ABSTRACT IDEAL THEORY*

BY OYSTEIN ORE

1. *Introduction.* Abstract ideal theory is a branch of algebra which has come into prominence only in recent years; its importance for algebraic problems and also for branches of mathematics outside of algebra proper has however been increasingly recognized; it seems established that the ideals, corresponding in many ways to the normal subgroups in the theory of groups, are the most convenient building stones in a large number of algebraic structures.

In the following I have tried to give a survey of the most important problems and results, but it should be realized that an account of this kind must necessarily be incomplete, since the field is too wide and too diverse to be covered in a single lecture. To limit the subject, only commutative ideal theory will be considered; demonstrations have been omitted, although reluctantly, since an occasional proof will often clarify more than any explanation the tools and working methods of a theory. Another difficulty in this case lies in the fact that the theory itself to a large extent is still in an evolutionary stage and has not reached the harmonious form it will probably assume later on. Only for domains in which the finite chain condition holds does it seem to have arrived at some degree of perfection. Historically several of the fundamental ideas can be traced to the work of Dedekind, Kronecker, and Lasker, but the main contributions to the theory have been made in the last ten years by E. Noether, Krull, van der Waerden, Henzelt, Grell, Stiemke, and others.

The first part of the paper contains some of the main properties of ideals, operations on ideals, quotient rings, and isomorphisms; then follows a discussion of prime and primary ideals and the consequences of the finite divisor chain condition. The four principal ideal representations by E. Noether are treated fairly completely, and to illustrate these abstract de-

* Symposium lecture delivered at the meeting of the Society in New York, April 14, 1933.

composition theorems I have given some of their applications to algebraic manifolds and the theorems of Hilbert and M. Noether. The rings in which every ideal is the product of prime ideal powers, that is, the integrally closed rings, are mentioned next; in the last part I have given some results for rings in which the chain condition does not hold and also discussed some of the novel ideas of Krull on a more topological introduction and definition of ideals by means of absolute values.

2. *Ideals and Operations on Ideals.* In the following we shall study the structural properties of an abstract ring R; we assume that R has the ordinary ring properties, that is, it is an abelian group with respect to addition, and that multiplication is associative, distributive, and commutative. An *ideal* $\mathfrak{a}$ in R is a subring of R with the following properties:

(a) When α and β are elements of R belonging to $\mathfrak{a}$, then $\alpha \pm \beta$ belongs to $\mathfrak{a}$.

(b) For an arbitrary element λ in R and α in $\mathfrak{a}$ the product $\lambda\alpha$ belongs to $\mathfrak{a}$.

This definition is due to Dedekind. An important class of ideals are the *principal ideals* (α) generated by a single element α in R; (α) must contain all sums $\alpha+\alpha \cdots$, and all multipla $\lambda\alpha$ such that every element can be written in the form $\alpha' = \lambda\alpha + n\alpha$, where n is a rational integer; when R contains a unit element ϵ we obtain the simpler representation $\alpha' = \lambda\alpha$. Another class of ideals are those having an *ideal basis*, $\mathfrak{a} = (\alpha_1, \cdots, \alpha_r)$; every element in $\mathfrak{a}$ can then be represented in the form

$$\alpha' = \lambda_2\alpha_1 + \cdots + \lambda_r\alpha_r + n_1\alpha_1 + \cdots + n_r\alpha_r,$$

where the λ_i belong to R and the n_i are rational integers. We suppose in the following that R does not consist only of the zero element; every ring then has at least two ideals, the *zero ideal* $\mathfrak{n} = (0)$ and the *unit ideal* R; when R contains a unit element then $R = (\epsilon)$ is a principal ideal.

The fact that an element α belongs to an ideal $\mathfrak{a}$ is usually expressed by a congruence $\alpha \equiv 0 \pmod{\mathfrak{a}}$; the more general congruence $\alpha \equiv \beta \pmod{\mathfrak{a}}$ denotes that $\alpha - \beta$ belongs to $\mathfrak{a}$. When all elements of an ideal $\mathfrak{b}$ belong to $\mathfrak{a}$, we write $\mathfrak{b} \equiv 0 \pmod{\mathfrak{a}}$ or $\mathfrak{a} > \mathfrak{b}$ and say that $\mathfrak{b}$ is *contained in* $\mathfrak{a}$ or $\mathfrak{a}$ is a *divisor of* $\mathfrak{b}$. It is obvious that the zero ideal $\mathfrak{n}$ is divisible by all ideals and that R divides all ideals.

The application of ideals to algebraic problems is based upon the existence of various processes by means of which one can derive new ideals from a set of given ideals. There are four fundamental ways of combining two given ideals $\mathfrak{a}$ and $\mathfrak{b}$ into new ideals, and since they will be used constantly in the following, their definitions and simplest properties shall be mentioned here.

(i). *The cross-cut* or *greatest common divisor* $\mathfrak{d}=(\mathfrak{a},\mathfrak{b})$ of two ideals consists of all elements of the form $\delta=\alpha+\beta$, where α belongs to $\mathfrak{a}$ and β to $\mathfrak{b}$; it has the properties

$$(1)\qquad \mathfrak{a}\equiv 0,\ \mathfrak{b}\equiv 0 \pmod{\mathfrak{d}},$$

and $\mathfrak{d}\equiv 0 \pmod{\mathfrak{d}_1}$ for all other ideals $\mathfrak{d}_1$ for which (1) holds.

(ii). The *union* or *least common multiplum* $\mathfrak{m}=[\mathfrak{a},\mathfrak{b}]$ consists of all elements contained both in $\mathfrak{a}$ and $\mathfrak{b}$; one has

$$(2)\qquad \mathfrak{m}\equiv 0 \pmod{\mathfrak{a}},\qquad \mathfrak{m}\equiv 0 \pmod{\mathfrak{b}},$$

and $\mathfrak{m}\equiv 0 \pmod{\mathfrak{m}}$ for all other ideals $\mathfrak{m}$ satisfying (2).

