

29. The Finiteness Theorem for the Invariants of Finite Linear Groups of Characteristic p .

Nachr. v. d. Ges. d. Wiss. zu Göttingen 1926, pp. 28–35

By Emmy Noether in Göttingen.

Presented by R. Courant in the session of 30 July 1926.

I show in what follows that the well-known finiteness theorem for the invariants of finite groups of linear substitutions¹ remains valid when, as coefficient domain, instead of an ordinary number field one takes an arbitrary field – hence in particular one of characteristic p .² However, the known proofs of finiteness fail as soon as the order of the group is divisible by p ; deeper arithmetical facts must be brought in, namely the following criterion, previously known only for characteristic zero:

Finiteness criterion³: An integral domain $\mathfrak{S}$ of polynomials – more generally of rational functions – with coefficients from a field is finite if and only if $\mathfrak{S}$ contains a finite subring $\mathfrak{R}$ such that $\mathfrak{S}$ depends algebraically and integrally on $\mathfrak{R}$. Each integral basis of $\mathfrak{R}$ is then completed, by a module basis of $\mathfrak{S}$ with respect to a certain subring of $\mathfrak{R}$, to an integral basis of $\mathfrak{S}$.

This criterion – which is of independent interest in itself – rests on the existence of the rational basis and on the fact that the divisor-chain theorem is preserved in passing to the integral quantities of a finite extension. This second theorem was proved in the preceding note of Artin and van der Waerden for arbitrary characteristic, only under a certain finiteness assumption on the original domain, an assumption fulfilled in the case of finite groups (the root ring represents a finite extension). For the existence of the rational basis I give a proof valid for arbitrary fields as coefficient domain; hence I can prove the finiteness criterion under the above restriction.

That, for invariants of finite groups, the finiteness criterion is fulfilled rests on the principle of symmetric functions. Whereas in characteristic zero the coefficients of the Galois resolvent already furnish the integral basis, in the general case they generate only the finite subring required in the finiteness criterion. From the existence of this finite subring the finiteness of the “relative” invariants and of the “modular” invariants follows by the same arguments.

The invariants considered here include, as special cases, the “projective invariants mod p ” treated by Dickson and his school.⁴ Here the finiteness theorem was known for modular invariants, but not for general “formal” invariants.

§ 1. The Finiteness Criterion

1. Theorem on the existence of the rational basis. First formulation: Every system S of rational functions of n indeterminates, with coefficients from a field P , possesses a finite rational basis; that is, there are finitely many functions of the system such that every function of the system can be expressed rationally, with coefficients from P , through these finitely many.

Second formulation: Let $\mathfrak{K}$ be an intermediate field between P and $P(x_1, \dots, x_n)$ – where $x_1, \dots, x_n$ denote indeterminates – of transcendence degree $t \leq n$; let $y_1, \dots, y_t$ be an irreducible system⁵ from $\mathfrak{K}$. Then $\mathfrak{K}$ becomes a finite algebraic extension of $P(y_1, \dots, y_t)$.

The two formulations are in fact equivalent. It is enough to prove the existence of the rational basis for all intermediate fields; for the field derived from a system S becomes such an intermediate field $\mathfrak{K}$, whose rational basis immediately gives a rational basis of S , since every element of $\mathfrak{K}$ becomes a rational combination of finitely many functions from S . From the second formulation it follows, however, that an arbitrary irreducible system $y_1, \dots, y_t$ from $\mathfrak{K}$, enlarged by the finitely many functions that characterize $\mathfrak{K}$ as a finite extension of $P(y_1, \dots, y_t)$, gives such a rational basis. Conversely, if according to the first formulation a rational basis of

¹For an elementary proof of finiteness see E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen. Math. Ann. 77 (1916), pp. 89–92.

²For the concepts of field theory see E. Steinitz, Algebraische Theorie der Körper. J. f. M., 137 (1910), pp. 167–309. Characteristic in § 4, root field in § 12, quotient field in § 3.

³Compare E. Noether, Algebraische und Differentialinvarianten. Jahresber. d. d. Math.-Ver. 32 (1923), pp. 177–184, no. 3, Theorem 4, and the literature cited there. In the last sentence of the criterion there it incorrectly says “module basis with respect to $\mathfrak{R}$ ” (fundamental system of integral quantities) instead of “with respect to a certain subring of $\mathfrak{R}$ ”.

