On Congruences.

By

Masazo Sono.

(Received March 13, 1917).

Objects to be treated in mathematics are sets of elements which contain definitions of equality and of composition, as well as postulates concerning the rules of composition. Is it possible in a given object, completely defined, to change the definition of equality, under the conditions that elements equal to one another remain equal after the change and that the object only reduces to another of the same kind? If so, in what ways can it be done? In the present paper we give the answer to this in the case of groups and of rings; we investigate the possibility and the conditions for changing the definition of equality, under the restriction that a given group or a given ring remains also a group or a ring after the change. We add also a few theorems on rings.

It is desirable to have this problem solved also for the treatment of the cases where the elements of a group or a ring are variables, independent or dependent.

Definitions of a Group and a Ring.

§ 1. To build up an object of mathematical research, we first define the equality of two elements, next the composition of the elements, and lastly give the postulates concerning the rules of composition.

I. Equality.[1] The equality and the inequality of two elements belonging to a set are determined by a definition which consists of the two statements: the one explains that the two elements are equal; the other that they are unequal. For its establishment there is no further restriction than that the given definition must satisfy the following conditions:

[1] O. Stolz and J. A. Gmeiner, Theoretische Arithmetik, p. 2.

1. Every element is equal to itself in consequence of the definition. If A is equal to B, B must be equal to A.

2. Two elements of the set are either equal or unequal.

3. From $A=B$ and $B=C$ follows $A=C$.

II. Composition. It is said that a *composition* upon the elements A and B of a set is defined, if, corresponding to the elements A and B and to a certain order of these elements, there exists a certain third elements C, which may or may not belong to the set. The new element C which is associated with the given elements in the given order, is called the *result* of the composition; the composition of A and B is written AB when the order of the elements is A, B. For convenience the symbol AB is considered to denote the result of the composition at the same time. Consequently, if the result of the composition of A and B is C, we have $AB=C$.

A composition is said to be *unique*[1] when from $A'=A$ and $B'=B$ follows $A'B'=AB$. In our case, groups and rings, the composition is defined as always unique. If there are two rules in regard to the composition of two elements A and B, say denoted by $+$ and $\times$, we distinguish them one from the other in writing by $A+B$ and $A\times B$.

III. The postulates for

(a) Group:[2] A set $\mathfrak{G}$ of elements, in which the composition among its elements is defined, is called a *group* with respect to the given composition when the following postulates hold:

1. If A and B are elements of $\mathfrak{G}$, AB is also an element of $\mathfrak{G}$.

2. If A, B and C are three elements of $\mathfrak{G}$, the result of the composition of A and BC is equal to that of AB and C. That is, $A(BC)=(AB)C$. This is the so-called associative law.

3. There exists in $\mathfrak{G}$ an element E, such that $AE=A$, for every element A of $\mathfrak{G}$.

4. There exists in $\mathfrak{G}$, corresponding to any element A of $\mathfrak{G}$, another A^{-1} such that $AA^{-1}=E$, where E is the said element.

(b) Ring: A set $\mathfrak{R}$ of elements with two rules of composition denoted by $+$ and $\times$ is called a *ring* when the following nine postulates hold:

1. If A and B are two elements of $\mathfrak{R}$, $A+B$ is also an element of $\mathfrak{R}$.

2. If A and B are elements of $\mathfrak{R}$, then $A+B=B+A$. (Commutative law).

[1] *Loc. cit.*, p. 4. G. Frobenius, Berliner Sitzber. (1895), p. 163.

[2] L. E. Dickson, Trans. Amer. Math. Soc., **6**, 199 (1905).

3. If A, B and C are three elements of $\mathfrak{R}$, then $(A+B)+C = A+(B+C)$. (Associative law).

4. There exists in $\mathfrak{R}$ an element Z, such that $Z+B=B$, for every element B of $\mathfrak{R}$.

5. There exists in $\mathfrak{R}$, corresponding to every element A of $\mathfrak{R}$, another X such that $A+X=Z$, where Z is the said element.

6. If A and B are two elements of $\mathfrak{R}$, $A\times B$ is also an element of $\mathfrak{R}$.

7. If A and B are two elements of $\mathfrak{R}$, then $A\times B=B\times A$. (Commutative law).

8. If A, B and C are elements of $\mathfrak{R}$, then $(A\times B)\times C= A\times(B\times C)$. (Associative law).

9. $A\times(B+C)=(A\times B)+(A\times C)$. (Distributive law).

We have defined a ring abstractly by the above nine postulates after consideration of the points which are essential in rings.[1] This set of postulates is a part of the set by which Prof. Dickson[2] has defined a field abstractly; hence there is no necessity of again showing the independency of the postulates.

N. B. The set $\mathfrak{R}$ becomes a field[3], when the following two postulates hold in addition to the above nine:

(i) There exists in $\mathfrak{R}$ an element U such that $U\times B=B$ for every element B of $\mathfrak{R}$.

(ii) Corresponding to every element A such that $C\times A\neq A$ for at least one element C of $\mathfrak{R}$, there exists in $\mathfrak{R}$ an element X for which $A\times X=U$, where U is the said element.

We now proceed to change the definition of equality under the restriction that elements equal to one another remain equal after the change and that a group or a ring remains also a group or a ring after the change, that is, that the conditions for equality are satisfied, the composition remains unique and moreover the postulates for a group or a ring hold.

When an element A becomes equal to another B by changing the definition of equality, we say for a time to avoid ambiguity that A is *congruent* to B, and this is expressed in writing by $A\equiv B$.

[1] Hilbert, Jahresber. D. Math. Ver. **4**, 237, (1894–95).
Dedekind used the word *Ordnung* for *Ring*; and he defined it as a modulus $\mathfrak{M}$ such that it contains the square $\mathfrak{M}^2$ and also the number 1. But, for some reason, we have omitted the second condition.

[2] Dickson, Trans. Amer. Math. Soc., **4**, 17, (1903).

[3] *Loc. cit.*

Since in the change considered the conditions for equality and the uniqueness of the composition hold, we have that from $A' \equiv A$, $B' \equiv B$ and $AB = C$ follows $A'B' \equiv C$.

Congruence in a Group.

§ 2. Let $\mathfrak{G}$ be a given group; and suppose that the definition of equality has been so changed that $\mathfrak{G}$ remains a group. Let $\mathfrak{H}$ be the set formed of all the elements of $\mathfrak{G}$ which become congruent to the identity E of $\mathfrak{G}$ after the change of the definition of equality. For any two elements H_1 and H_2 of $\mathfrak{H}$ we have

$$H_1H_2 \equiv EE,$$

and

$$EE = E,$$

since $H_1 \equiv E$, $H_2 \equiv E$ and the composition is unique; therefore, the product of two elements of $\mathfrak{H}$ is also congruent to the identity E of $\mathfrak{G}$ and consequently belongs to $\mathfrak{H}$. Hence the set $\mathfrak{H}$ is a subgroup of $\mathfrak{G}$. Let A and H be elements of $\mathfrak{G}$ and $\mathfrak{H}$ respectively, then we have

$$A^{-1}HA \equiv A^{-1}EA \equiv E,$$

since elements equal to one another become congruent after the change and the composition is unique; therefore the element $A^{-1}HA$ belongs to $\mathfrak{H}$, that is, $\mathfrak{H}$ is self-conjugate under $\mathfrak{G}$. Thus the elements which become congruent to the identity of $\mathfrak{G}$ by the change of the definition of equality constitute a self-conjugate subgroup $\mathfrak{H}$ of $\mathfrak{G}$.

If an element B of $\mathfrak{G}$ becomes congruent to another A by the said change, i.e. $B \equiv A$, then, since $A^{-1} \equiv A^{-1}$ and the composition is unique, we have

$$BA^{-1} \equiv AA^{-1} \equiv E,$$

which shows that BA^{-1} belongs to $\mathfrak{H}$ and therefore B is an element of the co-set $\mathfrak{H}A$ of $\mathfrak{G}$ as regards $\mathfrak{H}$. If, conversely, B' be an element of the co-set $\mathfrak{H}A$, B is of the form HA, where H denotes an element of $\mathfrak{H}$, and we have

$$B \equiv HA \equiv EA \equiv A,$$

since $H \equiv E$. Therefore the elements which become congruent to A belong to the same co-set $\mathfrak{H}A$; and, conversely, each element of $\mathfrak{H}A$ becomes congruent to A. Hence we have the

THEOREM: *In order that such a change as we desire can be made the following conditions must be satisfied:*

(i) *The elements of a given group $\mathfrak{G}$, which become congruent to the identity of $\mathfrak{G}$, constitute a self-conjugate subgroup $\mathfrak{H}$ of $\mathfrak{G}$.*

(ii) *The elements of the same co-set of $\mathfrak{G}$ as regards $\mathfrak{H}$ become congruent to one another.*

(iii) *The elements congruent to one another belong to the same co-set of $\mathfrak{G}$ as regards $\mathfrak{H}$.*

And, conversely, these conditions are sufficient.

