ON THE DECOMPOSITION THEOREMS OF ALGEBRA

By Øystein Ore, Yale University.

We shall in the following give an account of certain new ideas regarding the foundation of the so-called abstract algebra. These ideas, which have been developed only in the last couple of years, throw new light upon several of the basic problems of algebra. It should, however, be mentioned already at the beginning, that their application is in no way limited to algebra. They have originated principally in connection with algebraic problems and in the following we shall stress the algebraic consequences, but there are already important applications to geometry, to point-set theory and to the foundation of quantum mechanics. Since the theory is a very recent one and since it is in a state of rapid development, the following lecture cannot be expected to give any complete evaluation of its importance for algebra or for its several other domains of applications. It should serve to demonstrate, however, that a very fertile field or mathematical investigation has been opened up.

Let us recall to begin with a few facts about *abstract algebra*. One may say that abstract algebra has been developed from ordinary algebra through the realization that the various algebraic theories may be derived from a small number of axiomatic rules, to a large extent the same for all algebraic theories. The axiomatic synthesis is, however, only one side of the abstract theory. Among its most notable achievements, I should prefer to mention the solution of what one may call the *completeness problem* in several important cases, namely the determination of all algebraic systems with given properties. As a classical example one may mention Steinitz' theory of commutative fields and the determination of all fields for which the Galois theory of equations is valid.

In algebra one deals with algebraic systems or spaces consisting of certain symbols called *elements*. For these elements certain operations are defined, usually in such a way that to any pair of elements another element is given uniquely. One may also consider more general systems in which certain subsets define other subsets according to given rules. Ordinarily one deals with operations satisfying some or all of the axioms for addition and multiplication and the various systems are classified accordingly as fields, rings, groups, moduli etc. Finally let us mention the notion of *isomorphism* which is of considerable importance in the following. Two systems are said to be isomorphic with respect to given operations when there exists a one-to-one correspondence between them preserving the results of those operations. The properties of two isomorphic systems are identical in respect to the given operations.

A fundamental problem is the deduction of *theorems of decomposition* for algebraic systems, i. e. the reduction of a system to simpler parts. As the simplest example of such a decomposition one may take the representation of a rational integer as the unique product of its prime factors. Similarly we have, according to Dedekind, a unique prime ideal factorisation for the ideals of an algebraic field of finite degree. Another almost as simple decomposition theorem is furnished by the basis theorem for Abelian groups. In this case the basis representation is not unique, but the cyclic subgroups occuring in two different basis representations have the same orders and hence are isomorphic.

For arbitrary algebraic systems one cannot expect decomposition theorems as simple as these. In commutative rings the ideal theory and the corresponding decomposition theorems were first developed by EMMY NOTHER.[1] From this theory follows her solution of the completeness problem to determine all commutative rings in which there exists a unique prime ideal factorisation. Among the further important contributors to the theory of ideals in commutative and non-commutative rings one may mention: KRULL, GRELL, KÖTHE, MORI, SCHMEIDLER, SONO, V. D. WAERDEN and others. We shall not describe in details any of these general decomposition theorems for ideals. Their importance may best be judged by the numerous applications: Algebraic geometry (DUBREIL, KAPFERER, LASKER, MACAULAY, SCHMEIDLER, V. D. WAERDEN), the theory of elimination (HENTZELT, HERMANN, NOETHER) algebraic differential and difference equations (RITT, RAUDENBUSH), linear differential and non-commutative polynomials (KRULL, LOEWY, NOETHER-SCHMEIDLER, ORE), the decomposition theory and arithmetic theory of linear algebras or hypercomplex systems (ARTIN, BRANDT, DEURING, DICKSON, SPEISER, SHODA, WEDDERBURN). The theory of reduction of matrices is based upon the decomposition theorems for moduli. In this connection one should mention E. Noether's *moduli of representation* (Darstellungsmoduln) and their applications to the representation of groups. Another general type of decomposition theorems has been obtained by Krull for the so-called *generalized Abelian groups*. They are moduli with certain operators or multipliers. The residue systems of one-sided ideals belong to this type of system.

