# SOME RECENT DEVELOPMENTS IN ABSTRACT ALGEBRA*

BY OYSTEIN ORE

1. *Introduction.* If one should try to define algebra, it might be said that algebra deals with the formal combination of symbols according to prescribed rules. Such formal combinations are, however, obviously fundamental in most branches of mathematics even outside algebra in the ordinary sense. The recognition of this formal element in the mathematical theories has naturally led to an *algebraization*, which can easily be observed in the present state of many domains of mathematics; if one adopts the views of Hilbert, the whole system of mathematics can be formalized in this way.

When a certain number of formal operations have been laid down, a principal problem is to determine the structure of systems which are *closed* with respect to these operations, that is, have the property that any operation on elements again gives an element of the system. In this problem the notion of *isomorphism* is fundamental; two systems $S$ and $S'$ both closed with respect to a given system of operations, are said to be isomorphic or abstractly identical with respect to these operations if there exists a one-to-one correspondence between the elements of $S$ and $S'$, such that any formal combination of elements in $S$ corresponds to the analogous construction with corresponding elements in $S'$. An isomorphism between elements of the same system is called an *automorphism*. Two isomorphic systems are in algebra considered as equivalent, and it could therefore also be said, that algebra deals with those properties of systems, which are invariant for isomorphisms. Abstract systems and the notion of isomorphisms originated in the theory of finite groups, where the properties of groups were studied independently of the particular representation of the group.

In an algebraic system *equality* is usually defined and satisfies the following axioms:

---

* An address presented to the Society at the request of the program committee, December 31, 1930.

### E. Axioms of Equality

E I. *Determination.* For two arbitrary elements, either $a=b$ or $a\neq b$.
E II. *Reflexitivity.* $a=a$.
E III. *Symmetry.* From $a=b$ follows $b=a$.
E IV. *Transitivity.* From $a=b$, $b=c$ follows $a=c$.

Every such definition of equality, which is ordinarily not unique for the given system, constitutes a division of the elements into classes.

Usually algebra deals with systems which are closed with respect to one or two operations, addition and multiplication, satisfying all or some of the following axioms:

### A. Axioms of Addition

A I. For two arbitrary elements $a$ and $b$ in $S$ there exists a sum $a+b$, which is a uniquely defined element of $S$.
A II. *Equality.* If $a=b$ and $a_1=b_1$, then $a+a_1=b+b_1$.
A III. *Associative law.* $a+(b+c)=(a+b)+c$.
A IV. *Zero-element.* There exists an element 0 for which $0+a=a+0=a$ for all $a$.
A V. *Subtraction.* To every element $a$ there exists another $-a$ such that $a+(-a)=0$.
A VI. *Commutative law.* $a+b=b+a$.

### M. Axioms of Multiplication

M I. For two arbitrary elements $a$ and $b$ there exists a product $a\cdot b$ which is a uniquely defined element of $S$.
M II. *Equality.* From $a=b$, $a_1=b_1$, follows $aa_1=bb_1$.
M III. *Associative law.* $a(bc)=(ab)c$.
M IV. *Distributive law.* $(b+c)a=ba+ca$, $a(b+c)=ab+ac$.
M V. *Converse equality axiom.* From $ab=ac$ or $ba=ca$ follows $b=c$, when $a\neq 0$.
M VI. *Unit element.* There exists an element $\mathcal{E}$ for which $\mathcal{E}a=a\mathcal{E}=a$ for all $a$.
M VII. *Division.* For every $a\neq 0$ there exists an $a^{-1}$ such that $a\cdot a^{-1}=\mathcal{E}$.
M VIII. *Commutative law.* $ab=ba$.

By various choices among these axioms one obtains a series of different types of algebraic systems. Among the main types I

shall only mention the *moduli* (satisfying ordinarily A I–A VI), *groups* (M I–M VII except M IV), *rings* or *algebras* (satisfying A I–A VI and at least M I, M II) and finally *fields* or *division-algebras* satisfying all axioms except possibly M VIII. A survey of the nomenclature can be found in a recent paper by E. T. Bell.*

In the following I shall have to limit my topic mainly to the *commutative fields*,† that is, systems which satisfy *all* axioms mentioned above. Among the various algebraic sets these form a particularly important group, and they are also one of the few systems for which the principal features of the structure have been determined.

The theory of fields is closely connected with some of the most important problems of algebra.

