstruksi geometri dapat dilakukan.

Menggandakan kubus adalah mustahil. Untuk rusuk suatu kubus yang diberikan, mustahil mengonstruksi dengan penggaris lurus dan jangka rusuk kubus yang volumenya dua kali volume kubus semula. Misalkan kubus semula memiliki rusuk sepanjang 1 dan, oleh karena itu, volume 1. Jika kita dapat mengonstruksi kubus bervolume 2, kubus baru ini akan memiliki rusuk sepanjang $\sqrt[3]{2}$. Akan tetapi, $\sqrt[3]{2}$ merupakan nol dari polinomial tak tereduksi $x^3 - 2$ atas $\mathbb{Q}$; jadi,

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

Hal ini mustahil karena 3 bukan pangkat dari 2.

Menguadratkan lingkaran. Misalkan kita memiliki lingkaran berjari-jari 1. Luas lingkaran itu adalah π; oleh karena itu, kita harus dapat mengonstruksi persegi dengan sisi $\sqrt{\pi}$. Hal ini mustahil karena π dan, akibatnya, $\sqrt{\pi}$ keduanya transenden. Oleh karena itu, dengan menggunakan penggaris lurus dan jangka, kita tidak mungkin mengonstruksi persegi yang luasnya sama dengan lingkaran tersebut.

21.3.3 Mentriseksi Sudut

Mentriseksi sembarang sudut adalah mustahil. Kita akan menunjukkan bahwa sudut 20° mustahil dikonstruksi. Akibatnya, sudut 60° tidak dapat ditriseksi. Pertama-tama kita perlu menghitung rumus sudut rangkap tiga untuk kosinus:

$$\begin{aligned}
\cos 3\theta &= \cos(2\theta + \theta) \\
&= \cos 2\theta \cos\theta - \sin 2\theta \sin\theta \\
&= (2\cos^2\theta - 1)\cos\theta - 2\sin^2\theta \cos\theta \\
&= (2\cos^2\theta - 1)\cos\theta - 2(1 - \cos^2\theta)\cos\theta \\
&= 4\cos^3\theta - 3\cos\theta.
\end{aligned}$$

Sudut θ dapat dikonstruksi jika dan hanya jika $\alpha = \cos\theta$ dapat dikonstruksi. Misalkan $\theta = 20^\circ$. Maka $\cos 3\theta = \cos 60^\circ = 1/2$. Berdasarkan rumus sudut rangkap tiga untuk kosinus,

$$4\alpha^3 - 3\alpha = \frac{1}{2}.$$

Oleh karena itu, α merupakan nol dari $8x^3 - 6x - 1$. Polinomial ini tidak memiliki faktor di $\mathbb{Z}[x]$, sehingga tak tereduksi atas $\mathbb{Q}[x]$. Jadi, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Akibatnya, α tidak dapat dikonstruksi.

Catatan Sejarah

Teori bilangan aljabar menggunakan perangkat aljabar untuk menyelesaikan masalah dalam teori bilangan. Teori bilangan aljabar modern bermula dengan Pierre de Fermat (1601–1665). Tentu saja kita dapat menemukan banyak bilangan bulat positif yang memenuhi persamaan $x^2+y^2=z^2$; Fermat menduga bahwa persamaan $x^n+y^n=z^n$ tidak memiliki penyelesaian bilangan bulat positif untuk $n \geq 3$. Ia menulis pada margin salinan terjemahan Latin *Arithmetica* karya Diophantus bahwa ia telah menemukan bukti yang menakjubkan untuk teorema ini, tetapi margin buku tersebut terlalu sempit untuk memuatnya. Dengan melanjutkan karya matematikawan lain, Andrew Wiles akhirnya berhasil membuktikan Teorema Terakhir Fermat pada 1990-an. Pencapaian Wiles diberitakan di halaman depan *New York Times*.
Upaya membuktikan Teorema Terakhir Fermat telah menghasilkan sumbangan penting bagi teori bilangan aljabar dari matematikawan terkemuka seperti Leonhard Euler (1707–1783). Kemajuan penting dalam pemahaman Teorema Terakhir Fermat dicapai oleh Ernst Kummer (1810–1893). Murid Kummer, Leopold Kronecker (1823–1891), menjadi salah satu ahli aljabar terkemuka pada abad kesembilan belas. Teori ideal Kronecker dan kajiannya mengenai teori bilangan aljabar memberikan banyak sumbangan bagi pemahaman lapangan.
David Hilbert (1862–1943) dan Hermann Minkowski (1864–1909) termasuk matematikawan yang merintis bidang ini pada awal abad kedua puluh. Hilbert dan Minkowski sama-sama menjadi matematikawan di Universitas Göttingen, Jerman. Göttingen benar-benar merupakan salah satu pusat penelitian matematika terpenting selama dua abad terakhir. Banyak matematikawan luar biasa yang belajar di sana, termasuk Gauss, Dirichlet, Riemann, Dedekind, Noether, dan Weyl.
André Weil menjawab pertanyaan dalam teori bilangan dengan menggunakan geometri aljabar, bidang matematika yang mengkaji geometri melalui kajian gelanggang komutatif. Dari sekitar tahun 1955 hingga 1970, Alexander Grothendieck mendominasi bidang geometri aljabar. Pierre Deligne, seorang murid Grothendieck, menyelesaikan beberapa konjektur Weil dalam teori bilangan.
Salah satu sumbangan terbaru bagi aljabar dan teori bilangan adalah bukti Gerd Faltings atas konjektur Mordell. Konjektur Mordell ini, yang kini dikenal sebagai teorema Faltings, pada intinya menyatakan bahwa polinomial tertentu $p(x,y)$ di $\mathbb{Z}[x,y]$ hanya memiliki sejumlah hingga penyelesaian integral.

21.4 Pertanyaan Bacaan

1. Apa artinya perluasan lapangan E dari lapangan F merupakan perluasan sederhana dari F?

2. Apa definisi polinomial minimal dari elemen $\alpha \in E$, dengan E perluasan dari F, dan α aljabar atas F?

3. Jelaskan bagaimana aljabar linear berperan dalam bab ini. Hasil penting apa yang bergantung pada bukti yang hampir seluruhnya berupa aljabar linear?

4. Apa definisi lapangan yang tertutup secara aljabar?

5. Apa yang dimaksud dengan lapangan pemisah dari polinomial $p(x) \in F[x]$?

21.5 Latihan

1. Tunjukkan bahwa setiap bilangan berikut aljabar atas $\mathbb{Q}$ dengan menentukan polinomial minimal bilangan tersebut atas $\mathbb{Q}$.

(a) $\sqrt{1/3+\sqrt{7}}$

(b) $\sqrt{3}+\sqrt[3]{5}$

(c) $\sqrt{3}+\sqrt{2}\,i$

(d) $\cos\theta + i\sin\theta$ untuk $\theta = 2\pi/n$ dengan $n \in \mathbb{N}$

(e) $\sqrt{\sqrt[3]{2}-i}$

Petunjuk. (a) $x^4-(2/3)x^2-62/9$; (c) x^4-2x^2+25.

2. Tentukan suatu basis untuk setiap perluasan lapangan berikut. Berapakah derajat setiap perluasan?

(a) $\mathbb{Q}(\sqrt{3},\sqrt{6}\,)$ atas $\mathbb{Q}$

(b) $\mathbb{Q}(\sqrt[3]{2},\sqrt[3]{3}\,)$ atas $\mathbb{Q}$

(c) $\mathbb{Q}(\sqrt{2},i)$ atas $\mathbb{Q}$

(d) $\mathbb{Q}(\sqrt{3},\sqrt{5},\sqrt{7}\,)$ atas $\mathbb{Q}$

(e) $\mathbb{Q}(\sqrt{2},\sqrt[3]{2}\,)$ atas $\mathbb{Q}$

(f) $\mathbb{Q}(\sqrt{8}\,)$ atas $\mathbb{Q}(\sqrt{2}\,)$

(g) $\mathbb{Q}(i,\sqrt{2}+i,\sqrt{3}+i)$ atas $\mathbb{Q}$

(h) $\mathbb{Q}(\sqrt{2}+\sqrt{5}\,)$ atas $\mathbb{Q}(\sqrt{5}\,)$

(i) $\mathbb{Q}(\sqrt{2},\sqrt{6}+\sqrt{10}\,)$ atas $\mathbb{Q}(\sqrt{3}+\sqrt{5}\,)$

Petunjuk. (a) $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\,\}$; (c) $\{1,i,\sqrt{2},\sqrt{2}\,i\}$; (e) $\{1,2^{1/6},2^{1/3},2^{1/2},2^{2/3},2^{5/6}\}$.

3. Tentukan lapangan pemisah untuk setiap polinomial berikut.

(a) x^4-10x^2+21 atas $\mathbb{Q}$

(b) x^4+1 atas $\mathbb{Q}$

(c) x^3+2x+2 atas $\mathbb{Z}_3$

(d) x^3-3 atas $\mathbb{Q}$

Petunjuk. (a) $\mathbb{Q}(\sqrt{3},\sqrt{7}\,)$.

4. Tinjau perluasan lapangan $\mathbb{Q}(\sqrt[4]{3},i)$ atas $\mathbb{Q}$.

(a) Tentukan suatu basis untuk perluasan lapangan $\mathbb{Q}(\sqrt[4]{3},i)$ atas $\mathbb{Q}$. Simpulkan bahwa $[\mathbb{Q}(\sqrt[4]{3},i):\mathbb{Q}]=8$.

(b) Tentukan semua sublapangan F dari $\mathbb{Q}(\sqrt[4]{3},i)$ sedemikian sehingga $[F:\mathbb{Q}]=2$.

(c) Tentukan semua sublapangan F dari $\mathbb{Q}(\sqrt[4]{3},i)$ sedemikian sehingga $[F:\mathbb{Q}]=4$.

5. Tunjukkan bahwa $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ merupakan lapangan dengan delapan elemen. Buat tabel perkalian untuk grup perkalian lapangan tersebut.

Petunjuk. Gunakan fakta bahwa elemen-elemen $\mathbb{Z}_2[x]/\langle x^3+x+1\rangle$ adalah $0,\ 1,\ \alpha,\ 1+\alpha,\ \alpha^2,\ 1+\alpha^2,\ \alpha+\alpha^2,\ 1+\alpha+\alpha^2$ serta fakta bahwa $\alpha^3+\alpha+1=0$.

6. Tunjukkan bahwa segi-9 beraturan tidak dapat dikonstruksi dengan penggaris lurus dan jangka, tetapi segi-20 beraturan dapat dikonstruksi.

7. Buktikan bahwa kosinus satu derajat ($\cos 1^\circ$) aljabar atas $\mathbb{Q}$ tetapi tidak dapat dikonstruksi.

8. Dapatkah dikonstruksi suatu kubus dengan volume tiga kali volume kubus yang diberikan?

Petunjuk. Tidak.

9. Buktikan bahwa $\mathbb{Q}(\sqrt{3}, \sqrt[4]{3}, \sqrt[8]{3}, \ldots)$ merupakan perluasan aljabar dari $\mathbb{Q}$, tetapi bukan perluasan hingga.

10. Buktikan atau sangkal: π aljabar atas $\mathbb{Q}(\pi^3)$.

11. Misalkan $p(x)$ polinomial takkonstan berderajat n di $F[x]$. Buktikan bahwa terdapat lapangan pemisah E untuk $p(x)$ sedemikian sehingga $[E:F] \leq n!$.

12. Buktikan atau sangkal: $\mathbb{Q}(\sqrt{2}\,) \cong \mathbb{Q}(\sqrt{3}\,)$.

13. Buktikan bahwa lapangan $\mathbb{Q}(\sqrt[4]{3}\,)$ dan $\mathbb{Q}(\sqrt[4]{3}\,i)$ isomorfik tetapi tidak sama.

14. Misalkan K perluasan aljabar dari E, dan E perluasan aljabar dari F. Buktikan bahwa K aljabar atas F. [*Perhatian*: Jangan mengasumsikan bahwa perluasan-perluasan tersebut hingga.]

Petunjuk. Misalkan E aljabar atas F dan K aljabar atas E. Misalkan $\alpha \in K$. Cukup ditunjukkan bahwa α aljabar atas suatu perluasan hingga dari F. Karena α aljabar atas E, elemen tersebut harus merupakan nol dari suatu polinomial $p(x) = \beta_0+\beta_1 x+\cdots+\beta_n x^n$ di $E[x]$. Jadi, α aljabar atas $F(\beta_0, \ldots, \beta_n)$.

15. Buktikan atau sangkal: $\mathbb{Z}[x]/\langle x^3-2\rangle$ merupakan lapangan.

16. Misalkan F lapangan berkarakteristik p. Buktikan bahwa $p(x) = x^p - a$ tak tereduksi atas F atau terpisah di F.

17. Misalkan E penutupan aljabar dari lapangan F. Buktikan bahwa setiap polinomial $p(x)$ di $F[x]$ terpisah di E.

18. Jika setiap polinomial tak tereduksi $p(x)$ di $F[x]$ bersifat linear, tunjukkan bahwa F merupakan lapangan yang tertutup secara aljabar.

19. Buktikan bahwa jika α dan β bilangan yang dapat dikonstruksi sedemikian sehingga $\beta \neq 0$, maka α/β juga dapat dikonstruksi.

20. Tunjukkan bahwa himpunan semua elemen di $\mathbb{R}$ yang aljabar atas $\mathbb{Q}$ membentuk perluasan lapangan dari $\mathbb{Q}$ yang tidak hingga.

21. Misalkan E perluasan aljabar dari lapangan F, dan σ automorfisme dari E yang menetapkan F. Misalkan $\alpha \in E$. Tunjukkan bahwa σ menginduksi permutasi pada himpunan semua nol dari polinomial minimal α yang berada di E.

22. Tunjukkan bahwa $\mathbb{Q}(\sqrt{3}, \sqrt{7}\,) = \mathbb{Q}(\sqrt{3}+\sqrt{7}\,)$. Perluas bukti Anda untuk menunjukkan bahwa $\mathbb{Q}(\sqrt{a}, \sqrt{b}\,) = \mathbb{Q}(\sqrt{a}+\sqrt{b}\,)$, dengan $a \neq b$ dan a maupun b bukan kuadrat sempurna.

Petunjuk. Karena $\{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\,\}$ merupakan basis un-

tuk $\mathbb{Q}(\sqrt{3},\sqrt{7})$ atas $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3},\sqrt{7}) \supset \mathbb{Q}(\sqrt{3}+\sqrt{7})$. Karena $[\mathbb{Q}(\sqrt{3},\sqrt{7}) : \mathbb{Q}] = 4$, $[\mathbb{Q}(\sqrt{3}+\sqrt{7}) : \mathbb{Q}] = 2$ atau 4. Karena derajat polinomial minimal dari $\sqrt{3}+\sqrt{7}$ adalah 4, $\mathbb{Q}(\sqrt{3},\sqrt{7}) = \mathbb{Q}(\sqrt{3}+\sqrt{7})$.

23. Misalkan E perluasan hingga dari lapangan F. Jika $[E : F] = 2$, tunjukkan bahwa E merupakan lapangan pemisah dari F untuk suatu polinomial $f(x) \in F[x]$.

24. Buktikan atau sangkal: Untuk suatu polinomial $p(x)$ di $\mathbb{Z}_6[x]$, dapat dibangun gelanggang R sedemikian sehingga $p(x)$ memiliki akar di R.

25. Misalkan E perluasan lapangan dari F dan $\alpha \in E$. Tentukan $[F(\alpha) : F(\alpha^3)]$.

26. Misalkan α, β transenden atas $\mathbb{Q}$. Buktikan bahwa $\alpha\beta$ atau $\alpha+\beta$ juga transenden.

27. Misalkan E perluasan lapangan dari F dan $\alpha \in E$ transenden atas F. Buktikan bahwa setiap elemen di $F(\alpha)$ yang tidak berada di F juga transenden atas F.

Petunjuk. Misalkan $\beta \in F(\alpha)$ tidak berada di F. Maka $\beta = p(\alpha)/q(\alpha)$, dengan p dan q polinomial dalam α yang memiliki $q(\alpha) \neq 0$ dan koefisien di F. Jika β aljabar atas F, maka terdapat polinomial $f(x) \in F[x]$ sedemikian sehingga $f(\beta) = 0$. Misalkan $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Maka

$$0 = f(\beta) = f\left(\frac{p(\alpha)}{q(\alpha)}\right) = a_0 + a_1\left(\frac{p(\alpha)}{q(\alpha)}\right) + \cdots + a_n\left(\frac{p(\alpha)}{q(\alpha)}\right)^n.$$

Sekarang kalikan kedua ruas dengan $q(\alpha)^n$ untuk menunjukkan bahwa terdapat polinomial di $F[x]$ yang memiliki α sebagai nol.

28. Misalkan α akar dari polinomial monik tak tereduksi $p(x) \in F[x]$, dengan $\deg p = n$. Buktikan bahwa $[F(\alpha) : F] = n$.

Petunjuk. Lihat penjelasan setelah Teorema 21.1.13.

21.6 Referensi dan Bacaan yang Disarankan

[1] Dean, R. A. *Elements of Abstract Algebra* . Wiley, New York, 1966.

[2] Dudley, U. *A Budget of Trisections*. Springer-Verlag, New York, 1987. Uraian yang menarik dan menghibur tentang bagaimana tidak membagi tiga sebuah sudut.

[3] Fraleigh, J. B. *A First Course in Abstract Algebra*. 7th ed. Pearson, Upper Saddle River, NJ, 2003.

[4] Kaplansky, I. *Fields and Rings*, 2nd ed. University of Chicago Press, Chicago, 1972.

[5] Klein, F. *Famous Problems of Elementary Geometry*. Chelsea, New York, 1955.

[6] Martin, G. *Geometric Constructions*. Springer, New York, 1998.

[7] H. Pollard and H. G. Diamond. *Theory of Algebraic Numbers*, Dover, Mineola, NY, 2010.

[8] Walker, E. A. *Introduction to Abstract Algebra*. Random House, New York, 1987. Karya ini memuat bukti bahwa setiap lapangan memiliki penutupan aljabar.

22

Lapangan Hingga

Lapangan hingga muncul dalam banyak penerapan aljabar, termasuk teori pengodean dan kriptografi. Kita telah mengenal satu lapangan hingga, yaitu $\mathbb{Z}_p$, dengan p prima. Dalam bab ini kita akan menunjukkan bahwa terdapat lapangan hingga tunggal berorde p^n untuk setiap prima p, dengan n suatu bilangan bulat positif. Lapangan hingga juga disebut lapangan Galois untuk menghormati Évariste Galois, salah satu matematikawan pertama yang menyelidikinya.

22.1 Struktur Lapangan Hingga

Ingat bahwa lapangan F mempunyai **karakteristik** p jika p merupakan bilangan bulat positif terkecil sedemikian sehingga untuk setiap elemen tak nol α dalam F, berlaku $p\alpha = 0$. Jika bilangan bulat semacam itu tidak ada, maka F berkarakteristik 0. Dari Teorema 16.2.8 kita mengetahui bahwa p harus prima. Andaikan F suatu lapangan hingga dengan n elemen. Maka $n\alpha = 0$ untuk semua α dalam F. Akibatnya, karakteristik F haruslah p, dengan p suatu prima yang membagi n. Pembahasan ini dirangkum dalam proposisi berikut.

Proposisi 22.1.1 *Jika F merupakan lapangan hingga, maka karakteristik F adalah p, dengan p prima.*

Sepanjang bab ini kita akan mengandaikan bahwa p merupakan bilangan prima, kecuali dinyatakan lain.

Proposisi 22.1.2 *Jika F merupakan lapangan hingga berkarakteristik p, maka orde F adalah p^n untuk suatu $n \in \mathbb{N}$.*

Bukti. Misalkan $\phi : \mathbb{Z} \to F$ homomorfisma gelanggang yang didefinisikan oleh $\phi(n) = n \cdot 1$. Karena karakteristik F adalah p, kernel ϕ haruslah $p\mathbb{Z}$ dan citra ϕ harus merupakan sublapangan dari F yang isomorfik dengan $\mathbb{Z}_p$. Sublapangan ini akan kita nyatakan dengan K. Karena F merupakan lapangan hingga, lapangan tersebut harus merupakan perluasan hingga dari K dan, oleh karena itu, perluasan aljabar dari K. Andaikan bahwa $[F : K] = n$ merupakan dimensi F, dengan F sebagai ruang vektor atas K. Harus terdapat elemen-elemen $\alpha_1, \ldots, \alpha_n \in F$ sedemikian sehingga sebarang elemen α dalam F dapat ditulis secara tunggal dalam bentuk

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n,$$

dengan a_i berada dalam K. Karena terdapat p elemen dalam K, terdapat p^n

kombinasi linear yang mungkin dari α_i. Oleh karena itu, orde F haruslah p^n. ■

Lema 22.1.3 Impian Mahasiswa Baru. *Misalkan p prima dan D suatu daerah integral berkarakteristik p. Maka*

$$a^{p^n} + b^{p^n} = (a+b)^{p^n}$$

untuk semua bilangan bulat positif n.

BUKTI. Kita akan membuktikan lema ini dengan induksi matematika pada n. Kita dapat menggunakan rumus binomial (lihat Contoh 2.1.4) untuk memverifikasi kasus $n = 1$; yaitu,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}.$$

Jika $0 < k < p$, maka

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

harus dapat dibagi oleh p, karena p tidak dapat membagi $k!(p-k)!$. Perhatikan bahwa D merupakan daerah integral berkarakteristik p, sehingga semua suku dalam jumlah tersebut, kecuali suku pertama dan terakhir, harus nol. Oleh karena itu, $(a+b)^p = a^p + b^p$.

Sekarang andaikan bahwa hasil tersebut berlaku untuk semua k, dengan $1 \leq k \leq n$. Berdasarkan hipotesis induksi,

$$(a+b)^{p^{n+1}} = ((a+b)^p)^{p^n} = (a^p + b^p)^{p^n} = (a^p)^{p^n} + (b^p)^{p^n} = a^{p^{n+1}} + b^{p^{n+1}}.$$

Oleh karena itu, lema tersebut benar untuk $n+1$ dan bukti selesai. ■

Misalkan F suatu lapangan. Polinomial $f(x) \in F[x]$ berderajat n disebut **separabel** jika polinomial tersebut mempunyai n akar berbeda dalam lapangan pemisah dari $f(x)$; artinya, $f(x)$ separabel apabila dapat difaktorkan menjadi faktor-faktor linear berbeda di atas lapangan pemisah dari f. Suatu perluasan E dari F merupakan **perluasan separabel** dari F jika setiap elemen dalam E merupakan akar dari polinomial separabel dalam $F[x]$.

Contoh 22.1.4 Polinomial x^2-2 separabel di atas $\mathbb{Q}$ karena dapat difaktorkan sebagai $(x-\sqrt{2}\,)(x+\sqrt{2}\,)$. Bahkan, $\mathbb{Q}(\sqrt{2}\,)$ merupakan perluasan separabel dari $\mathbb{Q}$. Misalkan $\alpha = a + b\sqrt{2}$ sebarang elemen dalam $\mathbb{Q}(\sqrt{2}\,)$. Jika $b = 0$, maka α merupakan akar dari $x - a$. Jika $b \neq 0$, maka α merupakan akar dari polinomial separabel

$$x^2 - 2ax + a^2 - 2b^2 = (x - (a + b\sqrt{2}\,))(x - (a - b\sqrt{2}\,)).$$

▲

Untungnya, kita mempunyai uji yang mudah untuk menentukan separabilitas sebarang polinomial. Misalkan

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

sebarang polinomial dalam $F[x]$. Definisikan **turunan** dari $f(x)$ sebagai

$$f'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

Lema 22.1.5 *Misalkan F suatu lapangan dan $f(x) \in F[x]$. Maka $f(x)$ separabel jika dan hanya jika $f(x)$ dan $f'(x)$ relatif prima.*

BUKTI. Misalkan $f(x)$ separabel. Maka $f(x)$ dapat difaktorkan di atas suatu lapangan perluasan dari F sebagai $f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, dengan $\alpha_i \neq \alpha_j$ untuk $i \neq j$. Dengan mengambil turunan $f(x)$, kita melihat bahwa

$$\begin{aligned} f'(x) &= (x-\alpha_2)\cdots(x-\alpha_n) \\ &\quad + (x-\alpha_1)(x-\alpha_3)\cdots(x-\alpha_n) \\ &\quad + \cdots + (x-\alpha_1)\cdots(x-\alpha_{n-1}). \end{aligned}$$

Jadi, $f(x)$ dan $f'(x)$ tidak mungkin mempunyai faktor persekutuan.

Untuk membuktikan kebalikannya, kita akan menunjukkan bahwa kontraposisi pernyataan tersebut benar. Andaikan bahwa $f(x) = (x-\alpha)^k g(x)$, dengan $k > 1$. Dengan menurunkannya, kita memperoleh

$$f'(x) = k(x-\alpha)^{k-1}g(x) + (x-\alpha)^k g'(x).$$

Oleh karena itu, $f(x)$ dan $f'(x)$ mempunyai faktor persekutuan. ■

Teorema 22.1.6 *Untuk setiap prima p dan setiap bilangan bulat positif n, terdapat lapangan hingga F dengan p^n elemen. Lebih lanjut, setiap lapangan berorde p^n isomorfik dengan lapangan pemisah dari $x^{p^n} - x$ di atas $\mathbb{Z}_p$.*

BUKTI. Misalkan $f(x) = x^{p^n} - x$ dan misalkan F lapangan pemisah dari $f(x)$. Maka menurut Lema 22.1.5, $f(x)$ mempunyai p^n akar berbeda dalam F, karena $f'(x) = p^n x^{p^n-1} - 1 = -1$ relatif prima dengan $f(x)$. Kita mengklaim bahwa akar-akar $f(x)$ membentuk sublapangan dari F. Jelas bahwa 0 dan 1 merupakan akar dari $f(x)$. Jika α dan β merupakan akar dari $f(x)$, maka $\alpha+\beta$ dan $\alpha\beta$ juga merupakan akar dari $f(x)$, karena $\alpha^{p^n} + \beta^{p^n} = (\alpha+\beta)^{p^n}$ dan $\alpha^{p^n}\beta^{p^n} = (\alpha\beta)^{p^n}$. Kita juga perlu menunjukkan bahwa invers aditif dan invers multiplikatif dari setiap akar $f(x)$ merupakan akar dari $f(x)$. Untuk sebarang akar α dari $f(x)$, kita mengetahui bahwa $-\alpha$ juga merupakan akar dari $f(x)$, karena

$$f(-\alpha) = (-\alpha)^{p^n} - (-\alpha) = -\alpha^{p^n} + \alpha = -(\alpha^{p^n} - \alpha) = 0,$$

asalkan p ganjil. Jika $p = 2$, maka

$$f(-\alpha) = (-\alpha)^{2^n} - (-\alpha) = \alpha + \alpha = 0.$$

Jika $\alpha \neq 0$, maka $(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}$. Karena akar-akar $f(x)$ membentuk sublapangan dari F dan $f(x)$ terurai dalam sublapangan ini, sublapangan tersebut haruslah seluruh F.