Let $\mathfrak{H}$ be a self-conjugate subgroup of $\mathfrak{G}$ and suppose that the change has been made to satisfy the above three conditions. Then the conditions for equality are evidently satisfied. If H_1 and H_2 be two elements of $\mathfrak{H}$ and if A and B be two elements of $\mathfrak{G}$, we have

$$H_1A \cdot H_2B = HAB,$$

where H is an element of $\mathfrak{H}$; and therefore

$$H_1A \cdot H_2B \equiv A \cdot B,$$

which shows that the uniqueness of the composition holds. And, moreover, evidently the postulates for a group also hold.

§ 3. We see from the result obtained above that we can change completely the definition of equality, as we desire, by putting the elements of a self-conjugate subgroup $\mathfrak{H}$ of a given group $\mathfrak{G}$ congruent to the identity of $\mathfrak{G}$, and only by so doing. We, therefore, define again:

When, the definition of equality in a given group $\mathfrak{G}$ being so changed that each element of a self-conjugate subgroup $\mathfrak{H}$ becomes equal to the identity of $\mathfrak{G}$, two elements A and B of $\mathfrak{G}$ become equal to each other, A and B are said to be *congruent*[1] with respect to the modulus $\mathfrak{H}$, and this is expressed in writing by

$$A \equiv B \quad (\text{mod. } \mathfrak{H}).$$

The group, to which the given group $\mathfrak{G}$ reduces when we take its elements with respect to the self-conjugate subgroup $\mathfrak{H}$, is easily shown to be simply isomorphic with the quotient group $\frac{\mathfrak{G}}{\mathfrak{H}}$; this is available to define the quotient: the quotient $\frac{\mathfrak{G}}{\mathfrak{H}}$ may be considered for the group, to which $\mathfrak{G}$ reduces when its elements are taken with respect to the modulus $\mathfrak{H}$. This view will be found useful in simply solving certain problems concerning quotient groups.

[1] The term *congruent* is sometimes used in the same meaning.

Simple Applications.[1]

§ 4. (1) If each element of a group $\mathfrak{H}$ is permutable with another group $\mathfrak{K}$, the groups $\{\mathfrak{H}, \mathfrak{K}\}/\mathfrak{K}$ and $\mathfrak{H}/\mathfrak{L}$ are simply isomorphic, where $\mathfrak{L}$ is the subgroup common to $\mathfrak{H}$ and $\mathfrak{K}$.

$\mathfrak{K}$ and $\mathfrak{L}$ are evidently self-conjugate subgroups of $\{\mathfrak{H}, \mathfrak{K}\}$ and $\mathfrak{H}$ respectively. The elements of $\{\mathfrak{H}, \mathfrak{K}\}$ being taken with respect to the modulus $\mathfrak{K}$, each element of $\mathfrak{K}$ becomes $\equiv 1$ (mod. $\mathfrak{K}$); and the elements in $\mathfrak{H}$ which become congruent to 1 (mod. $\mathfrak{K}$) are those of $\mathfrak{L}$. If two elements A and B of $\mathfrak{H}$ are incongruent (mod. $\mathfrak{L}$), A and B are also incongruent (mod. $\mathfrak{K}$). Indeed, if $A \equiv B$ (mod. $\mathfrak{K}$), then $AB^{-1} \equiv 1$ (mod. $\mathfrak{K}$), that is AB^{-1} would belong to $\mathfrak{K}$, while it belongs to $\mathfrak{H}$. Therefore AB^{-1} must belong to $\mathfrak{L}$, i.e. $AB^{-1} \equiv 1$ (mod. $\mathfrak{L}$), whence $A \equiv B$ (mod. $\mathfrak{L}$). But this contradicts the assumption that $A \not\equiv B$ (mod. $\mathfrak{L}$). Therefore now let

$$A,\ B,\ C, \ldots\ldots \text{(mod. } \mathfrak{L})$$

be a complete set of incongruent (mod. $\mathfrak{L}$) elements of $\mathfrak{H}$, which is $\mathfrak{H}/\mathfrak{L}$, then the elements

$$A,\ B,\ C,\ \ldots\ldots\ \text{(mod. } \mathfrak{K}),$$

being taken with respect to the modulus $\mathfrak{K}$, form a complete set of incongruent (mod. $\mathfrak{K}$) elements of $\{\mathfrak{H}, \mathfrak{K}\}$, which is the group $\{\mathfrak{H}, \mathfrak{K}\}/\mathfrak{K}$. If a correspondence between the elements of $\{\mathfrak{H}, \mathfrak{K}\}/\mathfrak{K}$ and those of $\mathfrak{H}/\mathfrak{L}$ be established, so that to $A, B, C, \ldots$ (mod. $\mathfrak{K}$) of the former there correspond respectively $A, B, C, \ldots$ (mod. $\mathfrak{L}$) of the latter, then to the product AB (mod. $\mathfrak{K}$) of any two elements A and B of $\{\mathfrak{H}, \mathfrak{K}\}/\mathfrak{K}$ there corresponds the product AB (mod. $\mathfrak{L}$) of the corresponding elements of $\mathfrak{H}/\mathfrak{L}$. Hence the two groups are simply isomorphic. For, if $AB \equiv C$ (mod. $\mathfrak{K}$), then $ABC^{-1} \equiv 1$ (mod. $\mathfrak{K}$) and hence $ABC^{-1} \equiv 1$ (mod. $\mathfrak{L}$), since ABC^{-1} belongs to $\mathfrak{H}$. Consequently $AB \equiv C$ (mod. $\mathfrak{L}$). If, conversely, $AB \equiv C$ (mod. $\mathfrak{L}$), we evidently have $AB \equiv C$ (mod. $\mathfrak{K}$).

(2) If A and B are two elements of a group $\mathfrak{G}$, $A^{-1}B^{-1}AB$ is the commutator of A and B; it is a well-known fact that the commutator-group of a group is self-conjugate. If we now put $A^{-1}B^{-1}AB \equiv 1$, we have $AB \equiv BA$, which shows that the quotient of $\mathfrak{G}$ by the commutator-group is abelian. Conversely, if the quotient of $\mathfrak{G}$ by a self-conjugate subgroup $\mathfrak{H}$ is abelian, i.e.

[1] The facts stated in (1) and (2) are well known, but the author here gives simple proofs of them.

$$AB \equiv BA \pmod{\mathfrak{H}},$$

it follows that

$$A^{-1}B^{-1}AB \equiv 1 \pmod{\mathfrak{H}};$$

hence $\mathfrak{H}$ must contain the commutator-group.

(3) Words of application to permutation-groups. It is not necessary to consider that the letters on which a permutation are performed are all distinct: the operation of replacing each letter of a given set of letters by another, which may or may not be equal, when carried out under the condition that no two unequal letters are replaced by letters equal to each other, is called a permutation. When the equality between the letters on which the permutations of a permutation-group are performed are so changed that each permutation of the group remains also a permutation, the group reduces to another having fewer different letters. This fact somewhat facilitates certain discussions of intransitive and imprimitive groups.

Congruence in a Ring.

§ 5. Before considering congruences in a ring, we should mention a few properties of a ring which follow immediately from the postulates.

The first five of the postulates for a ring show that every ring is an abelian group with respect to addition[1]. Hence it follows that the element Z stated in the fourth postulate is the same for all the elements of a ring $\mathfrak{R}$ and that there exists only one, and also that, corresponding to any given element A, there exists only one element X such that $A+X=Z$. In other words, if $Z+B=B$ for a certain element B of a ring $\mathfrak{R}$, then $Z+C=C$ for every element C of $\mathfrak{R}$; and if $Z'+B=B$, then $Z'=Z$; if $A+X'=Z$ and $A+X=Z$ for a given element A, then $X'=X$. Hereafter the said element Z is denoted by the symbol 0 and the said element X corresponding to A by the symbol $-A$. According to these notations we have $A+(-A)=0$. And also for two elements A and B of $\mathfrak{R}$ there is uniquely determined an element Y such that $A+Y=B$.