Examples of fields are abundant: The sets of all rational, algebraic, real or complex numbers satisfy the axioms of a field; so do the sets of all rational or algebraic functions of one or more variables with coefficients in a given field. An example of a field with only a finite number of elements is the system of all remainders (mod $p$), where $p$ is an ordinary prime. I observe here, that the system of axioms for a field enumerated above is not *reduced*, that is, some axioms are consequences of others. Various reduced systems have been proposed by Dickson‡ and Huntington.§

Closely connected with the fields are the *domains of integrity*, which are rings satisfying all multiplication-axioms except M VI and M VII. An important property of these rings is the following: If $a$ and $b \neq 0$ are elements of a domain of integrity $D$, one can construct the formal quotients $(a/b)$ and define addition and multiplication for them much in the same way as the rational numbers are derived from the integers. The set of all these fractions then is a field $K$ containing $D$, and $K$ is usually called the *quotient-field* of $D$.

---

* E. T. Bell, *Unique decomposition*, American Mathematical Monthly, vol. 37 (1930), pp. 400–418.

† In the following the word "field" always stands for "commutative field."

‡ L. E. Dickson, Transactions of this Society, vol. 4 (1903), pp. 13–20; ibid., vol. 6 (1905), pp. 198–204.

§ E. V. Huntington, Transactions of this Society, vol. 4 (1903), pp. 31–37; ibid., vol. 6 (1905), pp. 181–197.

2. *Characteristics of a Field.* The necessity for a classification of all fields was first indicated by Weber* in the discussion of the following fundamental problem. Let $K$ be a field and let us consider equations with coefficients in $K$. For which fields $K$ does the Galois theory of equations hold? I shall only mention here, without stating the problem in a precise form at present, that not for all fields and equations is it possible to develop the Galois theory in its ordinary form.

The solution of this problem is mainly due to Steinitz† (using also ideas of Dedekind)‡ and is contained among a series of other results in his classical paper on the structure of fields.

All fields can, according to Steinitz, be divided into two principal types. Thus, let $K$ be an arbitrary field and let us consider all subfields of $K$; the elements which these fields have in common also form a field, the prime-field $P$ of $K$, which is contained in all other subfields of $K$. It is easy to see, that only two types of prime-fields are possible; the unit element obviously is contained in $P$ and $P$ therefore also contains all elements

$$\mathcal{E}, 2\mathcal{E}, \cdots, n\mathcal{E}, \cdots .$$

These elements are either all different or there exists a rational integer $p$ such that $p\mathcal{E}=0$. In the first case $P$ must also contain all fractions $(n\mathcal{E}/m\mathcal{E})$ and since these elements form a field one sees that $P=P_0$ is isomorphic to the field of rational numbers. $K$ is then said to have the *characteristic* 0.

When on the other hand $p\mathcal{E}=0$, it follows easily that the smallest $p$ must be a prime, and $P=P_p$ is in this case isomorphic to the finite field mentioned above consisting of the $p$ residues (mod $p$). We then say that $K$ has the *characteristic* $p$. Any subfield of $K$ has the same characteristic as $K$, and when the characteristic is a prime $p$, we have $pa=p\mathcal{E}a=0$, that is, all expressions in $K$ can be reduced (mod $p$).

3. *Algebraic and Transcendental Adjunctions.* From the

* H. Weber, *Die allgemeine Grundlagen der Galoisschen Gleichungstheorie*, Mathematische Annalen, vol. 43 (1893), pp. 521–549.

† E. Steinitz, *Algebraische Theorie der Körper*, Journal für Mathematik, vol. 137 (1910), pp. 167–309. This paper has recently been edited in book form and annotated by H. Hasse and R. Baer, 1930.

‡ Compare, for example, supplements to Dirichlet-Dedekind's *Zahlentheorie.*

prime-field the original field $K$ can be obtained by the process of *adjunction*. If $a$ is an element in $K$ not contained in $P$, then all rational functions $R(a)$ of $a$ with coefficients from $P$ form a field $P(a)$ contained in $K$ and containing $P$. If $P(a)$ is a proper subfield of $K$, we adjoin another element $b$ not contained in $P(a)$ and obtain the field $P(a, b)$ etc. In this way $K$ can be built up, if necessary by using a well-ordering of $K$, that is, assuming the axiom of Zermelo.

Let us therefore in general consider a field $K$ and the possible adjunctions to $K$. We shall first consider the *simple* adjunctions, that is, fields obtained by the adjunction of a single element. As we shall see, there exist two principal types of simple adjunctions.