Misalkan E sebarang lapangan lain berorde p^n. Untuk menunjukkan bahwa E isomorfik dengan F, kita harus menunjukkan bahwa setiap elemen dalam E merupakan akar dari $f(x)$. Jelas bahwa 0 merupakan akar dari $f(x)$. Misalkan α elemen tak nol dari E. Orde grup multiplikatif elemen tak nol dari E adalah $p^n - 1$; jadi, $\alpha^{p^n-1} = 1$ atau $\alpha^{p^n} - \alpha = 0$. Karena E memuat p^n elemen, E harus merupakan lapangan pemisah dari $f(x)$; tetapi, menurut Korolari 21.2.8, lapangan pemisah sebarang polinomial tunggal hingga isomorfisma. ■

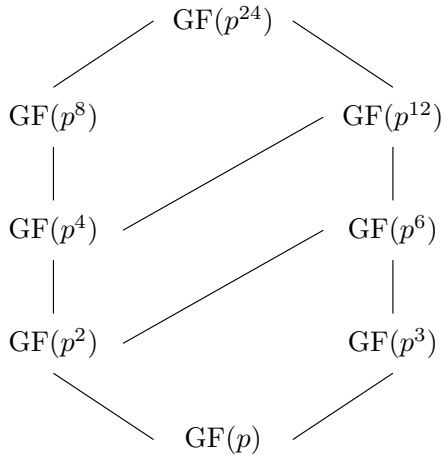
Lapangan hingga tunggal dengan p^n elemen disebut **lapangan Galois** berorde p^n. Lapangan ini akan kita nyatakan dengan $\mathrm{GF}(p^n)$.

Teorema 22.1.7 *Setiap sublapangan dari lapangan Galois $\mathrm{GF}(p^n)$ mempunyai p^m elemen, dengan m membagi n. Sebaliknya, jika $m \mid n$ untuk $m > 0$, maka terdapat sublapangan tunggal dari $\mathrm{GF}(p^n)$ yang isomorfik dengan $\mathrm{GF}(p^m)$.*

BUKTI. Misalkan F sublapangan dari $E = \mathrm{GF}(p^n)$. Maka F harus merupakan perluasan lapangan dari K yang memuat p^m elemen, dengan K isomorfik dengan $\mathbb{Z}_p$. Maka $m \mid n$, karena $[E : K] = [E : F][F : K]$.

Untuk membuktikan kebalikannya, andaikan bahwa $m \mid n$ untuk suatu $m > 0$. Maka $p^m - 1$ membagi $p^n - 1$. Akibatnya, $x^{p^m-1} - 1$ membagi $x^{p^n-1} - 1$. Oleh karena itu, $x^{p^m} - x$ harus membagi $x^{p^n} - x$, dan setiap akar dari $x^{p^m} - x$ juga merupakan akar dari $x^{p^n} - x$. Dengan demikian, $\mathrm{GF}(p^n)$ memuat, sebagai sublapangan, suatu lapangan pemisah dari $x^{p^m} - x$, yang harus isomorfik dengan $\mathrm{GF}(p^m)$. ■

Contoh 22.1.8 Kisi sublapangan dari $\mathrm{GF}(p^{24})$ diberikan dalam Gambar 22.1.9. ▲



Gambar 22.1.9 Sublapangan dari $\mathrm{GF}(p^{24})$

Untuk setiap lapangan F, kita mempunyai grup multiplikatif elemen tak nol dari F yang akan kita nyatakan dengan F^*. Grup multiplikatif sebarang lapangan hingga bersifat siklik. Hasil ini mengikuti hasil yang lebih umum yang akan kita buktikan dalam teorema berikut.

Teorema 22.1.10 *Jika G merupakan subgrup hingga dari F^*, yaitu grup multiplikatif elemen tak nol dari lapangan F, maka G bersifat siklik.*

BUKTI. Misalkan G subgrup hingga dari F^* yang berorde n. Menurut Teorema Dasar Grup Abelian Hingga (Teorema 13.1.4),

$$G \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}},$$

dengan $n = p_1^{e_1} \cdots p_k^{e_k}$ dan $p_1, \ldots, p_k$ merupakan prima (yang tidak harus berbeda). Misalkan m kelipatan persekutuan terkecil dari $p_1^{e_1}, \ldots, p_k^{e_k}$. Maka G memuat elemen berorde m. Karena setiap α dalam G memenuhi $x^r - 1$ untuk suatu r yang membagi m, α juga harus merupakan akar dari $x^m - 1$. Karena $x^m - 1$ mempunyai paling banyak m akar dalam F, $n \leq m$. Di sisi lain, kita mengetahui bahwa $m \leq |G|$; oleh karena itu, $m = n$. Dengan demikian, G memuat elemen berorde n dan harus bersifat siklik. ■

Korolari 22.1.11 *Grup multiplikatif semua elemen tak nol dari suatu lapangan hingga bersifat siklik.*

Korolari 22.1.12 *Setiap perluasan hingga E dari lapangan hingga F merupakan perluasan sederhana dari F.*

BUKTI. Misalkan α pembangkit bagi grup siklik E^* dari elemen-elemen tak nol E. Maka $E = F(\alpha)$. ■

Contoh 22.1.13 Lapangan hingga $\mathrm{GF}(2^4)$ isomorfik dengan lapangan $\mathbb{Z}_2[x]/\langle 1 + x + x^4\rangle$. Oleh karena itu, elemen-elemen $\mathrm{GF}(2^4)$ dapat diambil sebagai

$$\{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 : a_i \in \mathbb{Z}_2 \text{ dan } 1 + \alpha + \alpha^4 = 0\}.$$

Dengan mengingat bahwa $1 + \alpha + \alpha^4 = 0$, kita menjumlahkan dan mengalikan elemen-elemen $\mathrm{GF}(2^4)$ tepat seperti kita menjumlahkan dan mengalikan polinomial. Grup multiplikatif $\mathrm{GF}(2^4)$ isomorfik dengan $\mathbb{Z}_{15}$ dengan pembangkit α:

$$\begin{array}{lll}
\alpha^1 = \alpha & \alpha^6 = \alpha^2 + \alpha^3 & \alpha^{11} = \alpha + \alpha^2 + \alpha^3 \\
\alpha^2 = \alpha^2 & \alpha^7 = 1 + \alpha + \alpha^3 & \alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3 \\
\alpha^3 = \alpha^3 & \alpha^8 = 1 + \alpha^2 & \alpha^{13} = 1 + \alpha^2 + \alpha^3 \\
\alpha^4 = 1 + \alpha & \alpha^9 = \alpha + \alpha^3 & \alpha^{14} = 1 + \alpha^3 \\
\alpha^5 = \alpha + \alpha^2 & \alpha^{10} = 1 + \alpha + \alpha^2 & \alpha^{15} = 1.
\end{array}$$

▲

22.2 Kode Polinomial

Dengan pengetahuan tentang gelanggang polinomial dan lapangan hingga, kini kita dapat memperoleh kode yang lebih canggih daripada kode dalam Bab 8. Pertama-tama, ingat bahwa kode blok-(n, k) terdiri atas fungsi pengodean satu-ke-satu $E : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ dan fungsi pendekodean $D : \mathbb{Z}_2^n \to \mathbb{Z}_2^k$. Kode tersebut bersifat mengoreksi galat jika D surjektif. Suatu kode merupakan kode linear jika kode tersebut adalah ruang nol dari matriks $H \in \mathbb{M}_{k\times n}(\mathbb{Z}_2)$.

Kita tertarik pada suatu kelas kode yang dikenal sebagai **kode siklik**. Misalkan $\phi : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ suatu kode blok-(n, k) biner. Maka ϕ merupakan **kode siklik** jika untuk setiap kata kode $(a_1, a_2, \ldots, a_n)$, tupel-n yang digeser secara siklik, yaitu $(a_n, a_1, a_2, \ldots, a_{n-1})$, juga merupakan kata kode. Kode siklik sangat mudah diimplementasikan pada komputer dengan menggunakan register geser [2, 3].

Contoh 22.2.1 Tinjau kode linear-$(6, 3)$ yang dibangkitkan oleh dua matriks

$$G_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{dan} \quad G_2 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Pesan dalam kode pertama dikodekan sebagai berikut:

$$\begin{array}{llll}
(000) \mapsto (000000) & & (100) \mapsto (100100) \\
(001) \mapsto (001001) & & (101) \mapsto (101101) \\
(010) \mapsto (010010) & & (110) \mapsto (110110) \\
(011) \mapsto (011011) & & (111) \mapsto (111111).
\end{array}$$

Mudah dilihat bahwa kata-kata kode tersebut membentuk kode siklik. Dalam

kode kedua, tupel-3 dikodekan dengan cara berikut:

$$\begin{array}{lcllcl} (000) & \mapsto & (000000) & (100) & \mapsto & (111100) \\ (001) & \mapsto & (001111) & (101) & \mapsto & (110011) \\ (010) & \mapsto & (011110) & (110) & \mapsto & (100010) \\ (011) & \mapsto & (010001) & (111) & \mapsto & (101101). \end{array}$$

Kode ini tidak mungkin siklik, karena (101101) merupakan kata kode, tetapi (011011) bukan kata kode. ▲

22.2.1 Kode Polinomial

Kita ingin menemukan metode yang mudah untuk memperoleh kode linear siklik. Untuk melakukannya, kita dapat menggunakan pengetahuan tentang lapangan hingga dan gelanggang polinomial di atas $\mathbb{Z}_2$. Sebarang tupel-n biner dapat ditafsirkan sebagai polinomial dalam $\mathbb{Z}_2[x]$. Dengan kata lain, tupel-n $(a_0, a_1, \ldots, a_{n-1})$ bersesuaian dengan polinomial

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},$$

dengan derajat $f(x)$ paling tinggi $n-1$. Sebagai contoh, polinomial yang bersesuaian dengan tupel-5 (10011) adalah

$$1 + 0x + 0x^2 + 1x^3 + 1x^4 = 1 + x^3 + x^4.$$

Sebaliknya, dengan sebarang polinomial $f(x) \in \mathbb{Z}_2[x]$ yang memenuhi $\deg f(x) < n$, kita dapat mengaitkan suatu tupel-n biner. Polinomial $x + x^2 + x^4$ bersesuaian dengan tupel-5 (01101).

Tetapkan suatu polinomial tak konstan $g(x)$ dalam $\mathbb{Z}_2[x]$ yang berderajat $n-k$. Kita dapat mendefinisikan kode-(n,k) C dengan cara berikut. Jika $(a_0, \ldots, a_{k-1})$ merupakan tupel-k yang akan dikodekan, maka $f(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}$ merupakan polinomial yang bersesuaian dalam $\mathbb{Z}_2[x]$. Untuk mengodekan $f(x)$, kita mengalikannya dengan $g(x)$. Kata-kata kode dalam C adalah semua polinomial dalam $\mathbb{Z}_2[x]$ yang berderajat kurang dari n dan dapat dibagi oleh $g(x)$. Kode yang diperoleh dengan cara ini disebut **kode polinomial**.

Contoh 22.2.2 Jika kita mengambil $g(x) = 1 + x^3$, kita dapat mendefinisikan kode-$(6,3)$ C sebagai berikut. Untuk mengodekan tupel-3 (a_0, a_1, a_2), kita mengalikan polinomial yang bersesuaian, $f(x) = a_0 + a_1 x + a_2 x^2$, dengan $1 + x^3$. Kita mendefinisikan pemetaan $\phi : \mathbb{Z}_2^3 \to \mathbb{Z}_2^6$ dengan $\phi : f(x) \mapsto g(x)f(x)$. Mudah diperiksa bahwa pemetaan ini merupakan homomorfisma grup. Bahkan, jika kita memandang $\mathbb{Z}_2^n$ sebagai ruang vektor atas $\mathbb{Z}_2$, ϕ merupakan transformasi linear ruang vektor (lihat Latihan 20.5.15). Mari kita hitung kernel ϕ. Perhatikan bahwa $\phi(a_0, a_1, a_2) = (000000)$ tepat ketika

$$\begin{aligned} 0 + 0x + 0x^2 + 0x^3 + 0x^4 + 0x^5 &= (1 + x^3)(a_0 + a_1 x + a_2 x^2) \\ &= a_0 + a_1 x + a_2 x^2 + a_0 x^3 + a_1 x^4 + a_2 x^5. \end{aligned}$$

Karena polinomial di atas suatu lapangan membentuk daerah integral, $a_0 + a_1 x + a_2 x^2$ harus merupakan polinomial nol. Oleh karena itu, $\ker \phi = \{(000)\}$ dan ϕ satu-ke-satu.

Untuk menghitung matriks pembangkit bagi C, kita hanya perlu mengkaji cara polinomial 1, x, dan x^2 dikodekan:

$$(1 + x^3) \cdot 1 = 1 + x^3$$

$$(1+x^3)x = x + x^4$$
$$(1+x^3)x^2 = x^2 + x^5.$$

Kita memperoleh kode yang bersesuaian dengan matriks pembangkit G_1 dalam Contoh 22.2.1. Matriks pemeriksa paritas untuk kode ini adalah

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Karena bobot terkecil sebarang kata kode tak nol adalah 2, kode ini mampu mendeteksi semua galat tunggal. ▲

Gelanggang polinomial memiliki banyak struktur; oleh karena itu, tujuan langsung kita adalah membangun hubungan antara kode polinomial dan teori gelanggang. Ingat bahwa $x^n - 1 = (x-1)(x^{n-1} + \cdots + x + 1)$. Gelanggang hasil bagi

$$R_n = \mathbb{Z}_2[x]/\langle x^n - 1\rangle$$

dapat dipandang sebagai gelanggang polinomial berbentuk

$$f(t) = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1}$$

yang memenuhi syarat $t^n = 1$. Sebagai latihan mudah, tunjukkan bahwa $\mathbb{Z}_2^n$ dan R_n isomorfik sebagai ruang vektor. Kita akan sering mengidentifikasi elemen-elemen dalam $\mathbb{Z}_2^n$ dengan elemen-elemen dalam $\mathbb{Z}[x]/\langle x^n - 1\rangle$. Dengan cara ini, kita dapat menafsirkan kode linear sebagai himpunan bagian dari $\mathbb{Z}[x]/\langle x^n - 1\rangle$.

Struktur gelanggang tambahan pada kode polinomial sangat ampuh untuk mendeskripsikan kode siklik. Pergeseran siklik suatu tupel-n dapat dideskripsikan melalui perkalian polinomial. Jika $f(t) = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1}$ merupakan polinomial kode dalam R_n, maka

$$tf(t) = a_{n-1} + a_0 t + \cdots + a_{n-2}t^{n-1}$$

merupakan kata yang digeser secara siklik, yang diperoleh dengan mengalikan $f(t)$ dengan t. Teorema berikut memberikan klasifikasi indah bagi kode siklik dalam istilah ideal-ideal dari R_n.

Teorema 22.2.3 *Kode linear C dalam $\mathbb{Z}_2^n$ bersifat siklik jika dan hanya jika kode tersebut merupakan ideal dalam $R_n = \mathbb{Z}[x]/\langle x^n - 1\rangle$.*

Bukti. Misalkan C suatu kode linear siklik dan andaikan bahwa $f(t)$ berada dalam C. Maka $tf(t)$ juga harus berada dalam C. Akibatnya, $t^k f(t)$ berada dalam C untuk semua $k \in \mathbb{N}$. Karena C merupakan kode linear, setiap kombinasi linear kata-kata kode $f(t), tf(t), t^2 f(t), \ldots, t^{n-1}f(t)$ juga merupakan kata kode; oleh karena itu, untuk setiap polinomial $p(t)$, $p(t)f(t)$ berada dalam C. Jadi, C merupakan ideal.

Sebaliknya, misalkan C suatu ideal dalam $\mathbb{Z}_2[x]/\langle x^n + 1\rangle$. Andaikan bahwa $f(t) = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1}$ merupakan kata kode dalam C. Maka $tf(t)$ merupakan kata kode dalam C; artinya, $(a_1, \ldots, a_{n-1}, a_0)$ berada dalam C. ■

Teorema 22.2.3 memberi tahu kita bahwa mengetahui ideal-ideal dari R_n ekuivalen dengan mengetahui kode linear siklik dalam $\mathbb{Z}_2^n$. Untungnya, ideal-ideal dalam R_n mudah dideskripsikan. Homomorfisma gelanggang alami $\phi : \mathbb{Z}_2[x] \to R_n$ yang didefinisikan oleh $\phi[f(x)] = f(t)$ merupakan homomorfisma surjektif. Kernel ϕ adalah ideal yang dibangkitkan oleh $x^n - 1$. Menurut Teorema 16.3.15, setiap ideal C dalam R_n berbentuk $\phi(I)$, dengan I suatu

ideal dalam $\mathbb{Z}_2[x]$ yang memuat $\langle x^n - 1\rangle$. Menurut Teorema 17.3.10, kita mengetahui bahwa setiap ideal I dalam $\mathbb{Z}_2[x]$ merupakan ideal utama, karena $\mathbb{Z}_2$ merupakan lapangan. Oleh karena itu, $I = \langle g(x)\rangle$ untuk suatu polinomial monik tunggal dalam $\mathbb{Z}_2[x]$. Karena $\langle x^n - 1\rangle$ termuat dalam I, harus berlaku bahwa $g(x)$ membagi $x^n - 1$. Akibatnya, setiap ideal C dalam R_n berbentuk

$$C = \langle g(t)\rangle = \{f(t)g(t) : f(t) \in R_n \text{ dan } g(x) \mid (x^n - 1) \text{ dalam } \mathbb{Z}_2[x]\}.$$

Polinomial monik tunggal berderajat terkecil yang membangkitkan C disebut **polinomial pembangkit minimal** dari C.

Contoh 22.2.4 Jika kita memfaktorkan $x^7 - 1$ menjadi komponen-komponen tak tereduksi, kita memperoleh

$$x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3).$$

Kita melihat bahwa $g(t) = (1 + t + t^3)$ membangkitkan ideal C dalam R_7. Kode ini merupakan kode blok-$(7, 4)$. Seperti dalam Contoh 22.2.2, matriks pembangkit mudah dihitung dengan mengkaji tindakan $g(t)$ pada polinomial 1, t, t^2, dan t^3. Matriks pembangkit bagi C adalah

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

▲

Secara umum, kita dapat menentukan matriks pembangkit bagi kode-(n, k) C melalui cara elemen-elemen t^k dikodekan. Misalkan $x^n - 1 = g(x)h(x)$ dalam $\mathbb{Z}_2[x]$. Jika $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$ dan $h(x) = h_0 + h_1x + \cdots + h_kx^k$, maka matriks $n \times k$

$$G = \begin{pmatrix} g_0 & 0 & \cdots & 0 \\ g_1 & g_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_{n-k} & g_{n-k-1} & \cdots & g_0 \\ 0 & g_{n-k} & \cdots & g_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_{n-k} \end{pmatrix}$$

merupakan matriks pembangkit bagi kode C dengan polinomial pembangkit $g(t)$. Matriks pemeriksa paritas bagi C adalah matriks $(n - k) \times n$

$$H = \begin{pmatrix} 0 & \cdots & 0 & 0 & h_k & \cdots & h_0 \\ 0 & \cdots & 0 & h_k & \cdots & h_0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ h_k & \cdots & h_0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Perincian bukti proposisi berikut kita serahkan sebagai latihan.

Proposisi 22.2.5 *Misalkan $C = \langle g(t)\rangle$ suatu kode siklik dalam R_n dan andaikan bahwa $x^n - 1 = g(x)h(x)$. Maka G dan H masing-masing merupakan matriks*

pembangkit dan matriks pemeriksa paritas bagi C. Lebih lanjut, $HG = 0$.

Contoh 22.2.6 Dalam Contoh 22.2.4,

$$x^7 - 1 = g(x)h(x) = (1 + x + x^3)(1 + x + x^2 + x^4).$$

Oleh karena itu, matriks pemeriksa paritas untuk kode ini adalah

$$H = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

▲

Untuk menentukan kemampuan mendeteksi dan mengoreksi galat dari suatu kode siklik, kita perlu mengetahui sesuatu tentang determinan. Jika $\alpha_1, \ldots, \alpha_n$ merupakan elemen-elemen dalam lapangan F, maka matriks $n \times n$

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

disebut **matriks Vandermonde**. Determinan matriks ini disebut **determinan Vandermonde**. Kita akan memerlukan lema berikut dalam penyelidikan kode siklik.

Lema 22.2.7 *Misalkan $\alpha_1, \ldots, \alpha_n$ elemen-elemen dalam lapangan F dengan $n \geq 2$. Maka*

$$\det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix} = \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j).$$

Khususnya, jika α_i berbeda-beda, maka determinan tersebut tak nol.

Bukti. Kita akan melakukan induksi pada n. Jika $n = 2$, maka determinannya adalah $\alpha_2 - \alpha_1$. Andaikan hasil tersebut berlaku untuk $n - 1$ dan tinjau polinomial $p(x)$ yang didefinisikan oleh

$$p(x) = \det \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} & x \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{n-1}^2 & x^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_{n-1}^{n-1} & x^{n-1} \end{pmatrix}.$$

Dengan mengembangkan determinan ini menurut kofaktor pada kolom terakhir, kita melihat bahwa $p(x)$ merupakan polinomial berderajat paling tinggi $n - 1$. Selain itu, akar-akar $p(x)$ adalah $\alpha_1, \ldots, \alpha_{n-1}$, karena menyubstitusikan salah satu elemen ini pada kolom terakhir akan menghasilkan kolom yang identik dengan kolom terakhir dalam matriks. Ingat bahwa determinan suatu matriks bernilai nol jika matriks tersebut mempunyai dua kolom yang identik. Oleh karena itu,

$$p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_{n-1})\beta,$$

dengan

$$\beta = (-1)^{n+n} \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{n-1}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-2} & \alpha_2^{n-2} & \cdots & \alpha_{n-1}^{n-2} \end{pmatrix}.$$

Berdasarkan hipotesis induksi kita,

$$\beta = (-1)^{n+n} \prod_{1 \le j < i \le n-1} (\alpha_i - \alpha_j).$$

Jika kita mengambil $x = \alpha_n$, hasil tersebut langsung diperoleh. ■

Teorema berikut memberikan taksiran kemampuan mendeteksi dan mengoreksi galat bagi suatu polinomial pembangkit tertentu.

Teorema 22.2.8 *Misalkan $C = \langle g(t) \rangle$ suatu kode siklik dalam R_n dan andaikan bahwa ω merupakan akar kesatuan ke-n primitif di atas $\mathbb{Z}_2$. Jika s pangkat berurutan dari ω merupakan akar-akar $g(x)$, maka jarak minimum C setidaknya $s + 1$.*

Bukti. Andaikan bahwa

$$g(\omega^r) = g(\omega^{r+1}) = \cdots = g(\omega^{r+s-1}) = 0.$$

Misalkan $f(x)$ suatu polinomial dalam C dengan paling banyak s koefisien tak nol. Kita dapat mengandaikan bahwa

$$f(x) = a_{i_0} x^{i_0} + a_{i_1} x^{i_1} + \cdots + a_{i_{s-1}} x^{i_{s-1}}$$

merupakan suatu polinomial dalam C. Cukup ditunjukkan bahwa semua a_i harus bernilai 0. Karena

$$g(\omega^r) = g(\omega^{r+1}) = \cdots = g(\omega^{r+s-1}) = 0$$

dan $g(x)$ membagi $f(x)$,

$$f(\omega^r) = f(\omega^{r+1}) = \cdots = f(\omega^{r+s-1}) = 0.$$

Secara ekuivalen, kita mempunyai sistem persamaan berikut:

$$\begin{aligned} a_{i_0}(\omega^r)^{i_0} + a_{i_1}(\omega^r)^{i_1} + \cdots + a_{i_{s-1}}(\omega^r)^{i_{s-1}} &= 0 \\ a_{i_0}(\omega^{r+1})^{i_0} + a_{i_1}(\omega^{r+1})^{i_2} + \cdots + a_{i_{s-1}}(\omega^{r+1})^{i_{s-1}} &= 0 \\ &\vdots \\ a_{i_0}(\omega^{r+s-1})^{i_0} + a_{i_1}(\omega^{r+s-1})^{i_1} + \cdots + a_{i_{s-1}}(\omega^{r+s-1})^{i_{s-1}} &= 0. \end{aligned}$$

Oleh karena itu, $(a_{i_0}, a_{i_1}, \ldots, a_{i_{s-1}})$ merupakan solusi sistem homogen persamaan linear

$$\begin{aligned} (\omega^{i_0})^r x_0 + (\omega^{i_1})^r x_1 + \cdots + (\omega^{i_{s-1}})^r x_{n-1} &= 0 \\ (\omega^{i_0})^{r+1} x_0 + (\omega^{i_1})^{r+1} x_1 + \cdots + (\omega^{i_{s-1}})^{r+1} x_{n-1} &= 0 \\ &\vdots \\ (\omega^{i_0})^{r+s-1} x_0 + (\omega^{i_1})^{r+s-1} x_1 + \cdots + (\omega^{i_{s-1}})^{r+s-1} x_{n-1} &= 0. \end{aligned}$$

Akan tetapi, sistem ini mempunyai solusi tunggal, karena determinan matriks

$$\begin{pmatrix} (\omega^{i_0})^r & (\omega^{i_1})^r & \cdots & (\omega^{i_{s-1}})^r \\ (\omega^{i_0})^{r+1} & (\omega^{i_1})^{r+1} & \cdots & (\omega^{i_{s-1}})^{r+1} \\ \vdots & \vdots & \ddots & \vdots \\ (\omega^{i_0})^{r+s-1} & (\omega^{i_1})^{r+s-1} & \cdots & (\omega^{i_{s-1}})^{r+s-1} \end{pmatrix}$$

dapat ditunjukkan tak nol dengan menggunakan Lema 22.2.7 dan sifat-sifat dasar determinan (Latihan). Oleh karena itu, solusi ini haruslah $a_{i_0} = a_{i_1} = \cdots = a_{i_{s-1}} = 0$. ■

22.2.2 Kode BCH

Beberapa kode terpenting, yang ditemukan secara terpisah oleh A. Hocquenghem pada tahun 1959 serta oleh R. C. Bose dan D. V. Ray-Chaudhuri pada tahun 1960, adalah kode BCH. Sistem komunikasi Eropa dan transatlantik sama-sama menggunakan kode BCH. Kata informasi yang akan dikodekan memiliki panjang 231, dan polinomial berderajat 24 digunakan untuk membangkitkan kode. Karena $231 + 24 = 255 = 2^8 - 1$, kita berhadapan dengan kode blok-$(255, 231)$. Kode BCH ini akan mendeteksi enam galat dan mempunyai tingkat kegagalan 1 dalam 16 juta. Salah satu keunggulan kode BCH adalah tersedianya algoritma koreksi galat yang efisien.

Gagasan di balik kode BCH adalah memilih polinomial pembangkit berderajat terkecil yang mempunyai kemampuan terbesar dalam mendeteksi dan mengoreksi galat. Misalkan $d = 2r + 1$ untuk suatu $r \geq 0$. Andaikan bahwa ω merupakan akar kesatuan ke-n primitif di atas $\mathbb{Z}_2$, dan misalkan $m_i(x)$ polinomial minimal di atas $\mathbb{Z}_2$ dari ω^i. Jika

$$g(x) = \text{lcm}[m_1(x), m_2(x), \ldots, m_{2r}(x)],$$

maka kode siklik $\langle g(t) \rangle$ dalam R_n disebut **kode bch dengan panjang n dan jarak d**. Menurut Teorema 22.2.8, jarak minimum C setidaknya d.

Teorema 22.2.9 *Misalkan $C = \langle g(t) \rangle$ suatu kode siklik dalam R_n. Pernyataan-pernyataan berikut ekuivalen.*

1. *Kode C merupakan kode BCH yang jarak minimumnya setidaknya d.*
2. *Polinomial kode $f(t)$ berada dalam C jika dan hanya jika $f(\omega^i) = 0$ untuk $1 \leq i < d$.*
3. *Matriks*

$$H = \begin{pmatrix} 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{(n-1)(2)} \\ 1 & \omega^3 & \omega^6 & \cdots & \omega^{(n-1)(3)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{2r} & \omega^{4r} & \cdots & \omega^{(n-1)(2r)} \end{pmatrix}$$

merupakan matriks pemeriksa paritas bagi C.