Since

$$A\cdot 0+A\cdot B=A(0+B)=A\cdot B=0+AB,$$

we have

[1] The two rules of composition denoted by + and × are called respectively addition and multiplication. For simplicity we write AB or $A\cdot B$ for $A\times B$.

$$A\cdot 0 = 0$$

for each element A of $\mathfrak{R}$.

Since for two elements A and B of $\mathfrak{R}$

$$A\cdot B+A(-B) = A(B+(-B)) = A\cdot 0 = 0,$$

and $(-A)B+(-A)(-B) = (-A)(B+(-B)) = (-A)\cdot 0 = 0,$

we have $$A(-B) = -(AB),$$

and $$(-A)(-B) = AB.$$

§ 6. It may happen that certain elements of a ring $\mathfrak{R}$ taken by themselves form a ring $\mathfrak{S}$. This ring $\mathfrak{S}$ is called a *subring* of $\mathfrak{R}$, and is said to be contained in $\mathfrak{R}$.

If a set $\mathfrak{S}$ of certain elements of $\mathfrak{R}$ satisfies postulates 1, 4, 5 and 6 of § 1, III, (b), it is evidently a subring of $\mathfrak{R}$. The simplest possible subring is that which consists of the element 0 alone.

Now let $\mathfrak{S}$ be a subring of a given ring $\mathfrak{R}$, and A be an element of $\mathfrak{R}$. Denote by the symbol $\mathfrak{S}+A$ the set consisting of all the elements of $\mathfrak{R}$, which are expressed in the form $S+A$ where S is an element of $\mathfrak{S}$. This set $\mathfrak{S}+A$ is called a *co-set* of $\mathfrak{R}$ as regards $\mathfrak{S}$.

If A belongs to the subring $\mathfrak{S}$, the co-set $\mathfrak{S}+A$ evidently coincides with $\mathfrak{S}$; but if not, $\mathfrak{S}$ and $\mathfrak{S}+A$ have no common element. Two co-sets $\mathfrak{S}+A$ and $\mathfrak{S}+B$ either are identical or have no common element. Indeed, if $S_1+A=S_2+B$, where S_1 and S_2 are elements of $\mathfrak{S}$, we have

$$A = (S_2+(-S_1))+B$$

and, consequently, A belong to $\mathfrak{S}+B$; and similarly, B also belongs to $\mathfrak{S}+A$. Therefore $\mathfrak{S}+A$ and $\mathfrak{S}+B$ are identical. Therefore *if $\mathfrak{S}$ is a subring of the ring $\mathfrak{R}$, the elements of $\mathfrak{R}$ are divided into co-sets of $\mathfrak{R}$ as regards $\mathfrak{S}$, such that every element of $\mathfrak{R}$ belongs to one, and only one, of the co-sets.*

§ 7. The changeability of the definition of equality in a ring, under the conditions stated in § 1. Let $\mathfrak{R}$ be a ring; and suppose that the definition of equality has been changed so that $\mathfrak{R}$ remains also a ring. Let $\mathfrak{M}$ be the set formed by all the elements of $\mathfrak{R}$ which become congruent to the element 0 of $\mathfrak{R}$ after the change considered. If an element M belongs to $\mathfrak{M}$, the element $-M$ also belongs to $\mathfrak{M}$. For, since

$$M\equiv 0 \qquad \text{(by the assumption)}$$

and $$-M\equiv -M,$$

we have

$$M+(-M) \equiv 0+(-M) \qquad \text{(by the unique composition),}$$

or

$$0 \equiv -M;$$

therefore $-M$ belongs to $\mathfrak{M}$. Next, let M_1 and M_2 be any two elements of $\mathfrak{M}$, and A an element of $\mathfrak{R}$; then we have

$$\begin{aligned} M_1+M_2 &\equiv 0+0 \equiv 0,\\ M_1+(-M_2) &\equiv 0+0 \equiv 0, \end{aligned}$$

and

$$A \cdot M_1 \equiv A \cdot 0 \equiv 0.$$

Therefore, $\mathfrak{M}$ is a subring of $\mathfrak{R}$ such that every element of $\mathfrak{M}$ multiplied by an element of $\mathfrak{R}$ also belongs to $\mathfrak{M}$. This set $\mathfrak{M}$ is nothing but Dedekind's *ideal*[1], which is considered in the ring $\mathfrak{R}$, abstractly defined.

We here define an ideal in an abstract ring as follows:

A set $\mathfrak{M}$ of elements of a ring is called an *ideal* of the ring when it satisfies the following three conditions:

1. The sum of any two elements of $\mathfrak{M}$ is also an element of $\mathfrak{M}$.
2. If an element M belongs to $\mathfrak{M}$, $-M$ also belongs.
3. The product of any element of $\mathfrak{M}$ and any element of $\mathfrak{R}$ is an element of $\mathfrak{M}$.

In other words, an ideal $\mathfrak{M}$ is a subring of $\mathfrak{R}$ such that every element multiplied by an element of $\mathfrak{R}$ also belongs to $\mathfrak{M}$.

Returning to the subject in question, if A be an element of $\mathfrak{R}$, the elements of the co-set $\mathfrak{M}+A$ of $\mathfrak{R}$ as regards $\mathfrak{M}$ become congruent to one another by the change considered, because of the unique composition. When an element B of $\mathfrak{R}$ becomes congruent to another A by the change, i.e. $B \equiv A$, we have

$$B+(-A) \equiv A+(-A) \equiv 0;$$

hence

$$B+(-A) = M,$$

or

$$B = M+A,$$

where M denotes an element of $\mathfrak{M}$; this shows that B belongs to the co-set $\mathfrak{M}+A$. Therefore the elements which become congruent to A all belong to the same co-set $\mathfrak{M}+A$; and, conversely, each element of the co-set $\mathfrak{M}+A$ becomes congruent to A. Hence we have the

[1] Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 4. ed., § 177.

THEOREM: *A change of the definition of equality in a ring under the restriction stated in § 1 is possible when, and only when, the following three conditions are satisfied:*

(i) *The elements of a given ring $\mathfrak{R}$, which become congruent to the element* 0 *of $\mathfrak{R}$, form an ideal $\mathfrak{M}$ of $\mathfrak{R}$.*

(ii) *The elements of the same co-set of $\mathfrak{R}$ as regards $\mathfrak{M}$ become congruent to one another.*

(iii) *The elements congruent to one another belong to the same co-set of $\mathfrak{R}$ as regards $\mathfrak{M}$.*

To prove the sufficiency of these conditions, let $\mathfrak{M}$ be an ideal of $\mathfrak{R}$; and suppose that the change of the definition of equality is made as above. Then, the conditions for the equality are evidently satisfied. If A and B are two elements of $\mathfrak{R}$, and if M_1 and M_2 are two elements of $\mathfrak{M}$, then we have

$$(M_1+A)+(M_2+B) = (M_1+M_2)+(A+B),$$

and

$$(M_1+A)(M_2+B) = (M_1M_2+AM_2+BM_1)+AB,$$

which belong to the co-sets $\mathfrak{M}+(A+B)$ and $\mathfrak{M}+(AB)$ respectively; hence

$$(M_1+A)+(M_2+B) \equiv A+B,$$

and

$$(M_1+A)(M_2+B) \equiv AB.$$

These show the uniqueness of the composition; and it is easily shown that the postulates for a ring in §1, III hold.

§ 8. For such a change of the definition of equality as considered, an ideal must be introduced; and a given ideal determines the change completely, as desired. Therefore, we here define again.[1]

When, the definition of equality in a given ring $\mathfrak{R}$ being so changed that each element of an ideal $\mathfrak{M}$ of $\mathfrak{R}$ becomes equal to the element 0, two elements A and B become equal to each other, the elements A and B are said to be *congruent* with respect to the modulus $\mathfrak{M}$; and this is expressed in writing by

$$A \equiv B \text{ (mod. } \mathfrak{M}).$$

The concept of congruence in arithmetic is nothing but a change of the definition of equality; and, hence, ideals must be naturally introduced as moduli in congruences.

[1] This definition coincides with what is usually adopted.

When the definition of equality is changed in a field, the set of the elements which become congruent to the element 0 must have the same properties as the ideal above stated, and must consequently contain all the elements of the field, if it contains any one element other than 0. Hence in a field no congruence is considered.

N.B. This definition of cougruence is applicable also when the modulus $\mathfrak{M}$ is the ideal consisting of the element 0 alone ; this is the case when the definition of equality is not changed.

Quotient Rings.