Let $x$ be the element adjoined; then the enlarged field must contain all expressions of the form

$$a_0 + a_1x + \cdots + a_nx^n, \tag{1}$$

where the $a_i$ are elements of $K$. These expressions might be all different or some of them might be equal. In the first case an expression (1) can only be equal to zero if all coefficients vanish; these polynomials then obviously form a domain of integrity, and the quotient-field $K(x)$, consisting of all rational functions of $x$ with coefficients in $K$, is the least field containing $K$ and $x$. Such an adjunction is called a *transcendental adjunction*, and $K(x)$ is called a *transcendental enlargement* of $K$. The following fact is then obvious.

*To every field $K$ at least one simple transcendental enlargement exists, and all such fields are equivalent, that is, there exists an isomorphism between them having the particular property that the elements of $K$ correspond to themselves.*

For, if $K(y)$ is another transcendental enlargement, we can let $R(x)$ correspond to $R(y)$ for all rational functions $R$.

In the second case, where some of the expressions (1) are equal, there must exist a relation of the following form (writing $\alpha$ for $x$ to distinguish from the former case)

$$f(\alpha) = \alpha^m + b_1\alpha^{m-1} + \cdots + b_m = 0. \tag{2}$$

If $f(\alpha)$ is the polynomial of lowest degree having this property, $f(x)$ must be an irreducible polynomial in $K$. Every expression (1) is equal to a reduced expression

$$c_1\alpha^{m-1} + c_2\alpha^{m-2} + \cdots + c_m, \tag{3}$$

and two expressions $A(\alpha)$ and $B(\alpha)$ are only then equal when

$$A(\alpha) \equiv B(\alpha), \qquad (\text{mod } f(\alpha)).$$

It is easily seen that all the expressions (3) form a field; to prove, for example, that corresponding to every $A(\alpha) \neq 0$ there exists an $A(\alpha)^{-1}$, we determine $G(x)$ and $H(x)$ by Euclid's algorithm such that

$$G(x)A(x) + H(x)f(x) = 1.$$

Since $f(x)$ is irreducible, this can always be accomplished, and we obtain $G(\alpha) = A(\alpha)^{-1}$ since

$$G(\alpha)A(\alpha) \equiv 1, \qquad (\text{mod } f(\alpha)).$$

The field $K(\alpha)$ is called a *simple algebraic enlargement* of $K$. In $K(\alpha)$ the irreducible polynomial $f(x)$ in $K$ has a root, and conversely, when an arbitrary irreducible $f(x)$ in $K$ is chosen, this procedure gives a method for constructing a $K(\alpha)$ in which $f(x) = 0$ has a solution.

*If $f(x)$ is an irreducible polynomial in a field $K$ there always exists a simple algebraic enlargement $K(\alpha)$ such that $f(x) = 0$ has a root in $K(\alpha)$, and all other fields having this property must have a subfield equivalent to $K(\alpha)$.*

4. *Degree of Transcendency. Algebraically Complete Fields.* The last simple theorem replaces in modern algebra for most applications the following so-called *fundamental theorem of algebra*: In the field of all complex numbers every polynomial has a root.

From the results of §3 it follows that every field can be obtained from its prime-field by a series of algebraic and transcendental adjunctions. One of the fundamental results of Steinitz is this: *Every field can be obtained by first making a series of transcendental adjunctions and then a series of algebraic adjunctions to this purely transcendental field.* The number $t$ of transcendental adjunctions required is called the *degree of transcendency* of $K$ and is, like the characteristic, a characterizing invariant of the field. The degree of transcendency $t$ may be infinite and in this case the cardinal number of the set of transcendental elements to be adjoined is the invariant.

Since the properties of the purely transcendental fields are fairly simple, we shall take more interest in the algebraic adjunctions. A field $K'$ is said to be an *algebraic* enlargement of $K$, if it can be obtained from $K$ by successive simple algebraic adjunctions. This is equivalent to saying that all elements in $K'$ shall satisfy irreducible equations in $K$. The algebraic enlargements are again of two kinds: (a) the *finite* algebraic fields over $K$, which require only a finite number of adjunctions, and (b) the *infinite*, only obtainable by an *infinite* number of simple algebraic adjunctions to $K$. The finite algebraic fields over $K$ are also equivalent to the fields of *finite rank* over $K$, that is, there exists a basis

$$\omega_1, \omega_2, \cdots, \omega_n$$

of the field, such that every number $\alpha$ in the field can be expressed as

$$\alpha = a_1\omega_1 + a_2\omega_2 + \cdot \cdot + a_n\omega_n,$$

where the $a_i$ are elements of $K$.

We saw in §3 that every field $K$ had transcendental enlargements. It is interesting to notice that not every field can be enlarged by algebraic adjunctions. A field of this kind is, for instance, the field of all complex numbers, in which no irreducible polynomials of higher degree than the first can exist. The field of all algebraic numbers has the same property. A field in which every polynomial (with coefficients in the field) reduces to a product of linear factors is called *algebraically complete*. These are obviously the only fields to which no algebraic adjunctions can be made. Steinitz was able to prove the following theorem.