BUKTI. (1) $\Rightarrow$ (2). Jika $f(t)$ berada dalam C, maka $g(x) \mid f(x)$ dalam $\mathbb{Z}_2[x]$. Jadi, untuk $i = 1, \ldots, 2r$, berlaku $f(\omega^i) = 0$ karena $g(\omega^i) = 0$. Sebaliknya, andaikan bahwa $f(\omega^i) = 0$ untuk $1 \leq i \leq d$. Maka $f(x)$ dapat dibagi oleh setiap $m_i(x)$, karena $m_i(x)$ merupakan polinomial minimal dari ω^i. Oleh karena itu, $g(x) \mid f(x)$ berdasarkan definisi $g(x)$. Akibatnya, $f(x)$ merupakan kata kode.

(2) $\Rightarrow$ (3). Misalkan $f(t) = a_0 + a_1 t + \cdots + a_{n-1} v t^{n-1}$ berada dalam R_n.

Tupel-n yang bersesuaian dalam $\mathbb{Z}_2^n$ adalah $\mathbf{x} = (a_0 a_1 \cdots a_{n-1})^{\mathrm{t}}$. Menurut (2),

$$H\mathbf{x} = \begin{pmatrix} a_0 + a_1\omega + \cdots + a_{n-1}\omega^{n-1} \\ a_0 + a_1\omega^2 + \cdots + a_{n-1}(\omega^2)^{n-1} \\ \vdots \\ a_0 + a_1\omega^{2r} + \cdots + a_{n-1}(\omega^{2r})^{n-1} \end{pmatrix} = \begin{pmatrix} f(\omega) \\ f(\omega^2) \\ \vdots \\ f(\omega^{2r}) \end{pmatrix} = 0$$

tepat ketika $f(t)$ berada dalam C. Dengan demikian, H merupakan matriks pemeriksa paritas bagi C.

(3) $\Rightarrow$ (1). Menurut (3), polinomial kode $f(t) = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1}$ berada dalam C tepat ketika $f(\omega^i) = 0$ untuk $i = 1, \ldots, 2r$. Polinomial terkecil semacam itu adalah $g(t) = \mathrm{lcm}[m_1(t), \ldots, m_{2r}(t)]$. Oleh karena itu, $C = \langle g(t) \rangle$. ■

Contoh 22.2.10 Mudah diverifikasi bahwa $x^{15} - 1 \in \mathbb{Z}_2[x]$ mempunyai faktorisasi

$$x^{15} - 1 = (x+1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1),$$

dengan setiap faktornya berupa polinomial tak tereduksi. Misalkan ω suatu akar dari $1 + x + x^4$. Lapangan Galois $\mathrm{GF}(2^4)$ adalah

$$\{a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3 : a_i \in \mathbb{Z}_2 \text{ dan } 1 + \omega + \omega^4 = 0\}.$$

Menurut Contoh 22.1.8, ω merupakan akar kesatuan ke-15 primitif. Polinomial minimal dari ω adalah $m_1(x) = 1 + x + x^4$. Mudah dilihat bahwa ω^2 dan ω^4 juga merupakan akar dari $m_1(x)$. Polinomial minimal dari ω^3 adalah $m_2(x) = 1 + x + x^2 + x^3 + x^4$. Oleh karena itu,

$$g(x) = m_1(x)m_2(x) = 1 + x^4 + x^6 + x^7 + x^8$$

mempunyai akar-akar ω, ω^2, ω^3, ω^4. Karena $m_1(x)$ dan $m_2(x)$ keduanya membagi $x^{15} - 1$, kode BCH tersebut merupakan kode-$(15, 7)$. Jika $x^{15} - 1 = g(x)h(x)$, maka $h(x) = 1 + x^4 + x^6 + x^7$; oleh karena itu, matriks pemeriksa paritas untuk kode ini adalah

$$\begin{pmatrix} 0&0&0&0&0&0&0&1&1&0&1&0&0&0&1 \\ 0&0&0&0&0&0&1&1&0&1&0&0&0&1&0 \\ 0&0&0&0&0&1&1&0&1&0&0&0&1&0&0 \\ 0&0&0&0&1&1&0&1&0&0&0&1&0&0&0 \\ 0&0&0&1&1&0&1&0&0&0&1&0&0&0&0 \\ 0&0&1&1&0&1&0&0&0&1&0&0&0&0&0 \\ 0&1&1&0&1&0&0&0&1&0&0&0&0&0&0 \\ 1&1&0&1&0&0&0&1&0&0&0&0&0&0&0 \end{pmatrix}.$$

▲

22.3 Pertanyaan Bacaan

1. Kapan suatu perluasan lapangan bersifat separabel?
2. Apa saja orde yang mungkin bagi sublapangan dari suatu lapangan hingga?
3. Bagaimana struktur elemen-elemen tak nol dari suatu lapangan hingga?

4. Berikan karakterisasi lapangan hingga dengan menggunakan konsep lapangan pemisah.

5. Mengapa suatu teorema dalam bab ini diberi judul "Impian Mahasiswa Baru?"

22.4 Latihan

1. Hitung setiap nilai berikut.

(a) $[\mathrm{GF}(3^6) : \mathrm{GF}(3^3)]$

(b) $[\mathrm{GF}(128) : \mathrm{GF}(16)]$

(c) $[\mathrm{GF}(625) : \mathrm{GF}(25)]$

(d) $[\mathrm{GF}(p^{12}) : \mathrm{GF}(p^2)]$

Petunjuk. Pastikan bahwa yang ditinjau merupakan perluasan lapangan.

2. Hitung $[\mathrm{GF}(p^m) : \mathrm{GF}(p^n)]$, dengan $n \mid m$.

3. Apakah kisi sublapangan dari $\mathrm{GF}(p^{30})$?

4. Misalkan α suatu akar dari x^3+x^2+1 di atas $\mathbb{Z}_2$. Konstruksikan lapangan hingga berorde 8. Tunjukkan bahwa $x^3 + x^2 + 1$ terurai dalam $\mathbb{Z}_2(\alpha)$.

Petunjuk. Terdapat delapan elemen dalam $\mathbb{Z}_2(\alpha)$. Tunjukkan dua akar lain dari $x^3 + x^2 + 1$ selain α di antara kedelapan elemen tersebut.

5. Konstruksikan lapangan hingga berorde 27.

Petunjuk. Temukan polinomial tak tereduksi $p(x)$ dalam $\mathbb{Z}_3[x]$ yang berderajat 3 dan tunjukkan bahwa $\mathbb{Z}_3[x]/\langle p(x)\rangle$ mempunyai 27 elemen.

6. Buktikan atau bantah: $\mathbb{Q}^*$ bersifat siklik.

7. Faktorkan setiap polinomial berikut dalam $\mathbb{Z}_2[x]$.

(a) $x^5 - 1$

(b) $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

(c) $x^9 - 1$

(d) $x^4 + x^3 + x^2 + x + 1$

Petunjuk. (a) $x^5 - 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$; (c) $x^9 - 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1)$.

8. Buktikan atau bantah: $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle \cong \mathbb{Z}_2[x]/\langle x^3 + x^2 + 1\rangle$.

Petunjuk. Benar.

9. Tentukan banyaknya kode siklik dengan panjang n untuk $n = 6, 7, 8, 10$.

10. Buktikan bahwa ideal $\langle t + 1\rangle$ dalam R_n merupakan kode dalam $\mathbb{Z}_2^n$ yang terdiri atas semua kata berparitas genap.

11. Konstruksikan semua kode BCH dengan

(a) panjang 7.

(b) panjang 15.

Petunjuk. (a) Gunakan fakta bahwa $x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

12. Buktikan atau bantah: Terdapat lapangan hingga yang tertutup secara aljabar.

Petunjuk. Salah.

13. Misalkan p prima. Buktikan bahwa lapangan fungsi rasional $\mathbb{Z}_p(x)$ merupakan lapangan tak hingga berkarakteristik p.

14. Misalkan D suatu daerah integral berkarakteristik p. Buktikan bahwa $(a-b)^{p^n} = a^{p^n} - b^{p^n}$ untuk semua $a, b \in D$.

15. Tunjukkan bahwa setiap elemen dalam suatu lapangan hingga dapat ditulis sebagai jumlah dua kuadrat.

16. Misalkan E dan F sublapangan dari lapangan hingga K. Jika E isomorfik dengan F, tunjukkan bahwa $E = F$.

17. Misalkan $F \subset E \subset K$ lapangan-lapangan. Jika K merupakan perluasan separabel dari F, tunjukkan bahwa K juga merupakan perluasan separabel dari E.

Petunjuk. Jika $p(x) \in F[x]$, maka $p(x) \in E[x]$.

18. Misalkan E suatu perluasan dari lapangan hingga F, dengan F mempunyai q elemen. Misalkan $\alpha \in E$ aljabar atas F dan berderajat n. Buktikan bahwa $F(\alpha)$ mempunyai q^n elemen.

Petunjuk. Karena α aljabar atas F dan berderajat n, kita dapat menulis sebarang elemen $\beta \in F(\alpha)$ secara tunggal sebagai $\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ dengan $a_i \in F$. Terdapat q^n tupel-n yang mungkin, yaitu $(a_0, a_1, \ldots, a_{n-1})$.

19. Tunjukkan bahwa setiap perluasan hingga dari lapangan hingga F merupakan perluasan sederhana; artinya, jika E merupakan perluasan hingga dari lapangan hingga F, buktikan bahwa terdapat $\alpha \in E$ sedemikian sehingga $E = F(\alpha)$.

20. Tunjukkan bahwa untuk setiap n terdapat polinomial tak tereduksi berderajat n dalam $\mathbb{Z}_p[x]$.

21. Buktikan bahwa **pemetaan Frobenius** $\Phi : \mathrm{GF}(p^n) \to \mathrm{GF}(p^n)$ yang diberikan oleh $\Phi : \alpha \mapsto \alpha^p$ merupakan automorfisme berorde n.

22. Tunjukkan bahwa setiap elemen dalam $\mathrm{GF}(p^n)$ dapat ditulis dalam bentuk a^p untuk suatu $a \in \mathrm{GF}(p^n)$ yang tunggal.

23. Misalkan E dan F sublapangan dari $\mathrm{GF}(p^n)$. Jika $|E| = p^r$ dan $|F| = p^s$, berapakah orde $E \cap F$?

24. **Teorema Wilson.** Misalkan p prima. Buktikan bahwa $(p-1)! \equiv -1 \pmod{p}$.

Petunjuk. Faktorkan $x^{p-1} - 1$ di atas $\mathbb{Z}_p$.

25. Jika $g(t)$ merupakan polinomial pembangkit minimal bagi kode siklik C dalam R_n, buktikan bahwa suku konstan $g(x)$ adalah 1.

26. Sering kali mungkin terjadi rentetan galat selama transmisi, seperti ketika terjadi lonjakan listrik. Semburan gangguan sesaat semacam itu dapat mengubah beberapa bit berurutan dalam suatu kata kode. Kode siklik memungkinkan pendeteksian rentetan galat semacam itu. Misalkan C suatu kode siklik-(n, k). Buktikan bahwa setiap rentetan galat hingga $n - k$ digit dapat dideteksi.

27. Buktikan bahwa gelanggang R_n dan $\mathbb{Z}_2^n$ isomorfik sebagai ruang vektor.

28. Misalkan C suatu kode dalam R_n yang dibangkitkan oleh $g(t)$. Jika $\langle f(t) \rangle$ merupakan kode lain dalam R_n, tunjukkan bahwa $\langle g(t) \rangle \subset \langle f(t) \rangle$ jika dan hanya jika $f(x)$ membagi $g(x)$ dalam $\mathbb{Z}_2[x]$.

29. Misalkan $C = \langle g(t) \rangle$ suatu kode siklik dalam R_n dan andaikan bahwa $x^n - 1 = g(x)h(x)$, dengan $g(x) = g_0 + g_1 x + \cdots + g_{n-k}x^{n-k}$ dan $h(x) =$

$h_0 + h_1 x + \cdots + h_k x^k$. Definisikan G sebagai matriks $n \times k$

$$G = \begin{pmatrix} g_0 & 0 & \cdots & 0 \\ g_1 & g_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ g_{n-k} & g_{n-k-1} & \cdots & g_0 \\ 0 & g_{n-k} & \cdots & g_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & g_{n-k} \end{pmatrix}$$

dan H sebagai matriks $(n-k) \times n$

$$H = \begin{pmatrix} 0 & \cdots & 0 & 0 & h_k & \cdots & h_0 \\ 0 & \cdots & 0 & h_k & \cdots & h_0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ h_k & \cdots & h_0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

(a) Buktikan bahwa G merupakan matriks pembangkit bagi C.

(b) Buktikan bahwa H merupakan matriks pemeriksa paritas bagi C.

(c) Tunjukkan bahwa $HG = 0$.

22.5 Latihan Tambahan: Koreksi Galat untuk Kode BCH

Kode BCH mempunyai algoritma koreksi galat yang sangat menarik. Misalkan C suatu kode BCH dalam R_n, dan andaikan bahwa polinomial kode $c(t) = c_0 + c_1 t + \cdots + c_{n-1} t^{n-1}$ ditransmisikan. Misalkan $w(t) = w_0 + w_1 t + \cdots w_{n-1} t^{n-1}$ polinomial dalam R_n yang diterima. Jika galat terjadi pada bit $a_1, \ldots, a_k$, maka $w(t) = c(t) + e(t)$, dengan $e(t) = t^{a_1} + t^{a_2} + \cdots + t^{a_k}$ sebagai **polinomial galat**. Pendekode harus menentukan bilangan bulat a_i, kemudian memulihkan $c(t)$ dari $w(t)$ dengan membalik bit ke-a_i. Dari $w(t)$ kita dapat menghitung $w(\omega^i) = s_i$ untuk $i = 1, \ldots, 2r$, dengan ω suatu akar kesatuan ke-n primitif di atas $\mathbb{Z}_2$. Kita mengatakan **sindrom** dari $w(t)$ adalah $s_1, \ldots, s_{2r}$.

1. Tunjukkan bahwa $w(t)$ merupakan polinomial kode jika dan hanya jika $s_i = 0$ untuk semua i.

2. Tunjukkan bahwa

$$s_i = w(\omega^i) = e(\omega^i) = \omega^{ia_1} + \omega^{ia_2} + \cdots + \omega^{ia_k}$$

untuk $i = 1, \ldots, 2r$. **Polinomial pelacak galat** didefinisikan sebagai

$$s(x) = (x + \omega^{a_1})(x + \omega^{a_2}) \cdots (x + \omega^{a_k}).$$

3. Ingat kode blok-$(15, 7)$ BCH dalam Contoh 22.2.6. Menurut Teorema 8.1.13, kode ini mampu mengoreksi dua galat. Andaikan galat-galat ini terjadi pada bit a_1 dan a_2. Polinomial pelacak galatnya adalah $s(x) = (x + \omega^{a_1})(x + \omega^{a_2})$. Tunjukkan bahwa

$$s(x) = x^2 + s_1 x + \left(s_1^2 + \frac{s_3}{s_1} \right).$$

4. Misalkan $w(t) = 1 + t^2 + t^4 + t^5 + t^7 + t^{12} + t^{13}$. Tentukan polinomial kode yang semula ditransmisikan.

22.6 Referensi dan Bacaan yang Disarankan

[**1**] Childs, L. *A Concrete Introduction to Higher Algebra*. 2nd ed. Springer-Verlag, New York, 1995.

[**2**] Gåding, L. and Tambour, T. *Algebra for Computer Science*. Springer-Verlag, New York, 1988.

[**3**] Lidl, R. and Pilz, G. *Applied Abstract Algebra*. 2nd ed. Springer, New York, 1998. Sajian yang sangat baik tentang lapangan hingga dan penerapannya.

[**4**] Mackiw, G. *Applications of Abstract Algebra*. Wiley, New York, 1985.

[**5**] Roman, S. *Coding and Information Theory*. Springer-Verlag, New York, 1992.

[**6**] van Lint, J. H. *Introduction to Coding Theory*. Springer, New York, 1999.

23

Teori Galois

Salah satu masalah klasik dalam aljabar adalah mencari penyelesaian persamaan polinomial. Penyelesaian persamaan kuadrat telah dikenal sejak zaman kuno. Pada abad keenam belas, para matematikawan Italia menemukan penyelesaian umum untuk persamaan kubik dan kuartik umum; namun, upaya menyelesaikan polinomial berderajat lima, atau kuintik, yang umum terus menemui jalan buntu selama tiga ratus tahun berikutnya. Tentu saja, persamaan seperti $x^5 - 1 = 0$ atau $x^6 - x^3 - 6 = 0$ dapat diselesaikan, tetapi tidak ditemukan penyelesaian seperti rumus kuadrat untuk persamaan kuintik umum,

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0.$$

Akhirnya, pada awal abad kesembilan belas, Ruffini dan Abel masing-masing menemukan persamaan kuintik yang tidak dapat diselesaikan dengan rumus apa pun. Namun, Galois-lah yang memberikan penjelasan lengkap dengan menunjukkan polinomial mana yang dapat dan tidak dapat diselesaikan menggunakan rumus. Ia menemukan hubungan antara grup dan perluasan lapangan. Teori Galois menunjukkan kesalingbergantungan yang kuat antara teori grup dan teori lapangan, serta memiliki implikasi luas jauh melampaui tujuan awalnya.

Dalam bab ini kita akan membuktikan Teorema Dasar Teori Galois. Hasil ini akan digunakan untuk menetapkan ketakterselesaian persamaan kuintik dan membuktikan Teorema Dasar Aljabar.

23.1 Automorfisme Lapangan

Tugas pertama kita adalah membangun hubungan antara teori grup dan teori lapangan dengan menelaah automorfisme lapangan.

Proposisi 23.1.1 *Himpunan semua automorfisme suatu lapangan F merupakan grup di bawah komposisi fungsi.*

Bukti. Jika σ dan τ merupakan automorfisme dari F, maka $\sigma\tau$ dan σ^{-1} juga merupakan automorfisme. Identitas tentu merupakan automorfisme; dengan demikian, himpunan semua automorfisme suatu lapangan F memang merupakan grup. ■

Proposisi 23.1.2 *Misalkan E suatu perluasan lapangan dari F. Maka himpunan semua automorfisme dari E yang menetapkan F unsur demi unsur merupakan grup; yaitu, himpunan semua automorfisme $\sigma : E \to E$ sedemikian sehingga $\sigma(\alpha) = \alpha$ untuk semua $\alpha \in F$ merupakan grup.*

BUKTI. Kita hanya perlu menunjukkan bahwa himpunan automorfisme dari E yang menetapkan F unsur demi unsur merupakan subgrup dari grup semua automorfisme E. Misalkan σ dan τ dua automorfisme dari E sedemikian sehingga $\sigma(\alpha) = \alpha$ dan $\tau(\alpha) = \alpha$ untuk semua $\alpha \in F$. Maka $\sigma\tau(\alpha) = \sigma(\alpha) = \alpha$ dan $\sigma^{-1}(\alpha) = \alpha$. Karena identitas menetapkan setiap unsur dari E, himpunan automorfisme dari E yang membiarkan unsur-unsur F tetap merupakan subgrup dari seluruh grup automorfisme E. ■

Misalkan E suatu perluasan lapangan dari F. Grup lengkap automorfisme dari E kita nyatakan dengan $\mathrm{Aut}(E)$. Kita mendefinisikan **grup Galois** dari E atas F sebagai grup automorfisme dari E yang menetapkan F unsur demi unsur; yaitu,

$$G(E/F) = \{\sigma \in \mathrm{Aut}(E) : \sigma(\alpha) = \alpha \text{ untuk semua } \alpha \in F\}.$$

Jika $f(x)$ suatu polinomial dalam $F[x]$ dan E lapangan pemisah dari $f(x)$ atas F, kita mendefinisikan grup Galois dari $f(x)$ sebagai $G(E/F)$.

Contoh 23.1.3 Konjugasi kompleks, yang didefinisikan oleh $\sigma : a+bi \mapsto a-bi$, merupakan automorfisme bilangan kompleks. Karena

$$\sigma(a) = \sigma(a + 0i) = a - 0i = a,$$

automorfisme yang didefinisikan oleh konjugasi kompleks harus berada dalam $G(\mathbb{C}/\mathbb{R})$. ▲

Contoh 23.1.4 Perhatikan lapangan-lapangan $\mathbb{Q} \subset \mathbb{Q}(\sqrt{5}\,) \subset \mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$. Untuk $a, b \in \mathbb{Q}(\sqrt{5}\,)$,

$$\sigma(a + b\sqrt{3}\,) = a - b\sqrt{3}$$

merupakan automorfisme dari $\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ yang membiarkan $\mathbb{Q}(\sqrt{5}\,)$ tetap. Serupa dengan itu,

$$\tau(a + b\sqrt{5}\,) = a - b\sqrt{5}$$

merupakan automorfisme dari $\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ yang membiarkan $\mathbb{Q}(\sqrt{3}\,)$ tetap. Automorfisme $\mu = \sigma\tau$ memindahkan $\sqrt{3}$ maupun $\sqrt{5}$. Sebentar lagi akan jelas bahwa $\{\mathrm{id}, \sigma, \tau, \mu\}$ merupakan grup Galois dari $\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ atas $\mathbb{Q}$. Tabel berikut menunjukkan bahwa grup ini isomorfik dengan $\mathbb{Z}_2 \times \mathbb{Z}_2$.

	id	σ	τ	μ
id	id	σ	τ	μ
σ	σ	id	μ	τ
τ	τ	μ	id	σ
μ	μ	τ	σ	id

Kita juga dapat memandang lapangan $\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ sebagai ruang vektor atas $\mathbb{Q}$ yang memiliki basis $\{1, \sqrt{3}, \sqrt{5}, \sqrt{15}\,\}$. Bukan suatu kebetulan bahwa $|G(\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)/\mathbb{Q})| = [\mathbb{Q}(\sqrt{3}, \sqrt{5}\,) : \mathbb{Q})] = 4$. ▲

Proposisi 23.1.5 *Misalkan E suatu perluasan lapangan dari F dan $f(x)$ suatu polinomial dalam $F[x]$. Maka sebarang automorfisme dalam $G(E/F)$ mendefinisikan permutasi atas akar-akar $f(x)$ yang berada dalam E.*

BUKTI. Misalkan

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

dan andaikan $\alpha \in E$ merupakan akar dari $f(x)$. Maka untuk $\sigma \in G(E/F)$,

$$0 = \sigma(0)$$

$$
\begin{aligned}
&= \sigma(f(\alpha)) \\
&= \sigma(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n) \\
&= a_0 + a_1\sigma(\alpha) + a_2[\sigma(\alpha)]^2 + \cdots + a_n[\sigma(\alpha)]^n;
\end{aligned}
$$

oleh karena itu, $\sigma(\alpha)$ juga merupakan akar dari $f(x)$. ■

Misalkan E suatu perluasan aljabar dari lapangan F. Dua unsur $\alpha, \beta \in E$ disebut **konjugat** atas F jika keduanya memiliki polinomial minimal yang sama. Sebagai contoh, dalam lapangan $\mathbb{Q}(\sqrt{2})$, unsur $\sqrt{2}$ dan $-\sqrt{2}$ saling konjugat atas $\mathbb{Q}$ karena keduanya merupakan akar polinomial tak tereduksi $x^2 - 2$.

Kebalikan dari proposisi terakhir juga berlaku. Pembuktiannya langsung mengikuti Lema 21.2.4.

Proposisi 23.1.6 *Jika α dan β saling konjugat atas F, terdapat suatu isomorfisma $\sigma : F(\alpha) \to F(\beta)$ sedemikian sehingga pembatasan σ pada F merupakan identitas.*

Teorema 23.1.7 *Misalkan $f(x)$ suatu polinomial dalam $F[x]$ dan andaikan E merupakan lapangan pemisah untuk $f(x)$ atas F. Jika $f(x)$ tidak memiliki akar berulang, maka*

$$|G(E/F)| = [E : F].$$

BUKTI. Kita akan menggunakan induksi matematika pada $[E : F]$. Jika $[E : F] = 1$, maka $E = F$ dan tidak ada yang perlu dibuktikan. Jika $[E : F] > 1$, misalkan $f(x) = p(x)q(x)$, dengan $p(x)$ tak tereduksi dan berderajat d. Kita dapat mengasumsikan bahwa $d > 1$; jika tidak, $f(x)$ terurai atas F dan $[E : F] = 1$. Misalkan α suatu akar dari $p(x)$. Jika $\phi : F(\alpha) \to E$ sebarang homomorfisma injektif, maka $\phi(\alpha) = \beta$ merupakan akar dari $p(x)$, dan $\phi : F(\alpha) \to F(\beta)$ merupakan automorfisme lapangan. Karena $f(x)$ tidak memiliki akar berulang, $p(x)$ memiliki tepat d akar $\beta \in E$. Berdasarkan Proposisi 23.1.5, terdapat tepat d isomorfisma $\phi : F(\alpha) \to F(\beta_i)$ yang menetapkan F, satu untuk setiap akar $\beta_1, \ldots, \beta_d$ dari $p(x)$ (lihat Gambar 23.1.8).

$$
\begin{array}{ccc}
E & \xrightarrow{\psi} & E \\
\downarrow & & \downarrow \\
F(\alpha) & \xrightarrow{\phi} & F(\beta) \\
\downarrow & & \downarrow \\
F & \xrightarrow{\text{identitas}} & F
\end{array}
$$

Gambar 23.1.8 Diagram komutatif untuk Teorema 23.1.7

Karena E merupakan lapangan pemisah dari $f(x)$ atas F, lapangan tersebut juga merupakan lapangan pemisah atas $F(\alpha)$. Serupa dengan itu, E merupakan lapangan pemisah dari $f(x)$ atas $F(\beta)$. Karena $[E : F(\alpha)] = [E : F]/d$, induksi menunjukkan bahwa setiap dari d isomorfisma ϕ memiliki tepat $[E : F]/d$ perluasan, $\psi : E \to E$, dan kita telah menyusun $[E : F]$ isomorfisma yang menetapkan F. Akhirnya, andaikan σ sebarang automorfisme yang menetapkan F. Maka pembatasan σ pada $F(\alpha)$ adalah ϕ untuk suatu $\phi : F(\alpha) \to F(\beta)$. ■

Korolari 23.1.9 *Misalkan F suatu lapangan hingga dengan perluasan hingga E sedemikian sehingga $[E : F] = k$. Maka $G(E/F)$ bersifat siklik dengan orde k.*

BUKTI. Misalkan p karakteristik dari E dan F, serta andaikan orde E dan F masing-masing adalah p^m dan p^n. Maka $nk = m$. Kita juga dapat mengasumsikan bahwa E merupakan lapangan pemisah dari $x^{p^m} - x$ atas suatu sublapangan berorde p. Oleh karena itu, E juga harus merupakan lapangan pemisah dari $x^{p^m} - x$ atas F. Dengan menerapkan Teorema 23.1.7, kita memperoleh $|G(E/F)| = k$.