(iii). The *product* $\mathfrak{a}\mathfrak{b}$ consists of all elements $\gamma=\Sigma_1'\alpha\beta$ representable as the sum of products $\alpha\beta$, where α belongs to $\mathfrak{a}$ and β to $\mathfrak{b}$; the multiplication of ideals is obviously associative and commutative. When $\mathfrak{c}=\mathfrak{a}\mathfrak{b}$, we say that $\mathfrak{a}$ is a *factor* of $\mathfrak{c}$; it is seen that then $\mathfrak{c}\equiv 0 \pmod{\mathfrak{a}}$ so that $\mathfrak{a}$ is also a divisor of $\mathfrak{c}$, but not conversely. From the former definitions one concludes

$$\mathfrak{a}(\mathfrak{b},\mathfrak{c})=(\mathfrak{a}\mathfrak{b},\mathfrak{a}\mathfrak{c}),\qquad \mathfrak{a}\mathfrak{b}\equiv 0 \pmod{[\mathfrak{a},\mathfrak{b}]},$$

and it can also be shown that

$$[\mathfrak{a},\mathfrak{b}](\mathfrak{a},\mathfrak{b})\equiv 0 \pmod{\mathfrak{a}\mathfrak{b}}.$$

(iv). The *ideal quotient* $\mathfrak{a}:\mathfrak{b}$ is the set of all elements γ in R such that $\gamma\beta$ belongs to $\mathfrak{a}$ for any element β in $\mathfrak{b}$. If $\mathfrak{c}=\mathfrak{a}:\mathfrak{b}$, then

$$(3)\qquad \mathfrak{c}\mathfrak{b}\equiv 0 \pmod{\mathfrak{a}},$$

and $\mathfrak{c}_1\equiv 0 \pmod{\mathfrak{c}}$ for any other ideal $\mathfrak{c}_1$ satisfying (3). Among the most important properties of the ideal quotient are the following:

$$\mathfrak{a}:\mathfrak{b}=\mathfrak{a}:(\mathfrak{a},\mathfrak{b}),$$
$$[\mathfrak{a},\mathfrak{b}]:\mathfrak{c}=[\mathfrak{a}:\mathfrak{c},\mathfrak{b}:\mathfrak{c}],$$
$$(\mathfrak{a}:\mathfrak{b}):\mathfrak{c}=(\mathfrak{a}:\mathfrak{c}):\mathfrak{b}=\mathfrak{a}:\mathfrak{b}\mathfrak{c}.$$

All the operations introduced here can of course be extended to the case of an arbitrary finite number of ideals.

3. *Quotient Rings.* Let $\mathfrak{a}$ be an ideal and let us divide all of the elements of R into classes (mod $\mathfrak{a}$) by stipulating that two elements α and α_1 belong to the same class $\bar{\alpha}$ if and only if $\alpha \equiv \alpha_1$ (mod $\mathfrak{a}$). The sum and product of two classes $\bar{\alpha}+\bar{\beta}$ and $\bar{\alpha}\bar{\beta}$ are then defined as the classes containing $\alpha+\beta$ and $\alpha\beta$; by this definition the set of all residue classes forms a commutative ring, which we denote by $R/\mathfrak{a}$ and call the *quotient ring* or *ring of residue classes* of R with respect to $\mathfrak{a}$.

At this point it becomes clearer why we have chosen, from the beginning, to study ideals among the various possible types of subrings in R: *the ideals are the only subrings for which the quotient ring exists.* The ideals correspond to the normal subgroups in the group theory, these being the only sub-groups for which a quotient group exists. This analogy between ideals and normal sub-groups pervades the whole theory of ideals and we shall see several instances of it in the following; let us mention as an example: Every ideal $\bar{\mathfrak{c}}$ in the quotient ring $R/\mathfrak{a}$ is an ideal $\mathfrak{c}$ in R containing $\mathfrak{a}$ when considered as a set of elements in R and conversely.

This analogy appears most clearly in the study of homeomorphisms of rings. We say that R corresponds *homeomorphically* to a ring R' when to every element α in R there corresponds a unique α' in R' such that $\alpha \pm \beta$ corresponds to $\alpha' \pm \beta'$ and $\alpha\beta$ to $\alpha'\beta'$, while conversely there exists at least one α to each α'. When the homeomorphism is a one-to-one correspondence we say that R and R' are *isomorphic*; a homeomorphism is usually denoted by $R \sim R'$ and an isomorphism by $R \cong R'$.

In the case of a homeomorphism between R and R', one finds that all elements in R corresponding to the zero element $0'$ in R' form an ideal $\mathfrak{a}$ in R since from $\alpha \rightarrow 0'$, $\alpha_1 \rightarrow 0'$ follows $\alpha \pm \alpha' \rightarrow 0'$ and $\lambda\alpha \rightarrow 0'$ for an arbitrary λ in R. All the elements in an arbitrary residue class $\bar{\gamma}$ (mod $\mathfrak{a}$) in R must then correspond to the same element γ' in R and this correspondence is easily seen to be an isomorphism. This gives the fundamental theorem on the homeomorphisms of rings. *Every ring homeomorphic to R is isomorphic to a residue ring $R/\mathfrak{a}$, where $\mathfrak{a}$ is an ideal in R, and every such residue ring is homeomorphic to R.* The second part of the theorem is evident.

It should be observed that the construction of residue rings and homeomorphic rings is a very familiar process in algebra and even in analysis. Let us consider, as an example, the construction of the field of real numbers K from the field k of rational numbers. One forms the ring R of all convergent sequences $\alpha=(a_0, a_1, \cdots)$, where the a_i are rational numbers. The set of all sequences having the limit zero is an ideal σ in R. Next one proceeds to identify all zero sequences, that is, one constructs the quotient ring R/σ and after showing that this ring is a field, K is defined by the relation $K\cong R/\sigma$. The same process can obviously be applied in any ring in which an absolute value or the notion of a limit can be defined.