§ 9. Definitions. Let $\mathfrak{M}$ be an ideal of a ring $\mathfrak{R}$. The ring, to which $\mathfrak{R}$ reduces when we take the elements of $\mathfrak{R}$ with respect to the modulus $\mathfrak{M}$, is called the *quotient ring*[1] of $\mathfrak{R}$ as regards $\mathfrak{M}$; and it is represented by the symbol $\frac{\mathfrak{R}}{\mathfrak{M}}$.

The number of incongruent (mod. $\mathfrak{M}$) elements in the ring $\mathfrak{R}$ is called the *norm* of $\mathfrak{M}$ under $\mathfrak{R}$, as in the theory of ideals in algebraic number-fields.

A ring is said to be *composite* or *simple*, according as it does or does not possess at least one ideal other than the ring itself and that consisting of the element 0 alone.

Let $\mathfrak{A}$ and $\mathfrak{B}$ be two ideals of a ring $\mathfrak{R}$; and suppose that $\mathfrak{B}$ contains $\mathfrak{A}$. Then the ideal $\mathfrak{A}$ of $\mathfrak{R}$ is evidently also an ideal of $\mathfrak{B}$; and a complete set of incongruent (mod. $\mathfrak{A}$) elements of $\mathfrak{B}$, that is, the quotient ring $\frac{\mathfrak{B}}{\mathfrak{A}}$, is an ideal of $\frac{\mathfrak{R}}{\mathfrak{A}}$. For, if B_1 and B_2 (mod. $\mathfrak{A}$) be two elements of this set, and R (mod. $\mathfrak{A}$) an element of $\frac{\mathfrak{R}}{\mathfrak{A}}$, then we have

$$\begin{aligned} B_1+B_2 &\equiv 0 \quad (\text{mod. } \mathfrak{B}), \\ B_1+(-B_2) &\equiv 0 \quad (\text{mod. } \mathfrak{B}), \\ \text{and} \qquad RB_1 &\equiv 0 \quad (\text{mod. } \mathfrak{B}); \end{aligned}$$

and moreover each of these three elements B_1+B_2, $B_1+(-B_2)$ and RB_1 is congruent (mod. $\mathfrak{A}$) to one of the set considered. Hence the set is an ideal of $\frac{\mathfrak{R}}{\mathfrak{A}}$.

If, conversely, a set Γ of elements

[1] The term 'quotient ring' and the symbol $\frac{\mathfrak{R}}{\mathfrak{M}}$ are adopted, as in the case of groups, from the view that both come from the same idea congruence. If $\mathfrak{M}$ is the ideal consisting of the element 0 alone, the quotient $\frac{\mathfrak{R}}{\mathfrak{M}}$ coincides with the original $\mathfrak{R}$.

$$B,\ B',\ B'',\ \ldots\ldots \ (\text{mod. } \mathfrak{A})$$

of $\frac{\mathfrak{R}}{\mathfrak{A}}$ be an ideal of $\frac{\mathfrak{R}}{\mathfrak{A}}$, the elements of the co-sets

$$\mathfrak{A}+B,\ \mathfrak{A}+B',\ \mathfrak{A}+B'',\ \ldots\ldots$$

of $\mathfrak{R}$ as regards $\mathfrak{A}$, taken together, constitute an ideal of $\mathfrak{R}$. For, take any two elements, say $A+B$ and $A'+B'$, from the co-sets and an element R from $\mathfrak{R}$, and, since Γ is an ideal of $\frac{\mathfrak{R}}{\mathfrak{A}}$, we have

$$\begin{aligned} &(A+B)+(A'+B') &&\equiv B+B' &&\equiv B_1 \quad (\text{mod. } \mathfrak{A}),\\ &(A+B)+\{-(A'+B')\} &&\equiv B+(-B') &&\equiv B_2 \quad (\text{mod. } \mathfrak{A}),\\ \text{and}\quad &R(A+B) &&\equiv RB &&\equiv B_3 \quad (\text{mod. } \mathfrak{A}), \end{aligned}$$

where B_1, B_2, B_3 are certain elements of Γ. Therefore the elements $(A+B)+(A'+B')$, $(A+B)+\{-(A'+B')\}$ and $R(A+B)$ are contained in the co-sets $\mathfrak{A}+B_1$, $\mathfrak{A}+B_2$ and $\mathfrak{A}+B_3$ respectively, all of which belong to the said set of co-sets. Therefore the elements of the said co-sets, taken together, form an ideal of $\mathfrak{R}$, whose quotient as regards $\mathfrak{A}$ is Γ. Hence:

If $\mathfrak{B}$ is an ideal of $\mathfrak{R}$ which contains another $\mathfrak{A}$, $\frac{\mathfrak{B}}{\mathfrak{A}}$ is an ideal of $\frac{\mathfrak{R}}{\mathfrak{A}}$; and conversely if Γ is an ideal of $\frac{\mathfrak{R}}{\mathfrak{A}}$, there exists an ideal of $\mathfrak{R}$, whose quotient as regards $\mathfrak{A}$ is Γ.

From this follows:

Let $\mathfrak{A}$ be an ideal of a ring $\mathfrak{R}$. Then $\mathfrak{R}$ does or does not possess an ideal which contains $\mathfrak{A}$ and is distinct from both $\mathfrak{A}$ and $\mathfrak{R}$, according as the quotient ring $\frac{\mathfrak{R}}{\mathfrak{A}}$ is composite or simple.

Definition. If $\mathfrak{A}$, an ideal of a ring $\mathfrak{R}$, is such that there is no ideal of $\mathfrak{R}$, distinct from $\mathfrak{R}$, which contains $\mathfrak{A}$ and is distinct from $\mathfrak{A}$, then $\mathfrak{A}$ is called a *maximal* ideal of $\mathfrak{R}$.

If the norm of an ideal $\mathfrak{A}$ under $\mathfrak{R}$ is finite, there exists at least one maximal ideal of $\mathfrak{R}$.

§ 10. Let $\mathfrak{A}$ and $\mathfrak{B}$ be two ideals of a ring $\mathfrak{R}$. The set of all the elements which are expressed in the form $A+B$, where A and B mean elements of $\mathfrak{A}$ and $\mathfrak{B}$ respectively, is easily shown to be an ideal of $\mathfrak{R}$; this ideal derived from $\mathfrak{A}$ and $\mathfrak{B}$ is expressed by the symbol $(\mathfrak{A}, \mathfrak{B})$, as used commonly. The ideal $(\mathfrak{A}, \mathfrak{B})$ contains $\mathfrak{A}$ and $\mathfrak{B}$, and is contained in every ideal which contains both $\mathfrak{A}$ and $\mathfrak{B}$.

Next, if $\mathfrak{D}$ be the set of the elements common to $\mathfrak{A}$ and $\mathfrak{B}$, $\mathfrak{D}$

is also an ideal of $\mathfrak{R}$, which is called the *cross-cut* of $\mathfrak{A}$ and $\mathfrak{B}$. Indeed, if D be an element of $\mathfrak{D}$, the elements $-D$ and RD, where R is an element of R, belong to $\mathfrak{D}$, since D belongs to both $\mathfrak{A}$ and $\mathfrak{B}$.

Now let A and A_1 be two elements of the ideal $\mathfrak{A}$, and B and B_1 two of the ideal $\mathfrak{B}$. If

$$A+B \equiv A_1+B_1 \pmod{\mathfrak{D}},$$

then

$$A+(-A_1) \equiv B_1+(-B) \pmod{\mathfrak{D}}.$$

Hence $A+(-A_1)$ is an element of $\mathfrak{B}$, while it belongs to $\mathfrak{A}$; and consequently we have

$$A+(-A_1) \equiv 0 \pmod{\mathfrak{D}},$$

or

$$A \equiv A_1 \pmod{\mathfrak{D}},$$

and similarly

$$B \equiv B_1 \pmod{\mathfrak{D}}.$$

Thus from

$$A+B \equiv A_1+B_1 \pmod{\mathfrak{D}}$$

it follows that

$$A \equiv A_1 \pmod{\mathfrak{D}},$$

and

$$B \equiv B_1 \pmod{\mathfrak{D}};$$

and of this the converse is evidently true. Therefore *the elements of the form $A+B$, where A and B run over complete sets of incongruent (mod. $\mathfrak{D}$) elements of $\mathfrak{A}$ and $\mathfrak{B}$ respectively, form a complete set of incongruent (mod. $\mathfrak{D}$) elements of $(\mathfrak{A}, \mathfrak{B})$, which is the quotient* $\dfrac{(\mathfrak{A}, \mathfrak{B})}{\mathfrak{D}}$.

Composition-Series of a Ring.