⁴Compare Dickson, On Invariants and the theory of Numbers. The Madison Colloquium 1913. More recent literature is in the volumes of the Transactions of the American Mathematical Society that have appeared since then.

⁵A system is called irreducible, according to Steinitz, if it consists of algebraically independent functions. A system is said to have transcendence degree t if it contains at least one irreducible system of t elements, but none of more elements. For the simple theorems on irreducible systems used below, see Steinitz, § 22.

$\mathfrak{K}$ is given, then by the definition of transcendence degree each basis element must be algebraically dependent on $P(y_1, \dots, y_t)$; hence $\mathfrak{K}$ is thereby characterized as a finite algebraic extension of $P(y_1, \dots, y_t)$.

The theorem will be proved in the second formulation. First let $\mathfrak{K}$ have the same transcendence degree n as $P(x_1, \dots, x_n)$; let $y_1, \dots, y_n$ be an irreducible system from $\mathfrak{K}$ and consequently from $P(x_1, \dots, x_n)$. Because the transcendence degree of $y_1, \dots, y_n$ is n , each x_i becomes algebraic over $P(y_1, \dots, y_n)$; thus $P(x_1, \dots, x_n)$, and hence $\mathfrak{K}$ as an intermediate field, becomes a finite algebraic extension of $P(y_1, \dots, y_n)$.

Now let $t < n$; let the numbering of the x be chosen so that $y_1, \dots, y_t, x_{t+1}, \dots, x_n$ form an irreducible system from $P(x_1, \dots, x_n)$. Then $x_{t+1}, \dots, x_n$ are irreducible with respect to $P(y_1, \dots, y_t)$ and hence, by the transitive law of algebraic dependence, also irreducible with respect to $\mathfrak{K}$ and to every intermediate field $\mathfrak{M}$ between $P(y_1, \dots, y_t)$ and $\mathfrak{K}$. This means that $\bar{\mathfrak{K}} = \mathfrak{K}(x_{t+1}, \dots, x_n)$, respectively $\bar{\mathfrak{M}} = \mathfrak{M}(x_{t+1}, \dots, x_n)$, becomes a purely transcendental extension of $\mathfrak{K}$, respectively $\mathfrak{M}$; hence every element of $\bar{\mathfrak{K}}$ not belonging to $\mathfrak{K}$ is transcendental with respect to $\mathfrak{K}$, and similarly every element of $\bar{\mathfrak{M}}$ not belonging to $\mathfrak{M}$ is transcendental with respect to $\mathfrak{M}$. Likewise let $\bar{P}$ be set equal to the purely transcendental extension $P(x_{t+1}, \dots, x_n)$; then $y_1, \dots, y_t$ are irreducible with respect to $\bar{P}$.

The proof can now be reduced to the case already settled by taking $\bar{P}$ as coefficient domain. From $P < \mathfrak{K} < P(x_1, \dots, x_t; x_{t+1}, \dots, x_n)$ ⁶ it follows that $\bar{P} < \bar{\mathfrak{K}} < \bar{P}(x_1, \dots, x_t)$, where $\bar{\mathfrak{K}}$ has the same transcendence degree t over $\bar{P}$ as $\bar{P}(x_1, \dots, x_t)$. Hence $\bar{\mathfrak{K}}$ has a finite rational basis with respect to $\bar{P}$ as coefficient domain, say $y_1, \dots, y_t; z_1, \dots, z_s$. Here the z can be chosen from $\mathfrak{K}$, since $\bar{\mathfrak{K}}$ is the union field of $\mathfrak{K}$ and $\bar{P}$. It remains to show that $\mathfrak{K}$ equals $\mathfrak{M} = P(y_1, \dots, y_t; z_1, \dots, z_s)$. Now $\mathfrak{M}$ is an intermediate field between $P(y_1, \dots, y_t)$ and $\mathfrak{K}$; hence every element of $\mathfrak{K}$ is algebraic with respect to $\mathfrak{M}$. On the other hand, $\bar{\mathfrak{M}}$ equals $\bar{\mathfrak{K}}$, and hence $\mathfrak{K}$ is contained in $\bar{\mathfrak{M}}$. Thus $\mathfrak{K}$ is an intermediate field between $\mathfrak{M}$ and $\bar{\mathfrak{M}}$; since every element of $\bar{\mathfrak{M}}$ not belonging to $\mathfrak{M}$ is transcendental with respect to $\mathfrak{M}$, it necessarily follows that $\mathfrak{K}$ is identical with $\mathfrak{M}$.