[1] The references to the various investigations on ideal theory and other decomposition theorems may be found in the recent book by W. KRULL: *Idealtheorie*. Ergebnisse der Mathematik etc. v. 4 , Berlin 1935 or in ØYSTEIN ORE: *L'algèbre abstraite*, Actualités scient. et indust. Paris 1936.

The decomposition theorems we have mentioned have mostly been obtained under certain finiteness conditions. E. Noether assumes the so-called (descending) *chain condition* (Teilerkettensatz): Every chain of ideals

$$\mathfrak{A}_1 < \mathfrak{A}_2 < \cdots$$

breaks off after a finite number of terms. Still more restricted is the finite case where both ascending and descending chains are finite.

A few words should also be said about the decomposition theorems for groups. In the finite case we have the well-known theorem of Jordan-Hölder for composition and principal series. For the general case this theorem is replaced by the refinement theorem of Schreier-Zassenhaus. There also exists a decomposition theorem for the representation of a group by means of irreducible normal components. More difficult to prove is the theorem of Schmidt-Remak which states that if all chains of normal subgroups (or permissible subgroups in the case of groups with operators) are finite, then any two representations of a group as the direct product of direct indecomposable components is unique except for isomorphisms. Recently Kurosch has shown that this theorem is true for normal subgroups when only the descending chain condition is satisfied.

Even a superficial analysis of the various theorems of decomposition show their similarity in character. In all cases one deals with certain distinguished subsystems of the given system like normal subgroups, ideals, characteristic moduli etc. The decomposition theorems themselves refer mainly to properties of these distinguished subsystems while the properties of the elements of the original system play a minor role. This remark suggests the possibility of a further abstraction of the algebraic theories by introducing new systems whose elements are the subsystems themselves. These new systems which we shall define presently, shall be called *structures*. Our main object in the following is to show, that the decomposition theorems are only properties of these structures, while the properties of the elements of the original algebraic system are eliminated altogether. A consequence of this theory is naturally that it reduces the proofs to their essential foundation. More important is however that it gives new results and that it illuminates in new ways the character of the decomposition theorems. The situation is in many ways analogous to the familar one in *geometry*. A geometry is usually considered on the background of its points which are taken to be elements of an abstract space. However for the geometry and the geometric theorems these points are not the essential content. The geometric results refer to the properties of specified configurations like lines, planes, curves, surfaces and manifolds, cells, simplexes, neighbourhoods etc. This analogy to geometry is not a superficial one as we shall see, since it is actually based upon the fact that the axioms of the two theories to a large extent are the same. Hence we may also formulate our theory in saying that the decomposition theorems represent the results of a geometry of a simple type associated with the given algebraic system.

The idea that such a theory might be possible goes back to DEDEKIND[1] as do so many other fundamental ideas of abstract algebra. It occurs in connection with an investigation of the axiomatic foundation for the theorem of Jordan that in a group any two principal series of normal subgroups have the same length. In a group there exists to any two subgroups A and B a cross-cut (A, B) which is the maximal subgroup contained both in A and B. Similarly there exists a union $[A, B]$ which is the minimal subgroup containing both A and B. The union is generated by A and B, but it is not the element union of the two groups. A similar situation occurs in all algebraic systems. Hence we are led to define:

A *structure*[2] Σ is a system of element $A, B, \cdots$ having the property that to any pair A, B there exists a unique union $[A, B]$ and a unique cross-cut (A, B).

These operations satisfy the ordinary axioms

$$\begin{array}{ll} (A, B) = (B, A) & [A, B] = [B, A] \\ (A, A) = A & [A, A] = A \\ (A, (B, C)) = ((A, B), C), & [A, [B, C]] = [[A, B], C] \\ [A (A, B)] = A & (A, [A, B]) = A. \end{array}$$

On the basis of these axioms one defines the *inclusion relation* $A > B$ by the existence of either one of the two equivalent relations.

$$[A, B] = A, \quad (A, B) = B.$$

Usually a structure also contains an *all-element* O_0 and a *unit element* E_0 defined by the existence of the relations

$$[O_0, A] = O_0, (A, E_0) = E_0$$

for all A in Σ.