§ 11. Definition. Let $\mathfrak{R}$ and $\mathfrak{R}'$ be two rings. If a correspondence can be established between the elements of $\mathfrak{R}$ and those of $\mathfrak{R}'$, so that, if A and B be two elements of $\mathfrak{R}$ and A' and B' the two corresponding elements of $\mathfrak{R}'$, then (i) A' and B' are equal or unequal to each other, according as A and B are equal or unequal, (ii) to the sum $A+B$ there corresponds the sum $A'+B'$ and (iii) to the product AB there corresponds the product $A'B'$, then the two rings $\mathfrak{R}$ and $\mathfrak{R}'$ are said to be *isomorphic*, or of the same *type*.

THEOREM: *If $\mathfrak{A}$ and $\mathfrak{B}$ are two ideals of a ring and if $\mathfrak{D}$ is the cross-cut of $\mathfrak{A}$ and $\mathfrak{B}$, the quotient rings $(\mathfrak{A}, \mathfrak{B})/\mathfrak{B}$ and $\mathfrak{A}/\mathfrak{D}$ are of the same type, as also are the quotient rings $(\mathfrak{A}, \mathfrak{B})/\mathfrak{A}$ and $\mathfrak{B}/\mathfrak{D}$.*

When we take the elements of $(\mathfrak{A}, \mathfrak{B})$ with respect to the modulus $\mathfrak{B}$, the elements which become $\equiv 0$ (mod. $\mathfrak{B}$) are the elements of $\mathfrak{B}$, and those of $\mathfrak{A}$ which belong to $\mathfrak{D}$. If two elements A_1 and A_2 of $\mathfrak{A}$ are incongruent (mod. $\mathfrak{D}$), then these are also incongruent (mod. $\mathfrak{B}$), when A_1 and A_2 are considered for elements of $(\mathfrak{A}, \mathfrak{B})$. For, if it were true that $A_1 \equiv A_2$ (mod. $\mathfrak{B}$), then would

$$A_1 + (-A_2) \equiv 0 \ (\text{mod. } \mathfrak{B}),$$

i.e. $A_1+(-A_2)$ would be an element of $\mathfrak{B}$, while belonging to $\mathfrak{A}$. Hence $A_1+(-A_2)$ would belong to $\mathfrak{D}$, i.e. $A_1 \equiv A_2$ (mod. $\mathfrak{D}$); but this contradicts the assumption that A_1 and A_2 are incongruent (mod. $\mathfrak{D}$). Therefore, now, let

$$A_1, \ A_2, \ A_3, \ldots\ldots \ (\text{mod. } \mathfrak{D})$$

be a complete set of incongruent (mod. $\mathfrak{D}$) elements of $\mathfrak{A}$, which gives the ring $\mathfrak{A}/\mathfrak{D}$, then the elements

$$A_1, \ A_2, \ A_3, \ldots\ldots \ (\text{mod. } \mathfrak{B}),$$

being considered for elements of $(\mathfrak{A}, \mathfrak{B})$ and being taken with respect to the modulus $\mathfrak{B}$, give a complete set of incongruent (mod. $\mathfrak{B}$) elements of $(\mathfrak{A}, \mathfrak{B})$, which is the ring $(\mathfrak{A}, \mathfrak{B})/\mathfrak{B}$. And moreover if

$$\begin{aligned} & A_1 + A_2 \equiv A_3 \quad (\text{mod. } \mathfrak{B}), \\ \text{or} \qquad & A_1 A_2 \quad \equiv A_3 \quad (\text{mod. } \mathfrak{B}), \end{aligned}$$

then, as shown already, we have

$$\begin{aligned} & A_1 + A_2 \equiv A_3 \quad (\text{mod. } \mathfrak{D}), \\ \text{or} \qquad & A_1 A_2 \quad \equiv A_3 \quad (\text{mod. } \mathfrak{D}) \end{aligned}$$

respectively. Therefore, by establishing a correspondence between the elements of $(\mathfrak{A}, \mathfrak{B})/\mathfrak{B}$ and those of $\mathfrak{A}/\mathfrak{D}$, so that to $A_1, A_2, A_3, \ldots\ldots$ (mod. $\mathfrak{B}$) of the former there correspond respectively $A_1, A_2, A_3, \ldots\ldots$ (mod. $\mathfrak{D}$) of the latter, we can see that these two rings are of the the same type. Similarly the rings $(\mathfrak{A}, \mathfrak{B})/\mathfrak{A}$ and $\mathfrak{B}/\mathfrak{D}$ can be treated.

Cor. I. If $\mathfrak{A}$ and $\mathfrak{B}$ are two distinct maximal ideals of a ring $\mathfrak{R}$, and if $\mathfrak{D}$ is the cross-cut of $\mathfrak{A}$ and $\mathfrak{B}$, then the quotient rings $\mathfrak{R}/\mathfrak{B}$ and $\mathfrak{A}/\mathfrak{D}$ are of the same type, as also are the quotient rings $\mathfrak{R}/\mathfrak{A}$ and $\mathfrak{B}/\mathfrak{D}$; and consequently $\mathfrak{D}$ is a maximal ideal of both $\mathfrak{A}$ and $\mathfrak{B}$. (cf. §9).

Cor. 2. Let $\mathfrak{A}$ and $\mathfrak{B}$ be two distinct ideals of a ring $\mathfrak{R}$, and $\mathfrak{D}$ their cross-cut. If there is no ideal of $\mathfrak{R}$ which is contained in $\mathfrak{A}$ and contains $\mathfrak{D}$, there is no ideal of $\mathfrak{R}$ which is contained in $(\mathfrak{A}, \mathfrak{B})$ and contains $\mathfrak{B}$.

For, if there were an ideal $\mathfrak{C}$ of $\mathfrak{R}$, which was contained in $(\mathfrak{A}, \mathfrak{B})$ and contained $\mathfrak{B}$, $\mathfrak{C}$ would contain elements of $\mathfrak{A}$ which do not belong to $\mathfrak{B}$; but not all of the elements of $\mathfrak{A}$ would be contained in $\mathfrak{C}$. Hence the cross-cut of two ideals $\mathfrak{A}$ and $\mathfrak{C}$ of $\mathfrak{R}$ would be larger than $\mathfrak{D}$ and distinct from $\mathfrak{A}$. This contradicts the assumption that $\mathfrak{A}$ contains no ideal of $\mathfrak{R}$ which contains $\mathfrak{D}$.

§ 12. Let $\mathfrak{A}_1$ be a maximal ideal of a given ring $\mathfrak{R}$, $\mathfrak{A}_2$ a maximal ideal of $\mathfrak{A}_1$, and so on.

Definitions. When the series of rings

$$(A) \qquad \mathfrak{R},\ \mathfrak{A}_1,\ \mathfrak{A}_2,\ \ldots\ldots$$

can be obtained in the manner just described, the series (A) is called a *composition-series*[1] of $\mathfrak{R}$.

The set of rings

$$\frac{\mathfrak{R}}{\mathfrak{A}_1},\ \frac{\mathfrak{A}_1}{\mathfrak{A}_2},\ \ldots\ldots$$

is called a set of quotient rings of $\mathfrak{R}$ derived from the composition-series (A).

Take the first n terms from the series (A). And the series

$$\mathfrak{R},\ \mathfrak{A}_1,\ \mathfrak{A}_2,\ \ldots\ldots,\ \mathfrak{A}_{n-1}$$

thus obtained is called a composition-series of $\mathfrak{R}$ which has $\mathfrak{A}_{n-1}$ as the last term.

A ring under which the norm of each ideal is finite, such as a ring generated by an algebraic integer, has always a composition-series; and in this case each of the quotient rings is finite in number of elements.

It may happen that a ring has more than one distinct composition-series; but we can prove the

THEOREM[2]: *Any two composition-series of a ring, whose last terms are the same, consist of the same number of terms and lead to two sets*

[1] The series is named a composition-series as in the case of groups.

[2] This is analogous to the important theorem on composition-series of a group, due to Hölder, but somewhat generalized. Cf. Burnside, Theory of Groups of Finite Order, 2. de., pp. 64-69.

of quotient rings, which are identica! with each other except as regards the sequence in which they occur.