I also mention that from the definitions (i) and (ii) one can derive a second fundamental theorem on the isomorphisms of rings expressible in the formula

$$(\mathfrak{a}, \mathfrak{b})/\mathfrak{a} \cong \mathfrak{b}/[\mathfrak{a}, \mathfrak{b}]. \tag{4}$$

4. *Prime Ideals.* A natural generalization of prime ideals in the theory of algebraic numbers would be to define a *prime ideal* $\mathfrak{p}$ as *an ideal without divisors*, that is, there shall exist no ideal except $\mathfrak{p}$ itself and R containing it. A prime ideal might then also be called a *maximal ideal* and according to a remark in §3 the quotient ring $R/\mathfrak{p}$ must be simple, that is, have no ideals different from the ring itself and the zero ideal. A simple analysis yields the following result.* *A simple ring is a field or a ring isomorphic to the finite ring*

$$R_p = 0, p, 2p, \cdots, (p-1)p \pmod{p^2}. \tag{5}$$

This definition of a prime ideal was actually used by Sono, one of the earliest writers on abstract ideal theory. However, the applications of the theory have shown that this definition is too limited and that a more satisfactory definition is obtained by using another property of prime numbers. A prime ideal $\mathfrak{p}$ is an ideal such that from $\alpha\beta\equiv 0 \pmod{\mathfrak{p}}$ follows $\alpha\equiv 0$ or $\beta\equiv 0 \pmod{\mathfrak{p}}$. One may also state this definition in an equivalent form: *from an ideal relation* $\mathfrak{b}\mathfrak{a}\equiv 0 \pmod{\mathfrak{p}}$ *follows* $\mathfrak{b}\equiv 0$ or $\mathfrak{a}\equiv 0 \pmod{\mathfrak{p}}$, or finally as a property of the residue ring: *a prime ideal is an ideal such that the residue ring $R/\mathfrak{p}$ is a domain of integrity, that is, has no divisors of zero.*

* Sono, Memoirs of the College of Science, Kyoto, vol. 2 (1917).

In the following we shall adopt the last definition of a prime; it is easily seen that it is not equivalent to the former since the zero ideal $\mathfrak{n}$ in (5) is a prime ideal by the first definition, $R_p/\mathfrak{n} \cong R_p$ being simple and yet $R_p^2 = \mathfrak{n}$.

A very characteristic, but at the first glance somewhat surprising, property of our prime ideals is that they may have divisors. As an example let us consider the ring of all polynomials in two variables x and y with coefficients in a field K. The ideal $\mathfrak{p}_1 = (y)$ is seen to be prime and to consist of all polynomials divisible by y; the residue ring is the set of all polynomials in x. The ideal $\mathfrak{p}_2 = (x, y)$ is a prime ideal dividing $\mathfrak{p}_1$; it consists of all polynomials without constant term, and the residue ring is K. We shall see later that by certain geometrical applications, if there exists a chain

$$\mathfrak{p}_0 < \mathfrak{p}_1 < \cdots < \mathfrak{p}_r < R$$

of prime ideal divisors of a prime ideal $\mathfrak{p}_0$ such that no further prime ideal can be inserted in the chain, then r coincides with the dimension of the manifold corresponding to $\mathfrak{p}_0$.

5. *The Chain Condition.* We have introduced ideals in order to study the structure of a ring R and its subrings. In a special case, as for instance the ring of all integers in a finite algebraic field, we have the fundamental theorem that every ideal is uniquely representable as the product of prime ideals. For more general rings a result of this simple nature cannot be expected as examples show; as a matter of fact, the ideal theory for the most general rings is so complicated that it is at the present time not fully mastered. We shall therefore have to impose a condition on the rings we consider; this condition brings us closer to the case of ideals in algebraic fields, but it is at the same time sufficiently general to include the most important rings in algebra. We shall call it the *condition of finite divisor chains* or simply *the chain condition.*

Every chain of ideals $\mathfrak{a}_1 < \mathfrak{a}_2 < \cdots$, *each dividing the preceding, must break off after a finite number of terms.* One can also put the condition in the form, that if an infinite chain $\mathfrak{a}_1 \leqq \mathfrak{a}_2 \leqq \cdots$ exists, then (from a certain point on) all ideals must be equal. The chain condition corresponds to the condition usually imposed by the study of groups, that the series of composition shall be of finite length. The condition is obviously satisfied in rings of integers in a finite algebraic field, since all ideals have only a finite number of divisors.

One may state the finite chain condition in a different manner, which is sometimes more useful for applications. *When the chain condition holds for the ideals in a ring R, then every ideal has a finite ideal basis and conversely.* Suppose that the chain condition holds and let $\mathfrak{a}$ be an ideal in R; when α_1 is an element of $\mathfrak{a}$, then $\mathfrak{a}=(\alpha_1)$ or there exists an element α_2 in $\mathfrak{a}$, but not in (α_1); then we have $\mathfrak{a}=(\alpha_1, \alpha_2)$ or there exists an α_3 in $\mathfrak{a}$ not contained in (α_1, α_2), and so on. This process must finally give us a basis for $\mathfrak{a}$ since

$$(\alpha_1) < (\alpha_1, \alpha_2) < (\alpha_1, \alpha_2, \alpha_3) < \cdots$$

breaks off. Let us suppose conversely that every ideal has a basis and let $\mathfrak{a}_1 \leqq \mathfrak{a}_2 \leqq \cdots$ be an infinite chain of ideals. The union of all ideals $\mathfrak{a}_i$ is an ideal $\mathfrak{b}=(\beta_1, \cdots, \beta_r)$ in R, and since each β_i belongs to an ideal $\mathfrak{a}_j$ and to all following ideals, one must have $\mathfrak{a}_k=\mathfrak{b}$ from a certain index k.

