On the Reduction of Ideals.

By

Masazo Sono.

(Received Dec. 18, 1923)

This paper is intended to study the representation of ring-ideals as the cross-cut of others from a view of a chief-composition-series, and the main point is the following:—

When the elements of an ideal $\mathfrak{A}$ all belong to another $\mathfrak{B}$, $\mathfrak{A}$ is said to be *divisible* by $\mathfrak{B}$.

An ideal $\mathfrak{M}$ of a ring $\mathfrak{R}$ is called *maximal*, when there is no ideal, distinct from $\mathfrak{M}$ and $\mathfrak{R}$, which divides $\mathfrak{M}$.

The ideals of the ring $\mathfrak{R}$ are divided into two kinds: those which divide powers of $\mathfrak{R}$ belong to the second kind, and the others to the first kind. An ideal of the first kind is divisible by a finite number of maximal ideals of the first kind.

An ideal which is divisible by only one maximal ideal $\mathfrak{M}$ of the first kind divides a power of $\mathfrak{M}$, and this is named a *primary ideal* belonging to $\mathfrak{M}$.

An ideal of the first kind which is divisible by ν maximal ideals of the first kind is capable of representation as the cross-cut of ν primary ideals belonging to the respective maximal ideals.

PRELIMINARIES.

§ 1. When the elements of an ideal $\mathfrak{A}$ all belong to another $\mathfrak{B}$, $\mathfrak{A}$ is said to *be divisible by* $\mathfrak{B}$, and this is denoted by $\mathfrak{A}\equiv 0\ (\mathfrak{B})$.

In this case $\mathfrak{B}$ is called a *divisor* of $\mathfrak{A}$, and $\mathfrak{A}$ a *multiple* of $\mathfrak{B}$[1].

In ideals of an algebraic field *(Körper)*, if $\mathfrak{A}\equiv 0$ $(\mathfrak{B})$, $\mathfrak{A}$ can be represented as the product of $\mathfrak{B}$ and the third ideal. But for a general ring[2] this is not necessarily possible; in this sespect the definition of divisibility is extended.

The ideal $(\mathfrak{A}, \mathfrak{B})$, derived from two ideals $\mathfrak{A}$ and $\mathfrak{B}$, is called the *greatest common divisor* of $\mathfrak{A}$ and $\mathfrak{B}$, and the cross-cut of $\mathfrak{A}$ and $\mathfrak{B}$, i.e. the ideal consisting of the elements common to $\mathfrak{A}$ and $\mathfrak{B}$ the *least commom multiple* of $\mathfrak{A}$ and $\mathfrak{B}$. The latter is denoted by $[\mathfrak{A}, \mathfrak{B}]$.

We divide the ideals of a ring $\mathfrak{R}$ into two kinds: those which divide powers of $\mathfrak{R}$ belong to the *second kind*, and the others to the *first kind*.

§ 2. Let $\mathfrak{A}$ be an ideal divible by another, $\mathfrak{B}$. The ring, to which $\mathfrak{B}$ is reduced when we take the elements of $\mathfrak{B}$ with respect to the modulus $\mathfrak{A}$, is called the *quotient-ring*[3] of $\mathfrak{B}$ by $\mathfrak{A}$; and it is represented by the symbol $\mathfrak{B}/\mathfrak{A}$.

THEOREM[4]: *If $\mathfrak{A}$ and $\mathfrak{B}$ are two ideals of a ring, the quotient-rings $(\mathfrak{A}, \mathfrak{B})/\mathfrak{B}$ and $\mathfrak{A}/[\mathfrak{A}, \mathfrak{B}]$ are of the same type.*

§ 3. An ideal $\mathfrak{M}$ of a ring $\mathfrak{R}$ is called *maximal*[5], when there is no divisor of $\mathfrak{M}$, except $\mathfrak{M}$ and $\mathfrak{R}$.