*For every field $K$ there exists a unique algebraically complete field $K'$, which is algebraic over $K$. All other algebraically complete fields over $K$ contain a subfield equivalent to $K'$.*

5. *Galois Fields and Group Theory for Abstract Fields.* We shall now return to the general problem of determining the fields to which the Galois theory can be extended. A *Galois field* $\overline{K}$ over a given field $K$ is defined as an algebraic field in which every irreducible polynomial $f(x)$ in $K$ either remains irreducible or decomposes into a product of linear factors. A *simple* Galois field is the field of least rank in which a given irreducible polynomial $f(x)$ decomposes into linear factors.

To every Galois field $\overline{K}$ there exists a set of automorphisms, such that when $\alpha$ corresponds to another element $\alpha'$ (the conjugates of $\alpha$ in the ordinary Galois theory) also contained in $\overline{K}$, then $\alpha \pm \beta$, $\alpha\beta$ will correspond to $\alpha' \pm \beta'$, $\alpha'\beta'$, while all elements of $K$ shall remain unchanged. These automorphisms form a group $G$, which is the *Galois group* of $\overline{K}$ with respect to $K$. The well known main theorem of the Galois theory is then the following.

*There exists a unique correspondence between the subgroups of $G$ and the subfields of $\overline{K}$ (containing $K$), such that to any subgroup $G'$ corresponds a subfield $K'$ consisting of all elements left invariant by $G'$, and conversely.*

Even for a *simple* Galois field, this theorem does not always hold. It can be shown that a necessary and sufficient condition is that $f(x)$ shall have no equal roots. Steinitz says, that an irreducible polynomial $f(x)$ is of the *first kind*, when all its roots are different, and of the *second kind*, when some of them are equal. It can then be shown, that *the main theorem will only hold for Galois fields, which can be obtained from $K$ by a series of adjunctions of the first kind.*

At first glance it seems surprising that an irreducible polynomial can have equal roots, since by the ordinary procedure one would then find that $f(x)$ had a factor in common with $f'(x)$. For certain fields of characteristic $p$ it can happen, however, that $f'(x)$ vanishes identically. To take a simple example, let us consider the field $K = P_p(t)$ consisting of all rational functions of $t$ with rational coefficients (mod $p$). In this field

$$f(x) = x^p - t$$

is irreducible and nevertheless we have

$$f(x) = (x - t^{1/p})^p, \quad f'(x) = 0.$$

Fields in which all polynomials are of the first kind have been called *separable.** All fields of characteristic 0 are separable, and among the fields of characteristic $p$ only those are separable in which the $p$th root of every element again belongs to the field. The prime-field $P_p$ is separable since by Fermat's theorem $a^p = a$.

* Steinitz says "vollkommen." I prefer the term separable introduced by B. L. van der Waerden.

These problems are closely connected with the so-called theorems of the *primitive element* (Abel's theorem) and the *finite number of subfields*. In the fields of ordinary algebraic numbers we have the theorem, that if a field $K'=K(\alpha, \beta, \cdots, \delta)$ is obtained from an algebraic field $K$ by the adjunction of a finite number of algebraic numbers, then there exists in $K'$ a primitive algebraic number such that $K'=K(\theta)$, and $K'$ will only have a finite number of subfields containing $K$. The same theorems can be shown to hold for a general field $K$ for a finite number of adjunctions of the first kind, and under certain conditions, specified by Steinitz, for adjunctions of the second kind. That these theorems do not hold for arbitrary algebraic adjunctions can be seen by the following example. Let $K=P_p(x, y)$ be the field obtained from the prime-field $P_p$ by two transcendental adjunctions. Then the field $K'=K(x^{1/p}, y^{1/p})$ has no primitive element. Any element $R=R(x^{1/p}, y^{1/p})$ will always satisfy an equation

$$R^p = \overline{R}(x, y),$$

where $\overline{R}(x, y)$ is an element of $K$. If, therefore, it were true that

$$x^{1/p} = f_1(R), \quad y^{1/p} = f_2(R),$$

we would obtain

$$x = \bar{f}_1(\overline{R}), \quad y = \bar{f}_2(\overline{R}),$$

and there would exist an algebraic relation between $x$ and $y$, contrary to hypothesis. The existence of an infinite number of subfields between $K$ and $K'$ can also easily be shown.