Untuk membuktikan bahwa $G(E/F)$ bersifat siklik, kita harus mencari pembangkit untuk $G(E/F)$. Definisikan $\sigma : E \to E$ dengan $\sigma(\alpha) = \alpha^{p^n}$. Kita mengklaim bahwa σ merupakan unsur dalam $G(E/F)$ yang kita cari. Pertamatama kita perlu menunjukkan bahwa σ berada dalam $\mathrm{Aut}(E)$. Jika α dan β berada dalam E,

$$\sigma(\alpha + \beta) = (\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \sigma(\alpha) + \sigma(\beta)$$

berdasarkan Lema 22.1.3. Selain itu, mudah untuk menunjukkan bahwa $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$. Karena σ merupakan homomorfisma lapangan yang tak nol, Pemetaan tersebut harus injektif. Pemetaan ini juga harus surjektif karena E merupakan lapangan hingga. Kita mengetahui bahwa σ harus berada dalam $G(E/F)$, karena F merupakan lapangan pemisah dari $x^{p^n} - x$ atas lapangan dasar berorde p. Ini berarti bahwa σ membiarkan setiap unsur dalam F tetap. Akhirnya, kita harus menunjukkan bahwa orde σ adalah k. Berdasarkan Teorema 23.1.7, kita mengetahui bahwa

$$\sigma^k(\alpha) = \alpha^{p^{nk}} = \alpha^{p^m} = \alpha$$

merupakan identitas dari $G(E/F)$. Akan tetapi, σ^r tidak dapat menjadi identitas untuk $1 \leq r < k$; jika demikian, $x^{p^{nr}} - x$ akan memiliki p^m akar, yang mustahil. ■

Contoh 23.1.10 Sekarang kita dapat memastikan bahwa grup Galois dari $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ atas $\mathbb{Q}$ dalam Contoh 23.1.4 memang isomorfik dengan $\mathbb{Z}_2 \times \mathbb{Z}_2$. Jelas bahwa grup $H = \{\mathrm{id}, \sigma, \tau, \mu\}$ merupakan subgrup dari $G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$; namun, H harus merupakan seluruh $G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})$, karena

$$|H| = [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = |G(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q})| = 4.$$

▲

Contoh 23.1.11 Mari kita hitung grup Galois dari

$$f(x) = x^4 + x^3 + x^2 + x + 1$$

atas $\mathbb{Q}$. Kita mengetahui bahwa $f(x)$ tak tereduksi berdasarkan Latihan 17.5.20. Selanjutnya, karena $(x - 1)f(x) = x^5 - 1$, kita dapat menggunakan Teorema De Moivre untuk menentukan bahwa akar-akar $f(x)$ adalah ω^i, dengan $i = 1, \ldots, 4$ dan

$$\omega = \cos(2\pi/5) + i \sin(2\pi/5).$$

Oleh karena itu, lapangan pemisah dari $f(x)$ haruslah $\mathbb{Q}(\omega)$. Kita dapat mendefinisikan automorfisme σ_i dari $\mathbb{Q}(\omega)$ melalui $\sigma_i(\omega) = \omega^i$ untuk $i = 1, \ldots, 4$. Mudah untuk memeriksa bahwa pemetaan-pemetaan ini memang merupakan automorfisme berbeda dalam $G(\mathbb{Q}(\omega)/\mathbb{Q})$. Karena

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = |G(\mathbb{Q}(\omega)/\mathbb{Q})| = 4,$$

automorfisme-automorfisme σ_i tersebut harus mencakup semua unsur $G(\mathbb{Q}(\omega)/\mathbb{Q})$. Oleh karena itu, $G(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_4$ karena ω merupakan pembangkit grup Galois. ▲

23.1.1 Perluasan Separabel

Banyak hasil yang baru saja kita buktikan bergantung pada fakta bahwa polinomial $f(x)$ dalam $F[x]$ tidak memiliki akar berulang dalam lapangan pemisahnya. Jelas bahwa kita perlu mengetahui dengan tepat kapan suatu polinomial terfaktorkan menjadi faktor-faktor linear yang berbeda dalam lapangan pemisahnya. Misalkan E adalah lapangan pemisah dari suatu polinomial $f(x)$ dalam $F[x]$. Andaikan $f(x)$ terfaktorkan atas E sebagai

$$f(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r} = \prod_{i=1}^{r}(x-\alpha_i)^{n_i}.$$

Kita mendefinisikan **multiplisitas** suatu akar α_i dari $f(x)$ sebagai n_i. Akar bermultiplisitas 1 disebut **akar sederhana**. Ingat bahwa polinomial $f(x) \in F[x]$ berderajat n disebut **separabel** jika memiliki n akar yang berbeda dalam lapangan pemisahnya E. Secara ekuivalen, $f(x)$ separabel jika terfaktorkan menjadi faktor-faktor linear yang berbeda atas $E[x]$. Suatu perluasan E dari F disebut **perluasan separabel** dari F jika setiap elemen dalam E merupakan akar suatu polinomial separabel dalam $F[x]$. Ingat pula bahwa $f(x)$ separabel jika dan hanya jika $\gcd(f(x), f'(x)) = 1$ (Lema 22.1.5).

Proposisi 23.1.12 *Misalkan $f(x)$ adalah polinomial takthereduksi atas F. Jika karakteristik F adalah 0, maka $f(x)$ separabel. Jika karakteristik F adalah p dan $f(x) \neq g(x^p)$ untuk suatu $g(x)$ dalam $F[x]$, maka $f(x)$ juga separabel.*

BUKTI. Pertama, andaikan $\operatorname{char} F = 0$. Karena $\deg f'(x) < \deg f(x)$ dan $f(x)$ takthereduksi, satu-satunya cara agar $\gcd(f(x), f'(x)) \neq 1$ adalah jika $f'(x)$ merupakan polinomial nol; tetapi hal ini mustahil dalam lapangan berkarakteristik nol. Jika $\operatorname{char} F = p$, maka $f'(x)$ dapat menjadi polinomial nol jika setiap koefisien $f'(x)$ merupakan kelipatan p. Hal ini hanya dapat terjadi jika kita memiliki polinomial berbentuk $f(x) = a_0 + a_1x^p + a_2x^{2p} + \cdots + a_nx^{np}$. ■

Perluasan suatu lapangan F yang berbentuk $F(\alpha)$ tentu termasuk perluasan yang paling mudah dipelajari dan dipahami. Diberikan suatu perluasan lapangan E dari F, pertanyaan yang wajar adalah kapan kita dapat menemukan elemen $\alpha \in E$ sedemikian sehingga $E = F(\alpha)$. Dalam hal ini, α disebut **elemen primitif**. Kita telah mengetahui bahwa elemen primitif ada untuk perluasan tertentu. Sebagai contoh,

$$\mathbb{Q}(\sqrt{3}, \sqrt{5}\,) = \mathbb{Q}(\sqrt{3} + \sqrt{5}\,)$$

dan

$$\mathbb{Q}(\sqrt[3]{5}, \sqrt{5}\,i) = \mathbb{Q}(\sqrt[6]{5}\,i).$$

Korolari 22.1.12 menyatakan bahwa terdapat elemen primitif bagi setiap perluasan hingga dari suatu lapangan hingga. Teorema berikut menyatakan bahwa kita sering kali dapat menemukan elemen primitif.

Teorema 23.1.13 Teorema Elemen Primitif. *Misalkan E adalah perluasan separabel hingga dari suatu lapangan F. Maka terdapat $\alpha \in E$ sedemikian sehingga $E = F(\alpha)$.*

BUKTI. Kita telah mengetahui bahwa tidak ada masalah jika F merupakan lapangan hingga. Andaikan E adalah perluasan hingga dari suatu lapangan tak hingga. Kita akan membuktikan hasil tersebut untuk $F(\alpha, \beta)$. Kasus umum mudah diperoleh dengan menggunakan induksi matematika. Misalkan $f(x)$ dan $g(x)$ masing-masing adalah polinomial minimal dari α dan β. Misalkan K adalah lapangan tempat $f(x)$ maupun $g(x)$ terpisah. Andaikan $f(x)$ memiliki

akar $\alpha = \alpha_1, \ldots, \alpha_n$ dalam K dan $g(x)$ memiliki akar $\beta = \beta_1, \ldots, \beta_m$ dalam K. Semua akar ini bermultiplisitas 1, karena E separabel atas F. Karena F tak hingga, kita dapat menemukan a dalam F sedemikian sehingga

$$a \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}$$

untuk setiap i dan j dengan $j \neq 1$. Oleh karena itu, $a(\beta - \beta_j) \neq \alpha_i - \alpha$. Misalkan $\gamma = \alpha + a\beta$. Maka

$$\gamma = \alpha + a\beta \neq \alpha_i + a\beta_j;$$

sehingga $\gamma - a\beta_j \neq \alpha_i$ untuk semua i, j dengan $j \neq 1$. Definisikan $h(x) \in F(\gamma)[x]$ dengan $h(x) = f(\gamma - ax)$. Maka $h(\beta) = f(\alpha) = 0$. Namun, $h(\beta_j) \neq 0$ untuk $j \neq 1$. Jadi, $h(x)$ dan $g(x)$ memiliki tepat satu faktor bersama dalam $F(\gamma)[x]$; yaitu, polinomial minimal β atas $F(\gamma)$ harus linear, karena β adalah satu-satunya akar yang sama-sama dimiliki $g(x)$ dan $h(x)$. Jadi, $\beta \in F(\gamma)$ dan $\alpha = \gamma - a\beta$ berada dalam $F(\gamma)$. Oleh karena itu, $F(\alpha, \beta) = F(\gamma)$. ■

23.2 Teorema Fundamental

Tujuan bagian ini adalah membuktikan Teorema Fundamental Teori Galois. Teorema ini menjelaskan hubungan antara subgrup-subgrup $G(E/F)$ dan lapangan-lapangan antara E dan F.

Proposisi 23.2.1 *Misalkan $\{\sigma_i : i \in I\}$ suatu koleksi automorfisme dari lapangan F. Maka*

$$F_{\{\sigma_i\}} = \{a \in F : \sigma_i(a) = a \text{ untuk semua } \sigma_i\}$$

merupakan sublapangan dari F.

BUKTI. Misalkan $\sigma_i(a) = a$ dan $\sigma_i(b) = b$. Maka

$$\sigma_i(a \pm b) = \sigma_i(a) \pm \sigma_i(b) = a \pm b$$

dan

$$\sigma_i(ab) = \sigma_i(a)\sigma_i(b) = ab.$$

Jika $a \neq 0$, maka $\sigma_i(a^{-1}) = [\sigma_i(a)]^{-1} = a^{-1}$. Terakhir, $\sigma_i(0) = 0$ dan $\sigma_i(1) = 1$ karena σ_i merupakan automorfisme. ■

Korolari 23.2.2 *Misalkan F suatu lapangan dan G suatu subgrup dari* $\mathrm{Aut}(F)$. *Maka*

$$F_G = \{\alpha \in F : \sigma(\alpha) = \alpha \text{ untuk semua } \sigma \in G\}$$

merupakan sublapangan dari F.

Sublapangan $F_{\{\sigma_i\}}$ dari F disebut **lapangan tetap** dari $\{\sigma_i\}$. Lapangan yang ditetapkan oleh subgrup G dari $\mathrm{Aut}(F)$ akan dinotasikan dengan F_G.

Contoh 23.2.3 Misalkan $\sigma : \mathbb{Q}(\sqrt{3}, \sqrt{5}\,) \to \mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ automorfisme yang memetakan $\sqrt{3}$ ke $-\sqrt{3}$. Maka $\mathbb{Q}(\sqrt{5}\,)$ merupakan sublapangan dari $\mathbb{Q}(\sqrt{3}, \sqrt{5}\,)$ yang ditetapkan oleh σ. ▲

Proposisi 23.2.4 *Misalkan E lapangan pemisah atas F dari suatu polinomial separabel. Maka $E_{G(E/F)} = F$.*

BUKTI. Misalkan $G = G(E/F)$. Jelas bahwa $F \subset E_G \subset E$. Selain itu, E harus merupakan lapangan pemisah atas E_G dan $G(E/F) = G(E/E_G)$. Menurut Teorema 23.1.7,

$$|G| = [E : E_G] = [E : F].$$

Oleh karena itu, $[E_G : F] = 1$. Akibatnya, $E_G = F$. ■

Banyak matematikawan pertama kali mempelajari teori Galois dari monograf Emil Artin mengenai pokok ini [1]. Bukti yang sangat cerdik untuk lema berikut berasal dari Artin.

Lema 23.2.5 *Misalkan G suatu grup hingga automorfisme dari E dan misalkan $F = E_G$. Maka $[E : F] \leq |G|$.*

BUKTI. Misalkan $|G| = n$. Kita harus menunjukkan bahwa setiap himpunan yang terdiri atas $n+1$ elemen $\alpha_1, \ldots, \alpha_{n+1}$ dalam E bergantung linear atas F; yaitu, kita perlu menemukan elemen-elemen $a_i \in F$, yang tidak semuanya nol, sedemikian sehingga

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_{n+1}\alpha_{n+1} = 0.$$

Misalkan $\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n$ adalah automorfisme-automorfisme dalam G. Sistem persamaan linear homogen

$$\begin{aligned}
\sigma_1(\alpha_1)x_1 + \sigma_1(\alpha_2)x_2 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0 \\
\sigma_2(\alpha_1)x_1 + \sigma_2(\alpha_2)x_2 + \cdots + \sigma_2(\alpha_{n+1})x_{n+1} &= 0 \\
&\vdots \\
\sigma_n(\alpha_1)x_1 + \sigma_n(\alpha_2)x_2 + \cdots + \sigma_n(\alpha_{n+1})x_{n+1} &= 0
\end{aligned}$$

memiliki lebih banyak variabel yang tidak diketahui daripada persamaan. Dari aljabar linear kita mengetahui bahwa sistem ini memiliki solusi taktrivial, misalnya $x_i = a_i$ untuk $i = 1, 2, \ldots, n+1$. Karena σ_1 adalah identitas, persamaan pertama menjadi

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_{n+1}\alpha_{n+1} = 0.$$

Masalahnya adalah beberapa a_i mungkin berada dalam E, tetapi tidak dalam F. Kita harus menunjukkan bahwa hal ini mustahil.

Misalkan sekurang-kurangnya salah satu a_i berada dalam E, tetapi tidak dalam F. Dengan mengurutkan ulang α_i, kita boleh mengasumsikan bahwa a_1 taknol. Karena setiap kelipatan taknol dari suatu solusi juga merupakan solusi, kita juga dapat mengasumsikan bahwa $a_1 = 1$. Di antara semua solusi yang memenuhi deskripsi ini, kita pilih solusi dengan jumlah suku taknol paling sedikit. Sekali lagi, dengan mengurutkan ulang $\alpha_2, \ldots, \alpha_{n+1}$ jika perlu, kita dapat mengasumsikan bahwa a_2 berada dalam E, tetapi tidak dalam F. Karena F adalah sublapangan dari E yang setiap elemennya ditetapkan oleh G, terdapat σ_i dalam G sedemikian sehingga $\sigma_i(a_2) \neq a_2$. Dengan menerapkan σ_i pada setiap persamaan dalam sistem tersebut, kita memperoleh sistem homogen yang sama, karena G adalah suatu grup. Oleh karena itu, $x_1 = \sigma_i(a_1) = 1$, $x_2 = \sigma_i(a_2)$, ..., $x_{n+1} = \sigma_i(a_{n+1})$ juga merupakan solusi dari sistem semula. Kita mengetahui bahwa kombinasi linear dari dua solusi suatu sistem homogen juga merupakan solusi; akibatnya,

$$\begin{aligned}
x_1 &= 1 - 1 = 0 \\
x_2 &= a_2 - \sigma_i(a_2)
\end{aligned}$$

$$\vdots$$
$$x_{n+1} = a_{n+1} - \sigma_i(a_{n+1})$$

harus merupakan solusi lain dari sistem tersebut. Ini adalah solusi taktrivial karena $\sigma_i(a_2) \neq a_2$, dan memiliki lebih sedikit entri taknol daripada solusi semula. Ini merupakan kontradiksi, karena jumlah entri taknol dalam solusi semula diasumsikan minimal. Dengan demikian, kita dapat menyimpulkan bahwa $a_1, \ldots, a_{n+1} \in F$. ■

Misalkan E suatu perluasan aljabar dari F. Jika setiap polinomial takterereduksi dalam $F[x]$ yang memiliki sebuah akar dalam E memiliki semua akarnya dalam E, maka E disebut **perluasan normal** dari F; yaitu, setiap polinomial takterereduksi dalam $F[x]$ yang memiliki sebuah akar dalam E merupakan hasil kali faktor-faktor linear dalam $E[x]$.

Teorema 23.2.6 *Misalkan E suatu perluasan lapangan dari F. Maka pernyataan-pernyataan berikut ekuivalen.*

1. *E merupakan perluasan hingga, normal, dan separabel dari F.*
2. *E merupakan lapangan pemisah atas F dari suatu polinomial separabel.*
3. *$F = E_G$ untuk suatu grup hingga G yang terdiri atas automorfisme-automorfisme dari E.*

Bukti. (1) $\Rightarrow$ (2). Misalkan E suatu perluasan hingga, normal, dan separabel dari F. Menurut Teorema Elemen Primitif, kita dapat menemukan α dalam E sedemikian sehingga $E = F(\alpha)$. Misalkan $f(x)$ polinomial minimal dari α atas F. Lapangan E harus memuat semua akar $f(x)$ karena merupakan perluasan normal dari F; jadi, E merupakan lapangan pemisah untuk $f(x)$.

(2) $\Rightarrow$ (3). Misalkan E lapangan pemisah atas F dari suatu polinomial separabel. Menurut Proposisi 23.2.4, $E_{G(E/F)} = F$. Karena $|G(E/F)| = [E : F]$, grup ini hingga.

(3) $\Rightarrow$ (1). Misalkan $F = E_G$ untuk suatu grup hingga automorfisme G dari E. Karena $[E : F] \leq |G|$, E merupakan perluasan hingga dari F. Untuk menunjukkan bahwa E merupakan perluasan hingga dan normal dari F, misalkan $f(x) \in F[x]$ suatu polinomial monik takterereduksi yang memiliki akar α dalam E. Kita harus menunjukkan bahwa $f(x)$ merupakan hasil kali faktor-faktor linear berbeda dalam $E[x]$. Menurut Proposisi 23.1.5, automorfisme-automorfisme dalam G mempermutasikan akar-akar $f(x)$ yang berada dalam E. Jadi, jika kita membiarkan G bertindak pada α, kita memperoleh akar-akar berbeda $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ dalam E. Misalkan $g(x) = \prod_{i=1}^{n}(x - \alpha_i)$. Maka $g(x)$ separabel atas F dan $g(\alpha) = 0$. Setiap automorfisme σ dalam G mempermutasikan faktor-faktor $g(x)$ karena mempermutasikan akar-akar tersebut; jadi, ketika σ bertindak pada $g(x)$, automorfisme itu harus menetapkan koefisien-koefisien $g(x)$. Oleh karena itu, koefisien-koefisien $g(x)$ harus berada dalam F. Karena $\deg g(x) \leq \deg f(x)$ dan $f(x)$ adalah polinomial minimal dari α, diperoleh $f(x) = g(x)$. ■

Korolari 23.2.7 *Misalkan K suatu perluasan lapangan dari F sedemikian sehingga $F = K_G$ untuk suatu grup hingga automorfisme G dari K. Maka $G = G(K/F)$.*

Bukti. Karena $F = K_G$, G merupakan subgrup dari $G(K/F)$. Jadi,

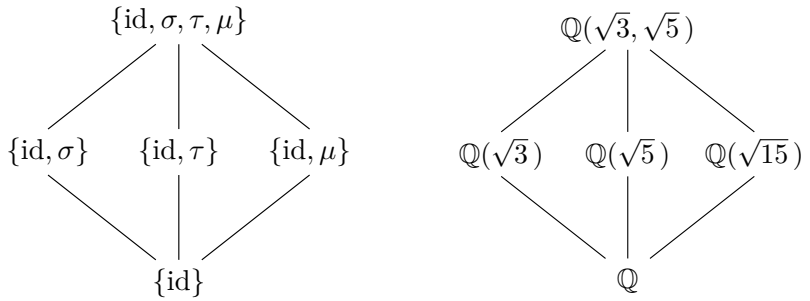
$$[K : F] \leq |G| \leq |G(K/F)| = [K : F].$$

Dengan demikian, $G = G(K/F)$, karena keduanya harus memiliki orde yang

sama. ■

Sebelum menentukan korespondensi yang tepat antara perluasan lapangan dan automorfisme lapangan, mari kita kembali ke sebuah contoh yang sudah dikenal.

Contoh 23.2.8 Dalam Contoh 23.1.4 kita telah menelaah automorfisme-automorfisme dari $\mathbb{Q}(\sqrt{3},\sqrt{5}\,)$ yang menetapkan $\mathbb{Q}$. Gambar 23.2.9 membandingkan kisi perluasan lapangan dari $\mathbb{Q}$ dengan kisi subgrup dari $G(\mathbb{Q}(\sqrt{3},\sqrt{5}\,)/\mathbb{Q})$. Teorema Fundamental Teori Galois menjelaskan hubungan antara kedua kisi tersebut. ▲



Gambar 23.2.9 $G(\mathbb{Q}(\sqrt{3},\sqrt{5}\,)/\mathbb{Q})$

Sekarang kita siap untuk menyatakan dan membuktikan Teorema Fundamental Teori Galois.

Teorema 23.2.10 Teorema Fundamental Teori Galois. *Misalkan F suatu lapangan hingga atau lapangan berkarakteristik nol. Jika E merupakan perluasan normal hingga dari F dengan grup Galois $G(E/F)$, maka pernyataan-pernyataan berikut berlaku.*

1. *Pemetaan $K \mapsto G(E/K)$ merupakan bijeksi antara sublapangan K dari E yang memuat F dan subgrup-subgrup dari $G(E/F)$.*
2. *Jika $F \subset K \subset E$, maka*
$$[E:K] = |G(E/K)| \text{ dan } [K:F] = [G(E/F) : G(E/K)].$$
3. *$F \subset K \subset L \subset E$ jika dan hanya jika $\{\mathrm{id}\} \subset G(E/L) \subset G(E/K) \subset G(E/F)$.*
4. *K merupakan perluasan normal dari F jika dan hanya jika $G(E/K)$ merupakan subgrup normal dari $G(E/F)$. Dalam hal ini*
$$G(K/F) \cong G(E/F)/G(E/K).$$

Bukti. (1) Misalkan $G(E/K) = G(E/L) = G$. Baik K maupun L merupakan lapangan tetap dari G; jadi, $K = L$ dan pemetaan yang didefinisikan oleh $K \mapsto G(E/K)$ bersifat satu-ke-satu. Untuk menunjukkan bahwa pemetaan tersebut bersifat pada, misalkan G suatu subgrup dari $G(E/F)$ dan K lapangan yang ditetapkan oleh G. Maka $F \subset K \subset E$; akibatnya, E merupakan perluasan normal dari K. Jadi, $G(E/K) = G$ dan pemetaan $K \mapsto G(E/K)$ merupakan bijeksi.

(2) Menurut Teorema Teorema 23.1.7, $|G(E/K)| = [E:K]$; oleh karena itu,

$$|G(E/F)| = [G(E/F) : G(E/K)] \cdot |G(E/K)| = [E:F] = [E:K][K:F].$$

Jadi, $[K:F] = [G(E/F) : G(E/K)]$.

Pernyataan (3) diilustrasikan dalam Gambar 23.2.11. Bukti sifat ini diserahkan sebagai latihan.

(4) Bagian ini memerlukan sedikit lebih banyak usaha. Misalkan K suatu perluasan normal dari F. Jika σ berada dalam $G(E/F)$ dan τ berada dalam $G(E/K)$, kita perlu menunjukkan bahwa $\sigma^{-1}\tau\sigma$ berada dalam $G(E/K)$; yaitu, kita perlu menunjukkan bahwa $\sigma^{-1}\tau\sigma(\alpha) = \alpha$ untuk semua $\alpha \in K$. Misalkan $f(x)$ polinomial minimal dari α atas F. Maka $\sigma(\alpha)$ juga merupakan akar dari $f(x)$ yang berada dalam K, karena K merupakan perluasan normal dari F. Jadi, $\tau(\sigma(\alpha)) = \sigma(\alpha)$ atau $\sigma^{-1}\tau\sigma(\alpha) = \alpha$.

Sebaliknya, misalkan $G(E/K)$ suatu subgrup normal dari $G(E/F)$. Kita perlu menunjukkan bahwa $F = K_{G(K/F)}$. Misalkan $\tau \in G(E/K)$. Untuk semua $\sigma \in G(E/F)$, terdapat $\overline{\tau} \in G(E/K)$ sedemikian sehingga $\tau\sigma = \sigma\overline{\tau}$. Akibatnya, untuk semua $\alpha \in K$,

$$\tau(\sigma(\alpha)) = \sigma(\overline{\tau}(\alpha)) = \sigma(\alpha);$$

jadi, $\sigma(\alpha)$ harus berada dalam lapangan tetap dari $G(E/K)$. Misalkan $\overline{\sigma}$ pembatasan σ pada K. Maka $\overline{\sigma}$ merupakan automorfisme dari K yang menetapkan F, karena $\sigma(\alpha) \in K$ untuk semua $\alpha \in K$; jadi, $\overline{\sigma} \in G(K/F)$. Selanjutnya, kita akan menunjukkan bahwa lapangan tetap dari $G(K/F)$ adalah F. Misalkan β suatu elemen dalam K yang ditetapkan oleh semua automorfisme dalam $G(K/F)$. Secara khusus, $\overline{\sigma}(\beta) = \beta$ untuk semua $\sigma \in G(E/F)$. Oleh karena itu, β termasuk dalam lapangan tetap F dari $G(E/F)$.