One may also obtain an equivalent definition of a structure by starting with a *semi-ordered* (partly ordered) set in the sense of HAUSDORF. In

[1] R. DEDEKIND: Über die von drei Moduln erzeugte Dualgruppe. Math. Ann. 53 (1900), Werke v. 2. pp. 371—403.

[2] DEDEKIND uses the word "Dualgruppe". Since the systems are not groups, this terminology is somewhat awkward. G. BIRKHOFF uses the term "lattice" (Gitter), which, however, has been used consistently in a different mathematical meaning. For this reason I have adopted the term structure which seems suggestive of the algebraic applications of the systems. KLEIN-BARMEN says "Verband".

such a set a transitive inclusion relation $A > B$ is defined for certain elements. A structure is then obtained by postulating the existence of a unique maximal element (A, B) contained in A and B and a unique minimal element $[A, B]$ containing A and B. It is also possible to extend any semi-ordered set under preservation of order into a structure as shown by MAC NEILLE[1] by introducing new elements by a method reminding of Dedekind cuts.

Our problem is now to investigate the properties of the structures defined by certain subsystems of algebraic systems. If one prefers the geometric point of view one may say that the structure represents the geometry of the subsystems. However, without further limitations on the structure one can say very little about general properties. The most important remark is that there exists a dualistic correspondence between cross-cut and union, and it seems that this dualism is the ultimate source for *theorems of duality* both in algebra and in geometry. In connection with the general properties of structures one should mention the investigations by KLEIN-BARMEN.[2]

To obtain theorems of decomposition it is necessary to impose further conditions on the structure. The case of a group may serve an illustration. While the set of all subgroups already form a structure, all decomposition theorems refer to the structure of normal subgroups. The reason for this lies in the fact that the latter structure satisfies a further condition given by Dedekind:

Dedekind axiom: If A, B and C are any three elements of the structure and $C > A$, then

$$(C, [A, B]) = [A, (C, B)]. \tag{1}$$

Any structure which satisfies the Dedekind axiom may be called a *Dedekind structure* or a *Dedekind geometry.*

The Dedekind axiom is satisfied in almost all instances of decomposition theorems in algebra. In most cases it is easily verified. As an example let $C > A$ and B be three normal subgroups of a group G. Any element of $[A, B]$ has the form $\alpha\beta$, where α and β belong to A and B respectively. An element of $(C, [A, B])$ must satisfy the relation

$$\gamma = \alpha\beta \tag{2}$$

[1] H. MAC NEILLE: Extensions of partially ordered sets. Proc. Nat. Acad. vol. 22 (1936) pp. 45—50.

[2] A complete list of the publications of this author on the subject of structures may be found in the latest article F. KLEIN-BARMEN: Dedekindsche und distributive Verbände. Math. Zeitschr. v. 41 (1936) pp. 261—280.

where γ is some element of C. Hence $\beta = \alpha^{-1} \cdot \gamma$ belongs both to B and to C and (2) shows that the left-hand side of (1) is contained in the right-hand. This proves our relation since the converse is true in any structure. In the same simple manner follows that the Dedekind axiom is satisfied for all one-sided or double-sided ideals in any ring. The Dedekind axiom may be formulated in several ways. We shall only mention the equivalent relations

$$([A, B], [A, C]) = [A, (B, [A, C])]$$
$$[(A, B), (A, C)] = (A, [B, (A, C)])$$

and the *self-dualistic formulation*

$$[(A, B), (C, [A, B])] = ([A, B], [C, (A, B)]). \tag{3}$$

All these relations hold for arbitrary elements A, B, C of the structure. The various possible relations may also be united in the statement that in a Dedekind structure three elements A, B, C generate a structure containing in general 28 different elements. From a geometric point of view these various relations may be said to represent geometric theorems.

The principal result of Dedekind may now be stated as follows: a chain

$$A > A_1 > \cdots\cdots > A_n > B$$

of elements in the structure shall be called a ***principal chain,*** when each term is ***prime*** over the next, i. e. there is no term in the structure between them. The theorem is then: ***In a Dedekind structure all principal chains between two elements A and B have the same length.*** Conversely: The necessary and sufficient condition that this be true for a finite structure Σ and all its substructures is that Σ be a Dedekind structure.