For fields in which the Galois theory holds, most of the ordinary conclusions can be drawn in an analogous way. In certain cases the fields of characteristic $p$ present difficulties; for example, the general quadratic equation

$$x^2 + u_1 x + u_2 = 0$$

cannot be solved by radicals in a field of characteristic 2.

6. *Infinite Galois Fields.* In §5 the conditions for the validity of the Galois theory have been completely determined for all Galois fields of finite rank. Let us now consider the Galois theory of Galois fields of infinite rank. The first investigations

of this kind are due to Dedekind* who in a well known paper considered the permutations of the field of all algebraic numbers. This field has a set of automorphisms of the power of the continuum, and by a special example Dedekind was able to prove that not all subgroups will correspond to fields.

Dedekind also considered, without great success however, the automorphisms of the field of all complex numbers, and made the conjecture that the only automorphism of this field besides the identity was the correspondence between conjugate elements. From some later investigations by Ostrowski† it follows that this is not correct, since any automorphism of the field of all algebraic numbers can be extended to an automorphism of the field of complex numbers.

The general theory of groups of infinite Galois fields (of the first kind) was developed with remarkable completeness by Krull.‡ He was able to show that even for Galois fields obtained by a countable number of adjunctions, the group has the power of the continuum, and while every subfield corresponds to a subgroup, not all subgroups will correspond uniquely to a subfield.

In order to find out which subgroups would correspond to subfields, Krull introduced various topological notions for groups, like limits for a set of automorphisms, limit points and neighborhoods. The main result can then be stated briefly as follows.

*A necessary and sufficient condition that a subgroup corresponds to a field in the way indicated by the main theorem is that the subgroup be closed in the topological sense, that is, contain all its limit-substitutions.*

It will lead too far to go into further details about these interesting investigations; I shall only mention that for non-commutative fields also groups of automorphisms can be introduced and various remarkable results can be deduced.

7. *The Notion of Absolute Value.* Among the various other

* R. Dedekind, *Ueber die Permutationen des Körpers aller algebraischen Zahlen*, Festschrift der Gesellschaft der Wissenschaften, Göttingen, 1901. Werke, vol. 2.

† A. Ostrowski, *Ueber einige Fragen der allgemeinen Körpertheorie*, Journal für Mathematik, vol. 143 (1913), pp. 255–284.

‡ W. Krull, *Galoissche Theorie der unendlichen algebraischen Erweiterungen*, Mathematische Annalen, vol. 100 (1928), pp. 687–698.

investigations concerning fields, I shall only mention the analysis of the notion of *absolute value*.* Kürschak† defines the absolute value $\|\alpha\|$ of a number $\alpha$ in a given field $K$ as a real number, such that $\|0\| = 0$, $\|\alpha\| > 0$ when $\alpha \neq 0$. Furthermore, we have

$$\|\alpha\beta\| = \|\alpha\| \cdot \|\beta\|$$

and

$$\|\alpha + \beta\| \leqq \|\alpha\| + \|\beta\| . \tag{4}$$

The absolute value corresponds in many ways to the *metric* in the theory of point sets; the inequality (4) corresponds to the triangular inequality.

When the absolute value is defined, convergence and limits can be introduced in the ordinary way. A series

$$\alpha_1, \alpha_2, \cdots, \alpha_n, \cdots \tag{5}$$

is said to be convergent if it satisfies $\|a_n - a_{n+k}\| < \epsilon$ for arbitrary $\epsilon$ and sufficiently large $n$; the series (5) has a limit $a$ if $\|a_n - a\| < \epsilon$.

Kürschak calls a field *perfect* if all convergent series have limits in the field. A perfect field can always be obtained by adjoining the convergent series to the field, corresponding to the construction of the real field from the rational field. Kürschak's main theorem is as follows.

*Every field in which an absolute value is defined, can be enlarged to a perfect, algebraically closed field.*

An example is the rational field and the complex field.

Ostrowski‡ has in a number of papers continued the investigations of Kürschak; one of his results is that the least algebraically closed field $K'$ of a perfect field $K$ can only be perfect if $K'$ is finite with respect to $K$.

The possible absolute values which can be defined for a given field are by no means unique. Let us consider the rational field $R$.

---

* Corresponding to the German "Bewertung."

† I. Kürschak, *Ueber Limesbildung und allgemeine Körpertheorie*, Journal für Mathematik, vol. 142 (1913), pp. 211–253.

‡ A. Ostrowski, Journal für Mathematik, vol. 143 (1913) pp. 255–284; ibid., vol. 147 (1917), pp. 191–204; Acta Mathematica, vol. 41 (1918), pp. 271–284.