6. *Irreducible Ideals.* The idea of decomposition theorems for ideals in rings where unique decomposition into prime ideal factors does not exist, seems to have originated with Dedekind; Lasker* realized their importance for polynomial ideals and proved the existence of a decomposition into primary components; an account of Lasker's work can be found in Macaulay's tract: *Algebraic Theory of Modular Systems.* The first general investigation of the decomposition of ideals in rings (satisfying the chain condition) is due, however, to E. Noether;† in the following, we shall give the principal results which have been obtained.

An ideal $\mathfrak{a}$ is said to be *reducible* when it can be represented as the union $\mathfrak{a}=[\mathfrak{b}, \mathfrak{c}]$ of two proper divisors $\mathfrak{b}$ and $\mathfrak{c}$; $\mathfrak{a}$ is *irreducible* when no such representation exists. When $\mathfrak{a}$ is reducible, the divisors $\mathfrak{b}$ and $\mathfrak{c}$ may be decomposed further, and from the chain condition, it follows that one can finally obtain a representation

$$\mathfrak{a} = [\mathfrak{a}_1, \mathfrak{a}_2, \cdots, \mathfrak{a}_r], \tag{6}$$

* Mathematische Annalen, vol. 60 (1905).

† Mathematische Annalen, vol. 83 (1921).

where all $\mathfrak{a}_i$ are irreducible. It may occur that some of the ideals $\mathfrak{a}_i$ in the representation (6) are superfluous, $\mathfrak{a}_i$ being a divisor of the union of the remaining ideals; we shall suppose that all such ideals are omitted. It may also happen that a component can be replaced by a proper divisor. When all such reductions have been made, we say that (6) is a *reduced representation of* $\mathfrak{a}$ *by means of irreducible components.* This is the first decomposition given by E. Noether; it is usually not unique, but one can show: *The number of irreducible components in two different reduced representations is always the same.*

7. *Primary Ideals.* In the ring of rational integers the reduced representation (6) corresponds to the representation of an integer as the product or least common multiplum of prime powers. It may, therefore, be natural to seek a connection between the reduced representation and the prime ideals dividing $\mathfrak{a}$; this connection is obtained through the introduction of *primary ideals.* These ideals form a generalization and a substitute for the prime ideal powers in the general case and reduce to them in the case of unique prime ideal factorization. *An ideal* $\mathfrak{q}$ *is said to be primary if a congruence* $\alpha\beta\equiv 0 \pmod{\mathfrak{q}}$, *where* $\alpha\equiv 0 \pmod{\mathfrak{q}}$, *implies the existence of an exponent k such that* $\beta^k\equiv 0 \pmod{\mathfrak{q}}$. When $k=1$ for all elements in R, then $\mathfrak{q}$ is a prime ideal. To every primary ideal $\mathfrak{q}$ there exists, as for the prime powers, a unique prime ideal $\mathfrak{p}$ associated with it; this prime ideal is defined as the set of all elements π in R having the property that a power π^2 belongs to $\mathfrak{q}$. A simple study shows that these elements actually form an ideal which must be prime. The definition of $\mathfrak{p}$ and the primary ideal $\mathfrak{q}$ shows that a congruence $\alpha\beta\equiv 0 \pmod{\mathfrak{q}}$, where $\alpha\equiv 0 \pmod{\mathfrak{q}}$, implies that β belongs to $\mathfrak{p}$.

Since we suppose that the chain condition holds, there exists a representation $\mathfrak{p}=(\beta_1, \cdots, \beta_2)$. A power of each β_i belongs to $\mathfrak{q}$ according to definition and a power of $\mathfrak{p}$ must consequently also be divisible by $\mathfrak{q}$. *To every primary ideal* $\mathfrak{q}$ *there belongs a unique prime such that*

$$\mathfrak{p}, \mathfrak{q} > \mathfrak{p}^r. \tag{7}$$

One might have used the relation (7) to define a primary ideal and its corresponding prime ideal. A primary ideal is sometimes defined by an ideal condition, namely, that the ideal congruence

$$\mathfrak{a}\mathfrak{b} \equiv 0 \pmod{\mathfrak{q}}, \quad \mathfrak{a} \not\equiv 0 \pmod{\mathfrak{q}},$$

shall imply $\mathfrak{b}^k \not\equiv 0 \pmod{\mathfrak{q}}$. An ideal having this property is said to be *strongly primary*; while the former definition yields *weakly primary* ideals. The two concepts are identical in rings in which the chain condition holds.

The study of the structure of primary ideals seems to be one of the most important problems in abstract ideal theory. Various authors have dealt with this problem directly or with questions which can be interpreted in this way. I shall only mention papers by Sono, Schmeidler, van der Waerden, and a series of contributions by Krull. The problem is equivalent to the investigation of *primary rings*, that is, the rings of residue classes of primary ideals. The definition of a primary shows that these rings have the characteristic property that a power of every divisor of zero must vanish.

8. *Decomposition Theorems.* We now return to the representation (6) of an ideal by means of irreducible components. It can be shown, that *every irreducible ideal is primary*; each component, consequently, has a characteristic prime ideal and it can be proved, furthermore, that not only is the number of irreducible components in any representation (6) of an ideal $\mathfrak{a}$ the same, but also the corresponding prime ideals must be the same and have the same multiplicity.