Almost identical considerations to these were made by Garret Birkhoff.[1] At this point one should also mention some similar investigations by Kurosch[2] in regard to another theorem of decomposition. An element A in Σ may be said to be decomposable if there exists a representation

$$A = [B, C], \quad A > B, \quad A > C,$$

and indecomposable otherwise. Kurosch then proves that if an element in a Dedekind structure can be represented as the union of a finite number

[1] Garret Birkhoff: On the combination of subalgebras. Proc. Cambridge Phil. Soc. v. 29 (1933) pp. 441—464. Note on the paper: On the combination of subalgebras ibid. v. 30 (1934) p. 200. Applications of lattice algebra, ibid. v. 30 (1934) pp. 115—122.

[2] A. Kurosch: Durchschnittsdarstellungen mit irreduziblen Komponenten in Ringen und in sogenannten Dualgruppen. Mathematičeski Sbornik v. 42 (1935) pp. 613—616.

of indecomposable elements, then any two such representations must contain the same number of components. This is a part of a wellknown decomposition theorem in ideal theory.

While these theorems give an approximation to the corresponding algebraic theorems it is obvious that something essential is lacking. For instance in the formulation of the ordinary theorems of Jordan-Hölder one emphasises that the quotient groups are isomorphic in some order. This statement already contains two notions for which no suitable definition has been provided in the structure, namely *quotient group* and *isomorphism.*

In a recent paper[1] in which I have taken up this question of the application of structures to algebra, it has been shown how these difficulties may be overcome. The question of an analogue to quotient groups or residue system is fairly simple. To any structure Σ one can construct a *quotient structure* Σ' in the following manner. To all pairs of elements $A > B$ in Σ we associate a *quotient* $\mathfrak{A} = A/B$. The set of all quotients is made into a structure Σ' by defining for

$$\mathfrak{A}_1 = A_1/B_1, \quad \mathfrak{A}_2 = A_2/B_2$$

the cross-cut and union

$$(\mathfrak{A}_1, \mathfrak{A}_2) = (A_1, A_2)/(B_1, B_2), \quad [\mathfrak{A}_1, \mathfrak{A}_2] = [A_1, A_2]/[B_1, B_2].$$

To each quotient $\mathfrak{A} = A/B$ is associated a substructure of Σ, namely the set of all elements containing B and contained in A.

If the original structure is a Dedekind structure then the quotient structure Σ' has the same property. In the following we draw into our consideration the whole quotient structure Σ' rather than the original structure. The algebraic analogy is obvious. It should also be mentioned that it is convenient to introduce the *product* of certain quotients by putting

$$\mathfrak{A} \times \mathfrak{B} = A/C$$

when

$$\mathfrak{A} = A/B, \quad \mathfrak{B} = B/C.$$

On the face of it it seems more difficult to find a suitable substitute for the notion of isomorphism, since the isomorphism of two algebraic systems is essentially a property of their elements. The solution lies in the fact that for the decomposition theorems one needs only a special kind of isomorphism, namely isomorphism defined through the iterated use of the so-called *second law of isomorphism.* This law says that in a group or ring the quotient groups or residue rings

[1] Øystein Ore: On the foundation of abstract algebra, Part I, Annals of Math. v. 36 (1935) pp. 406—437, Part II, v. 37 (1936) pp. 265—292.

$$\mathfrak{A} = [A, B]/A, \quad \mathfrak{B} = B/(A, B) \tag{4}$$

are isomorphic. If one considers (4) to be quotients in a Dedekind structure, then one can prove the fundamental theorem, that *the two structures associated with* $\mathfrak{A}$ *and* $\mathfrak{B}$ *are structure isomorphic*, i. e. there exists a one-to-one correspondence between them preserving the result of union and cross-cut. It is convenient to say that in (4) the quotient $\mathfrak{A}$ has been obtained by *extension* from $\mathfrak{B}$ and conversely $\mathfrak{B}$ has been obtained by *reduction* from $\mathfrak{A}$. We define then that two quotients $\mathfrak{A}$ and $\mathfrak{A}'$ are similar if one is obtainable from the other through a series of reductions and extensions.