Let us suppose that, if the number of terms of one of two composition-series of a given ring, whose last terms are the same, is not greater than a given number n, it has already been shown that these two series contain the same number of terms and that the quotient rings derived from them are identical except as regards their sequence. If a ring $\mathfrak{R}$ has two composition-series having the same last term, one of which consists of $n+1$ terms, let them be

(1) $$\mathfrak{R},\ \mathfrak{A}_1,\ \mathfrak{A}_2,\ \ldots\ldots,\ \mathfrak{A}_n,$$

and

(2) $$\mathfrak{R},\ \mathfrak{B}_1,\ \mathfrak{B}_2,\ \ldots\ldots,\ \mathfrak{B}_m,$$

where $\mathfrak{B}_m$ is identical with $\mathfrak{A}_n$, and $m \geqq n$. If $\mathfrak{A}_1$ and $\mathfrak{B}_1$ are identical, it evidently follows, from the supposition, that $m=n$ and that the two sets of quotient rings derived from them are identical except as regards their sequence. If on the contrary $\mathfrak{A}_1$ and $\mathfrak{B}_1$ are distinct, let $\mathfrak{D}$ be the cross-cut of $\mathfrak{A}_1$ and $\mathfrak{B}_1$. Then $\mathfrak{D}$ is a maximal ideal of both $\mathfrak{A}_1$ and $\mathfrak{B}_1$ (§ 11, cor. 1). And $\mathfrak{D}$ contains $\mathfrak{A}_n$; because $\mathfrak{A}_1$ and $\mathfrak{B}_1$ contain $\mathfrak{A}_a$ and $\mathfrak{B}_m$ respectively, while $\mathfrak{A}_n$ and $\mathfrak{B}_m$ are identical. If $\mathfrak{D}$ coincides with $\mathfrak{A}_2$, $\mathfrak{D}$ has a composition-series consisting of $n-1$ terms, having the last term $\mathfrak{A}_n$. If $\mathfrak{D}$ does not coincide with $\mathfrak{A}_2$, let $\mathfrak{D}_1$ be the cross-cut of $\mathfrak{D}$ and $\mathfrak{A}_2$. Then $\mathfrak{D}_1$ is a maximal ideal of both $\mathfrak{D}$ and $\mathfrak{A}_2$, and contains $\mathfrak{A}_n$. If $\mathfrak{D}_1$ coincides with $\mathfrak{A}_3$, $\mathfrak{D}$ has a composition-series containing $n-1$ terms, with the last term $\mathfrak{A}_n$. If not, take $\mathfrak{D}_2$ as the cross-cut of $\mathfrak{D}_1$ and $\mathfrak{A}_3$ Then $\mathfrak{D}_2$ is a maximal ideal of both $\mathfrak{D}_1$ and $\mathfrak{A}_3$, and contains $\mathfrak{A}_n$. If $\mathfrak{D}_2$ does not yet coincide with $\mathfrak{A}_4$, continue this process. Since the number of terms of the series (1) is finite, it can be shown that, after a finite number of repetitions, we reach a composition-series

$$\mathfrak{D},\ \mathfrak{D}_1,\ \mathfrak{D}_2,\ \ldots\ldots,\ \mathfrak{D}_{n-2}\ (\mathfrak{D}_{n-2}=\mathfrak{A}_n)$$

of $\mathfrak{D}$ which has $\mathfrak{A}_n$ as the last term; and that the series

(3) $$\mathfrak{R},\ \mathfrak{A}_1,\ \mathfrak{D},\ \mathfrak{D}_1,\ \ldots\ldots,\ \mathfrak{D}_{n-2}\ (\mathfrak{D}_{n-2}=\mathfrak{A}_n),$$

and

(4) $$\mathfrak{R},\ \mathfrak{B}_1,\ \mathfrak{D},\ \mathfrak{D}_1,\ \ldots\ldots,\ \mathfrak{D}_{n-2}\ (\mathfrak{D}_{n-2}=\mathfrak{A}_n)$$

are two composition-series of $\mathfrak{R}$, which have the same last term, contain the same number of terms and give the same quotient rings. For it has been shown in § 11, cor. 1 that $\mathfrak{R}/\mathfrak{A}_1$ and $\mathfrak{B}_1/\mathfrak{D}$ are of the same type, as also are $\mathfrak{R}/\mathfrak{B}_1$ and $\mathfrak{A}_1/\mathfrak{D}$. But the two composition-series

$$\mathfrak{A}_1,\ \mathfrak{A}_2,\ \mathfrak{A}_3,\ \ldots\ldots,\ \mathfrak{A}_n,$$

and

$$\mathfrak{A}_1,\ \mathfrak{D},\ \mathfrak{D}_1,\ \ldots\ldots,\ \mathfrak{D}_{n-2}\ (\mathfrak{D}_{n-2} = \mathfrak{A}_n)$$

of $\mathfrak{A}_1$ have the same last term $\mathfrak{A}_n$, and the former contains just n terms. Hence they give the same quotient rings by supposition. Since the composition-series

$$\mathfrak{B}_1,\ \mathfrak{B}_2,\ \ldots\ldots,\ \mathfrak{B}_m \quad (\mathfrak{B}_m = \mathfrak{A}_n),$$

and

$$\mathfrak{B}_1,\ \mathfrak{D},\ \mathfrak{D}_1,\ \ldots\ldots\ \mathfrak{D}_{n-2} \quad (\mathfrak{D}_{n-2} = \mathfrak{A}_n)$$

of $\mathfrak{B}_1$ also have the same last term, and the latter contains n terms, they by supposition contain the same number of terms and give the same quotient rings. Hence the series (1) and (3) must contain the same number of terms and give the same quotient rings, as also do the series (2) and (4), while the same holds for the series (3) and (4). The theorem, therefore, is also true when the number of terms of one of two composition-series of a ring is $n+1$. The theorem is true when $n=3$. For let

$$\mathfrak{R},\ \mathfrak{A}_1,\ \mathfrak{A}_2,$$

and

$$\mathfrak{R},\ \mathfrak{B}_1,\ \mathfrak{B}_2,\ \ldots\ldots$$

be two composition-series of $\mathfrak{R}$ which have $\mathfrak{A}_2$ as the last terms. If $\mathfrak{B}_1$ coincides with $\mathfrak{A}_1$, $\mathfrak{B}_2$ must be identical with $\mathfrak{A}_2$; because $\mathfrak{B}_2$ contains the maximal ideal $\mathfrak{A}_2$ of $\mathfrak{A}_1$. Hence we need only consider the case where $\mathfrak{A}_1$ and $\mathfrak{B}_1$ are distinct. The cross-cut of $\mathfrak{A}_1$ and $\mathfrak{B}_1$ is a maximal ideal of both $\mathfrak{A}_1$ and $\mathfrak{B}_1$, and moreover contains $\mathfrak{A}_2$; hence the cross-cut must coincide with $\mathfrak{A}_2$ and also with $\mathfrak{B}_2$, since $\mathfrak{B}_2$ is a maximal ideal of $\mathfrak{B}_1$, which contains $\mathfrak{A}_2$. Therefore both the series contain three terms, and have $\mathfrak{A}_2$, which is the cross-cut of $\mathfrak{A}_1$ and $\mathfrak{B}_1$, as their last terms; and consequently give the same quotient rings (by § 11, cor. 1). The theorem is therefore universally true.

§ 13. Definition. Let

$$\mathfrak{R},\ \mathfrak{A}_1,\ \mathfrak{A}_2,\ \ldots\ldots$$

be a series of ideals of a ring $\mathfrak{R}$, in which each ideal is contained in the preceding one, while there is no ideal of $\mathfrak{R}$ contained in any single ideal of the series also containing the next ideal. The series, if it exists, shall be called a *chief-composition-series* of $\mathfrak{R}$.

The series

$$\mathfrak{R},\ \mathfrak{A}_1,\ \mathfrak{A}_2,\ \ldots\ldots,\ \mathfrak{A}_{n-1},$$

which consists of the first n terms of the said chief-composition-series of $\mathfrak{R}$, is called a chief-composition-series of $\mathfrak{R}$ which has $\mathfrak{A}_{n-1}$ as the last term.