Another theorem on primary ideals is the following. *The union of primary ideals belonging to the same prime ideal is again primary, but the union of primary ideals belonging to different prime ideals is never primary.* We now unite all primary ideals in (6) belonging to the same prime ideal $\mathfrak{p}$ into a new primary ideal $\mathfrak{b}_y$, and call $\mathfrak{b}_y$ a *maximal primary component* of $\mathfrak{a}$. Our former results then yield this: *Every ideal* $\mathfrak{a}$ *can be represented as the union of maximal primary components*

$$\mathfrak{a} = [\mathfrak{b}_1, \mathfrak{b}_2, \cdots, \mathfrak{b}_s]; \tag{8}$$

the number of components and the corresponding prime ideals

$$\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_s \tag{9}$$

are the same for all such decompositions. The prime ideals (9) are all different and uniquely determined; we shall call them the *prime ideals belonging to* $\mathfrak{a}$.

E. Noether gives two other types of decomposition theorems;

the two last types are distinguished by the fact that the decompositions are unique.

An ideal $\mathfrak{b}$ is said to be *relatively prime* to $\mathfrak{a}$ if any relation $\mathfrak{b}\mathfrak{c}\equiv 0 \pmod{\mathfrak{a}}$ implies $\mathfrak{c}\equiv 0 \pmod{\mathfrak{b}}$. If we suppose $\mathfrak{a}<R$, then the necessary and sufficient condition that $\mathfrak{b}$ be relatively prime to $\mathfrak{a}$ is that no prime ideal belonging to $\mathfrak{b}$ is divisible by a prime ideal belonging to $\mathfrak{a}$. This criterion shows that the notion of being relatively prime is not mutual, that is, $\mathfrak{b}$ may be relatively prime to $\mathfrak{a}$, but not $\mathfrak{a}$ to $\mathfrak{b}$. Krull defines relatively prime by the equivalent condition $\mathfrak{a}:\mathfrak{b}=\mathfrak{a}$. An ideal $\mathfrak{a}$ is said to be *relatively-prime decomposable* when there exists no representation $\mathfrak{a}=[\mathfrak{b}, \mathfrak{c}]$, where $\mathfrak{b}$ and $\mathfrak{c}$ are mutually relatively prime. One can then show that *every ideal has a unique decomposition,*

$$\mathfrak{a} = [\mathfrak{c}_1, \mathfrak{c}_2, \cdots, \mathfrak{c}_t], \tag{10}$$

as the union of relatively-prime indecomposable components. The decomposition (10) can be obtained from the maximal primary decomposition (8) by joining all primary components into sets such that when a set contains a primary ideal with the corresponding prime ideal $\mathfrak{p}$, then it contains all primary ideals belonging to prime divisors or multipla of $\mathfrak{p}$. The uniqueness of the decomposition (10) also gives some information about the components in (8), and a certain class of maximal primary components, the so-called *isolated components*, can be shown to be uniquely determined.

The final decomposition theorem does not possess quite the same generality as the preceding since we shall have to suppose that *the ring contains a unit element* ϵ. On the other hand, this decomposition claims additional interest since it gives not only a representation as the union of ideal components, but also a product representation by means of the same ideals. Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals without common divisors, that is, $(\mathfrak{a}, \mathfrak{b})=R=(\epsilon)$; this implies that $\mathfrak{a}$ and $\mathfrak{b}$ are mutually relatively prime, and the definitions in §2 show that in this case $\mathfrak{a}\mathfrak{b}=[\mathfrak{a}, \mathfrak{b}]$; *for ideals without common divisors the union is equal to the product.* An ideal is *direct indecomposable,* when no identity $\mathfrak{a}=[\mathfrak{b}, \mathfrak{c}]$ holds, where $\mathfrak{b}$ and $\mathfrak{c}$ are without common divisors. It can then be shown that *every ideal is uniquely representable as the union or product of direct indecomposable ideals,*

$$(11) \qquad \mathfrak{a} = [\mathfrak{d}_1, \cdots, \mathfrak{d}_n] = \mathfrak{d}_1 \cdots \mathfrak{d}_n,$$

where each $\mathfrak{d}_i$ has no common divisor with the union of the rest.

The four decompositions (6), (8), (10), (11) give the main results on the structure of ideals; they have been given, as in the original paper by E. Noether, in order of decreasing decomposition, each being deducible from the preceding by joining some of its components into larger groups. Space does not permit a discussion of other properties of these decompositions, but it should be mentioned that Krull* has simplified the proofs of the main theorems through a systematic use of the ideal quotient. In another paper† Krull deduces the theory on an axiomatic basis, considering the ideals not as sets in rings, but as symbols having the operational properties defined in §2.‡

9. *Polynomial Ideals and Algebraic Manifolds.* To clarify the significance of this abstract theory it may be well to consider a concrete illustration; a suitable example of sufficient generality can be found in the theory of polynomial ideals and the related theory of algebraic manifolds. We shall suppose that K is an algebraically closed field and consider the ring $R(x_1, \cdots, x_n)$ of all polynomials in n variables with coefficients in K; according to a well known theorem by Hilbert the chain condition will hold in this ring since every ideal has a basis.

An *algebraic manifold* in the corresponding n-dimensional space S_n is the totality of points $\xi = (\xi_1, \cdots, \xi_n)$ with coordinates in K satisfying a set of algebraic relations

$$(12) \qquad f_i(x) = f_i(x_1, \cdots, x_n) = 0, \quad (i = 1, 2, \cdots).$$

To every ideal $\mathfrak{a}$ in $R\ (x_1, \cdots, x_n)$ then corresponds a unique algebraic manifold $\mathfrak{M}(\mathfrak{a})$ defined as the totality of points at which all polynomials of $\mathfrak{a}$ vanish; it coincides with the manifold defined by the basis polynomials of $\mathfrak{a}$. Two different ideals may have the same manifold, for instance, $\mathfrak{M}(\mathfrak{a}) = \mathfrak{M}(\mathfrak{a}^n)$; when $\mathfrak{a} > \mathfrak{b}$, then obviously

$$\mathfrak{M}(\mathfrak{a}) \leqq \mathfrak{M}(\mathfrak{b}).$$

To every algebraic manifold $\mathfrak{M}$ corresponds conversely a unique

* Mathematische Annalen, vol. 90 (1923).