This notion of similarity of two quotients replaces and implies ordinary isomorphism in the applications to algebraic systems. It completes our program of formalisation of the algebraic theory. It is now possible to formulate and prove general decomposition theorems for Dedekind structures containing as special cases all the ordinary algebraic decomposition theorems to their full extent. Various new decompositions are also obtained, but we shall not discuss any of these results in detail. Most interesting is perhaps the theorem about *direct decompositions* corresponding in the case of groups to the Schmidt-Remak theorem. This theorem is easily proved in the ordinary finite case. When only the descending chain condition is satisfied, peculiar difficulties arise and the theorem is only valid under certain restriction. This was, however, to be expected according to investigations of Steinitz and Krull[1] in the special case of moduli whose coefficients are algebraic integers. The formulation of the theorem of Jordan-Hölder may be of interest. The application of quotient products gives it a form reminding strongly of the ordinary arithmetic factorisation theorem: *If a quotient* $\mathfrak{A}$ *may be represented in two ways as the product of prime quotients*

$$\mathfrak{A} = \mathfrak{P}_1 \times \ldots \times \mathfrak{P}_r = \mathfrak{Q}_1 \times \ldots \times \mathfrak{Q}_r$$

then both factorisations have the same number of factors similar in pairs. The general theorem of Schreier-Zassenhaus may be expressed: *If a quotient is factored in two ways*

$$\mathfrak{A} = \mathfrak{B}_1 \times \ldots \times \mathfrak{B}_r = \mathfrak{C}_1 \times \ldots \times \mathfrak{C}_s$$

then these factors may be factored further such that both sides have the same number of factors similar in pairs.

[1] A further discussion of this theorem will be found in a paper which is to appear shortly in Duke Mathematical Journal. [Vol. 2 (1936), pp. 581—596.]

We have deduced our decomposition theorems only under the assumption of the Dedekind axiom and hence they have been obtained in their most general form. For many algebraic systems we have however more special decomposition theorems like in E. NOETHER's ideal theory, in rings with unique factorisation, in Abelian groups, etc. This is due to further conditions satisfied by the structures associated with the system. We shall not discuss these properties here, but only observe that they may be used to classify the algebraic systems from a new point of view.

Another remark which may be of interest is the following: When the theory of structures is applied to *ideal theory* one obtains only decomposition theorems regarding cross-cut and union while the existence of a *multiplication* only plays a minor role in the most general cases. In the special cases where the multiplicative decomposition are of importance it is mostly possible to define multiplication on the basis of the special structure axioms and hence also these theorems may be obtained from conditions on the structure.

The theory of structures brings forth another interesting property of algebraic system, namely their *self-dualistic character.* We indicated the dualism between union and cross-cut in a structure. The further conditions which the structures corresponding to algebraic systems satisfy, preserve this dualism because the conditions are self-dualistic, that is they remain identically the same when cross-cut and union are interchanged. The Dedekind axiom may serve as our first example. The formulation (3) immediately shows its self-dualistic character. The *distributive structures* in which the much stranger *distributive law*

$$(5) \qquad (A, [B, C]) = [(A, B), (A, C)]$$

holds, form another important type of structures. A special case to which they apply is to ideals in rings with unique factorisation. The self-dualistic formulation of the distributive law (5) is

$$([A, B], [B, C], [C, A]) = [(A, B), (B, C), (C, A)]$$

a relation which not even in numbertheory is a familar one. The distributive structures have been studied particularly by G. BIRKHOFF.[1] One of the principal results is, that to a finite distributive structure there exists an abstract set S. such that the structure is structure isomorphic to the ordinary set-theoretical cross-cut and union of some of the subsets of S. Related to these investigations are certain results by MAC NEILLE[2] on the possibility of imbedding semi-ordered sets or structures with given properties.

[1] See the first paper quoted in note 1 page 242.

[2] Loc. cit.