When $\mathfrak{M}$ is maximal, the quotient-ring $\mathfrak{R}/\mathfrak{M}$ is a field, unless $\mathfrak{R}^2\equiv 0$ $(\mathfrak{M})$; and conversely if $\mathfrak{R}/\mathfrak{M}$ is a field, $\mathfrak{M}$ is maximal[6]. So that we have

THEOREM: *If $\mathfrak{M}$ is a maximal ideal of the first kind, the quotient-ring $\mathfrak{R}/\mathfrak{M}$ is a field; and so conversely.*

N. B. A ring is difined by nine postulates; when a set $\mathfrak{K}$ of elements satisfies the following two postulates in addition to the nine, it is called a *field* (Körper): (i) there exists in $\mathfrak{K}$ an element U such

---

1 E. Noether, Math. Ann., **83**, 26 (1921).
2 These Memoirs **2**, 204 (1917).
3 These Memoirs, **2**, 213 (1917).
4 Loc. cit. p. 215.
5 Loc. cit. p. 214.
6 Loc. cit. p. 222.

that UK=K for every element K of $\mathfrak{K}$; (ii) corresponding to every element A such that CA$\neq$A for at least one element C of $\mathfrak{K}$, there exists in $\mathfrak{K}$ an element X for which AX=U, where U is the said element[1].

§ 4. Let

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

be a series of ideals of a ring $\mathfrak{R}$ in which each ideal is divisible by the preceding one, while there is no ideal divisible by $\mathfrak{A}_i$ and dividing $\mathfrak{A}_{i+1}$, except $\mathfrak{A}_i$ and $\mathfrak{A}_{i+1}$. This series is called a *chief-composition-series*[2], or simply a *chief-series* of the ring $\mathfrak{R}$. And also the series

$$\mathfrak{R},\ \mathfrak{A}_1,\ \mathfrak{A}_2,\cdots\cdots\cdot\mathfrak{A}_n$$

which consists of the first n terms of the above chief-series, is called a chief-series with the last term $\mathfrak{A}_n$.

THEOREM[4]: *Any two chief-series of a ring*

$$\mathfrak{R},\ \mathfrak{A}_1,\ \mathfrak{A}_2,\cdots\cdots\cdot\mathfrak{A}_n,$$

$$\mathfrak{R},\ \mathfrak{A}'_1,\ \mathfrak{A}'_2,\cdots\cdots\cdot\mathfrak{A}'_m\ (\mathfrak{A}_n=\mathfrak{A}'_m),$$

of which the last terms are the same, consist of the same number of terms, and lead to two sets of quotient-rings

$$\mathfrak{R}/\mathfrak{A}_1,\quad \mathfrak{A}_1/\mathfrak{A}_2,\cdots\cdots\cdots\cdots,$$

$$\mathfrak{R}/\mathfrak{A}'_1,\quad \mathfrak{A}'_1/\mathfrak{A}'_2,\cdots\cdots\cdots\cdots,$$

which are identical with each other except as regards the sequence in which they occur.

THEOREM[4]: *If $\mathfrak{A}_i$ and $\mathfrak{A}_{i+1}$ are two consecutive terms of a chief-series, the quotient-ring $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ is either a field or not. When $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ is no field, $\mathfrak{A}_i^2\equiv 0\ (\mathfrak{A}_{i+1})$.*

In the present paper we study the ring-ideals under the condition that corresponding to an ideal there is one or more than one chief-series having it as the last term.

---

1 Loc. cit. p. 205.

2, 3 Loc. cit. p. 220.

4 Loc. cit. p. 224.

REPRESENTATION OF IDEALS AS THE CROSS-CUT OF PRIMARY IDEALS.

§ 5. THEOREM[1]: *In two ideals* $\mathfrak{A}$, $\mathfrak{B}$ *of a ring* $\mathfrak{R}$, *if* $\mathfrak{B}\equiv 0\ (\mathfrak{A})$ *and the quotient-ring* $\mathfrak{A}/\mathfrak{B}$ *is a field, the ideal* $\mathfrak{B}$ *is the cross-cut of* $\mathfrak{A}$ *and the maximal ideal* $\mathfrak{M}$ *of the first kind which is uniquely determined by the congruence*

$$\mathfrak{A}\mathfrak{M}\equiv 0\ (\mathfrak{B}).$$

Herein $\mathfrak{A}$ is assumed to be distinct from $\mathfrak{R}$.