† Sitzungsberichte Erlangen, vol. 56 (1924).

‡ See also Sono, Memoirs of the College of Science, Kyoto, vol. 7 (1923).

ideal $\mathfrak{a}_{\mathfrak{M}}$ defined as the set of all polynomials vanishing in all points of $\mathfrak{M}$.

One easily finds that the cross-cut of two algebraic manifolds $\mathfrak{M}$ and $\mathfrak{N}$ is an algebraic manifold defined by $(\mathfrak{a}_{\mathfrak{M}}, \mathfrak{a}_{\mathfrak{N}})$, while the union is an algebraic manifold defined by the union $[\mathfrak{a}_{\mathfrak{M}}, \mathfrak{a}_{\mathfrak{N}}]$ or also by the product $\mathfrak{a}_{\mathfrak{M}}\mathfrak{a}_{\mathfrak{N}}$. We say, as usual, that an algebraic manifold is *irreducible* if it is not the union of two manifolds contained in it; one can then show that *the necessary and sufficient condition that a manifold be irreducible is that the corresponding ideal be a prime ideal*; *every prime ideal defines a unique irreducible algebraic manifold.*

This result illustrates clearly the occurrence of divisors of prime ideals as has already been mentioned in §4. For instance, in three-dimensional space any irreducible surface will correspond to a prime ideal $\mathfrak{p}_2$ of dimension 2; any irreducible curve on the surface corresponds to a prime ideal $\mathfrak{p}_1$ dividing $\mathfrak{p}_2$, while every point on the curve is a zero-dimensional prime ideal $\mathfrak{p}_0$ dividing $\mathfrak{p}_2$ and $\mathfrak{p}_1$.

Since the manifolds defined by prime ideals are known, the manifolds of all other ideals can be determined; the manifold of a primary ideal $\mathfrak{q}$ is equal to the manifold of its prime ideal $\mathfrak{p}$, since $\mathfrak{p}$ divides $\mathfrak{q}$ and a power of $\mathfrak{p}$ is divisible by $\mathfrak{q}$; the manifold of the union of two ideals is equal to the union of the manifolds. If we represent an ideal $\mathfrak{a}$ as the union of maximal primary components, *the manifold of* $\mathfrak{a}$ *must then be equal to the union of the manifolds defined by the prime ideals belonging to* $\mathfrak{a}$. The fact that these prime ideals were uniquely defined is only a new way of stating that every algebraic manifold can be represented uniquely as the union of irreducible manifolds.

These remarks give us a simple access to various fundamental theorems in the theory of algebraic manifolds. Let $f(x)$ be a polynomial vanishing at all the points of the manifold $\mathfrak{M}$ defined by the relations (12); $f(x)$ is then divisible by all prime ideals belonging to the ideal

$$\mathfrak{a} = (f_1(x), \cdots, f_r(x)), \tag{13}$$

and if ρ is an upper bound for the exponents of the primary components of $\mathfrak{a}$, then $f(x)^\rho$ must belong to $\mathfrak{a}$. This is equivalent to a theorem of Hilbert: *If a polynomial* $f(x_1, \cdots, x_n)$ *vanishes* *at all points satisfying* (12), *then there exists an exponent such that*

$$f(x)^\rho = g_1(x)f_1(x) + g_2(x)f_2(x) + \cdots + g_r(x)f_r(x).$$

Another important problem is to determine when a polynomial $f(x)$ belongs to a given ideal $\mathfrak{a}$; we first consider the simplest case of an ideal $\mathfrak{a}=(f_1(x, y), f_2(x, y))$ in two variables and suppose that the curves $f_1(x, y)=0, f_2(x, y)=0$ have only a finite number of points $(x_1, y_1), \cdots, (x_r, y_r)$ in common. The manifold of $\mathfrak{a}$ is then determined by the zero-dimensional prime ideals $\mathfrak{p}=(x-x_i, y-y_i)$, and $\mathfrak{a}$ has a representation of the form $\mathfrak{a}=[\mathfrak{g}_1, \cdots, \mathfrak{g}_r]$ as the union of maximal primary components $\mathfrak{g}_i$ with the corresponding prime ideals $\mathfrak{p}$. For a polynomial $f(x, y)$ to belong to $\mathfrak{a}$ it is necessary and sufficient that it belong to all primary components $\mathfrak{g}_i$; the ideals $\mathfrak{g}_i$ are not known directly, but since $\mathfrak{g}$ divides $\mathfrak{p}_i^{\rho_i}$, one finds that $\mathfrak{g}_i=(\mathfrak{a}, \mathfrak{p}_i^{\rho_i})$ and we obtain the condition of M. Noether,

$$f(x, y) \equiv 0 \pmod{(\mathfrak{a}, \mathfrak{p}_i^{\rho_i})}. \tag{14}$$

Since $\mathfrak{p}_i^{\rho_i}$ consists of all terms of the form $\Sigma c_{a,b}\,(x-x_i)^a\,(y-y_i)^b$, $a+b \geqq \rho_i$, it follows that $f(x, y)$ belongs to $\mathfrak{a}$, that is, is representable in the form

$$f(x, y) = g_1(x, y)f_1(x, y) + g_2(x, y)f_2(x, y) \tag{15}$$

if and only if such a representation (15) exists for all intersections when terms of degree ρ in $x-x_i$ and $y-y_i$ are disregarded. The importance of the theorem of M. Noether for algebraic geometry is well known; a condition similar to (14) for an arbitrary ideal (13) was given by Henzelt.*

10. *Unique Prime Ideal Decomposition.* It is a problem of considerable interest to determine the necessary and sufficient conditions which a ring must satisfy in order that every ideal be representable uniquely as the product of a finite number of prime ideal factors. This problem has been investigated systematically by E. Noether.† We shall consider a ring R with

* Henzelt, Mathematische Annalen, vol. 88 (1923); E. Noether, Mathematische Annalen, vol. 90 (1923); Hermann, Mathematische Annalen, vol. 95 (1925); Kapferer, Mathematische Annalen, vol. 97 (1927); v. d. Waerden, Mathematische Annalen, vol. 96 (1927) and vol. 99 (1928), *Algebra*, Chap. 13.