Another type of structures are the *completely reducible* (*flat*, *complemented*) structures in which there exists to each element A a (not necessarily unique) *complement* $\bar{A}$ such that

$$(A, \bar{A}) = E_0, \ [A, \bar{A}] = O_0.$$

The property of being completely reducible is also seen to be self-dualistic. Such structures, which have several algebraic applications, have been studied by G. BIRKHOFF[1] and the author[2].

If one requires that a distributive structure shall be completely reducible one obtains the well-known *Boolean algebras*. The application of these structures to logic and the calculus of classes is so familar that it need not be mentioned here. It is of interest however that a Boolean algebra is structure isomorphic with the element cross-cut and union of the subsets of a certain set associated with the structure. This property has been used by STONE[3] to base the theory of *topological spaces* directly upon the Boolean algebras.

This last remark brings us back to our former point of view on the close connection between geometry and the theory of structures. This is however most clearly illustrated by the axiomatic foundation of *projective geometry* by means of structures which has been given within the last year both by G. BIRKHOFF[4] and MENGER.[5] In our former terminology the main ideas of these papers are easily explained. One begins with a completely reducible Dedekind structure. Furthermore it is supposed that the descending chains have a finite maximal length n, eventually defining the dimension of the geometry. In addition only one further axiom is needed:

Axiom of irreducibility (tertium datur). The complement of an element is not unique, except for E_0 and O_0.

In the construction of projective geometry on this basis the element of the structure represents the various configurations like points, lines, planes. The cross-cut signifies common part and the union the least configuration containing two given ones. The Dedekind axiom together

[1] GARRET BIRKHOFF: Combinatorial relations in projective geometries. Annals of Math. v. 36 (1935) pp. 743—748.

[2] ORE, loc. cit. Part 2.

[3] M. STONE: Boolean algebras and their application to topology. Proc. Nat. Acad. v. 20 (1934) pp. 197—202. See also A. TARSKI: Zur Grundlegung der Boole'schen Algebra I. Fundamenta Mathematicae v. 24 (1935) pp. 177—198.

[4] See note 1 this page.

[5] K. MENGER: New Foundations of projective and affine geometry. Annals of Math. v. 37 (1936) pp. 456—482. One of the principal axioms of Menger is easily seen to be equivalent to the Dedekind axiom.

with the finiteness condition classifies the elements as to dimension by means of the length of the corresponding Jordan-Hölder chain. The axiom of irreducibility insures the existence of at least three points on each line. Beside its simplicity this axiomatic theory possesses certain advantages from a systematic point of view. In HILBERT's foundation of three-dimensional geometry one starts with three different types of elements, points, lines and planes. In VEBLEN and YOUNG's treatment the points play an exceptional role, all other elements being considered as classes of points. By the foundation on structures all configurations appear in a symmetric manner.

The situation is quite analogous to our former theory of algebraic systems where we have reduced the importance of the elements while here the same thing is being done in regard to the points.

MENGER also gives a similar foundation for *affine geometry* through the introduction of a certain paralel axiom in structures.

To obtain the ordinary projective geometry of finite dimension a strong finiteness condition was required. Recently v. NEUMANN[1] has considered the case where this condition is omitted and replaced only by certain requirements on the existence and properties of union and cross-cut of an infinite number of elements. In this case one obtains what one may call a *continuous projective geometry* with a dimension function for the elements which takes on all values in a continuous range from 0 to 1. Hence there is no classification of the elements as points, lines etc. This geometry at the first glance seems curious and far-fetched. It has been shown however in a joint paper by MURRAY and v. NEUMANN[2] that this geometry has important applications to the theory of operators in Hilbert space and to quantum mechanics because the general operator theory in Hilbert space naturally may be based upon such a geometry. Various central problems of the theory may be solved by this new approach.

[1] J. v. NEUMANN: Continuous geometry. Examples of continuous geometry. Proc. Nat. Acad. v. 22 (1936) pp. 92—100, 101—108.

[2] F. J. MURRAY and J. v. NEUMANN: On rings of operators. Annals of Math. v. 37 (1936) pp. 116—229.