Take an element a of $\mathfrak{A}$ which does not belong to $\mathfrak{B}$, and consider the ideal $\mathfrak{M}$ consisting of the elements X of the ring, which satisfy the congruence

$$aX\equiv 0\ (\mathfrak{B}).$$

1° $\mathfrak{M}$ evidently contains all the elements of $\mathfrak{B}$, but no element of $\mathfrak{A}$, which does not belong to $\mathfrak{B}$; because, since $\mathfrak{A}/\mathfrak{B}$ is a field, the product of two elements of $\mathfrak{A}$ is congruent (mod. $\mathfrak{B}$) to zero, when and only when at least one of them belongs to $\mathfrak{B}$. Therefore $\mathfrak{B}$ is the cross-cut of $\mathfrak{A}$ and $\mathfrak{M}$, i.e.

$$\mathfrak{B}=[\mathfrak{A},\ \mathfrak{M}].$$

2° $\mathfrak{M}$ contains elements not belonging to $\mathfrak{A}$.

For, since $\mathfrak{A}/\mathfrak{B}$ is a field, there exists in $\mathfrak{A}$ such an element U that

$$AU\equiv A\ (\mathfrak{B})$$

for every element A of $\mathfrak{A}$. And hence we have

$$a\rho U\equiv a\rho\ (\mathfrak{B}),$$

or

$$a(\rho U-\rho)\equiv 0\ (\mathfrak{B}),$$

where ρ denotes an element not belonging to $\mathfrak{A}$.

But $\rho U-\rho\equiv-\rho\not\equiv 0\ (\mathfrak{A}).\ \ [\because U\equiv 0\ (\mathfrak{A})]$

Therefore $\mathfrak{M}$ contains the element $(\rho U-\rho)$ not belonging to $\mathfrak{A}$.

3° $(\mathfrak{A},\ \mathfrak{M})=\mathfrak{R}$.

---

1 This is an extension of the theorem which has been given in the previous paper. These Memoirs, 3 189 (1918).

For, if the product αR, R being an element of $\mathfrak{R}$, belongs to $\mathfrak{M}$, it must belong to $\mathfrak{B}$; indeed $\alpha \equiv 0$ ($\mathfrak{A}$), $[\mathfrak{A}, \mathfrak{M}]=\mathfrak{B}$. Therefore, the ideal consisting of the elements Y for which $\alpha Y \equiv 0$ ($\mathfrak{M}$) is coincident with $\mathfrak{M}$. But the quotient-rings $(\mathfrak{A}, \mathfrak{M})/\mathfrak{M}$ and $\mathfrak{A}/[\mathfrak{A}, \mathfrak{M}]$ are of the same type [§ 2], while $\mathfrak{B}=[\mathfrak{A}, \mathfrak{M}]$ and $\mathfrak{A}/\mathfrak{B}$ is a field. Therefore, $(\mathfrak{A}, \mathfrak{M})/\mathfrak{M}$ is also a field; hence, if $(\mathfrak{A}, \mathfrak{M})$ were distinct from $\mathfrak{R}$, the ideal consisting of the elements Y which satisfy the congruence $\alpha Y \equiv 0$ ($\mathfrak{M}$) would contain elements not belonging to $\mathfrak{M}$, as can be shown similarly in 2°. This contradicts thc fact that it must coincide with $\mathfrak{M}$. Therefore, $(\mathfrak{A}, \mathfrak{M})=\mathfrak{R}$.

4° $\mathfrak{M}$ is a maximal ideal of the first kind; because $(\mathfrak{A}, \mathfrak{M})/\mathfrak{M}$ is a field, while $(\mathfrak{A}, \mathfrak{M})=\mathfrak{R}$. (by § 3, theorem.)

5° Since $\mathfrak{M}$ consists of the elements X which satisfy the congruence $\alpha X \equiv 0$ ($\mathfrak{B}$), if $\mathfrak{B}=[\mathfrak{A}, \mathfrak{N}]$, $\mathfrak{N} \equiv 0$ ($\mathfrak{M}$) and hence, if $\mathfrak{N}$ is maximal, $\mathfrak{N}=\mathfrak{M}$.