Corollary: If $P < \mathfrak{K} < \mathfrak{L} < P(x_1, \dots, x_n)$ and $\mathfrak{L}$ is algebraic with respect to $\mathfrak{K}$, then $\mathfrak{L}$ is a finite algebraic extension of $\mathfrak{K}$. For every element of a rational basis of $\mathfrak{L}$ is then algebraic with respect to $\mathfrak{K}$; hence $\mathfrak{L}$ is characterized as a finite extension of $\mathfrak{K}$.

2. Proof of the finiteness criterion. The condition is plainly necessary; for if $\mathfrak{S}$ is a finite integral domain, then $\mathfrak{S}$ itself can be regarded as the finite subring $\mathfrak{R}$ occurring in the criterion.

The condition is sufficient under the assumption that the root field $P^{1/p}$ is a finite extension of the coefficient field⁷ whenever the latter has characteristic p ; for characteristic zero no restrictive assumption is needed. To prove this one has to show that $\mathfrak{S}$ has a finite module basis with respect to a subring of $\mathfrak{R}$.

Let $\bar{\mathfrak{K}}$ denote the quotient field⁸ of $\mathfrak{R}$, and let $\mathfrak{L}$ denote the quotient field of $\mathfrak{S}$. These quotient fields exist since the rings involved have no zero divisors; and one has $P < \bar{\mathfrak{K}} < \mathfrak{L} < P(x_1, \dots, x_n)$. Hence by the corollary under 1., $\mathfrak{L}$ becomes a finite algebraic extension field of $\bar{\mathfrak{K}}$. Moreover, by hypothesis every element of $\mathfrak{S}$ is integral with respect to $\mathfrak{R}$, and thus $\mathfrak{S}$ becomes a subring of the ring $\mathfrak{S}'$ consisting of all elements of $\mathfrak{L}$ integral over $\mathfrak{R}$. But since nothing is assumed about the integral closedness of $\mathfrak{R}$ in $\bar{\mathfrak{K}}$, the fact that the divisor-chain theorem is preserved under finite extension cannot be applied directly. Rather, one must first pass to a likewise finite subring $\mathfrak{T}$ of $\mathfrak{R}$ for which this integral closedness is fulfilled.

First suppose that the coefficient domain P contains infinitely many elements. Then one can select from $\mathfrak{R}$ an irreducible system $g_1(x), \dots, g_t(x)$ in such a way that $\mathfrak{R}$, and hence $\mathfrak{S}$, is integral over $\mathfrak{T} = P[g_1(x), \dots, g_t(x)]$. Namely, let $f_1(x), \dots, f_k(x)$ be the integral basis of $\mathfrak{R}$ existing by hypothesis; if this does not form an irreducible system, then – after a possible renumbering of the indices – let $F(f_k; f_1, \dots, f_{k-1}) = 0$ be a relation satisfied by f_k . If one replaces $f_1, \dots, f_{k-1}$ by

$$f_1 + t_1 f_k, \dots, f_{k-1} + t_{k-1} f_k;$$

then f_k , and hence also $f_1, \dots, f_{k-1}$, is integral over these new functions when the t_i are chosen as indeterminates. Since P has infinitely many elements, the t_i can be specialized to elements of P in such a way that this integral dependence is preserved. After finitely many steps, using the transitive law of integral dependence, one therefore arrives at the required ring $\mathfrak{T} = P[g_1(x), \dots, g_t(x)]$ ⁹. Then $\mathfrak{L}$ is a finite extension field of the quotient field $P(g_1(x), \dots, g_t(x))$ of $\mathfrak{T}$, and the ring $\mathfrak{S}'$ of all elements of $\mathfrak{L}$ integral over $\mathfrak{R}$ is identical with the ring of all elements of $\mathfrak{L}$ integral over $\mathfrak{T}$.

In $\mathfrak{T}$ the divisor-chain theorem holds for the system of all ideals, and $\mathfrak{T}$ is integrally closed in its quotient field, both because $\mathfrak{T}$ is isomorphic to the polynomial domain in t indeterminates. From the assumption that

⁶ $P < \mathfrak{K}$ means: P is contained in $\mathfrak{K}$, hence is a subfield of $\mathfrak{K}$.