THEOREM: *Any two chief-composition-series of a ring, whose last terms are the same, consist of the same number of terms and lead to two sets of quotient rings, which are identical with each other except as regards the sequence in which they occur.*

Let us suppose that, when the number of terms of one of two chief-composition-series of a given ring is not greater than a given number n, the theorem holds true. If a ring $\mathfrak{R}$ has two chief-composition-series which have the same last terms and one of which is of $(n+1)$ terms, let them be

$$\mathfrak{R},\ \mathfrak{A}_1,\ \ldots\ldots,\ \mathfrak{A}_{n-1},\ \mathfrak{A}_n,$$

and

$$\mathfrak{R},\ \mathfrak{B}_1,\ \ldots\ldots,\ \mathfrak{B}_{m-1},\ \mathfrak{B}_m,$$

where $\mathfrak{B}_m$ is identical with $\mathfrak{A}_n$, and $m \geqq n$. If $\mathfrak{A}_{n-1}$ and $\mathfrak{B}_{m-1}$ are identical, the theorem holds true for these series by our supposition. If not, take the ideal $(\mathfrak{A}_{n-1}, \mathfrak{B}_{m-1})$ of $\mathfrak{R}$. Then we see by § 11, cor. 2 that there is no ideal of $\mathfrak{R}$ which is contained in $(\mathfrak{A}_{n-1}, \mathfrak{B}_{m-1})$ and contains $\mathfrak{A}_{n-1}$ or $\mathfrak{B}_{m-1}$. If $(\mathfrak{A}_{n-1}, \mathfrak{B}_{m-1})$ is distinct from $\mathfrak{A}_{n-2}$, this process is repeated. By proceeding thus in reverse order, as in the proof of the last theorem, we have a chief-composition-series of $\mathfrak{R}$ which has $(\mathfrak{A}_{n-1}, \mathfrak{B}_{m-1})$ as its last term. And it is shown similarly that the theorem is also true when the number of terms of one of the series is $n+1$, and moreover that it is true for $n=3$. Therefore it is universally true.

Simple Rings.

§ 14. Let $\mathfrak{R}$ be a ring and A a given element of $\mathfrak{R}$. *The set $\mathfrak{M}$ of all the elements X for which $AX=0$ is an ideal of $\mathfrak{R}$.* Indeed, if X_1 and X_2 are two elements of $\mathfrak{M}$ and if R is an element of $\mathfrak{R}$, we have

$$A(-X_1) = 0,$$

$$A(X_1+X_2) = AX_1+AX_2 = 0,$$

and $$A \cdot X_1R = 0,$$

which show that $\mathfrak{M}$ is an ideal of $\mathfrak{R}$.

In case $\mathfrak{R}$ is simple, $\mathfrak{M}$ must be either $\mathfrak{R}$ itself or the ideal consisting of the element 0 alone. Therefore if $A=0$, $\mathfrak{M}$ evidently coincides with $\mathfrak{R}$; but if $A \neq 0$, the equation $AX=0$ as regards X is satisfied either by the element 0 only or by each element of $\mathfrak{R}$. If for each element A, except 0, the equation $AX=0$ as regards X has only one root $X=0$, then the product BC of two elements B and C of $\mathfrak{R}$ is equal to 0 when, and only when, at least one of B and C is equal to 0. Suppose, on the contrary, that for a certain element A, not equal to 0, the equation $AX=0$ is satisfied by each element of $\mathfrak{R}$. Take any two elements B and C from $\mathfrak{R}$. If $BC \neq 0$, then the ideal of $\mathfrak{R}$, which consists of all the roots of the equation $BX=0$, contains 0 and A, but not C; consequently $\mathfrak{R}$ can not be simple. Therefore if $\mathfrak{R}$ is simple, the product of any two elements of $\mathfrak{R}$ must be equal to 0, under the above assumption. Thus if the ring $\mathfrak{R}$ is simple, there occur the two cases:

(i) The product of two elements of $\mathfrak{R}$ is equal to 0 when, and only when, at least one of the factors is equal to 0;

(ii) The product of any two elements is equal to 0.

Considering the first case, let A and B be two elements of $\mathfrak{R}$, and $A \neq 0$. If there is in $\mathfrak{R}$ no element X such that $AX=B$, the set of the elements C, for which the equation $AX=C$ has at least one root, must be an ideal of $\mathfrak{R}$, which is distinct from both $\mathfrak{R}$ itself and the ideal consisting of the element 0 alone. But, since $\mathfrak{R}$ is simple, the equation $AX=B$ as regards X must have a root. Therefore the postulates (i) and (ii) of § 1 hold, and $\mathfrak{R}$ must be a field. It has been shown already in § 8 that a field is a simple ring.

Considering the second case, take an element V not equal to 0 from $\mathfrak{R}$. If the sum of a finite number of V is never equal to 0, the set

$$0, \pm V, \pm 2V, \ldots\ldots,$$

where nV means V taken n times, must be an ideal of $\mathfrak{R}$ and must coincide with $\mathfrak{R}$, because of the simpleness of $\mathfrak{R}$. But in this case $\mathfrak{R}$ can not be simple, since it contains the ideal consisting of the elements

$$0, \pm 2V, \pm 4V, \ldots\ldots.$$

Therefore the sum of a certain number n of V must be equal to 0, i.e. $nV=0$, and $\mathfrak{R}$ consists of

$$0, V, 2V, \ldots\ldots, (n-1)V.$$

If n is composite and p a factor of n, $\mathfrak{R}$ contains the ideal consisting of the elements

$$0, pV, 2pV, \ldots\ldots, \left(\frac{n}{p}-1\right)pV,$$

and can not be simple. But, since $\mathfrak{R}$ is supposed to be simple, n must be a prime. If, conversely, n is a prime, the ring consisting of

$$0, V, 2V, \ldots\ldots, (n-1)V$$

is simple; because an ideal of a ring is a subring of the ring and the number of the elements of a finite ring is divisible by that of its subring (§ 6). Hence we have the

THEOREM: *A simple ring is either a field or one which consists of p elements*

$$0, V, 2V, \ldots\ldots, (p-1)V,$$

where p is a prime, $pV=0$ but $iV \neq 0$ when $0 < i < p$, and $V^2 = 0$; and conversely.

Let us, further, consider an element V for which $V^2=0$[1]. Then the elements

$$0, \pm V, \pm 2V, \ldots\ldots,$$

where nV means V taken n times, constitute a ring, which we denote by $[V]$. And the elements

$$0, \pm nV, \pm 2nV, \ldots\ldots$$

constitute an ideal of $[V]$, which we denote by $[nV]$. The quotient ring $[V]/[nV]$ consists of

$$0, V, 2V, \ldots\ldots, (n-1)V \pmod{[nV]};$$

and, if n is a prime, it is simple, as stated before.

§ 15. If $\mathfrak{A}$ is a maximal ideal of a ring $\mathfrak{R}$, the quotient ring $\frac{\mathfrak{R}}{\mathfrak{A}}$ is simple, as shown before; and consequently $\frac{\mathfrak{R}}{\mathfrak{A}}$ is either a field or a simple ring of the type $\frac{[V]}{[pV]}$. When $\mathfrak{R}$ contains especially an element U by which every element of $\mathfrak{R}$ multiplied is equal to itself, the quotient ring $\frac{\mathfrak{R}}{\mathfrak{A}}$ as regards the maximal ideal $\mathfrak{A}$ must be a field, because $U^2=U$, and U can not belong to $\mathfrak{A}$.

[1] Such as let V be a vector and let V^2 denote the vector-square.

Minimal Ideals. Types of the Quotient Rings of a Chief-Composition-Series.

§ 16. An ideal $\mathfrak{A}$ of a ring $\mathfrak{R}$ is said to be *minimal* when there is no ideal of $\mathfrak{R}$ which is contained in $\mathfrak{A}$ and is distinct from both $\mathfrak{A}$ and the ideal[1] consisting of the element o alone.

Let $\mathfrak{A}$ be a subring of a ring $\mathfrak{R}$ and R an element of $\mathfrak{R}$. We denote by $R\mathfrak{A}$ the set of all the products formed by multiplying R into each element of $\mathfrak{A}$. Then, if $\mathfrak{A}$ is an ideal of $\mathfrak{R}$, $R\mathfrak{A}$ must be also an ideal of $\mathfrak{R}$, which is contained in $\mathfrak{A}$; and, if the ideal $\mathfrak{A}$ is minimal, $R\mathfrak{A}$ is either coincident with $\mathfrak{A}$ or the o-ideal.

When an element R of $\mathfrak{R}$ is given, the elements X of the ideal $\mathfrak{A}$ of $\mathfrak{R}$, for which $RX=0$, evidently constitute an ideal of $\mathfrak{R}$, which is contained in $\mathfrak{A}$. Therefore, when $\mathfrak{A}$ is minimal, if an element R of $\mathfrak{R}$ multiplied by a certain one, not equal to the element o, of $\mathfrak{A}$ gives o, the element R multiplied by one of $\mathfrak{A}$ must give o. In other words, the elements S of $\mathfrak{R}$, for which $S\mathfrak{A}=0$, form an ideal $\mathfrak{S}$ of $\mathfrak{R}$; and, if $\mathfrak{A}$ is minimal, the product SA, A being an element contained in $\mathfrak{A}$ and not equal to o, is equal to o when, and only when, $S \equiv 0 \pmod{\mathfrak{S}}$.