† Mathematische Annalen, vol. 96 (1927).

unit element and without divisors of zero. It is obvious that it is necessary first to impose the *chain condition* on the ring; secondly it must be assumed that the *prime ideals in R have no divisors$\neq R$.* This condition either may be postulated or may be derived as a consequence of the so-called *chain condition for multipla of ideals. Every chain* $\mathfrak{a}_1 > \mathfrak{a}_2 > \cdots$ *of ideals, each divisible by the preceding, must break off when all the ideals in the chain are divisors of a fixed ideal* $\mathfrak{a}\neq 0$. When the two chain conditions are satisfied the three decompositions for ideals given in §8 are identical and every ideal in R is representable uniquely as the product of its maximal primary components. It remains then to find the condition which will make every primary ideal equal to a prime ideal power; this condition is closely connected with the notion of *integral elements.*

Let S and T be two rings; S shall be a subring of T and have a unit element. An element t in T is said to be *integral with respect to* S, when the powers of t can be expressed by a basis $t_1, \cdots, t_n$ in the form

$$t^m = s_1^{(m)} t_1 + \cdots + s_n^{(m)} t_n, \tag{16}$$

with coefficients $s_j^{(i)}$ in S. When S satisfies the chain condition, (16) is equivalent to the condition that t shall satisfy an algebraic equation

$$t^n + s_1 t^{n-1} + \cdots + s_n = 0.$$

We say that S is *integrally closed* with respect to T when every element in T which is integral with respect to S is already contained in S.

Let us now return to the ring R considered above, and impose the third condition: *R shall be integrally closed with respect to its quotient field.* Every primary ideal can then be shown to be a prime ideal power and there is a unique prime ideal decomposition of each ideal in R. The theory is completed by the converse theorem, that if there exists a unique prime ideal decomposition then the ring must satisfy the three conditions mentioned.*

Some of the most important rings in algebra are integrally closed and satisfy the chain condition, but prime ideal divisors

* See also Krull, Sitzungsberichte Heidelberg, 1924, 1925; Mathematische Annalen, vol. 99 (1928).

may exist. The rings of polynomials are of this type. In this case, however, a certain class of ideals, namely the principal ideals, have a unique decomposition into prime factors. Van der Waerden* has pointed out that the decomposition theorem holds even for rings with prime ideal divisors, when only the so-called *highest prime ideals* are considered. A highest prime ideal is then defined as a prime ideal not dividing any other prime ideal; in the case of polynomial ideals these prime ideals define the algebraic manifolds of dimension $n-1$ and are ordinary prime polynomials. Through a suitable definition of equivalence of ideals van der Waerden shows that every primary ideal is equivalent to a prime ideal power, and that every ideal is equivalent to a unique product of prime ideals; in the case of rings without prime ideal divisors this reduces to the ordinary decomposition theorem.

11. *Rings without Chain Condition.* We shall conclude this survey by considering briefly the results obtained for the ideal theory in rings without chain condition. The examples which lie closest at hand are the infinite algebraic fields; the ideal theory of the ring of all integers in such fields has been discussed in a remarkable posthumous paper by Stiemke.† There exist prime ideals and also an enumerable basis for each ideal. One can usually not expect any representation of ideals as product of prime ideals since the prime ideal divisors of even a single prime may form a set having the power of the continuum. There are, however, special infinite algebraic fields in which there exists only an enumerable set of prime ideals and in such fields every integral element can be represented uniquely as the product of prime ideal factors and certain primary factors, which can be characterized by fractional exponents. An example of a field satisfying the condition of Stiemke is the field of all p^mth roots of unity ($m=0, 1, 2, \cdots$), where p is a fixed prime.

The investigations of Stiemke have been continued by Krull,‡ who has obtained a method of handling the set of ideals in an infinite ring of algebraic numbers through the introduction

* Mathematische Annalen, vol. 99 (1928); *Algebra*, §103.

† Mathematische Zeitschrift, vol. 25 (1926).

‡ Mathematische Zeitschrift, vol. 29 (1929); vol. 31 (1930).

and systematic use of the notion of *absolute values.** Let K be any field. We say that an absolute value is defined in K when to each element α in K there corresponds a real number $\|\alpha\|$ with the properties

$$(17)\qquad \begin{gathered} \|0\| = 0,\ \|\alpha\| > 0, \text{ when } \alpha \neq 0, \\ \|\alpha\beta\| = \|\alpha\|\cdot\|\beta\|,\ \|\alpha+\beta\| \leqq \|\alpha\| + \|\beta\|. \end{gathered}$$

Let us consider the rational field P as an example. In this field there are only two different types of absolute values; the first is the trivial type

$$(18)\qquad \|\alpha\| = |\alpha|^\rho,\ 0 \leqq \rho \leqq 1,$$

where ρ is a constant and $|\alpha|$ denotes the ordinary absolute value. To obtain the second type let p be a prime and let us write all rational numbers in the form

$$(19)\qquad r = p^a\frac{u}{v},\ (u, v) = 1,$$

where u and v are integers not divisible by p; the correspondence

$$(20)\qquad \|r\| = c^a,\ 0 < c \leqq 1,$$

then satisfies the conditions for an absolute value. The main difference between the two types (18) and (20) of absolute values lies in the *triangular inequality* (17); in the case of the type (20) the inequality may be strengthened to

$$(21)\qquad \|\alpha+\beta\| \leqq \text{Max}\,(\|\alpha\|, \|\beta\|)$$

and we say that the absolute value is *non-Archimedian.* Ostrowski† has shown that every field with Archimedian absolute values is isomorphic to a subfield of the field of all complex numbers, and that the absolute value can then be defined as in (18).