Terakhir, kita harus menunjukkan bahwa apabila K merupakan perluasan normal dari F,

$$G(K/F) \cong G(E/F)/G(E/K).$$

Untuk $\sigma \in G(E/F)$, misalkan σ_K automorfisme dari K yang diperoleh dengan membatasi σ pada K. Karena K merupakan perluasan normal, argumen pada paragraf sebelumnya menunjukkan bahwa $\sigma_K \in G(K/F)$. Akibatnya, kita memiliki pemetaan $\phi : G(E/F) \to G(K/F)$ yang didefinisikan oleh $\sigma \mapsto \sigma_K$. Pemetaan ini merupakan homomorfisma grup karena

$$\phi(\sigma\tau) = (\sigma\tau)_K = \sigma_K\tau_K = \phi(\sigma)\phi(\tau).$$

Kernel dari ϕ adalah $G(E/K)$. Menurut (2),

$$|G(E/F)|/|G(E/K)| = [K : F] = |G(K/F)|.$$

Jadi, citra dari ϕ adalah $G(K/F)$ dan ϕ bersifat pada. Dengan menerapkan Teorema Isomorfisma Pertama, diperoleh

$$G(K/F) \cong G(E/F)/G(E/K).$$

■

$$\begin{array}{ccc} E & \longrightarrow & \{\text{id}\} \\ \uparrow & & \downarrow \\ L & \longrightarrow & G(E/L) \\ \uparrow & & \downarrow \\ K & \longrightarrow & G(E/K) \\ \uparrow & & \downarrow \\ F & \longrightarrow & G(E/F) \end{array}$$

Gambar 23.2.11 Subgrup dari $G(E/F)$ dan sublapangan dari E

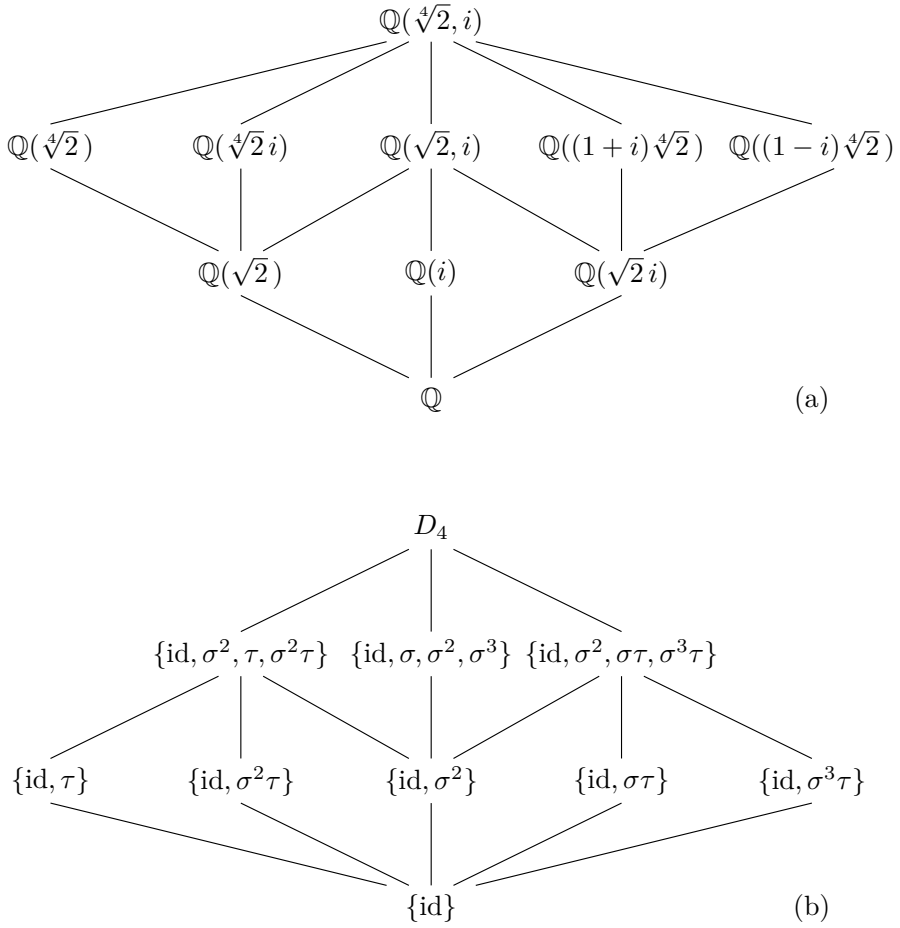
Contoh 23.2.12 Dalam contoh ini kita akan mengilustrasikan Teorema Fundamental Teori Galois dengan menentukan kisi subgrup dari grup Galois untuk $f(x) = x^4 - 2$. Kita akan membandingkan kisi ini dengan kisi perluasan lapangan dari $\mathbb{Q}$ yang termuat dalam lapangan pemisah dari $x^4 - 2$. Lapangan pemisah dari $f(x)$ adalah $\mathbb{Q}(\sqrt[4]{2}, i)$. Untuk melihat hal ini, perhatikan bahwa $f(x)$ dapat difaktorkan sebagai $(x^2 + \sqrt{2})(x^2 - \sqrt{2})$; jadi, akar-akar dari $f(x)$ adalah $\pm\sqrt[4]{2}$ dan $\pm\sqrt[4]{2}\, i$. Pertama-tama kita adjoin akar $\sqrt[4]{2}$ pada $\mathbb{Q}$, lalu mengadjoin akar i dari $x^2 + 1$ pada $\mathbb{Q}(\sqrt[4]{2})$. Dengan demikian, lapangan pemisah dari $f(x)$ adalah $\mathbb{Q}(\sqrt[4]{2})(i) = \mathbb{Q}(\sqrt[4]{2}, i)$.

Karena $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ dan i tidak berada dalam $\mathbb{Q}(\sqrt[4]{2})$, haruslah $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$. Jadi, $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$. Himpunan

$$\{1, \sqrt[4]{2}, (\sqrt[4]{2})^2, (\sqrt[4]{2})^3, i, i\sqrt[4]{2}, i(\sqrt[4]{2})^2, i(\sqrt[4]{2})^3\}$$

merupakan basis dari $\mathbb{Q}(\sqrt[4]{2}, i)$ atas $\mathbb{Q}$. Kisi perluasan lapangan dari $\mathbb{Q}$ yang termuat dalam $\mathbb{Q}(\sqrt[4]{2}, i)$ diilustrasikan dalam Gambar 23.2.13(a).

Grup Galois G dari $f(x)$ harus berorde 8. Misalkan σ automorfisme yang didefinisikan oleh $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ dan $\sigma(i) = i$, serta τ automorfisme yang didefinisikan oleh konjugasi kompleks; yaitu, $\tau(i) = -i$. Maka G memiliki suatu elemen berorde 4 dan suatu elemen berorde 2. Mudah diverifikasi melalui perhitungan langsung bahwa elemen-elemen dari G adalah $\{\text{id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$ dan bahwa relasi-relasi $\tau^2 = \text{id}$, $\sigma^4 = \text{id}$, dan $\tau\sigma\tau = \sigma^{-1}$ dipenuhi; jadi, G harus isomorfik dengan D_4. Kisi subgrup dari G diilustrasikan dalam Gambar 23.2.13(b). ▲



Gambar 23.2.13 Grup Galois dari $x^4 - 2$

Catatan Sejarah

Penyelesaian untuk persamaan kubik dan kuartik ditemukan pada tahun 1500-an. Upaya menemukan penyelesaian untuk persamaan kuintik membingungkan beberapa matematikawan terbaik sepanjang sejarah. Pada tahun 1798, P. Ruffini menyerahkan sebuah makalah yang menyatakan bahwa penyelesaian semacam itu tidak dapat ditemukan; namun, makalah tersebut tidak diterima dengan baik. Pada tahun 1826, Niels Henrik Abel (1802–1829) akhirnya memberikan bukti benar pertama bahwa persamaan kuintik tidak selalu dapat diselesaikan dengan radikal.

Abel mengilhami karya Évariste Galois. Lahir pada tahun 1811, Galois mulai menunjukkan bakat matematika yang luar biasa pada usia 14 tahun. Ia beberapa kali mendaftar ke École Polytechnique; namun, ia sangat kesulitan memenuhi persyaratan penerimaan formal, dan para penguji gagal mengenali kejeniusannya dalam matematika. Ia akhirnya diterima di École Normale pada tahun 1829.

Galois berupaya mengembangkan teori keterpecahan polinomial. Pada tahun 1829, ketika berusia 17 tahun, Galois menyerahkan dua makalah tentang penyelesaian persamaan aljabar kepada Académie des Sciences de Paris. Makalah-makalah tersebut dikirim kepada Cauchy, yang kemudian menghilangkannya. Makalah ketiga diserahkan kepada Fourier, yang meninggal sebelum sempat membacanya. Sebuah makalah lain diajukan, tetapi baru diterbitkan pada

tahun 1846.
Simpati Galois terhadap demokrasi menyeretnya ke dalam Revolusi 1830. Ia dikeluarkan dari sekolah dan dipenjarakan karena keterlibatannya dalam pergolakan tersebut. Setelah dibebaskan pada tahun 1832, ia terseret ke dalam sebuah duel, mungkin akibat persoalan cinta. Karena yakin akan terbunuh, pada malam sebelum kematiannya ia merangkum karya dan gagasan dasar penelitiannya dalam sebuah surat panjang kepada sahabatnya, Chevalier. Ia benar-benar meninggal keesokan harinya, pada usia 20 tahun.

23.3 Penerapan

23.3.1 Keterpecahan dengan Radikal

Sepanjang bagian ini kita akan mengasumsikan bahwa semua lapangan berkarakteristik nol untuk memastikan bahwa polinomial takthereduksi tidak memiliki akar ganda. Tujuan langsung bagian ini adalah menentukan kapan akar-akar suatu polinomial $f(x)$ dapat dihitung melalui sejumlah hingga operasi pada koefisien-koefisien $f(x)$. Operasi yang diperbolehkan adalah penjumlahan, pengurangan, perkalian, pembagian, dan pengambilan akar pangkat n. Tentu saja, penyelesaian persamaan kuadrat $ax^2+bx+c=0$ mengilustrasikan proses ini:

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}.$$

Satu-satunya operasi di antara operasi-operasi tersebut yang mungkin memerlukan lapangan lebih besar adalah pengambilan akar pangkat n. Hal ini membawa kita pada definisi berikut.

Lapangan perluasan E dari lapangan F merupakan suatu **perluasan dengan radikal** jika terdapat rantai sublapangan

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r = E$$

sedemikian sehingga untuk $i = 1, 2, \ldots, r$, berlaku $F_i = F_{i-1}(\alpha_i)$ dan $\alpha_i^{n_i} \in F_{i-1}$ untuk suatu bilangan bulat positif n_i. Suatu polinomial $f(x)$ **dapat diselesaikan dengan radikal** atas F jika lapangan pemisah K dari $f(x)$ atas F termuat dalam suatu perluasan dengan radikal dari F. Tujuan kita adalah memperoleh kriteria yang menentukan dapat atau tidaknya suatu polinomial $f(x)$ diselesaikan dengan radikal dengan menelaah grup Galois dari $f(x)$.

Polinomial yang paling mudah diselesaikan dengan radikal adalah polinomial berbentuk $x^n - a$. Seperti yang dibahas dalam Bab 4, akar-akar dari $x^n - 1$ disebut **akar-akar kesatuan pangkat n**. Akar-akar ini membentuk subgrup hingga dari lapangan pemisah $x^n - 1$. Menurut Korolari 22.1.11, akar-akar kesatuan pangkat n membentuk suatu grup siklik. Setiap pembangkit grup ini disebut **akar kesatuan primitif pangkat n**.

Contoh 23.3.1 Polinomial $x^n - 1$ dapat diselesaikan dengan radikal atas $\mathbb{Q}$. Akar-akar polinomial ini adalah $1, \omega, \omega^2, \ldots, \omega^{n-1}$, dengan

$$\omega = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right).$$

Lapangan pemisah dari $x^n - 1$ atas $\mathbb{Q}$ adalah $\mathbb{Q}(\omega)$. ▲

Kita akan membuktikan bahwa suatu polinomial dapat diselesaikan dengan radikal jika grup Galoisnya dapat diselesaikan. Ingat bahwa deret subnormal dari suatu grup G adalah barisan hingga subgrup

$$G = H_n \supset H_{n-1} \supset \cdots \supset H_1 \supset H_0 = \{e\},$$

dengan H_i normal dalam H_{i+1}. Suatu grup G dapat diselesaikan jika memiliki deret subnormal $\{H_i\}$ sedemikian sehingga semua grup hasil bagi H_{i+1}/H_i abelian. Sebagai contoh, jika kita menelaah deret $\{\mathrm{id}\} \subset A_3 \subset S_3$, kita melihat bahwa S_3 dapat diselesaikan. Di sisi lain, S_5 tidak dapat diselesaikan, menurut Teorema 10.2.4.

Lema 23.3.2 *Misalkan F suatu lapangan berkarakteristik nol dan E lapangan pemisah dari $x^n - a$ atas F dengan $a \in F$. Maka $G(E/F)$ merupakan grup yang dapat diselesaikan.*

Bukti. Akar-akar dari $x^n - a$ adalah $\sqrt[n]{a}, \omega\sqrt[n]{a}, \ldots, \omega^{n-1}\sqrt[n]{a}$, dengan ω suatu akar kesatuan primitif pangkat n. Misalkan F memuat semua akar kesatuan pangkat n. Jika ζ adalah salah satu akar dari $x^n - a$, maka akar-akar berbeda dari $x^n - a$ adalah $\zeta, \omega\zeta, \ldots, \omega^{n-1}\zeta$, dan $E = F(\zeta)$. Karena $G(E/F)$ mempermutasikan akar-akar dari $x^n - a$, elemen-elemen dalam $G(E/F)$ harus ditentukan oleh tindakannya pada akar-akar tersebut. Misalkan σ dan τ berada dalam $G(E/F)$ dan andaikan bahwa $\sigma(\zeta) = \omega^i\zeta$ dan $\tau(\zeta) = \omega^j\zeta$. Jika F memuat akar-akar kesatuan tersebut, maka

$$\sigma\tau(\zeta) = \sigma(\omega^j\zeta) = \omega^j\sigma(\zeta) = \omega^{i+j}\zeta = \omega^i\tau(\zeta) = \tau(\omega^i\zeta) = \tau\sigma(\zeta).$$

Oleh karena itu, $\sigma\tau = \tau\sigma$ dan $G(E/F)$ abelian, sehingga $G(E/F)$ dapat diselesaikan.

Sekarang andaikan bahwa F tidak memuat akar kesatuan primitif pangkat n. Misalkan ω suatu pembangkit dari grup siklik akar-akar kesatuan pangkat n. Misalkan α suatu akar dari $x^n - a$. Karena α dan $\omega\alpha$ keduanya berada dalam lapangan pemisah dari $x^n - a$, $\omega = (\omega\alpha)/\alpha$ juga berada dalam E. Misalkan $K = F(\omega)$. Maka $F \subset K \subset E$. Karena K adalah lapangan pemisah dari $x^n - 1$, K merupakan perluasan normal dari F. Oleh karena itu, setiap automorfisme σ dalam $G(F(\omega)/F)$ ditentukan oleh $\sigma(\omega)$. Haruslah $\sigma(\omega) = \omega^i$ untuk suatu bilangan bulat i, karena semua akar dari $x^n - 1$ merupakan pangkat dari ω. Jika $\tau(\omega) = \omega^j$ berada dalam $G(F(\omega)/F)$, maka

$$\sigma\tau(\omega) = \sigma(\omega^j) = [\sigma(\omega)]^j = \omega^{ij} = [\tau(\omega)]^i = \tau(\omega^i) = \tau\sigma(\omega).$$

Oleh karena itu, $G(F(\omega)/F)$ abelian. Menurut Teorema Fundamental Teori Galois, deret

$$\{\mathrm{id}\} \subset G(E/F(\omega)) \subset G(E/F)$$

merupakan deret normal. Menurut argumen sebelumnya, $G(E/F(\omega))$ abelian. Karena

$$G(E/F)/G(E/F(\omega)) \cong G(F(\omega)/F)$$

juga abelian, $G(E/F)$ dapat diselesaikan. ■

Lema 23.3.3 *Misalkan F suatu lapangan berkarakteristik nol dan misalkan*

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r = E$$

suatu perluasan dengan radikal dari F. Maka terdapat perluasan normal dengan radikal

$$F = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_r = K$$

sedemikian sehingga K memuat E dan K_i merupakan perluasan normal dari K_{i-1}.

Bukti. Karena E merupakan perluasan dengan radikal dari F, terdapat rantai

sublapangan

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_r = E$$

sedemikian sehingga untuk $i = 1, 2, \ldots, r$, berlaku $F_i = F_{i-1}(\alpha_i)$ dan $\alpha_i^{n_i} \in F_{i-1}$ untuk suatu bilangan bulat positif n_i. Kita akan membangun suatu perluasan normal dengan radikal dari F,

$$F = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_r = K$$

sedemikian sehingga $K \supseteq E$. Definisikan K_1 sebagai lapangan pemisah dari $x^{n_1} - \alpha_1^{n_1}$. Akar-akar polinomial ini adalah $\alpha_1, \alpha_1\omega, \alpha_1\omega^2, \ldots, \alpha_1\omega^{n_1-1}$, dengan ω suatu akar kesatuan primitif pangkat n_1. Jika F memuat semua akar kesatuan pangkat n_1, maka $K_1 = F(\alpha_1)$. Di sisi lain, andaikan bahwa F tidak memuat akar kesatuan primitif pangkat n_1. Jika β adalah suatu akar dari $x^{n_1} - \alpha_1^{n_1}$, maka semua akar dari $x^{n_1} - \alpha_1^{n_1}$ harus berupa $\beta, \omega\beta, \ldots, \omega^{n_1-1}\beta$, dengan ω suatu akar kesatuan primitif pangkat n_1. Dalam hal ini, $K_1 = F(\omega\beta)$. Jadi, K_1 merupakan perluasan normal dengan radikal dari F yang memuat F_1. Dengan melanjutkan cara ini, kita memperoleh

$$F = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_r = K$$

sedemikian sehingga K_i merupakan perluasan normal dari K_{i-1} dan $K_i \supseteq F_i$ untuk $i = 1, 2, \ldots, r$. ■

Sekarang kita akan membuktikan teorema utama mengenai keterpecahan dengan radikal.

Teorema 23.3.4 *Misalkan $f(x)$ berada dalam $F[x]$, dengan* $\operatorname{char} F = 0$. *Jika $f(x)$ dapat diselesaikan dengan radikal, maka grup Galois dari $f(x)$ atas F dapat diselesaikan.*

BUKTI. Karena $f(x)$ dapat diselesaikan dengan radikal, terdapat suatu perluasan dengan radikal E dari F, yaitu $F = F_0 \subset F_1 \subset \cdots \subset F_n = E$. Menurut Lema 23.3.3, kita dapat mengasumsikan bahwa E merupakan lapangan pemisah dari $f(x)$ dan F_i normal atas F_{i-1}. Menurut Teorema Fundamental Teori Galois, $G(E/F_i)$ merupakan subgrup normal dari $G(E/F_{i-1})$. Oleh karena itu, kita memiliki deret subnormal subgrup dari $G(E/F)$:

$$\{\mathrm{id}\} \subset G(E/F_{n-1}) \subset \cdots \subset G(E/F_1) \subset G(E/F).$$

Sekali lagi menurut Teorema Fundamental Teori Galois, kita mengetahui bahwa

$$G(E/F_{i-1})/G(E/F_i) \cong G(F_i/F_{i-1}).$$

Menurut Lema 23.3.2, $G(F_i/F_{i-1})$ dapat diselesaikan; jadi, $G(E/F)$ juga dapat diselesaikan. ■

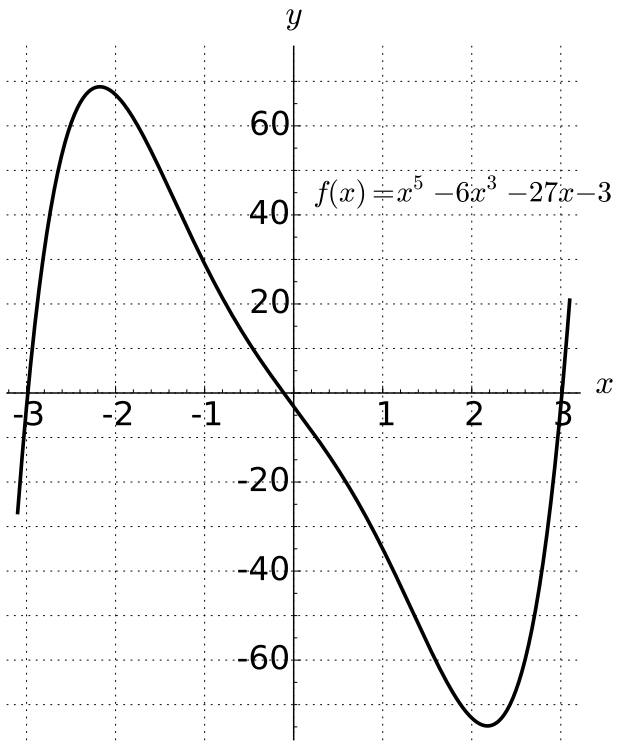
Kebalikan dari Teorema 23.3.4 juga benar. Untuk buktinya, lihat salah satu referensi pada akhir bab ini.

23.3.2 Ketakterpecahan Persamaan Kuintik

Sekarang kita dapat menemukan suatu polinomial berderajat lima yang tidak dapat diselesaikan dengan radikal. Kita hanya perlu menemukan polinomial yang grup Galoisnya adalah S_5. Kita mulai dengan membuktikan sebuah lema.

Lema 23.3.5 *Jika p prima, maka setiap subgrup dari S_p yang memuat suatu transposisi dan siklus dengan panjang p harus sama dengan seluruh S_p.*

BUKTI. Misalkan G suatu subgrup dari S_p yang memuat suatu transposisi σ dan suatu siklus τ dengan panjang p. Kita boleh mengasumsikan bahwa $\sigma = (1\,2)$. Orde dari τ adalah p dan τ^n harus merupakan siklus dengan panjang p untuk $1 \leq n < p$. Oleh karena itu, kita boleh mengasumsikan bahwa $\mu = \tau^n = (1, 2, i_3, \ldots, i_p)$ untuk suatu n, dengan $1 \leq n < p$ (lihat Latihan 5.4.13 dalam Bab 5). Dengan memperhatikan bahwa $(1\,2)(1, 2, i_3, \ldots, i_p) = (2, i_3, \ldots, i_p)$ dan $(2, i_3, \ldots, i_p)^k(1\,2)(2, i_3, \ldots, i_p)^{-k} = (1\,i_k)$, kita dapat memperoleh semua transposisi berbentuk $(1n)$ untuk $1 \leq n < p$. Namun, transposisi-transposisi ini membangkitkan semua transposisi dalam S_p, karena $(1\,j)(1\,i)(1\,j) = (i\,j)$. Transposisi-transposisi tersebut membangkitkan S_p. ■



Gambar 23.3.6 Grafik $f(x) = x^5 - 6x^3 - 27x - 3$

Contoh 23.3.7 Kita akan menunjukkan bahwa $f(x) = x^5 - 6x^3 - 27x - 3 \in \mathbb{Q}[x]$ tidak dapat diselesaikan. Kita mengklaim bahwa grup Galois dari $f(x)$ atas $\mathbb{Q}$ adalah S_5. Menurut Kriteria Eisenstein, $f(x)$ takthereduksi dan, oleh karena itu, harus separabel. Turunan dari $f(x)$ adalah $f'(x) = 5x^4 - 18x^2 - 27$; jadi, dengan menetapkan $f'(x) = 0$ dan menyelesaikannya, kita menemukan bahwa akar real dari $f'(x)$ hanyalah

$$x = \pm\sqrt{\frac{6\sqrt{6} + 9}{5}}.$$

Oleh karena itu, $f(x)$ dapat memiliki paling banyak satu maksimum dan satu minimum. Mudah ditunjukkan bahwa $f(x)$ berganti tanda antara -3 dan -2, antara -2 dan 0, serta sekali lagi antara 0 dan 4 (Gambar 23.3.6). Oleh karena itu, $f(x)$ memiliki tepat tiga akar real yang berbeda. Dua akar $f(x)$ yang tersisa harus berupa pasangan konjugat kompleks. Misalkan K lapangan pemisah dari $f(x)$. Karena $f(x)$ memiliki lima akar berbeda dalam K dan setiap automorfisme dari K yang menetapkan $\mathbb{Q}$ ditentukan oleh caranya mempermutasikan akar-akar $f(x)$, kita mengetahui bahwa $G(K/\mathbb{Q})$ merupakan subgrup

dari S_5. Karena f takthereduksi, terdapat elemen $\sigma \in G(K/\mathbb{Q})$ sedemikian sehingga $\sigma(a) = b$ untuk dua akar a dan b dari $f(x)$. Automorfisme dari $\mathbb{C}$ yang memetakan $a + bi \mapsto a - bi$ menetapkan akar-akar real dan mempertukarkan akar-akar kompleks; akibatnya, $G(K/\mathbb{Q})$ memuat suatu transposisi. Jika α adalah salah satu akar real dari $f(x)$, maka $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ menurut Latihan 21.5.28. Karena $\mathbb{Q}(\alpha)$ merupakan sublapangan dari K, haruslah $[K : \mathbb{Q}]$ habis dibagi 5. Karena $[K : \mathbb{Q}] = |G(K/\mathbb{Q})|$ dan $G(K/\mathbb{Q}) \subset S_5$, kita mengetahui bahwa $G(K/\mathbb{Q})$ memuat suatu siklus dengan panjang 5. Menurut Lema 23.3.5, S_5 dibangkitkan oleh suatu transposisi dan suatu elemen berorde 5; oleh karena itu, $G(K/\mathbb{Q})$ harus sama dengan seluruh S_5. Menurut Teorema 10.2.4, S_5 tidak dapat diselesaikan. Akibatnya, $f(x)$ tidak dapat diselesaikan dengan radikal. ▲

23.3.3 Teorema Fundamental Aljabar

Sudah selayaknya teorema terakhir yang akan kita nyatakan dan buktikan adalah Teorema Fundamental Aljabar. Teorema ini pertama kali dibuktikan oleh Gauss dalam disertasi doktoralnya. Sebelum bukti Gauss, para matematikawan menduga bahwa mungkin terdapat polinomial atas bilangan real dan kompleks yang tidak memiliki penyelesaian. Teorema Fundamental Aljabar menyatakan bahwa setiap polinomial atas bilangan kompleks dapat difaktorkan menjadi faktor-faktor linear yang berbeda.

Teorema 23.3.8 Teorema Fundamental Aljabar. *Lapangan bilangan kompleks tertutup secara aljabar; yaitu, setiap polinomial dalam $\mathbb{C}[x]$ memiliki akar dalam $\mathbb{C}$.*

Bukti. Andaikan E merupakan perluasan lapangan hingga sejati dari bilangan kompleks. Karena setiap perluasan hingga dari lapangan berkarakteristik nol merupakan perluasan sederhana, terdapat $\alpha \in E$ sedemikian sehingga $E = \mathbb{C}(\alpha)$, dengan α suatu akar dari polinomial takthereduksi $f(x)$ dalam $\mathbb{C}[x]$. Lapangan pemisah L dari $f(x)$ merupakan perluasan hingga, normal, dan separabel dari $\mathbb{C}$ yang memuat E. Kita harus menunjukkan bahwa L mustahil merupakan perluasan sejati dari $\mathbb{C}$.

Andaikan L merupakan perluasan sejati dari $\mathbb{C}$. Karena L merupakan lapangan pemisah dari $f(x) = (x^2 + 1)$ atas $\mathbb{R}$, L merupakan perluasan hingga, normal, dan separabel dari $\mathbb{R}$. Misalkan K lapangan tetap dari suatu subgrup Sylow 2, yaitu G, dari $G(L/\mathbb{R})$. Maka $L \supset K \supset \mathbb{R}$ dan $|G(L/K)| = [L : K]$. Karena $[L : \mathbb{R}] = [L : K][K : \mathbb{R}]$, kita mengetahui bahwa $[K : \mathbb{R}]$ harus ganjil. Akibatnya, $K = \mathbb{R}(\beta)$, dengan β memiliki polinomial minimal $f(x)$ berderajat ganjil. Oleh karena itu, $K = \mathbb{R}$.

Sekarang kita mengetahui bahwa $G(L/\mathbb{R})$ harus merupakan suatu grup-2. Akibatnya, $G(L/\mathbb{C})$ merupakan grup-2. Kita telah mengasumsikan bahwa $L \neq \mathbb{C}$; oleh karena itu, $|G(L/\mathbb{C})| \geq 2$. Menurut Teorema Sylow pertama dan Teorema Fundamental Teori Galois, terdapat suatu subgrup G dari $G(L/\mathbb{C})$ berindeks 2 dan suatu lapangan E yang setiap elemennya ditetapkan oleh G. Maka $[E : \mathbb{C}] = 2$ dan terdapat elemen $\gamma \in E$ dengan polinomial minimal $x^2 + bx + c$ dalam $\mathbb{C}[x]$. Polinomial ini memiliki akar $(-b \pm \sqrt{b^2 - 4c})/2$ yang berada dalam $\mathbb{C}$, karena $b^2 - 4c$ berada dalam $\mathbb{C}$. Ini mustahil; jadi, $L = \mathbb{C}$. ■

Meskipun bukti kita sepenuhnya bersifat aljabar, kita terpaksa mengandalkan hasil-hasil dari kalkulus. Aksioma kelengkapan dari analisis perlu diasumsikan untuk menunjukkan bahwa setiap polinomial berderajat ganjil memiliki akar real dan bahwa setiap bilangan real positif memiliki akar kuadrat. Tampaknya tidak mungkin menghindari kesulitan ini dan merumuskan argumen yang murni aljabar. Cukup menakjubkan bahwa terdapat beberapa bukti

elegan untuk Teorema Fundamental Aljabar yang menggunakan analisis kompleks. Menarik pula untuk dicatat bahwa kita dapat memperoleh bukti bagi teorema sepenting ini dari dua bidang matematika yang sangat berbeda.