⁷ See p. 28, note 2.

⁸ See p. 28, note 2.

⁹ Compare Hilbert, Über die vollen Invariantensysteme, § 1. Math. Ann. 42 (1893), pp. 313–373.

$P^{1/p}$ is finite over P it follows further that $\mathfrak{T}^{1/p}$ is finite over $\mathfrak{T}$.¹⁰ Hence in $\mathfrak{S}'$ the divisor-chain theorem holds for the system of all $\mathfrak{T}$ -modules; in particular, $\mathfrak{S}$, as a subring of $\mathfrak{S}'$ containing $\mathfrak{T}$, has a finite $\mathfrak{T}$ -module basis¹⁰. The existence of the finite $\mathfrak{T}$ -module basis for $\mathfrak{S}$ continues to hold without any restrictive assumption on the coefficient domain P if $\mathfrak{L}$ is an extension of the first kind of $P(g_1(x), \dots, g_t(x))$, hence in particular always when P has characteristic zero.¹¹

Let $h_1(x), \dots, h_s(x)$ be a $\mathfrak{T}$ -module basis of $\mathfrak{S}$. Then the representation

$$f(x) = A_1(g)h_1(x) + \dots + A_s(g)h_s(x)$$

for an arbitrary $f(x)$ from $\mathfrak{S}$ – where the A , as elements of $\mathfrak{T}$, denote polynomials in the g – shows that $g_1(x), \dots, g_t(x), h_1(x), \dots, h_s(x)$ form the required integral basis.

If the field P contains only finitely many elements, then the field $P(u)$ obtained by adjoining an indeterminate u – that is, an element transcendental over $\mathfrak{S}$ – contains infinitely many elements. Thus the ring $\mathfrak{S}(u)$ has a finite integral basis with respect to $P(u)$ as coefficient domain; and since $\mathfrak{S}(u)$ is the union ring of $\mathfrak{S}$ and $P(u)$, this basis can be chosen from $\mathfrak{S}$ by splitting according to powers of u , although the basis elements g_i of $\mathfrak{S}$ will now no longer form an irreducible system. Accordingly every polynomial $f(x)$ from $\mathfrak{S}$ admits a representation $C(u)f(x) = G(u, g_i, h_i)$, where $C(u)$ denotes a nonzero polynomial from $P[u]$ and G becomes integral in u, g_i, h_i . Comparing the coefficients of a suitable power of u shows that $g_i(x)$ and $h_i(x)$ give an integral basis of $\mathfrak{S}$. Hence the **finiteness criterion is proved in full generality**.

§ 2. Finiteness of the Invariants

1. By a **finite linear group of characteristic p** is meant a group $\mathfrak{H}$ of h linear substitutions $A_1, \dots, A_h$ (of nonzero determinant) with coefficients from a field P of characteristic p . Here A_k is the linear substitution

$$x_1^{(k)} = a_{11}^{(k)}x_1 + \dots + a_{1n}^{(k)}x_n, \dots, \quad x_n^{(k)} = a_{n1}^{(k)}x_1 + \dots + a_{nn}^{(k)}x_n,$$

or, in abbreviated form, $(x^{(k)}) = A_k(x)$. Thus the group $\mathfrak{H}$ carries the row (x) with elements $x_1, \dots, x_n$ into the rows $(x^{(k)})$ with elements $x_1^{(k)}, \dots, x_n^{(k)}$. Since the identity must be contained among $A_1, \dots, A_h$, the row (x) is also contained among the rows $(x^{(k)})$.

By an **integral rational (absolute) invariant of the group** is meant such an integral rational function of $x_1, \dots, x_n$ – with coefficients from P ¹² – that remains identically unchanged under application of $A_1, \dots, A_h$. Thus all symmetric functions, with coefficients from P , of the rows $(x^{(k)})$ belong to these invariants. Conversely, for every such invariant one has

$$f(x) = f(x^{(1)}) = \dots = f(x^{(h)}) \quad \text{or} \quad h \cdot f(x) = f(x^{(1)}) + \dots + f(x^{(h)}).$$