6° Take any element A of $\mathfrak{A}$. Since $\mathfrak{A}/\mathfrak{B}$ is a field and $\alpha \not\equiv 0$ ($\mathfrak{B}$), we can chose an element X so that $\alpha X \equiv A$ ($\mathfrak{B}$), or $A=\alpha X+B$, B being an element of $\mathfrak{B}$. Hence, we have

$$A\mathfrak{M}=(\alpha X+B)\mathfrak{M}\equiv 0 \ (\mathfrak{B}). \quad \therefore \quad \mathfrak{A}\mathfrak{M}\equiv 0(\mathfrak{B}).$$

And if $\mathfrak{A}\mathfrak{M}' \equiv 0$ ($\mathfrak{B}$), evidently $\mathfrak{M}' \equiv 0$ ($\mathfrak{M}$). Therefore, $\mathfrak{M}$ is a maximal ideal of the first kind uniquely determined by the congruence $\mathfrak{A}\mathfrak{M} \equiv 0$ ($\mathfrak{B}$).

§ 6. THEOREM: *Let*

$$\mathfrak{A}_i, \mathfrak{A}_{i+1}, \ldots\ldots\ldots \mathfrak{A}_{i+n}$$

be (n+1) consecutive terms of a chief-series of a ring $\mathfrak{R}$, *and let none of quotient-rings*

$$\frac{\mathfrak{A}_i}{\mathfrak{A}_{i+1}}, \frac{\mathfrak{A}_{i+1}}{\mathfrak{A}_{i+2}}, \ldots\ldots, \frac{\mathfrak{A}_{i+n-1}}{\mathfrak{A}_{i+n}}$$

be a field, i.e.

$$\mathfrak{A}^2_{i+j} \equiv 0 \ (\mathfrak{A}_{i+j+1}), \ j=0,1,2,\ldots\ldots\ldots n-1.$$

Then, we have

$$\mathfrak{A}_i\mathfrak{A}_{i+n-1} \equiv 0 \ (\mathfrak{A}_{i+n}),$$

and consequently, $\mathfrak{A}_i^{n+1} \equiv 0$ ($\mathfrak{A}_{i+n}$).

Herein $\mathfrak{A}_i$ may be $\mathfrak{R}$. We prove this by induction.

1° The case n=2.

Take the ideal $(\mathfrak{A}_i\mathfrak{A}_{i+1}, \mathfrak{A}_{i+2})$, then we have immediately

$$\mathfrak{A}_{i+2}\equiv 0 \ (\text{mod.}\ (\mathfrak{A}_i\mathfrak{A}_{i+1}, \mathfrak{A}_{i+2})\ ),\ (\mathfrak{A}_i \mathfrak{A}_{i+1}, \mathfrak{A}_{i+2})\equiv 0\ (\mathfrak{A}_{i+1}),$$

while $\mathfrak{A}_i, \mathfrak{A}_{i+1}$ are consecutive terms of the chief-series. Therefore,

$$(\mathfrak{A}_i\mathfrak{A}_{i+1}, \mathfrak{A}_{i+2})=\text{either } \mathfrak{A}_{i+1} \text{ or } \mathfrak{A}_{i+2}.$$

If $(\mathfrak{A}_i\mathfrak{A}_{i+1}, \mathfrak{A}_{i+2})$ were $= \mathfrak{A}_{i+1}$,

we should have

$$(\mathfrak{A}_i^2\mathfrak{A}_{i+1}, \mathfrak{A}_i\mathfrak{A}_{i+2}, \mathfrak{A}_{i+2})=(\mathfrak{A}_i\mathfrak{A}_{i+1}, \mathfrak{A}_{i+2})=\mathfrak{A}_{i+1},$$

which contradicts the consequence

$$(\mathfrak{A}_i^2\mathfrak{A}_{i+1}, \mathfrak{A}_i\mathfrak{A}_{i+2}, \mathfrak{A}_{i+2})\equiv 0\ (\mathfrak{A}_{i+2})$$

from the hypothesis. Therefore, we have

$$(\mathfrak{A}_i\mathfrak{A}_{i+1}, \mathfrak{A}_{i+2})=\mathfrak{A}_{i+2}.$$

$$\therefore\ \mathfrak{A}_i\mathfrak{A}_{i+1}\equiv 0\ (\mathfrak{A}_{i+2}).$$

2° From the assumption $\mathfrak{A}_{i+1}\ \mathfrak{A}_{i+n-1}\equiv 0\ (\mathfrak{A}_{i+n})$ it follows that $\mathfrak{A}_i\mathfrak{A}_{i+n-1}\equiv 0\ (\mathfrak{A}_{i+n})$, if $\mathfrak{A}_i^2\equiv 0\ (\mathfrak{A}_{i+1})$. For

$$(\mathfrak{A}_i\mathfrak{A}_{i+n-1}, \mathfrak{A}_{i+n})=\mathfrak{A}_{i+n},$$

as can similarly be shown as before, and hence, $\mathfrak{A}_i\mathfrak{A}_{i+n-1}\equiv 0\ (\mathfrak{A}_{i+n})$.