23.4 Pertanyaan Bacaan

1. Apa yang dimaksud dengan grup Galois dari suatu perluasan lapangan?

2. Kapan dua elemen dari suatu perluasan lapangan disebut saling konjugat? (Dengan kata lain, apa definisinya?)

3. Rangkum sifat dan arti penting Teorema Fundamental Teori Galois. Tangkap inti hasilnya tanpa terjebak dalam terlalu banyak perincian.

4. Mengapa grup yang "dapat diselesaikan" dinamai demikian? Mengungkapkan kembali teorema yang relevan dengan kata-kata sendiri akan menjadi jawaban yang baik.

5. Berikan argumen yang mendukung maupun menentang pernyataan berikut. Pihak mana yang memenangkan perdebatan?

> Segala sesuatu yang telah kita kerjakan sepanjang mata kuliah ini merupakan persiapan untuk bab ini.

23.5 Latihan

1. Hitung masing-masing grup Galois berikut. Manakah di antara perluasan lapangan ini yang merupakan perluasan lapangan normal? Jika perluasannya tidak normal, temukan suatu perluasan normal dari $\mathbb{Q}$ yang memuat lapangan perluasan tersebut.

(a) $G(\mathbb{Q}(\sqrt{30})/\mathbb{Q})$

(b) $G(\mathbb{Q}(\sqrt[4]{5})/\mathbb{Q})$

(c) $G(\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q})$

(d) $G(\mathbb{Q}(\sqrt{2},\sqrt[3]{2},i)/\mathbb{Q})$

(e) $G(\mathbb{Q}(\sqrt{6},i)/\mathbb{Q})$

Petunjuk. (a) $\mathbb{Z}_2$; (c) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

2. Tentukan separabilitas dari masing-masing polinomial berikut.

(a) $x^3 + 2x^2 - x - 2$ atas $\mathbb{Q}$

(b) $x^4 + 2x^2 + 1$ atas $\mathbb{Q}$

(c) $x^4 + x^2 + 1$ atas $\mathbb{Z}_3$

(d) $x^3 + x^2 + 1$ atas $\mathbb{Z}_2$

Petunjuk. (a) Separabel atas $\mathbb{Q}$ karena $x^3 + 2x^2 - x - 2 = (x-1)(x+1)(x+2)$; (c) tidak separabel atas $\mathbb{Z}_3$ karena $x^4+x^2+1 = (x+1)^2(x+2)^2$.

3. Berikan orde dan deskripsikan suatu pembangkit dari grup Galois GF(729) atas GF(9).

Petunjuk. Jika

$$[\mathrm{GF}(729) : \mathrm{GF}(9)] = [\mathrm{GF}(729) : \mathrm{GF}(3)]/[\mathrm{GF}(9) : \mathrm{GF}(3)] = 6/2 = 3,$$

maka $G(\mathrm{GF}(729)/\,\mathrm{GF}(9)) \cong \mathbb{Z}_3$. Suatu pembangkit untuk $G(\mathrm{GF}(729)/\,\mathrm{GF}(9))$ adalah σ, dengan $\sigma_{3^6}(\alpha) = \alpha^{3^6} = \alpha^{729}$ untuk $\alpha \in \mathrm{GF}(729)$.

4. Tentukan grup Galois dari masing-masing polinomial berikut dalam $\mathbb{Q}[x]$; kemudian tentukan keterpecahan dengan radikal dari masing-masing polinomial tersebut.

(a) $x^5 - 12x^2 + 2$
(b) $x^5 - 4x^4 + 2x + 2$
(c) $x^3 - 5$
(d) $x^4 - x^2 - 6$
(e) $x^5 + 1$
(f) $(x^2 - 2)(x^2 + 2)$
(g) $x^8 - 1$
(h) $x^8 + 1$
(i) $x^4 - 3x^2 - 10$

Petunjuk. (a) S_5; (c) S_3; (g) lihat Contoh 23.1.11.

5. Temukan suatu elemen primitif dalam lapangan pemisah dari masing-masing polinomial berikut dalam $\mathbb{Q}[x]$.

(a) $x^4 - 1$
(b) $x^4 - 8x^2 + 15$
(c) $x^4 - 2x^2 - 15$
(d) $x^3 - 2$

Petunjuk. (a) $\mathbb{Q}(i)$

6. Buktikan bahwa grup Galois dari suatu polinomial kuadrat takthereduksi isomorfik dengan $\mathbb{Z}_2$.

7. Buktikan bahwa grup Galois dari suatu polinomial kubik takthereduksi isomorfik dengan S_3 atau $\mathbb{Z}_3$.

Petunjuk. Misalkan E lapangan pemisah dari suatu polinomial kubik dalam $F[x]$. Tunjukkan bahwa $[E : F]$ kurang dari atau sama dengan 6 dan habis dibagi 3. Karena $G(E/F)$ merupakan subgrup dari S_3 yang ordenya habis dibagi 3, simpulkan bahwa grup ini harus isomorfik dengan $\mathbb{Z}_3$ atau S_3.

8. Misalkan $F \subset K \subset E$ lapangan-lapangan. Jika E merupakan perluasan normal dari F, tunjukkan bahwa E juga harus merupakan perluasan normal dari K.

9. Misalkan G grup Galois dari suatu polinomial berderajat n. Buktikan bahwa $|G|$ membagi $n!$.

Petunjuk. G merupakan subgrup dari S_n.

10. Misalkan $F \subset E$. Jika $f(x)$ dapat diselesaikan atas F, tunjukkan bahwa $f(x)$ juga dapat diselesaikan atas E.

11. Bangun suatu polinomial $f(x)$ dalam $\mathbb{Q}[x]$ berderajat 7 yang tidak dapat diselesaikan dengan radikal.

12. Misalkan p prima. Buktikan bahwa terdapat suatu polinomial $f(x) \in \mathbb{Q}[x]$ berderajat p dengan grup Galois yang isomorfik dengan S_p. Simpulkan bahwa untuk setiap bilangan prima p dengan $p \geq 5$, terdapat suatu polinomial berderajat p yang tidak dapat diselesaikan dengan radikal.

13. Misalkan p suatu bilangan prima dan $\mathbb{Z}_p(t)$ lapangan fungsi rasional atas $\mathbb{Z}_p$. Buktikan bahwa $f(x) = x^p - t$ merupakan polinomial takthereduksi dalam $\mathbb{Z}_p(t)[x]$. Tunjukkan bahwa $f(x)$ tidak separabel.

14. Misalkan E suatu lapangan perluasan dari F. Andaikan K dan L dua lapangan antara. Jika terdapat elemen $\sigma \in G(E/F)$ sedemikian sehingga $\sigma(K) = L$, maka K dan L disebut **lapangan-lapangan konjugat.** Buktikan bahwa K dan L konjugat jika dan hanya jika $G(E/K)$ dan $G(E/L)$

merupakan subgrup-subgrup konjugat dari $G(E/F)$.

15. Misalkan $\sigma \in \text{Aut}(\mathbb{R})$. Jika a suatu bilangan real positif, tunjukkan bahwa $\sigma(a) > 0$.

16. Misalkan K lapangan pemisah dari $x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$. Buktikan atau sangkal bahwa K merupakan perluasan dengan radikal.

Petunjuk. Benar.

17. Misalkan F suatu lapangan sedemikian sehingga $\text{char}(F) \neq 2$. Buktikan bahwa lapangan pemisah dari $f(x) = ax^2 + bx + c$ adalah $F(\sqrt{\alpha}\,)$, dengan $\alpha = b^2 - 4ac$.

18. Buktikan atau sangkal: Dua subgrup berbeda dari suatu grup Galois akan memiliki lapangan tetap yang berbeda.

19. Misalkan K lapangan pemisah dari suatu polinomial atas F. Buktikan bahwa jika E merupakan perluasan lapangan dari F yang termuat dalam K dan $[E : F] = 2$, maka E merupakan lapangan pemisah dari suatu polinomial dalam $F[x]$.

20. Kita mengetahui bahwa polinomial siklotomik

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

takтereduksi atas $\mathbb{Q}$ untuk setiap bilangan prima p. Misalkan ω suatu akar dari $\Phi_p(x)$, dan tinjau lapangan $\mathbb{Q}(\omega)$.

(a) Tunjukkan bahwa $\omega, \omega^2, \ldots, \omega^{p-1}$ merupakan akar-akar berbeda dari $\Phi_p(x)$, dan simpulkan bahwa semuanya adalah seluruh akar dari $\Phi_p(x)$.

(b) Tunjukkan bahwa $G(\mathbb{Q}(\omega)/\mathbb{Q})$ abelian dan berorde $p - 1$.

(c) Tunjukkan bahwa lapangan tetap dari $G(\mathbb{Q}(\omega)/\mathbb{Q})$ adalah $\mathbb{Q}$.

Petunjuk.

(a) Jelas bahwa $\omega, \omega^2, \ldots, \omega^{p-1}$ berbeda karena $\omega \neq 1$ atau 0. Untuk menunjukkan bahwa ω^i merupakan akar dari Φ_p, hitung $\Phi_p(\omega^i)$.

(b) Konjugat-konjugat dari ω adalah $\omega, \omega^2, \ldots, \omega^{p-1}$. Definisikan suatu pemetaan $\phi_i : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega^i)$ dengan

$$\phi_i(a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}) = a_0 + a_1\omega^i + \cdots + c_{p-2}(\omega^i)^{p-2},$$

dengan $a_i \in \mathbb{Q}$. Buktikan bahwa ϕ_i merupakan isomorfisma lapangan. Tunjukkan bahwa ϕ_2 membangkitkan $G(\mathbb{Q}(\omega)/\mathbb{Q})$.

(c) Tunjukkan bahwa $\{\omega, \omega^2, \ldots, \omega^{p-1}\}$ merupakan basis untuk $\mathbb{Q}(\omega)$ atas $\mathbb{Q}$, dan tinjau kombinasi linear mana dari $\omega, \omega^2, \ldots, \omega^{p-1}$ yang ditetapkan oleh semua elemen dari $G(\mathbb{Q}(\omega)/\mathbb{Q})$.

21. Misalkan F suatu lapangan hingga atau lapangan berkarakteristik nol. Misalkan E suatu perluasan normal hingga dari F dengan grup Galois $G(E/F)$. Buktikan bahwa $F \subset K \subset L \subset E$ jika dan hanya jika $\{\text{id}\} \subset G(E/L) \subset G(E/K) \subset G(E/F)$.

22. Misalkan F suatu lapangan berkarakteristik nol dan misalkan $f(x) \in F[x]$ suatu polinomial separabel berderajat n. Jika E merupakan lapangan pemisah dari $f(x)$, misalkan $\alpha_1, \ldots, \alpha_n$ akar-akar dari $f(x)$ dalam E. Mi-

salkan $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$. Kita mendefinisikan **diskriminan** dari $f(x)$ sebagai Δ^2.

(a) Jika $f(x) = x^2 + bx + c$, tunjukkan bahwa $\Delta^2 = b^2 - 4c$.

(b) Jika $f(x) = x^3 + px + q$, tunjukkan bahwa $\Delta^2 = -4p^3 - 27q^2$.

(c) Buktikan bahwa Δ^2 berada dalam F.

(d) Jika $\sigma \in G(E/F)$ merupakan transposisi dua akar dari $f(x)$, tunjukkan bahwa $\sigma(\Delta) = -\Delta$.

(e) Jika $\sigma \in G(E/F)$ merupakan permutasi genap dari akar-akar $f(x)$, tunjukkan bahwa $\sigma(\Delta) = \Delta$.

(f) Buktikan bahwa $G(E/F)$ isomorfik dengan suatu subgrup dari A_n jika dan hanya jika $\Delta \in F$.

(g) Tentukan grup Galois dari $x^3 + 2x - 4$ dan $x^3 + x - 3$.

23.6 Referensi dan Bacaan yang Disarankan

[1] Artin, E. *Theory: Lectures Delivered at the University of Notre Dame (Notre Dame Mathematical Lectures, Number 2).* Dover, Mineola, NY, 1997.

[2] Edwards, H. M. *Galois Theory.* Springer-Verlag, New York, 1984.

[3] Fraleigh, J. B. *A First Course in Abstract Algebra.* 7th ed. Pearson, Upper Saddle River, NJ, 2003.

[4] Gaal, L. *Classical Galois Theory with Examples.* American Mathematical Society, Providence, 1979.

[5] Garling, D. J. H. *A Course in Galois Theory.* Cambridge University Press, Cambridge, 1986.

[6] Kaplansky, I. *Fields and Rings.* 2nd ed. University of Chicago Press, Chicago, 1972.

[7] Rothman, T. "The Short Life of Évariste Galois," *Scientific American*, April 1982, 136–49.

A

GNU Free Documentation License

Version 1.3, 3 November 2008

Copyright © 2000, 2001, 2002, 2007, 2008 Free Software Foundation, Inc. <www.fsf.org>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE. The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS. This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or

authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

The "publisher" means any person or entity that distributes copies of the Document to the public.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers

may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING. You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY. If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS. You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You

may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties — for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS. You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS. You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS. A compilation of the Document or its derivatives with other separate and independent

documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION. Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION. You may not copy, modify, sublicense, or distribute the Document except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, or distribute it is void, and will automatically terminate your rights under this License.

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, receipt of a copy of some or all of the same material does not give you any rights to use it.

10. FUTURE REVISIONS OF THIS LICENSE. The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See www.gnu.org/copyleft.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or

any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation. If the Document specifies that a proxy can decide which future versions of this License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Document.

11. RELICENSING. "Massive Multiauthor Collaboration Site" (or "MMC Site") means any World Wide Web server that publishes copyrightable works and also provides prominent facilities for anybody to edit those works. A public wiki that anybody can edit is an example of such a server. A "Massive Multiauthor Collaboration" (or "MMC") contained in the site means any set of copyrightable works thus published on the MMC site.

"CC-BY-SA" means the Creative Commons Attribution-Share Alike 3.0 license published by Creative Commons Corporation, a not-for-profit corporation with a principal place of business in San Francisco, California, as well as future copyleft versions of that license published by that same organization.

"Incorporate" means to publish or republish a Document, in whole or in part, as part of another Document.

An MMC is "eligible for relicensing" if it is licensed under this License, and if all works that were first published under this License somewhere other than this MMC, and subsequently incorporated in whole or in part into the MMC, (1) had no cover texts or invariant sections, and (2) were thus incorporated prior to November 1, 2008.

The operator of an MMC Site may republish an MMC contained in the site under CC-BY-SA on the same site at any time before August 1, 2009, provided the MMC is eligible for relicensing.

ADDENDUM: How to use this License for your documents. To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
Copyright (C)  YEAR  YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.3
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with… Texts." line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

B

Petunjuk dan Jawaban untuk Latihan Terpilih

1 · Pendahuluan
1.4 · Latihan

1.4.1. Petunjuk. (a) $A \cap B = \{2\}$; (b) $B \cap C = \{5\}$.

1.4.2. Petunjuk. (a) $A \times B = \{(a,1),(a,2),(a,3),(b,1),(b,2),(b,3),(c,1),(c,2),(c,3)\}$; (d) $A \times D = \emptyset$.

1.4.6. Petunjuk. Perhatikan bahwa $x \in A \cup B$ jika dan hanya jika $x \in A$ atau $x \in B$. Secara ekuivalen, $x \in B$ atau $x \in A$, yang sama dengan $x \in B \cup A$. Oleh karena itu, $A \cup B = B \cup A$.

1.4.10. Petunjuk. $(A \cap B) \cup (A \setminus B) \cup (B \setminus A) = (A \cap B) \cup (A \cap B') \cup (B \cap A') = [A \cap (B \cup B')] \cup (B \cap A') = A \cup (B \cap A') = (A \cup B) \cap (A \cup A') = A \cup B$.

1.4.14. Petunjuk. $A \setminus (B \cup C) = A \cap (B \cup C)' = (A \cap A) \cap (B' \cap C') = (A \cap B') \cap (A \cap C') = (A \setminus B) \cap (A \setminus C)$.

1.4.17. Petunjuk. (a) Bukan pemetaan karena $f(2/3)$ tidak terdefinisi; (b) ini merupakan pemetaan; (c) bukan pemetaan, karena $f(1/2) = 3/4$ tetapi $f(2/4) = 3/8$; (d) ini merupakan pemetaan.

1.4.18. Petunjuk. (a) f injektif tetapi tidak surjektif. $f(\mathbb{R}) = \{x \in \mathbb{R} : x > 0\}$. (c) f tidak injektif maupun surjektif. $f(\mathbb{R}) = \{x : -1 \leq x \leq 1\}$.

1.4.20. Petunjuk. (a) $f(n) = n + 1$.

1.4.22. Petunjuk. (a) Misalkan $x, y \in A$. Maka $g(f(x)) = (g \circ f)(x) = (g \circ f)(y) = g(f(y))$. Jadi, $f(x) = f(y)$ dan $x = y$, sehingga $g \circ f$ injektif. (b) Misalkan $c \in C$, maka $c = (g \circ f)(x) = g(f(x))$ untuk suatu $x \in A$. Karena $f(x) \in B$, g surjektif.

1.4.23. Petunjuk. $f^{-1}(x) = (x+1)/(x-1)$.

1.4.24. Petunjuk. (a) Misalkan $y \in f(A_1 \cup A_2)$. Maka terdapat $x \in A_1 \cup A_2$ sedemikian sehingga $f(x) = y$. Jadi, $y \in f(A_1)$ atau $f(A_2)$. Oleh karena itu, $y \in f(A_1) \cup f(A_2)$. Akibatnya, $f(A_1 \cup A_2) \subset f(A_1) \cup f(A_2)$. Sebaliknya, jika $y \in f(A_1) \cup f(A_2)$, maka $y \in f(A_1)$ atau $f(A_2)$. Jadi, terdapat x dalam A_1 atau A_2 sedemikian sehingga $f(x) = y$. Dengan demikian, terdapat $x \in A_1 \cup A_2$ sedemikian sehingga $f(x) = y$. Oleh karena itu, $f(A_1) \cup f(A_2) \subset f(A_1 \cup A_2)$, dan $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

1.4.25. Petunjuk. (a) Relasi tersebut tidak simetris. (b) Relasi tersebut tidak refleksif, karena 0 tidak ekuivalen dengan dirinya sendiri. (c) Relasi tersebut tidak transitif.

1.4.28. Petunjuk. Misalkan $X = \mathbb{N} \cup \{\sqrt{2}\}$ dan definisikan $x \sim y$ jika $x + y \in \mathbb{N}$.

2 · Bilangan Bulat
2.4 · Latihan

2.4.1. Petunjuk. Kasus dasar, $S(1) : [1(1+1)(2(1)+1)]/6 = 1 = 1^2$, benar. Andaikan $S(k) : 1^2 + 2^2 + \cdots + k^2 = [k(k+1)(2k+1)]/6$ benar. Maka

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= [k(k+1)(2k+1)]/6 + (k+1)^2 \\ &= [(k+1)((k+1)+1)(2(k+1)+1)]/6, \end{aligned}$$

sehingga $S(k+1)$ benar. Jadi, $S(n)$ benar untuk setiap bilangan bulat positif n.

2.4.3. Petunjuk. Kasus dasar, $S(4) : 4! = 24 > 16 = 2^4$, benar. Andaikan $S(k) : k! > 2^k$ benar. Maka $(k+1)! = k!(k+1) > 2^k \cdot 2 = 2^{k+1}$, sehingga $S(k+1)$ benar. Jadi, $S(n)$ benar untuk setiap bilangan bulat positif n.

2.4.8. Petunjuk. Ikuti pembuktian dalam Contoh 2.1.4.

2.4.11. Petunjuk. Kasus dasar, $S(0) : (1+x)^0 - 1 = 0 \geq 0 = 0 \cdot x$, benar. Andaikan $S(k) : (1+x)^k - 1 \geq kx$ benar. Maka

$$\begin{aligned} (1+x)^{k+1} - 1 &= (1+x)(1+x)^k - 1 \\ &= (1+x)^k + x(1+x)^k - 1 \\ &\geq kx + x(1+x)^k \\ &\geq kx + x \\ &= (k+1)x, \end{aligned}$$

sehingga $S(k+1)$ benar. Oleh karena itu, $S(n)$ benar untuk setiap bilangan bulat positif n.

2.4.17. Bilangan Fibonacci.

Petunjuk. Untuk (a) dan (b), gunakan induksi matematis. (c) Tunjukkan bahwa $f_1 = 1$, $f_2 = 1$, dan $f_{n+2} = f_{n+1} + f_n$. (e) Gunakan bagian (b) dan Latihan 2.4.16.

2.4.19. Petunjuk. Gunakan Teorema Dasar Aritmetika.

2.4.23. Petunjuk. Gunakan Prinsip Urutan Baik dan algoritma pembagian.

2.4.27. Petunjuk. Karena $\gcd(a, b) = 1$, terdapat bilangan bulat r dan s sedemikian sehingga $ar + bs = 1$. Jadi, $acr + bcs = c$.

2.4.29. Petunjuk. Setiap bilangan prima harus berbentuk 2, 3, $6n + 1$, atau $6n + 5$. Misalkan hanya terdapat berhingga banyaknya bilangan prima berbentuk $6k + 5$.

3 · Grup
3.5 · Latihan

3.5.1. Petunjuk. (a) $3 + 7\mathbb{Z} = \{\ldots, -4, 3, 10, \ldots\}$; (c) $18 + 26\mathbb{Z}$; (e) $5 + 6\mathbb{Z}$.

3.5.2. Petunjuk. (a) Bukan grup; (c) grup.

3.5.6. Petunjuk.

·	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

3.5.8. Petunjuk. Pilih dua matriks. Hampir setiap pasangan akan memenuhi.

3.5.15. Petunjuk. Terdapat grup nonabelian yang memuat enam unsur.

3.5.16. Petunjuk. Perhatikan grup simetri segitiga sama sisi atau persegi.

3.5.17. Petunjuk. Terdapat lima grup berbeda yang berorde 8.

3.5.18. Petunjuk. Misalkan

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

berada dalam S_n. Semua a_i harus berbeda. Terdapat n cara memilih a_1, $n-1$ cara memilih a_2, ..., dua cara memilih a_{n-1}, dan hanya satu cara memilih a_n. Oleh karena itu, kita dapat membentuk σ dengan $n(n-1)\cdots 2\cdot 1 = n!$ cara.

3.5.25. Petunjuk.

$$\begin{aligned}(aba^{-1})^n &= (aba^{-1})(aba^{-1})\cdots(aba^{-1}) \\ &= ab(aa^{-1})b(aa^{-1})b\cdots b(aa^{-1})ba^{-1} \\ &= ab^n a^{-1}.\end{aligned}$$

3.5.31. Petunjuk. Karena $abab = (ab)^2 = e = a^2b^2 = aabb$, kita mengetahui bahwa $ba = ab$.

3.5.35. Petunjuk. $H_1 = \{\mathrm{id}\}$, $H_2 = \{\mathrm{id}, \rho_1, \rho_2\}$, $H_3 = \{\mathrm{id}, \mu_1\}$, $H_4 = \{\mathrm{id}, \mu_2\}$, $H_5 = \{\mathrm{id}, \mu_3\}$, S_3.

3.5.41. Petunjuk. Identitas dari G adalah $1 = 1 + 0\sqrt{2}$. Karena $(a + b\sqrt{2}\,)(c + d\sqrt{2}\,) = (ac + 2bd) + (ad + bc)\sqrt{2}$, G tertutup terhadap perkalian. Terakhir, $(a + b\sqrt{2}\,)^{-1} = a/(a^2 - 2b^2) - b\sqrt{2}/(a^2 - 2b^2)$.

3.5.46. Petunjuk. Perhatikan S_3.

3.5.49. Petunjuk. $ba = a^4b = a^3ab = ab$

4 · Grup Siklik

4.5 · Latihan

4.5.1. Petunjuk. (a) Salah; (c) salah; (e) benar.

4.5.2. Petunjuk. (a) 12; (c) tak hingga; (e) 10.

4.5.3. Petunjuk. (a) $7\mathbb{Z} = \{\ldots, -7, 0, 7, 14, \ldots\}$; (b) $\{0, 3, 6, 9, 12, 15, 18, 21\}$; (c) $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, $\{0, 2, 4, 6, 8, 10\}$; (g) $\{1, 3, 7, 9\}$; (j) $\{1, -1, i, -i\}$.

4.5.4. Petunjuk. (a)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(c)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

4.5.10. Petunjuk. (a) 0; (b) $1, -1$.

4.5.11. Petunjuk. $1, 2, 3, 4, 6, 8, 12, 24$.

4.5.15. Petunjuk. (a) $-3 + 3i$; (c) $43 - 18i$; (e) i

4.5.16. Petunjuk. (a) $\sqrt{3} + i$; (c) -3.

4.5.17. Petunjuk. (a) $\sqrt{2}\,\mathrm{cis}(7\pi/4)$; (c) $2\sqrt{2}\,\mathrm{cis}(\pi/4)$; (e) $3\,\mathrm{cis}(3\pi/2)$.

4.5.18. Petunjuk. (a) $(1 - i)/2$; (c) $16(i - \sqrt{3}\,)$; (e) $-1/4$.

4.5.22. Petunjuk. (a) 292; (c) 1523.

4.5.27. Petunjuk. $|\langle g\rangle \cap \langle h\rangle| = 1$.

4.5.31. Petunjuk. Elemen identitas dalam sebarang grup berorde hingga. Misalkan $g, h \in G$ masing-masing berorde m dan n. Karena $(g^{-1})^m = e$ dan $(gh)^{mn} = e$, elemen-elemen berorde hingga dalam G membentuk subgrup dari G.

4.5.37. Petunjuk. Jika g merupakan elemen yang berbeda dari identitas dalam G, g harus membangkitkan G; jika tidak, $\langle g\rangle$ merupakan subgrup sejati nontrivial dari G.

5 · Grup Permutasi

5.4 · Latihan

5.4.1. Petunjuk. (a) $(1\,2\,4\,5\,3)$; (c) $(1\,3)(2\,5)$.

5.4.2. Petunjuk. (a) $(1\,3\,5)(2\,4)$; (c) $(1\,4)(2\,3)$; (e) $(1\,3\,2\,4)$; (g) $(1\,3\,4)(2\,5)$; (n) $(1\,7\,3\,5\,2)$.

5.4.3. Petunjuk. (a) $(1\,6)(1\,5)(1\,3)(1\,4)$; (c) $(1\,6)(1\,4)(1\,2)$.

5.4.4. Petunjuk. $(a_1, a_2, \ldots, a_n)^{-1} = (a_1, a_n, a_{n-1}, \ldots, a_2)$

5.4.5. Petunjuk. (a) $\{(1\,3), (1\,3)(2\,4), (1\,3\,2), (1\,3\,4), (1\,3\,2\,4), (1\,3\,4\,2)\}$ bukan subgrup.

5.4.8. Petunjuk. $(1\,2\,3\,4\,5)(6\,7\,8)$.

5.4.11. Petunjuk. Permutasi berbentuk

$$(1), (a_1, a_2)(a_3, a_4), (a_1, a_2, a_3), (a_1, a_2, a_3, a_4, a_5)$$

mungkin terdapat dalam A_5.