For the study of divisibility properties only the non-Archimedian absolute values are, therefore, of importance; in this case the exponent a in (19) is the characteristic to be investi-

* See for instance the exposition of this theory in O. Ore, *Some recent developments in abstract algebra,* this Bulletin, vol. 37 (1931), pp. 537–548.

† Acta Mathematica, vol. 41 (1917).

gated and it is, consequently, more convenient to define the absolute value $v(\alpha)$ in the *additive form*

$$(22) \qquad v(\alpha\beta) = v(\alpha) + v(\beta), \; v(\alpha + \beta) \geqq \text{Min}\,(v(\alpha), v(\beta)).$$

One obtains (22) from (17) and (21) by putting $v(\alpha) = -\log\|\alpha\|$, and for the rational case (19) it reduces to $v(r) = ka$, where the positive constant k may be taken equal to unity.

We return again to the representation (19) of the rational numbers; the numbers r for which the exponent a is non-negative form a ring P_p which we shall call an *evaluation ring* (*Bewertungsring*) with respect to p. This ring has a series of properties which all have their analogues in the more general evaluation rings considered later; P_p is a maximal ring in P, that is, there is no ring containing P_p except P; P_p is integrally closed in P; when r_1 and r_2 are two elements in P_p, then r_1 is divisible by r_2, or conversely; the ideals in P_p are all of the form $\mathfrak{a} = (p^n)$ and an absolute value for the ideals can be defined by putting $v(\mathfrak{a}) = n$; the ideal $\mathfrak{a}$ consists of all elements r such that $v(r) \geqq v(\mathfrak{a})$; the only prime ideal is $\mathfrak{p} = (p)$ consisting of all elements with positive absolute values. The ring of rational integers is equal to the cross-cut of all rings P_p for all p, and the divisibility properties of any rational integer are determined by its values in the various evaluation rings.

Krull now shows that for each definition of absolute value in a field there exists a corresponding evaluation ring consisting of the elements with non-negative values; this ring is maximal and conversely every maximal ring defines an absolute value. These rings have the properties mentioned above: An evaluation ring is integrally closed; when two elements are given, one always divides the other; there exists only one prime ideal $\mathfrak{p}$ consisting of all elements having positive absolute values. There are now two different possibilities. The values of the elements may form a discrete set; in this case we have perfect analogy to the rational case and all ideals are powers of $\mathfrak{p}$. In the second case the values may be everywhere dense; in both cases the ideals $\mathfrak{a}$ consist of the elements whose values lie above a certain limit κ. We define a value of $\mathfrak{a}$ by putting $v(\mathfrak{a}) = \kappa$; to each κ there may correspond two ideals, namely, the ideal $\mathfrak{a}$ containing all α such that $v(\alpha) > v(\mathfrak{a}) = \kappa$ and the ideal $\mathfrak{b}$ containing also elements β such that $v(\beta) = v(\mathfrak{b}) = \kappa$. We shall call

$\mathfrak{a}$ an *open ideal* and $\mathfrak{b}$ a *closed ideal* and say that $v(\mathfrak{a}) > v(\mathfrak{b})$; in the case of continuous values $\mathfrak{p}$ is an open ideal with the value 0 and the unit ideal is a closed ideal with the same value.

This theory may be applied to the ring R of all integers in an infinite algebraic field K. One can show that the maximal rings in K are defined by the prime ideals $\mathfrak{p}$ in R and that $R_{\mathfrak{p}}$ consists of all fractional elements in K whose denominators are not divisible by $\mathfrak{p}$; and that the ring of integers R is equal to the cross-cut of all maximal rings $R_{\mathfrak{p}}$ as in the rational field. To each ideal $\mathfrak{a}$ in R corresponds an ideal $\mathfrak{a}_{\mathfrak{p}}$ in $R_{\mathfrak{p}}$ and this permits us to define a set of values $v_{\mathfrak{p}}(\mathfrak{a})$ for each ideal $\mathfrak{a}$, where $\mathfrak{p}$ runs through all prime ideals of R. These values may be considered as a *generalization of the exponents* in the case of prime ideal decompositions in the finite fields. They satisfy the addition theorem, $v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b})$, and the fundamental theorem is, that *an ideal* $\mathfrak{a}$ *can only be divisible by an ideal* $\mathfrak{c}$ *when* $v_{\mathfrak{p}}(\mathfrak{a}) \geqq v_{\mathfrak{p}}(\mathfrak{c})$ *for all prime ideals* $\mathfrak{p}$; one can also find a necessary and sufficient condition that an ideal be a factor of another. The inverse problem, namely, finding all sets of values to which there correspond ideals, Krull was able to solve, through topological considerations, by making the set of all evaluation rings a topological space.

In a recent paper, Krull* generalizes the notion of absolute value by letting correspond to each element of a field not a real number as formerly, but an element of an ordered abelian group, such that the conditions (22) are satisfied. This absolute value corresponds to a generalized type of evaluation rings with a number of properties in common with the evaluation rings studied above. One of the most interesting results of this theory is the following characterization of the integrally closed rings. *A necessary and sufficient condition that a ring be integrally closed is that it be the cross-cut of general evaluation rings.* Krull also gives various other results which cannot be discussed here; a paper by Prüfer† on the divisibility of ideals in rings without chain condition and a paper by v. Dantzig‡ on topological algebra should be mentioned in this connection.

YALE UNIVERSITY

* Journal für Mathematik, vol. 167 (1932).

† Journal für Mathematik, vol. 168 (1932).

‡ Mathematische Annalen, vol. 107 (1932).