§ 17. Proceeding to investigate the type of a minimal ideal of a ring, let $\mathfrak{A}$ be a minimal ideal of a ring $\mathfrak{R}$. Then there occur the following three cases to be considered: (i) there exists in $\mathfrak{A}$ at least one element A such that $A\mathfrak{A}$ coincides with $\mathfrak{A}$; (ii) for every element R of $\mathfrak{R}$, $R\mathfrak{A}$ is the o-ideal; (iii) there exists in $\mathfrak{R}$ at least one element R for which $R\mathfrak{A}=\mathfrak{A}$, but $\mathfrak{A}$ multiplied by every element of it gives the o-ideal.

Considering the first case, if A_1 and A_2 are two elements of $\mathfrak{A}$ such that $A_1\mathfrak{A}=0$ and $A_2\mathfrak{A}=0$, then $\{A_1+(\pm A_2)\}\mathfrak{A}=0$, and $RA_1\mathfrak{A}=0$, where R is an element of $\mathfrak{R}$; and moreover $A_1+(\pm A_2)$ and RA_1 both belong to $\mathfrak{A}$. Therefore the elements X of $\mathfrak{A}$ for which $X\mathfrak{A}=0$ form an ideal of $\mathfrak{R}$ which is contained in $\mathfrak{A}$; and must be either the o-ideal or $\mathfrak{A}$ itself, because $\mathfrak{A}$ is minimal. But, since there is assumed the existence of an element of $\mathfrak{A}$ by which $\mathfrak{A}$ multiplied coincides with itself, the said ideal must be the o-ideal. Hence for every element A, except o, of $\mathfrak{A}$ the ideal $A\mathfrak{A}$ coincides with $\mathfrak{A}$. Consequently for any two elements A and B of $\mathfrak{A}$, provided that A is not equal to o, there exists in $\mathfrak{A}$ at least one element X such that $AX=B$; showing that $\mathfrak{A}$ is a field.

[1] Hereafter the ideal consisting of the element o alone will be called the o-ideal.

In the second case the products of every two elements of $\mathfrak{A}$ are all equal to o, and every ideal of $\mathfrak{A}$ is also an ideal of $\mathfrak{R}$. Hence $\mathfrak{A}$ must be a simple ring in which every product of its elements is equal to o; consequently $\mathfrak{A}$ is a finite simple ring of the type

$$0,\ V,\ 2V,\ \ldots\ldots,\ (p-1)\,V,$$

where $V^2 = 0$, $pV = 0$ but $iV \neq 0\,(0 < i < p)$, and p is a prime (§ 14).

Lastly, in the third case every product of elements of $\mathfrak{A}$ is equal to o; and there are again to be considered two cases: there exists or there does not exist in $\mathfrak{A}$ at least one element, not equal to o, such that it, taken a finite number of times, is equal to o. If such elements exist, there must evidently exist at least one element which, taken a prime number of times, makes o. Let it be V, i.e. $pV=0$, but $iV \neq 0\,(0 < i < p)$, where p is a prime and pV means V taken p times. Then the p elements

$$0,\ V,\ 2V,\ \ldots,\ (p-1)\,V$$

form an ideal $\mathfrak{B}$ of $\mathfrak{A}$. If an element R of $\mathfrak{R}$, for which $RV \neq 0$, is taken, the product $R(iV)$, $(0 < i < p)$, is not equal to o (§ 16), and the set $R\mathfrak{B}$ is also an ideal of $\mathfrak{A}$, which either coincides with $\mathfrak{B}$ or has no element, except o, common to $\mathfrak{B}$. Hence by multiplying $\mathfrak{B}$ by each element of $\mathfrak{R}$ we obtain a finite or infinite number of distinct ideals of $\mathfrak{A}$, all of which are of the same type as $\mathfrak{B}$, and every two of which have no common element other than o. They, taken together, produce an ideal of $\mathfrak{R}$ contained in $\mathfrak{A}$; consequently it must coincides with $\mathfrak{A}$. Therefore, if there exists in $\mathfrak{A}$ at least one element, unequal to o, such that it, taken a finite number of times, makes o, the minimal ideal $\mathfrak{A}$ is what is derived from a finite or infinite number of rings of the same type as the said ring $\mathfrak{B}$. Hence we have the

THEOREM: *A minimal ideal of a ring is one of the following four: (i) a field; (ii) a finite simple ring of the type*

$$0,\ V,\ 2V,\ \ldots,\ (p-1)\,V,$$

where $V^2=0$, $pV=0$, and p is prime; (iii) a ring such that every element of it multiplied by any one of it gives o, and it is derived from a finite or infinite number of rings of the type (ii); (iv) a ring such that every element of it multiplied by any one of it gives o, but no element taken a finite number of times is equal to o.

§ 18. Now every field of finite order, according to Prof. Dickson's study[1], is of order p^n, p being a prime, and may be represented as a Galois field of order p^n; and a Galois field is defined uniquely by its order. If, in the case of the type (iii) in the last theorem, the minimal ideal is derived from n rings, it contains p^n unequal elements, and is an Abelian group of order p^n and type (1, 1, 1, ... , with n units) with respect to addition[2]; and consequently it is also uniquely determined by the number of elements. Thus *the type of a minimal ideal of a ring consisting of a finite number of elements is determined uniquely by the number of elements in each case, a field or not.*

§ 19. An example for case (iv). Take the set of pairs (a, b) of real numbers; define addition and multiplication among them as

$$(a,\ b)+(a',\ b') = (a+a',\ b+b')$$

and

$$(a,\ b)(a',\ b') = (aa',\ ab'+a'b),$$

and we have a ring of elements $(a,\ b)$. The elements $(0,\ b)$ form a minimal ideal of this ring, which is of type (iv).

§ 20. Let $\mathfrak{A}$, $\mathfrak{B}$ be two distinct ideals of a ring $\mathfrak{R}$; assume that $\mathfrak{B}$ contains $\mathfrak{A}$. We have shown in § 9 that the quotient ring $\frac{\mathfrak{B}}{\mathfrak{A}}$ is an ideal of $\frac{\mathfrak{R}}{\mathfrak{A}}$ and that to an ideal Γ of $\frac{\mathfrak{R}}{\mathfrak{A}}$, there corresponds the ideal of $\mathfrak{R}$ whose quotient as regards $\mathfrak{A}$ is Γ. If Γ is contained in $\frac{\mathfrak{B}}{\mathfrak{A}}$, the corresponding ideal of $\mathfrak{R}$ is evidently contained in $\mathfrak{B}$. Therefore, if there is no ideal of $\mathfrak{R}$ contained in $\mathfrak{B}$ and containing $\mathfrak{A}$, $\frac{\mathfrak{B}}{\mathfrak{A}}$ must be a minimal ideal of $\frac{\mathfrak{R}}{\mathfrak{A}}$. Hence, *if $\mathfrak{A}_r$ and $\mathfrak{A}_{r+1}$ are two consecutive terms of a chief-composition-series of a ring, there are applicable the facts stated in §§ 17, 18 to the investigation of the type of the quotient ring* $\frac{\mathfrak{A}_r}{\mathfrak{A}_{r+1}}$.

For example, let $\mathfrak{r}$ be the set of the algebraic integers of an algebraic field, and $\mathfrak{p}$, $\mathfrak{q}$ two distinct prime ideals of the field. Then $\mathfrak{p}$ and $\mathfrak{q}$ both are maximal ideals of $\mathfrak{r}$; and there is no ideal of $\mathfrak{r}$ contained in $\mathfrak{p}$ and containing $\mathfrak{p}\mathfrak{q}$ or $\mathfrak{p}^2$, so that the quotient rings

[1] L. E. Dickson, Linear Groups with an exposition of the Galois Field Theory, p. 14.

[2] An Abelian group with respect to addition was called a *Modul* by Dedekind: Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 4 ed., § 168.

$\frac{\mathfrak{p}}{\mathfrak{pq}}$ and $\frac{\mathfrak{p}}{\mathfrak{p}^2}$ are minimal ideals of $\frac{\mathfrak{r}}{\mathfrak{pq}}$ and $\frac{\mathfrak{r}}{\mathfrak{p}^2}$ respectively. And $\frac{\mathfrak{p}}{\mathfrak{pq}}$ is a field, but $\frac{\mathfrak{p}}{\mathfrak{p}^2}$ not.

December, 1916.