5.4.17. Petunjuk. Hitung $(1\,2\,3)(1\,2)$ dan $(1\,2)(1\,2\,3)$.

5.4.25. Petunjuk. Perhatikan kasus $(a, b)(b, c)$ dan $(a, b)(c, d)$.

5.4.29. Petunjuk. Tunjukkan bahwa pusat D_n hanya terdiri atas identitas jika n ganjil, serta terdiri atas identitas dan rotasi $180°$ jika n genap.

5.4.30. Petunjuk. Untuk (a), tunjukkan bahwa $\sigma\tau\sigma^{-1}(\sigma(a_i)) = \sigma(a_{i+1})$.

6 · Koset dan Teorema Lagrange

6.5 · Latihan

6.5.1. Petunjuk. Orde g dan orde h keduanya harus membagi orde G.

6.5.2. Petunjuk. Orde yang mungkin harus membagi 60.

6.5.3. Petunjuk. Pernyataan ini benar untuk setiap subgrup sejati nontrivial.

6.5.4. Petunjuk. Salah.

6.5.5. Petunjuk. (a) $\langle 8\rangle$, $1 + \langle 8\rangle$, $2 + \langle 8\rangle$, $3 + \langle 8\rangle$, $4 + \langle 8\rangle$, $5 + \langle 8\rangle$, $6 + \langle 8\rangle$, dan $7 + \langle 8\rangle$; (c) $3\mathbb{Z}$, $1 + 3\mathbb{Z}$, dan $2 + 3\mathbb{Z}$.

6.5.7. Petunjuk. $4^{\phi(15)} \equiv 4^8 \equiv 1 \pmod{15}$.

6.5.12. Petunjuk. Misalkan $g_1 \in gH$. Tunjukkan bahwa $g_1 \in Hg$, sehingga $gH \subset Hg$.

6.5.19. Petunjuk. Tunjukkan bahwa $g(H \cap K) = gH \cap gK$.

6.5.22. Petunjuk. Jika $\gcd(m, n) = 1$, maka $\phi(mn) = \phi(m)\phi(n)$ (Latihan 2.4.26 dalam Bab 2).

7 · Pengantar Kriptografi
7.4 · Latihan

7.4.1. Petunjuk. `LAORYHAPDWK`

7.4.3. Petunjuk. Petunjuk: `V = E`, `E = X` (juga digunakan untuk spasi dan tanda baca), `K = R`.

7.4.4. Petunjuk. $26! - 1$

7.4.7. Petunjuk. (a) 2791; (c) 11213525032442.

7.4.9. Petunjuk. (a) 31 (c) 14.

7.4.10. Petunjuk. (a) $n = 11 \cdot 41$; (c) $n = 8779 \cdot 4327$.

8 · Teori Pengodean Aljabar
8.6 · Latihan

8.6.2. Petunjuk. Ini tidak dapat menjadi kode grup karena $(0000) \notin C$.

8.6.3. Petunjuk. (a) 2; (c) 2.

8.6.4. Petunjuk. (a) 3; (c) 4.

8.6.6. Petunjuk. (a) $d_{\min} = 2$; (c) $d_{\min} = 1$.

8.6.7. Petunjuk.

(a) $(00000), (00101), (10011), (10110)$

$$G = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$$

(b) $(000000), (010111), (101101), (111010)$

$$G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}$$

8.6.9. Petunjuk. Beberapa kesalahan terjadi dalam salah satu kata yang diterima.

8.6.11. Petunjuk. (a) Matriks pemeriksa paritas kanonik dengan matriks

pembangkit standar

$$G = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

(c) Matriks pemeriksa paritas kanonik dengan matriks pembangkit standar

$$G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

8.6.12. Petunjuk. (a) Semua sindrom yang mungkin muncul.

8.6.15. Petunjuk. (a) C, $(10000)+C$, $(01000)+C$, $(00100)+C$, $(00010)+C$, $(11000)+C$, $(01100)+C$, $(01010)+C$. Tabel pendekodean tidak ada untuk C karena kode ini hanya mendeteksi kesalahan tunggal.

8.6.19. Petunjuk. Misalkan $\mathbf{x} \in C$ berbobot ganjil dan definisikan suatu pemetaan dari himpunan kata kode berbobot ganjil ke himpunan kata kode berbobot genap dengan $\mathbf{y} \mapsto \mathbf{x}+\mathbf{y}$. Tunjukkan bahwa pemetaan ini merupakan bijeksi.

8.6.23. Petunjuk. Untuk 20 posisi informasi, diperlukan sekurang-kurangnya 6 bit pemeriksa untuk menjamin diperolehnya kode pengoreksi kesalahan.

9 · Isomorfisma

9.4 · Latihan

9.4.1. Petunjuk. Setiap grup siklik tak hingga isomorfik dengan $\mathbb{Z}$ berdasarkan Teorema 9.1.7.

9.4.2. Petunjuk. Definisikan $\phi : \mathbb{C}^* \to GL_2(\mathbb{R})$ dengan

$$\phi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

9.4.3. Petunjuk. Salah.

9.4.6. Petunjuk. Definisikan pemetaan dari $\mathbb{Z}_n$ ke akar-akar kesatuan ke-n dengan $k \mapsto \text{cis}(2k\pi/n)$.

9.4.8. Petunjuk. Andaikan $\mathbb{Q}$ siklik dan cobalah mencari pembangkitnya.

9.4.11. Petunjuk. Terdapat dua grup nonabelian dan tiga grup abelian yang saling takisomorfik.

9.4.16. Petunjuk. (a) 12; (c) 5.

9.4.19. Petunjuk. Gambarlah diagramnya.

9.4.20. Petunjuk. Benar.

9.4.25. Petunjuk. Benar.

9.4.27. Petunjuk. Misalkan a suatu pembangkit dari G. Jika $\phi : G \to H$ adalah isomorfisma, tunjukkan bahwa $\phi(a)$ merupakan pembangkit dari H.

9.4.38. Petunjuk. Setiap automorfisme dari $\mathbb{Z}_6$ harus memetakan 1 ke pembangkit lain dari $\mathbb{Z}_6$.

9.4.45. Petunjuk. Untuk menunjukkan bahwa ϕ injektif, misalkan $g_1 = h_1k_1$ dan $g_2 = h_2k_2$, lalu tinjau $\phi(g_1) = \phi(g_2)$.

10 · Subgrup Normal dan Grup Hasil Bagi
10.4 · Latihan

10.4.1. Petunjuk. (a)

	A_4	$(1\,2)A_4$
A_4	A_4	$(1\,2)A_4$
$(1\,2)A_4$	$(1\,2)A_4$	A_4

(c) D_4 tidak normal dalam S_4.

10.4.8. Petunjuk. Jika $a \in G$ merupakan pembangkit G, maka aH merupakan pembangkit G/H.

10.4.11. Petunjuk. Untuk setiap $g \in G$, tunjukkan bahwa pemetaan $i_g : G \to G$ yang didefinisikan oleh $i_g : x \mapsto gxg^{-1}$ merupakan isomorfisma dari G ke dirinya sendiri. Kemudian perhatikan $i_g(H)$.

10.4.12. Petunjuk. Andaikan $\langle g \rangle$ normal dalam G dan misalkan y suatu elemen sembarang dari G. Jika $x \in C(g)$, kita harus menunjukkan bahwa yxy^{-1} juga berada dalam $C(g)$. Tunjukkan bahwa $(yxy^{-1})g = g(yxy^{-1})$.

10.4.14. Petunjuk. (a) Misalkan $g \in G$ dan $h \in G'$. Jika $h = aba^{-1}b^{-1}$, maka

$$\begin{aligned} ghg^{-1} &= gaba^{-1}b^{-1}g^{-1} \\ &= (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \\ &= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}. \end{aligned}$$

Kita juga perlu menunjukkan bahwa jika $h = h_1 \cdots h_n$ dengan $h_i = a_i b_i a_i^{-1} b_i^{-1}$, maka ghg^{-1} merupakan hasil kali elemen-elemen berjenis sama. Namun, $ghg^{-1} = gh_1 \cdots h_n g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) \cdots (gh_ng^{-1})$.

11 · Homomorfisma
11.4 · Latihan

11.4.2. Petunjuk. (a) merupakan homomorfisma dengan kernel $\{1\}$; (c) bukan homomorfisma.

11.4.4. Petunjuk. Karena $\phi(m+n) = 7(m+n) = 7m + 7n = \phi(m) + \phi(n)$, ϕ merupakan homomorfisma.

11.4.5. Petunjuk. Untuk setiap homomorfisma $\phi : \mathbb{Z}_{24} \to \mathbb{Z}_{18}$, kernel ϕ harus merupakan subgrup dari $\mathbb{Z}_{24}$ dan citra ϕ harus merupakan subgrup dari $\mathbb{Z}_{18}$. Sekarang gunakan fakta bahwa suatu pembangkit harus dipetakan ke pembangkit.

11.4.9. Petunjuk. Misalkan $a, b \in G$. Maka $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$.

11.4.17. Petunjuk. Carilah contoh penyangkal.

12 · Grup Matriks dan Simetri
12.4 · Latihan

12.4.1. Petunjuk.

$$\begin{aligned} \frac{1}{2}\left[\|\mathbf{x}+\mathbf{y}\|^2 + \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2\right] &= \frac{1}{2}\left[\langle x+y, x+y\rangle - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2\right] \\ &= \frac{1}{2}\left[\|\mathbf{x}\|^2 + 2\langle x, y\rangle + \|\mathbf{y}\|^2 - \|\mathbf{x}\|^2 - \|\mathbf{y}\|^2\right] \\ &= \langle \mathbf{x}, \mathbf{y}\rangle. \end{aligned}$$

12.4.3. Petunjuk. (a) berada dalam $SO(2)$; (c) tidak berada dalam $O(3)$.

12.4.5. Petunjuk. (a) $\langle \mathbf{x}, \mathbf{y} \rangle = \langle \mathbf{y}, \mathbf{x} \rangle$.

12.4.7. Petunjuk. Gunakan matriks unimodular

$$\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}.$$

12.4.10. Petunjuk. Tunjukkan bahwa kernel pemetaan $\det : O(n) \to \mathbb{R}^*$ adalah $SO(n)$.

12.4.13. Petunjuk. Benar.

12.4.17. Petunjuk. $p6m$

13 · Struktur Grup

13.4 · Latihan

13.4.1. Petunjuk. Terdapat tiga grup yang mungkin.

13.4.4. Petunjuk. (a) $\{0\} \subset \langle 6 \rangle \subset \langle 3 \rangle \subset \mathbb{Z}_{12}$; (e) $\{(1)\} \times \{0\} \subset \{(1), (1\,2\,3), (1\,3\,2)\} \times \{0\} \subset S_3 \times \{0\} \subset S_3 \times \langle 2 \rangle \subset S_3 \times \mathbb{Z}_4$.

13.4.7. Petunjuk. Gunakan Teorema Dasar Grup Abelian yang Dibangkitkan secara Hingga.

13.4.12. Petunjuk. Jika N dan G/N solvabel, maka keduanya memiliki deret solvabel

$$N = N_n \supset N_{n-1} \supset \cdots \supset N_1 \supset N_0 = \{e\}$$
$$G/N = G_n/N \supset G_{n-1}/N \supset \cdots G_1/N \supset G_0/N = \{N\}.$$

13.4.16. Petunjuk. Gunakan fakta bahwa D_n memiliki subgrup siklik berindeks 2.

13.4.21. Petunjuk. G/G' abelian.

14 · Aksi Grup

14.5 · Latihan

14.5.1. Petunjuk. Contoh 14.1.1: 0, $\mathbb{R}^2 \setminus \{0\}$. Contoh 14.1.2: $X = \{1, 2, 3, 4\}$.

14.5.2. Petunjuk. (a) $X_{(1)} = \{1, 2, 3\}$, $X_{(1\,2)} = \{3\}$, $X_{(1\,3)} = \{2\}$, $X_{(2\,3)} = \{1\}$, $X_{(1\,2\,3)} = X_{(1\,3\,2)} = \emptyset$. $G_1 = \{(1), (2\,3)\}$, $G_2 = \{(1), (1\,3)\}$, $G_3 = \{(1), (1\,2)\}$.

14.5.3. Petunjuk. (a) $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1, 2, 3\}$.

14.5.6. Petunjuk. Kelas-kelas konjugasi untuk S_4 adalah

$$\mathcal{O}_{(1)} = \{(1)\},$$
$$\mathcal{O}_{(12)} = \{(1\,2), (1\,3), (1\,4), (2\,3), (2\,4), (3\,4)\},$$
$$\mathcal{O}_{(1\,2)(3\,4)} = \{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\},$$
$$\mathcal{O}_{(123)} = \{(1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3)\},$$
$$\mathcal{O}_{(1234)} = \{(1\,2\,3\,4), (1\,2\,4\,3), (1\,3\,2\,4), (1\,3\,4\,2), (1\,4\,2\,3), (1\,4\,3\,2)\}.$$

Persamaan kelasnya adalah $1 + 3 + 6 + 6 + 8 = 24$.

14.5.8. Petunjuk. $(3^4 + 3^1 + 3^2 + 3^1 + 3^2 + 3^2 + 3^3 + 3^3)/8 = 21$.

14.5.11. Petunjuk. Grup gerak kaku kubus dapat dideskripsikan oleh permutasi yang diizinkan pada keenam permukaannya dan isomorfik dengan S_4. Terdapat siklus identitas, 6 permutasi berstruktur $(abcd)$ yang bersesuaian de-

ngan putaran seperempat, 3 permutasi berstruktur $(ab)(cd)$ yang bersesuaian dengan putaran setengah, 6 permutasi berstruktur $(ab)(cd)(ef)$ yang bersesuaian dengan rotasi kubus terhadap pusat sisi-sisi yang berhadapan, dan 8 permutasi berstruktur $(abc)(def)$ yang bersesuaian dengan rotasi kubus terhadap titik-titik sudut yang berhadapan.

14.5.15. Petunjuk. $(1 \cdot 2^6 + 3 \cdot 2^4 + 4 \cdot 2^3 + 2 \cdot 2^2 + 2 \cdot 2^1)/12 = 13$.

14.5.17. Petunjuk. $(1 \cdot 2^8 + 3 \cdot 2^6 + 2 \cdot 2^4)/6 = 80$.

14.5.22. Petunjuk. Gunakan fakta bahwa $x \in gC(a)g^{-1}$ jika dan hanya jika $g^{-1}xg \in C(a)$.

15 · Teorema Sylow
15.4 · Latihan

15.4.1. Petunjuk. Jika $|G| = 18 = 2 \cdot 3^2$, maka orde subgrup Sylow-2 adalah 2, dan orde subgrup Sylow-3 adalah 9.

15.4.2. Petunjuk. Keempat subgrup Sylow-3 dari S_4 adalah $P_1 = \{(1), (1\,2\,3), (1\,3\,2)\}$, $P_2 = \{(1), (1\,2\,4), (1\,4\,2)\}$, $P_3 = \{(1), (1\,3\,4), (1\,4\,3)\}$, $P_4 = \{(1), (2\,3\,4), (2\,4\,3)\}$.

15.4.5. Petunjuk. Karena $|G| = 96 = 2^5 \cdot 3$, menurut Teorema Sylow Ketiga, G memiliki satu atau tiga subgrup Sylow-2. Jika hanya ada satu subgrup, pembuktian selesai. Jika terdapat tiga subgrup Sylow-2, misalkan H dan K dua di antaranya. Maka $|H \cap K| \geq 16$; jika tidak, HK akan memiliki $(32 \cdot 32)/8 = 128$ elemen, yang mustahil. Jadi, $H \cap K$ normal di H maupun K karena berindeks 2 dalam kedua grup.

15.4.8. Petunjuk. Tunjukkan bahwa G memiliki subgrup Sylow-p normal berorde p^2 dan subgrup Sylow-q normal berorde q^2.

15.4.10. Petunjuk. Salah.

15.4.17. Petunjuk. Jika G abelian, maka G siklik, karena $|G| = 3 \cdot 5 \cdot 17$. Sekarang perhatikan Contoh 15.2.6.

15.4.23. Petunjuk. Definisikan pemetaan antara koset-koset kanan dari $N(H)$ di G dan konjugat-konjugat dari H di G melalui $N(H)g \mapsto g^{-1}Hg$. Buktikan bahwa pemetaan ini bijektif.

15.4.26. Petunjuk. Misalkan $aG', bG' \in G/G'$. Maka $(aG')(bG') = abG' = ab(b^{-1}a^{-1}ba)G' = (abb^{-1}a^{-1})baG' = baG'$.

16 · Gelanggang
16.7 · Latihan

16.7.1. Petunjuk. (a) $7\mathbb{Z}$ merupakan gelanggang tetapi bukan lapangan; (c) $\mathbb{Q}(\sqrt{2}\,)$ merupakan lapangan; (f) R bukan gelanggang.

16.7.3. Petunjuk. (a) $\{1, 3, 7, 9\}$; (c) $\{1, 2, 3, 4, 5, 6\}$; (e)

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \right\}.$$

16.7.4. Petunjuk. (a) $\{0\}$, $\{0, 9\}$, $\{0, 6, 12\}$, $\{0, 3, 6, 9, 12, 15\}$, $\{0, 2, 4, 6, 8, 10, 12, 14, 16\}$; (c) tidak ada ideal taktrivial.

16.7.7. Petunjuk. Andaikan terdapat isomorfisma $\phi : \mathbb{C} \to \mathbb{R}$ dengan $\phi(i) = a$.

16.7.8. Petunjuk. Salah. Andaikan terdapat isomorfisma $\phi : \mathbb{Q}(\sqrt{2}\,) \to \mathbb{Q}(\sqrt{3}\,)$ sedemikian sehingga $\phi(\sqrt{2}\,) = a$.

16.7.13. Petunjuk. (a) $x \equiv 17 \pmod{55}$; (c) $x \equiv 214 \pmod{2772}$.

16.7.16. Petunjuk. Jika $I \neq \{0\}$, tunjukkan bahwa $1 \in I$.

16.7.18. Petunjuk. (a) $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$.

16.7.26. Petunjuk. Misalkan $a \in R$ dengan $a \neq 0$. Maka ideal utama yang dibangun oleh a adalah R. Jadi, terdapat $b \in R$ sedemikian sehingga $ab = 1$.

16.7.28. Petunjuk. Hitung $(a+b)^2$ dan $(-ab)^2$.

16.7.33. Petunjuk. Misalkan $a/b, c/d \in \mathbb{Z}_{(p)}$. Maka $a/b+c/d = (ad+bc)/bd$ dan $(a/b)\cdot(c/d) = (ac)/(bd)$ keduanya berada dalam $\mathbb{Z}_{(p)}$, karena $\gcd(bd, p) = 1$.

16.7.37. Petunjuk. Misalkan $x^2 = x$ dan $x \neq 0$. Karena R merupakan daerah integral, $x = 1$. Untuk menemukan idempoten taktrivial, carilah dalam $\mathbb{M}_2(\mathbb{R})$.

17 · Polinomial

17.5 · Latihan

17.5.2. Petunjuk. (a) $9x^2 + 2x + 5$; (b) $8x^4 + 7x^3 + 2x^2 + 7x$.

17.5.3. Petunjuk. (a) $5x^3 + 6x^2 - 3x + 4 = (5x^2 + 2x + 1)(x - 2) + 6$; (c) $4x^5 - x^3 + x^2 + 4 = (4x^2 + 4)(x^3 + 3) + 4x^2 + 2$.

17.5.5. Petunjuk. (a) Tidak ada nol di $\mathbb{Z}_{12}$; (c) 3, 4.

17.5.7. Petunjuk. Tinjau $(2x + 1)$.

17.5.8. Petunjuk. (a) Tereduksi; (c) tak tereduksi.

17.5.10. Petunjuk. Salah satu faktorisasinya adalah $x^2+x+8 = (x+2)(x+9)$.

17.5.13. Petunjuk. Bilangan bulat $\mathbb{Z}$ tidak membentuk lapangan.

17.5.14. Petunjuk. Salah.

17.5.16. Petunjuk. Misalkan $\phi : R \to S$ suatu isomorfisma. Definisikan $\overline{\phi} : R[x] \to S[x]$ dengan $\overline{\phi}(a_0+a_1x+\cdots+a_nx^n) = \phi(a_0)+\phi(a_1)x+\cdots+\phi(a_n)x^n$.

17.5.20. Polinomial Siklotomik.

Petunjuk. Polinomial

$$\Phi_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1$$

disebut **polinomial siklotomik.** Tunjukkan bahwa $\Phi_p(x)$ tak tereduksi atas $\mathbb{Q}$ untuk setiap bilangan prima p.

17.5.26. Petunjuk. Tentukan ideal sejati taktrivial di $F[x]$.

18 · Daerah Integral

18.4 · Latihan

18.4.1. Petunjuk. Perhatikan bahwa $z^{-1} = 1/(a+b\sqrt{3}\,i) = (a-b\sqrt{3}\,i)/(a^2+3b^2)$ berada dalam $\mathbb{Z}[\sqrt{3}\,i]$ jika dan hanya jika $a^2+3b^2 = 1$. Satu-satunya solusi bilangan bulat untuk persamaan tersebut adalah $a = \pm 1, b = 0$.

18.4.2. Petunjuk. (a) $5 = -i(1+2i)(2+i)$; (c) $6+8i = -i(1+i)^2(2+i)^2$.

18.4.4. Petunjuk. Benar.

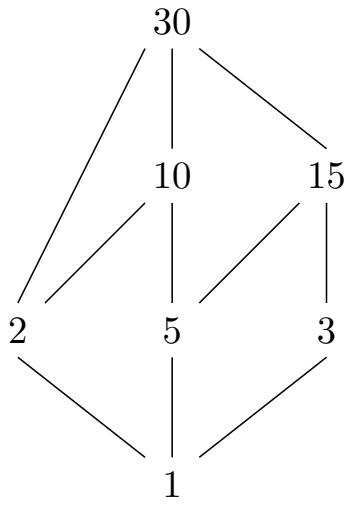
18.4.9. Petunjuk. Misalkan $z = a + bi$ dan $w = c + di \neq 0$ berada dalam $\mathbb{Z}[i]$. Buktikan bahwa $z/w \in \mathbb{Q}(i)$.

18.4.15. Petunjuk. Misalkan $a = ub$ dengan u suatu unit. Maka $\nu(b) \leq \nu(ub) \leq \nu(a)$. Demikian pula, $\nu(a) \leq \nu(b)$.

18.4.16. Petunjuk. Tunjukkan bahwa 21 dapat difaktorkan dengan dua cara berbeda.

19 · Latis dan Aljabar Boolean
19.5 · Latihan

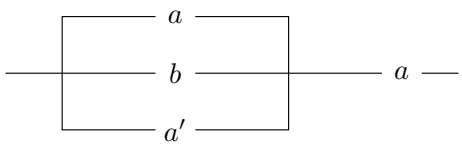
19.5.2. Petunjuk.



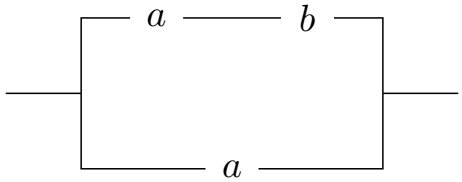
19.5.4. Petunjuk. Apa saja atom dari B?

19.5.5. Petunjuk. Salah.

19.5.6. Petunjuk. (a) $(a \vee b \vee a') \wedge a$



(c) $a \vee (a \wedge b)$



19.5.8. Petunjuk. Tidak ekuivalen.

19.5.10. Petunjuk. (a) $a' \wedge [(a \wedge b') \vee b] = a \wedge (a \vee b)$.

19.5.14. Petunjuk. Misalkan I, J merupakan ideal dalam R. Kita perlu menunjukkan bahwa $I + J = \{r + s : r \in I \text{ dan } s \in J\}$ merupakan ideal terkecil dalam R yang memuat I dan J. Jika $r_1, r_2 \in I$ dan $s_1, s_2 \in J$, maka $(r_1 + s_1) + (r_2 + s_2) = (r_1 + r_2) + (s_1 + s_2)$ berada dalam $I + J$. Untuk $a \in R$, $a(r_1 + s_1) = ar_1 + as_1 \in I + J$; dengan demikian, $I + J$ merupakan ideal dalam R.

19.5.18. Petunjuk. (a) Tidak.

19.5.20. Petunjuk. ($\Rightarrow$). $a = b \Rightarrow (a \wedge b') \vee (a' \wedge b) = (a \wedge a') \vee (a' \wedge a) = O \vee O = O$. ($\Leftarrow$). $(a \wedge b') \vee (a' \wedge b) = O \Rightarrow a \vee b = (a \vee a) \vee b = a \vee (a \vee b) = a \vee [I \wedge (a \vee b)] = a \vee [(a \vee a') \wedge (a \vee b)] = [a \vee (a \wedge b')] \vee [a \vee (a' \wedge b)] = a \vee [(a \wedge b') \vee (a' \wedge b)] = a \vee 0 = a$. Argumen yang simetris menunjukkan bahwa

$a \vee b = b$.

20 · Ruang Vektor
20.5 · Latihan

20.5.3. Petunjuk. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ memiliki basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ atas $\mathbb{Q}$.

20.5.5. Petunjuk. Himpunan $\{1, x, x^2, \ldots, x^{n-1}\}$ merupakan basis bagi P_n.

20.5.7. Petunjuk. (a) Subruang berdimensi 2 dengan basis $\{(1, 0, -3), (0, 1, 2)\}$; (d) bukan subruang

20.5.10. Petunjuk. Karena $0 = \alpha 0 = \alpha(-v + v) = \alpha(-v) + \alpha v$, diperoleh $-\alpha v = \alpha(-v)$.

20.5.12. Petunjuk. Misalkan $v_0 = 0, v_1, \ldots, v_n \in V$ dan $\alpha_0 \neq 0, \alpha_1, \ldots, \alpha_n \in F$. Maka $\alpha_0 v_0 + \cdots + \alpha_n v_n = 0$.

20.5.15. Transformasi Linear.

Petunjuk. (a) Misalkan $u, v \in \ker(T)$ dan $\alpha \in F$. Maka

$$T(u + v) = T(u) + T(v) = 0$$
$$T(\alpha v) = \alpha T(v) = \alpha 0 = 0.$$

Oleh karena itu, $u + v, \alpha v \in \ker(T)$, dan $\ker(T)$ merupakan subruang dari V.

(c) Pernyataan $T(u) = T(v)$ ekuivalen dengan $T(u - v) = T(u) - T(v) = 0$, yang benar jika dan hanya jika $u - v = 0$ atau $u = v$.

20.5.17. Jumlah Langsung.

Petunjuk. (a) Misalkan $u, u' \in U$ dan $v, v' \in V$. Maka

$$(u + v) + (u' + v') = (u + u') + (v + v') \in U + V$$
$$\alpha(u + v) = \alpha u + \alpha v \in U + V.$$

21 · Lapangan
21.5 · Latihan

21.5.1. Petunjuk. (a) $x^4 - (2/3)x^2 - 62/9$; (c) $x^4 - 2x^2 + 25$.

21.5.2. Petunjuk. (a) $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$; (c) $\{1, i, \sqrt{2}, \sqrt{2}\, i\}$; (e) $\{1, 2^{1/6}, 2^{1/3}, 2^{1/2}, 2^{2/3}, 2^{5/6}\}$.