It follows that in the case where the order h of the group is not divisible by the characteristic – in particular in characteristic zero – the symmetric functions of the rows $(x^{(k)})$, with coefficients from P , exhaust the totality of invariants. Since these symmetric functions possess a finite integral basis, the proof of finiteness is accomplished in this case; at the same time the integral basis is obtained as the system $G_{\alpha\alpha_1\dots\alpha_n}(x)$ of coefficients of the Galois resolvent:¹³

$$\begin{aligned} \Phi(z, u) &= \prod (z - u_1x_1^{(k)} - \dots - u_nx_n^{(k)}) \\ &= z^h + \sum G_{\alpha\alpha_1\dots\alpha_n}(x)z^\alpha u_1^{\alpha_1} \dots u_n^{\alpha_n} \quad (\alpha \neq h; \alpha + \alpha_1 + \dots + \alpha_n = h). \end{aligned}$$

2. In the case where h is divisible by p , it is not necessary that every invariant of the group be a symmetric function of the rows $(x^{(k)})$, since one can no longer conclude from $h \cdot f(x)$ to $f(x)$. But the ring $\mathfrak{R}$ derived from the finitely many invariants $G_{\alpha\alpha_1\dots\alpha_n}(x)$ – the coefficients of the Galois resolvent – forms a finite subring of the system $\mathfrak{S}$ of all invariants, and it remains to show that $\mathfrak{S}$, with respect to $\mathfrak{R}$, satisfies the hypotheses of the finiteness criterion.

¹⁰Compare the note of Artin and van der Waerden cited in the introduction.

¹¹Compare, for example, E. Noether, Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern, § 3. Math. Ann. 96 (1926), pp. 26–61.

¹²This is not a restriction of generality inasmuch as every invariant with coefficients from a field of characteristic p – which must possess a common overfield with P in order for the invariants to be defined – can be linearly decomposed into finitely many invariants with coefficients from P . In the general case one need only express the coefficients through ones that are linearly independent over P ; then the property of invariance is satisfied identically in these independent coefficients.

¹³See p. 28, note 1.

First, without loss of generality,¹⁴ the subfield $\overline{P}$ of P derived from all substitution coefficients $a_{\mu\nu}^{(k)}$ may be taken as coefficient domain. This field, derived from finitely many elements, is thus obtained by adjoining finitely many algebraic or transcendental elements to the prime field; and since the prime field is perfect, it follows that $\overline{P}^{1/p}$ is finite with respect to $\overline{P}$.¹⁵

It remains to show that $\mathfrak{S}$ depends algebraically and integrally on $\mathfrak{R}$. By 1., among the h rows $x^{(k)}$ there also occurs the original $x_1, \dots, x_n$; hence the Galois resolvent $\Phi(z, u)$ vanishes identically in u for $z = u_1x_1 + \dots + u_nx_n$. If one specializes in each case all u to zero except u_i , which is set equal to one, one obtains a relation

$$x_i^h + \sum x_i^\alpha G_{\alpha 0 \dots \alpha_i \dots 0}(x) = 0 \quad (\alpha \neq h; \alpha + \alpha_i = h),$$

which shows that each x_i depends algebraically and integrally on $\mathfrak{R}$. But then the same holds for every polynomial in x ; in particular $\mathfrak{S}$ is integral over $\mathfrak{R}$. Thus the hypotheses of the finiteness criterion are fulfilled, and the **finiteness of the invariants is proved**.

3. It should be noted that the same arguments give the **finiteness of the relative and modular invariants**. A polynomial $f(x)$ is called a **relative invariant** of the group if all $f(x^{(k)})$ differ from $f(x)$ only by a nonzero factor from $\overline{P}$. The system of absolute invariants – in particular the ring $\mathfrak{R}$ derived from the $G_{\alpha\alpha_1 \dots \alpha_n}(x)$ – therefore forms a finite subring of the ring derived from all relative invariants; and, as above, the hypotheses of the finiteness criterion with respect to $\mathfrak{R}$ are fulfilled.

A polynomial $f(x)$ is called a **modular invariant** of the group if $f(x)$ becomes equal to $f(x^{(k)})$ for every special value system $x_1 = \alpha_1, \dots, x_n = \alpha_n$ from $\overline{P}$. Every absolute invariant is at the same time a modular invariant; if, however, $\overline{P}$ contains only finitely many elements, the converse need not hold. Here too the hypotheses of the finiteness criterion are fulfilled with respect to the subring $\mathfrak{R}$ derived from the $G_{\alpha\alpha_1 \dots \alpha_n}(x)$.

¹⁴See p. 33, note.

¹⁵See p. 32, note 2.