§ 7. Let

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

be a chief-series of a ring $\mathfrak{R}$, and

(2) $\dfrac{\mathfrak{R}}{\mathfrak{A}_1}, \dfrac{\mathfrak{A}_1}{\mathfrak{A}_2}, \cdots\cdots\cdots, \dfrac{\mathfrak{A}_{n-1}}{\mathfrak{A}_n}$

the set of quotient-rings derived from (1).

THEOREM: *If $\mathfrak{A}_n$ is an ideal of the second kind, i.e., if $\mathfrak{A}_n$ divides a power of $\mathfrak{R}$, none of the quotient-rings is a field; and so conversely.*

In other words: whether a given ideal $\mathfrak{A}$ belongs to the first kind or to the second kind, is determined by the existence or non-existence of the field in the set of quotient-rings derived from a chief-series with $\mathfrak{A}$ as the last term.

Proof. If $\mathfrak{R}^e\equiv 0\ (\mathfrak{A}_n)$ for a certain index e, the quotient-ring $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ can not be a field; because otherwise we should have, for an element a_i of $\mathfrak{A}_i$ which does not belong to $\mathfrak{A}_{i+1}$,

$$\alpha_i^e \not\equiv 0 \ (\mathfrak{A}_{i+1}),$$

and consequently $\mathfrak{R}^e \not\equiv 0 \ (\mathfrak{A}_n)$.

If, conversely, none of the quotient-rings is a field, we have, by the last theorem, $\mathfrak{R}^{n+1} \equiv 0 \ (\mathfrak{A}_n)$.

§ 8. THEOREM : *If in set (2) of quotient-rings there are ν fields, the distinct maximal ideals of the first kind which are divisors of $\mathfrak{A}_n$ are ν in number.*

Let $\mathfrak{M}$ be a maximal ideal of the first kind which is a divisor of $\mathfrak{A}_n$. Beginning with $\mathfrak{A}_n$, examine the ideals $\mathfrak{A}_n, \mathfrak{A}_{n-1}, \ldots\ldots$ in series (1), whether they are divisible by $\mathfrak{M}$, then we shall have the ideal $\mathfrak{A}_i$ such that

$$\mathfrak{A}_i \not\equiv 0 \ (\mathfrak{M}), \text{ while } \mathfrak{A}_{i+1} \equiv 0 \ (\mathfrak{M}).$$

And, since $\mathfrak{A}_i$, $\mathfrak{A}_{i+1}$ are consecutive terms of the chief-series, we have

$$[\mathfrak{A}_i, \ \mathfrak{M}] = \mathfrak{A}_{i+1}.$$

If $\mathfrak{A}_i = \mathfrak{R}$, evidently $\mathfrak{A}_{i+1} = \mathfrak{M}$ and $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ is a field (§ 3, theorem). If on the contrary $\mathfrak{A}_i \neq \mathfrak{R}$, the quotient $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ is of the same type as $(\mathfrak{A}_i, \mathfrak{M})/\mathfrak{M}$; and moreover $(\mathfrak{A}_i, \mathfrak{M}) = \mathfrak{R}$. Therefore $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ is also a field. Thus to a maximal ideal of the first kind which divides $\mathfrak{A}_n$ there corresponds one field in set (2).

If $\mathfrak{N}$ be another maximal ideal of the first kind which divides $\mathfrak{A}_n$, there corresponds to $\mathfrak{N}$ a field distinct from $\mathfrak{A}_i/\mathfrak{A}_{i+1}$. Indeed, if we had

$$\mathfrak{A}_i \not\equiv 0 \ (\mathfrak{N}), \quad \mathfrak{A}_{i+1} \equiv 0 \ (\mathfrak{N}),$$

it would be

$$[\mathfrak{A}_i, \ \mathfrak{N}] = \mathfrak{A}_{i+1}$$

and consequently $\mathfrak{N} = \mathfrak{M}$. [§ 5, 5°].