21.5.3. Petunjuk. (a) $\mathbb{Q}(\sqrt{3}, \sqrt{7})$.

21.5.5. Petunjuk. Gunakan fakta bahwa elemen-elemen $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ adalah 0, 1, α, $1 + \alpha$, α^2, $1 + \alpha^2$, $\alpha + \alpha^2$, $1 + \alpha + \alpha^2$ serta fakta bahwa $\alpha^3 + \alpha + 1 = 0$.

21.5.8. Petunjuk. Tidak.

21.5.14. Petunjuk. Misalkan E aljabar atas F dan K aljabar atas E. Misalkan $\alpha \in K$. Cukup ditunjukkan bahwa α aljabar atas suatu perluasan hingga dari F. Karena α aljabar atas E, elemen tersebut harus merupakan nol dari suatu polinomial $p(x) = \beta_0 + \beta_1 x + \cdots + \beta_n x^n$ di $E[x]$. Jadi, α aljabar atas $F(\beta_0, \ldots, \beta_n)$.

21.5.22. Petunjuk. Karena $\{1, \sqrt{3}, \sqrt{7}, \sqrt{21}\}$ merupakan basis untuk $\mathbb{Q}(\sqrt{3}, \sqrt{7})$ atas $\mathbb{Q}$, $\mathbb{Q}(\sqrt{3}, \sqrt{7}) \supset \mathbb{Q}(\sqrt{3} + \sqrt{7})$. Karena $[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}] = 4$, $[\mathbb{Q}(\sqrt{3} + \sqrt{7}) : \mathbb{Q}] = 2$ atau 4. Karena derajat polinomial minimal dari $\sqrt{3} + \sqrt{7}$ adalah 4, $\mathbb{Q}(\sqrt{3}, \sqrt{7}) = \mathbb{Q}(\sqrt{3} + \sqrt{7})$.

21.5.27. Petunjuk. Misalkan $\beta \in F(\alpha)$ tidak berada di F. Maka $\beta = p(\alpha)/q(\alpha)$, dengan p dan q polinomial dalam α yang memiliki $q(\alpha) \neq 0$ dan koefisien di F. Jika β aljabar atas F, maka terdapat polinomial $f(x) \in F[x]$

sedemikian sehingga $f(\beta) = 0$. Misalkan $f(x) = a_0 + a_1x + \cdots + a_nx^n$. Maka

$$0 = f(\beta) = f\left(\frac{p(\alpha)}{q(\alpha)}\right) = a_0 + a_1\left(\frac{p(\alpha)}{q(\alpha)}\right) + \cdots + a_n\left(\frac{p(\alpha)}{q(\alpha)}\right)^n.$$

Sekarang kalikan kedua ruas dengan $q(\alpha)^n$ untuk menunjukkan bahwa terdapat polinomial di $F[x]$ yang memiliki α sebagai nol.

21.5.28. Petunjuk. Lihat penjelasan setelah Teorema 21.1.13.

22 · Lapangan Hingga
22.4 · Latihan

22.4.1. Petunjuk. Pastikan bahwa yang ditinjau merupakan perluasan lapangan.

22.4.4. Petunjuk. Terdapat delapan elemen dalam $\mathbb{Z}_2(\alpha)$. Tunjukkan dua akar lain dari $x^3 + x^2 + 1$ selain α di antara kedelapan elemen tersebut.

22.4.5. Petunjuk. Temukan polinomial tak tereduksi $p(x)$ dalam $\mathbb{Z}_3[x]$ yang berderajat 3 dan tunjukkan bahwa $\mathbb{Z}_3[x]/\langle p(x)\rangle$ mempunyai 27 elemen.

22.4.7. Petunjuk. (a) $x^5 - 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$; (c) $x^9 - 1 = (x + 1)(x^2 + x + 1)(x^6 + x^3 + 1)$.

22.4.8. Petunjuk. Benar.

22.4.11. Petunjuk. (a) Gunakan fakta bahwa $x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

22.4.12. Petunjuk. Salah.

22.4.17. Petunjuk. Jika $p(x) \in F[x]$, maka $p(x) \in E[x]$.

22.4.18. Petunjuk. Karena α aljabar atas F dan berderajat n, kita dapat menulis sebarang elemen $\beta \in F(\alpha)$ secara tunggal sebagai $\beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ dengan $a_i \in F$. Terdapat q^n tupel-n yang mungkin, yaitu $(a_0, a_1, \ldots, a_{n-1})$.

22.4.24. Teorema Wilson.

Petunjuk. Faktorkan $x^{p-1} - 1$ di atas $\mathbb{Z}_p$.

23 · Teori Galois
23.5 · Latihan

23.5.1. Petunjuk. (a) $\mathbb{Z}_2$; (c) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

23.5.2. Petunjuk. (a) Separabel atas $\mathbb{Q}$ karena $x^3+2x^2-x-2 = (x-1)(x+1)(x+2)$; (c) tidak separabel atas $\mathbb{Z}_3$ karena $x^4 + x^2 + 1 = (x + 1)^2(x + 2)^2$.

23.5.3. Petunjuk. Jika

$$[\mathrm{GF}(729) : \mathrm{GF}(9)] = [\mathrm{GF}(729) : \mathrm{GF}(3)]/[\mathrm{GF}(9) : \mathrm{GF}(3)] = 6/2 = 3,$$

maka $G(\mathrm{GF}(729)/\mathrm{GF}(9)) \cong \mathbb{Z}_3$. Suatu pembangkit untuk $G(\mathrm{GF}(729)/\mathrm{GF}(9))$ adalah σ, dengan $\sigma_{3^6}(\alpha) = \alpha^{3^6} = \alpha^{729}$ untuk $\alpha \in \mathrm{GF}(729)$.

23.5.4. Petunjuk. (a) S_5; (c) S_3; (g) lihat Contoh 23.1.11.

23.5.5. Petunjuk. (a) $\mathbb{Q}(i)$

23.5.7. Petunjuk. Misalkan E lapangan pemisah dari suatu polinomial kubik dalam $F[x]$. Tunjukkan bahwa $[E : F]$ kurang dari atau sama dengan 6 dan habis dibagi 3. Karena $G(E/F)$ merupakan subgrup dari S_3 yang ordenya habis dibagi 3, simpulkan bahwa grup ini harus isomorfik dengan $\mathbb{Z}_3$ atau S_3.

23.5.9. Petunjuk. G merupakan subgrup dari S_n.

23.5.16. Petunjuk. Benar.

23.5.20. Petunjuk.

(a) Jelas bahwa $\omega, \omega^2, \ldots, \omega^{p-1}$ berbeda karena $\omega \neq 1$ atau 0. Untuk menunjukkan bahwa ω^i merupakan akar dari Φ_p, hitung $\Phi_p(\omega^i)$.

(b) Konjugat-konjugat dari ω adalah $\omega, \omega^2, \ldots, \omega^{p-1}$. Definisikan suatu pemetaan $\phi_i : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega^i)$ dengan

$$\phi_i(a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}) = a_0 + a_1\omega^i + \cdots + c_{p-2}(\omega^i)^{p-2},$$

dengan $a_i \in \mathbb{Q}$. Buktikan bahwa ϕ_i merupakan isomorfisma lapangan. Tunjukkan bahwa ϕ_2 membangkitkan $G(\mathbb{Q}(\omega)/\mathbb{Q})$.

(c) Tunjukkan bahwa $\{\omega, \omega^2, \ldots, \omega^{p-1}\}$ merupakan basis untuk $\mathbb{Q}(\omega)$ atas $\mathbb{Q}$, dan tinjau kombinasi linear mana dari $\omega, \omega^2, \ldots, \omega^{p-1}$ yang ditetapkan oleh semua elemen dari $G(\mathbb{Q}(\omega)/\mathbb{Q})$.

C

Notasi

Tabel berikut mendefinisikan notasi yang digunakan dalam buku ini. Nomor halaman atau referensi merujuk pada kemunculan pertama setiap simbol.

Simbol	Deskripsi	Halaman
$a \in A$	a berada dalam himpunan A	4
$\mathbb{N}$	bilangan asli	4
$\mathbb{Z}$	bilangan bulat	4
$\mathbb{Q}$	bilangan rasional	4
$\mathbb{R}$	bilangan real	4
$\mathbb{C}$	bilangan kompleks	4
$A \subset B$	A merupakan himpunan bagian dari B	4
$\emptyset$	himpunan kosong	4
$A \cup B$	gabungan himpunan A dan B	5
$A \cap B$	irisan himpunan A dan B	5
A'	komplemen himpunan A	5
$A \setminus B$	selisih himpunan A dan B	5
$A \times B$	hasil kali Kartesius himpunan A dan B	7
A^n	$A \times \cdots \times A$ (sebanyak n kali)	7
id	pemetaan identitas	11
f^{-1}	invers fungsi f	11
$a \equiv b \pmod{n}$	a kongruen dengan b modulo n	14
$n!$	faktorial n	20
$\binom{n}{k}$	koefisien binomial $n!/(k!(n-k)!)$	20
$a \mid b$	a membagi b	23
$\gcd(a, b)$	faktor persekutuan terbesar dari a dan b	23
$\mathcal{P}(X)$	himpunan kuasa dari X	27
$\operatorname{lcm}(m, n)$	kelipatan persekutuan terkecil dari m dan n	29
$\mathbb{Z}_n$	bilangan bulat modulo n	31
$U(n)$	grup satuan dalam $\mathbb{Z}_n$	38
$\mathbb{M}_n(\mathbb{R})$	matriks $n \times n$ dengan entri dalam $\mathbb{R}$	38
$\det A$	determinan dari A	38
$GL_n(\mathbb{R})$	grup linear umum	38
Q_8	grup kuaternion	39
$\mathbb{C}^*$	grup perkalian bilangan kompleks	39

(Bersambung pada halaman berikutnya)

Simbol	Deskripsi	Halaman
$\|G\|$	orde suatu grup	39
$\mathbb{R}^*$	grup perkalian bilangan real	41
$\mathbb{Q}^*$	grup perkalian bilangan rasional	41
$SL_n(\mathbb{R})$	grup linear khusus	42
$Z(G)$	pusat suatu grup	47
$\langle a \rangle$	grup siklik yang dibangkitkan oleh a	51
$\|a\|$	orde suatu elemen a	52
$\operatorname{cis}\theta$	$\cos\theta + i\sin\theta$	56
$\mathbb{T}$	grup lingkaran	57
S_n	grup simetris pada n huruf	66
$(a_1, a_2, \ldots, a_k)$	siklus dengan panjang k	68
A_n	grup alternasi pada n huruf	72
D_n	grup dihedral	73
$[G : H]$	indeks suatu subgrup H dalam grup G	83
$\mathcal{L}_H$	himpunan koset kiri dari suatu subgrup H dalam grup G	84
$\mathcal{R}_H$	himpunan koset kanan dari suatu subgrup H dalam grup G	84
$a \nmid b$	a tidak membagi b	86
$d(\mathbf{x}, \mathbf{y})$	jarak Hamming antara $\mathbf{x}$ dan $\mathbf{y}$	106
$d_{\min}$	jarak minimum suatu kode	106
$w(\mathbf{x})$	bobot dari $\mathbf{x}$	106
$\mathbb{M}_{m\times n}(\mathbf{Z}_2)$	himpunan matriks $m \times n$ dengan entri dalam $\mathbb{Z}_2$	111
$\operatorname{Null}(H)$	ruang nol matriks H	111
δ_{ij}	delta Kronecker	114
$G \cong H$	G isomorfik dengan grup H	127
$\operatorname{Aut}(G)$	grup automorfisme dari suatu grup G	137
i_g	$i_g(x) = gxg^{-1}$	138
$\operatorname{Inn}(G)$	grup automorfisme dalam dari suatu grup G	138
ρ_g	representasi reguler kanan	138
G/N	grup hasil bagi G modulo N	141
G'	subgrup komutator dari G	147
$\ker\phi$	kernel dari ϕ	151
(a_{ij})	matriks	159
$O(n)$	grup ortogonal	161
$\|\mathbf{x}\|$	panjang vektor $\mathbf{x}$	162
$SO(n)$	grup ortogonal khusus	164
$E(n)$	grup Euklides	165
$\mathcal{O}_x$	orbit dari x	187
X_g	himpunan titik tetap dari g	188
G_x	subgrup isotropi dari x	188
$N(H)$	penormal subgrup H	204
$\mathbb{H}$	gelanggang kuaternion	214
$\mathbb{Z}[i]$	bilangan bulat Gauss	216
$\operatorname{char} R$	karakteristik suatu gelanggang R	217
$\mathbb{Z}_{(p)}$	gelanggang bilangan bulat yang dilokalkan di p	231
$\deg f(x)$	derajat suatu polinomial	235

(Bersambung pada halaman berikutnya)

Simbol	**Deskripsi**	**Halaman**
$R[x]$	gelanggang polinomial atas gelanggang R	235
$R[x_1, x_2, \ldots, x_n]$	gelanggang polinomial dalam n peubah tak tentu	237
ϕ_α	homomorfisma evaluasi di α	237
$\mathbb{Q}(x)$	lapangan fungsi rasional di atas $\mathbb{Q}$	255
$\nu(a)$	valuasi Euklides dari a	259
$F(x)$	lapangan fungsi rasional dalam x	264
$F(x_1, \ldots, x_n)$	lapangan fungsi rasional dalam $x_1, \ldots, x_n$	264
$a \preceq b$	a kurang dari b	267
$a \vee b$	gabung dari a dan b	269
$a \wedge b$	temu dari a dan b	269
I	unsur terbesar dalam suatu latis	271
O	unsur terkecil dalam suatu latis	271
a'	komplemen dari a dalam suatu latis	271
$\dim V$	dimensi suatu ruang vektor V	287
$U \oplus V$	jumlah langsung ruang vektor U dan V	290
$\mathrm{Hom}(V, W)$	himpunan semua transformasi linear dari U ke V	291
V^*	dual dari suatu ruang vektor V	291
$F(\alpha_1, \ldots, \alpha_n)$	lapangan terkecil yang memuat F dan $\alpha_1, \ldots, \alpha_n$	295
$[E : F]$	dimensi perluasan lapangan E atas F	297
$\mathrm{GF}(p^n)$	lapangan Galois berorde p^n	314
F^*	grup multiplikatif dari lapangan F	315
$G(E/F)$	grup Galois dari E atas F	329
$F_{\{\sigma_i\}}$	lapangan yang ditetapkan oleh automorfisme σ_i	333
F_G	lapangan yang ditetapkan oleh grup automorfisme G	333
Δ^2	diskriminan suatu polinomial	348

Indeks

Abel, Niels Henrik, 339
Adleman, L., 93
Akar kesatuan ke-n, 58
Akar kesatuan ke-n primitif, 58
Akar kesatuan pangkat n, 340
Akar kesatuan primitif pangkat n, 340
Akar nol
    multiplisitas, 332
Akar sederhana, 332
Algoritma
    Euklides, 24
    pembagian, 238
Algoritma Euklides, 24
Algoritma faktorisasi Fermat, 98
Algoritma pembagian
    untuk bilangan bulat, 22
    untuk polinomial, 238
Aljabar Boolean
    atom dalam, 274
    definisi, 272
    hingga, 273
    isomorfisma, 273
Atom, 274
Automorfisme
    dalam, 156

Basis kisi, 168
Batas atas, 268
Batas atas terkecil, 269
Batas bawah, 269
Batas bawah terbesar, 269
Bieberbach, L., 171
Bilangan aljabar, 295
Bilangan bulat Gauss, 216
Bilangan bulat komposit, 24
Bilangan bulat prima, 24
Bilangan Carmichael, 99
Bilangan transenden, 295
Bilangan yang dapat dikonstruksi, 304
Bobot kata kode, 106
Boole, George, 278
Burnside, William, 41, 145, 197

Cardano, Gerolamo, 245
Cauchy, Augustin-Louis, 73
Cayley, Arthur, 131
Citra homomorfik, 149

Daerah integral, 213
De Morgan, Augustus, 278
Deligne, Pierre, 308
Delta Kronecker, 162
delta Kronecker, 114
Deret komposisi, 181
Deret normal suatu grup, 180
Deret prinsipal, 181
Deret subnormal suatu grup, 180
Determinan Vandermonde, 320
Determinan, Vandermonde, 320
Diagram komutatif, 152
Dickson, L. E., 145
Diffie, W., 93
Diskriminan
    persamaan kuadrat, 249
    persamaan kubik, 250
Domain
    Euklides, 259
    faktorisasi tunggal, 256
    ideal utama, 257
Domain Euklides, 259
Domain faktorisasi tunggal (UFD), 256
Domain ideal utama (PID), 257

Ekuivalen-G, 187

Elemen
orde, 52
prima, 256
primitif, 332
sekawan, 256
tak tereduksi, 256
transenden, 294
Elemen prima, 256
Elemen primitif, 332
Elemen sekawan, 256
Elemen tak tereduksi, 256
Elemen transenden, 294
Euler, Leonhard, 86, 308

Faktor persekutuan terbesar
dari dua bilangan bulat, 22
dua polinomial, 239
Faltings, Gerd, 308
Feit, W., 145, 197
Fermat, Pierre de, 86, 308
Ferrari, Ludovico, 245
Ferro, Scipione del, 245
Fior, Antonio, 245
Fungsi
bijektif, 8
Boolean, 195, 282
daerah hasil, 7
dapat dibalik, 10
definisi, 7
domain, 7
identitas, 10
injektif, 8
komposisi, 8
pensakelaran, 195, 282
satu-ke-satu, 8
surjektif, 8
Fungsi ϕ Euler, 86
Fungsi Ackermann, 30
Fungsi Boolean, 195, 282
Fungsi pensakelaran, 195, 282

Gabung, 269
Galois, Évariste, 41, 339
Gauss, Karl Friedrich, 262
Gelanggang
definisi, 212
dengan identitas, 213
dengan satuan, 213
hasil bagi, 220
homomorfisma, 218
isomorfisma, 218
karakteristik, 217
komutatif, 213
Noetherian, 258
pembagian, 213
Gelanggang komutatif, 213
Gelanggang pembagian, 213
Gerak kaku, 34, 165
Gorenstein, Daniel, 145
Greiss, R., 145
Grothendieck, Alexander, 308
Grup
abelian, 37
aksi, 186
alternasi, 72
berhingga, 39
definisi, 36
dibangkitkan secara hingga, 176
dihedral, 73
Euklides, 164
Galois, 329
grup-p, 176, 202
hasil bagi, 141
homomorfisma, 149
isomorfik, 127
isomorfisma dari, 127
komutatif, 37
kuaternion, 39
kuosien, 141
linear khusus, 42, 160
linear umum, 38, 160
lingkaran, 57
nonabelian, 37
nonkomutatif, 37
orde, 39
ortogonal, 161
ortogonal khusus, 164
pembangkit dari, 175
permutasi, 67
pusat, 189
ruang, 169
satuan, 38
sederhana, 142, 145
siklik, 52
simetri, 166
simetris, 66
solvabel, 182
tak berhingga, 39
titik, 169
Grup abelian, 37
Grup Euklides, 164
Grup Galois, 329
Grup ortogonal, 161
Grup permutasi, 67
Grup sederhana, 142
Grup yang dibangkitkan secara hingga, 176

Gödel, Kurt, 278

Hamming, R., 108
Hasil kali dalam, 110
Hasil kali dalam Euklides, 161
Hasil kali langsung eksternal, 132
Hasil kali langsung grup
    eksternal, 132
    internal, 134
Hasil kali langsung internal, 134
Hasil kali skalar, 283
Hellman, M., 93
Hilbert, David, 171, 223, 278, 308
Himpunan kuasa, 267
Himpunan ortonormal, 162
Himpunan perentang, 285
Himpunan terurut baik, 21
Himpunan terurut parsial, 267
Himpunan titik tetap, 188
Himpunan-G, 186
Homomorfisma
    alami, 151, 220
    evaluasi, 218, 237
    gelanggang, 218
    grup, 149
    kanonik, 151, 220
    kernel gelanggang, 218
    kernel grup, 151
Hukum De Morgan
    untuk aljabar Boolean, 273
hukum De Morgan
    untuk himpunan, 6
Hukum kanselasi
    untuk daerah integral, 216
Hukum pencoretan
    untuk grup, 40

Ideal
    definisi, 219
    dua sisi, 220
    maksimal, 221
    prima, 222
    satu sisi, 220
    trivial, 219
    utama, 219
Ideal maksimal, 221
Ideal prima, 222
Ideal utama, 219
Impian Mahasiswa Baru, 313
Indeks suatu subgrup, 83
Induksi
    prinsip kedua, 21
    prinsip pertama, 20
Infimum, 269
International Standard Book Number, 49
Isometri, 165
Isomorfisma
    aljabar Boolean, 273
    gelanggang, 218
    grup, 127

Jarak Hamming, 106
Jordan, C., 145

Karakteristik gelanggang, 217
Kebebasan linear, 286
Kebergantungan linear, 286
Kelas ekuivalensi, 13
Kelas konjugasi, 189
Kernel
    homomorfisma gelanggang, 218
    homomorfisma grup, 151
Keterpecahan dengan radikal, 340
Kisi titik, 168
Klein, Felix, 41, 158, 223
Kode
    BCH, 322
    grup, 109
    jarak minimum, 106
    linear, 111
    polinomial, 317
    siklik, 316
Kombinasi linear, 285
Kongruensi modulo n, 14
Konjektur Mordell, 308
Konjugasi, 187
Konjugat, kompleks, 54
Koset
    kanan, 82
    kiri, 82
    pemimpin, 119
    wakil, 82
Kriptanalisis, 91
Kriteria Eisenstein, 243
Kronecker, Leopold, 308
Kuaternion, 39, 214
Kummer, Ernst, 308
Kunci
    definisi, 90
    privat, 91
    publik, 90
    tunggal, 91

Lagrange, Joseph-Louis, 41, 72, 86
Lapangan, 213
    dasar, 292
    Galois, 314

hasil bagi, 254
pecahan, 254
pemisah, 301
perluasan, 292
tertutup secara aljabar, 300
tetap, 333
Lapangan Galois, 314
Lapangan pemisah, 301
Laplace, Pierre-Simon, 73
Latis
berkomplemen, 271
definisi, 269
distributif, 271
Latis, Prinsip Dualitas untuk, 269
Lema Gauss, 261
Lie, Sophus, 41, 205

Matriks
dapat dibalik, 159
mempertahankan hasil kali dalam, 163
mempertahankan jarak, 163
mempertahankan panjang, 163
nonsingular, 160
ortogonal, 161
pembangkit, 112
pemeriksa paritas, 112
ruang nol, 110
serupa, 13
unimodular, 168
Matriks ortogonal, 161
Matriks Vandermonde, 320
Matriks, Vandermonde, 320
Menggandakan kubus, 307
Menguadratkan lingkaran adalah mustahil, 307
Minkowski, Hermann, 308
Multiplisitas suatu akar, 332

Noether, A. Emmy, 223
Noether, Max, 223
Nol
polinomial, 239

Operasi biner, 36
Orbit, 187

Partisi, 13
Pembagi nol, 213
Pembangkit suatu grup, 175
Pembangkit suatu subgrup siklik, 52
Pemetaan, *lihat* Fungsi
Pemetaan linear, 158
Pemetaan terdefinisi dengan baik, 8
Pemusat
dari suatu subgrup, 189
Pencerminan luncur, 165
Pendekodean kemungkinan maksimum, 105
Pendekodean koset, 118
Pendekodean standar, 118
Penormal, 204
Penutupan aljabar, 300
Perluasan
aljabar, 294
hingga, 297
lapangan, 292
normal, 335
radikal, 340
sederhana, 295
separabel, 313, 332
Perluasan aljabar, 294
Perluasan normal, 335
Perluasan sederhana, 295
Permutasi
definisi, 10, 66
ganjil, 72
genap, 72
struktur siklus, 88
Persamaan kelas, 189
Persamaan kubik resolven, 250
Peubah tak tentu, 234
Polinomial
akar, 239
definisi, 234
derajat, 235
faktor persekutuan terbesar, 239
galat, 326
kode, 317
koefisien utama, 235
konten, 260
minimal, 296
monik, 235
nol, 239
pelacak galat, 326
pembangkit minimal, 319
primitif, 260
separabel, 332
tak tereduksi, 241
Polinomial dalam n peubah tak tentu, 237
Polinomial minimal, 296
Polinomial monik, 235
Polinomial pembangkit minimal, 319

Polinomial primitif, 260
Polinomial separabel, 313
Polinomial tak tereduksi, 241
Poset
    definisi, 267
    unsur terbesar dalam, 271
    unsur terkecil dalam, 271
Pseudoprima, 99

Rangkaian
    paralel, 276
    seri, 276
    seri-paralel, 276
Relasi ekuivalensi, 12
Representasi reguler kiri, 131
Rivest, R., 93
Ruang nol
    suatu matriks, 110
Ruang vektor
    basis, 287
    definisi, 283
    dimensi, 287
    subruang, 285
Ruffini, P., 339
Russell, Bertrand, 278

Sakelar
    definisi, 276
    terbuka, 276
    tertutup, 276
Saluran simetris biner, 105
Sandi, 90
Saringan Eratosthenes, 29
Shamir, A., 93
Shannon, C., 108
Siklus
    definisi, 68
    saling lepas, 68
Sindrom suatu kode, 117, 326
Sistem kriptografi
    RSA, 93
    afin, 92
    definisi, 90
    kunci privat, 91
    kunci publik, 90
    kunci tunggal, 91
    monoalfabetik, 91
    polialfabetik, 92
Sistem kriptografi RSA, 93
Subgelanggang, 215
Subgrup
    definisi, 41
    indeks, 83
    isotropi, 188
    komutator, 206
    normal, 140
    pemusat, 189
    penormal dari, 204
    penstabil, 188
    sejati, 41
    siklik, 52
    subgrup Sylow-p, 203
    translasi, 169
    trivial, 41
Subgrup normal, 140
Subgrup Sylow-p, 203
Subgrup-p, 202
Supremum, 269
Syarat rantai naik, 258
Sylow, Ludvig, 205

Tabel Cayley, 37
Tabel pendekodean, 119
Tartaglia, 245
Teks terang, 90
Teks tersandi, 90
Temu, 269
Teorema Cauchy, 202
Teorema Cayley, 130
Teorema Dasar
    Aritmetika, 25
    Grup Abelian Hingga, 176
Teorema DeMoivre, 57
Teorema Elemen Primitif, 332
Teorema Fundamental
    Aljabar, 301, 344
Teorema Fundamental Teori Galois, 336
Teorema Isomorfisma Kedua
    untuk gelanggang, 221
    untuk grup, 152
Teorema Isomorfisma Ketiga
    untuk gelanggang, 221
    untuk grup, 154
Teorema Isomorfisma Pertama
    untuk gelanggang, 220
    untuk grup, 151
Teorema Jordan-Hölder, 181
Teorema Kecil Fermat, 86
Teorema Korespondensi
    untuk gelanggang, 221
    untuk grup, 153
Teorema Lagrange, 84
Teorema Orde Ganjil, 208
Teorema Pencacahan Burnside, 192
Teorema Sisa Cina
    untuk bilangan bulat, 225

Thompson, J., 145, 197
Transformasi linear
definisi, 10, 158
Transposisi, 70
Triseksi sudut, 307
Turunan, 313

Unit, 255
Universal Product Code, 48
Unsur
identitas, 37
invers, 37
Unsur konjugat, 330
Unsur satuan, 213
Urutan parsial, 267

Valuasi Euklides, 259

Weil, André, 308
Whitehead, Alfred North, 278

Kolofon

Buku ini ditulis dan diproduksi dengan PreTeXt. Catatan produksi terjemahan: OpenAI Codex gpt-5.6-sol, Ultra. Catatan ini menyatakan metode produksi, bukan kepengarangan.