Therefore the number of maximal ideals of the first kind which divide $\mathfrak{A}_n$ is either equal or less than that of the fields in set (2).

If, conversely, $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ is a field, we have

$$\mathfrak{A}_{i+1} = [\mathfrak{A}_i, \ \mathfrak{M}],$$

$\mathfrak{M}$ being a maximal ideal of the first kind [§ 5], and evidently

$\mathfrak{A}_n \equiv 0$ ($\mathfrak{M}$). Let $\mathfrak{A}_{i+j}/\mathfrak{A}_{i+j+1}$ be another field in set (2), and

$$\mathfrak{A}_{i+j+1} = [\mathfrak{A}_{i+j}, \mathfrak{N}] \quad (1 \leqq j > n-i-1).$$

Then we have

$$\mathfrak{A}_{i+j} \not\equiv 0 (\mathfrak{N}), \text{ while } \mathfrak{A}_{i+j} \equiv 0 \ (\mathfrak{A}_{i+1}),$$

and hence $\mathfrak{N} \neq \mathfrak{M}$.

Therefore if in set (2) of quotient-rings there are ν fields, the maximal ideals of the first kind which divide $\mathfrak{A}_n$ are at least ν in number.

The two results above obtained give the theorem.

The theorem may also be stated as follows:

An ideal of the first kind is divisible by a finite number of maximal ideals of the first kind; this number is equal to that of the fields in the quotient-rings derived from a chief-series having that ideal as the last term.

§ 9. THEOREM: *If in set (2) of quotient-rings there is only one field, $\mathfrak{A}_n$ is of the first kind and divides a power of a maximal ideal of the first kind; this maximal ideal is a divisor of $\mathfrak{A}_n$. Conversely, if $\mathfrak{A}_n$ is of the first kind and a divisor of a power of a maximal ideal of the first kind, there is one and only one field in set (2).*

Let $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ be a field and the others no field. Then

$$\mathfrak{A}_{i+1} = [\mathfrak{A}_i, \mathfrak{M}],$$

where $\mathfrak{M}$ is a maximal ideal of first kind. Since $\mathfrak{N}/\mathfrak{A}_1$, $\mathfrak{A}_1/\mathfrak{A}_2$, ... $\mathfrak{A}_{i-1}/\mathfrak{A}_i$ are no fields by assumption, we have

$$\mathfrak{N}^{i+1} \equiv 0 \ (\mathfrak{A}_i) \quad [\text{by § 6, theorem}],$$

and consequently $\mathfrak{M}^{i+1} \equiv 0 \ (\mathfrak{A}_i)$,

while $[\mathfrak{A}_i, \mathfrak{M}] = \mathfrak{A}_{i+1}$.

$$\therefore \quad \mathfrak{M}^{i+1} \equiv 0 \ (\mathfrak{A}_{i+1}).$$

And, moreover, $\mathfrak{A}_{i+1}/\mathfrak{A}_{i+2}$, ... $\mathfrak{A}_{n-1}/\mathfrak{A}_n$ are no fields by supposition.

$$\therefore \quad \mathfrak{A}_{i+1}^{n-i} \equiv 0 \quad (\mathfrak{A}_n).$$

Therefore, we have

$$\mathfrak{M}^{(i+1)(n-i)} \equiv 0 \ (\mathfrak{A}_n).$$

Next, to prove the converse, let $\mathfrak{M}$ be a maximal ideal of first kind and $\mathfrak{M}^e \equiv 0 \ (\mathfrak{A}_n)$. Since $\mathfrak{A}_n$ is assumed to be of the first kind, there must exist a field in set (2) [§ 7, theorem]; hence, $\mathfrak{A}_n$ is divisible by a maximal ideal of the first kind [by the last theorem], and let it be $\mathfrak{N}$. If $\mathfrak{N} \neq \mathfrak{M}$, we should have

$$(\mathfrak{N}, \mathfrak{M}) = \mathfrak{R},$$

whence follows

$$(\mathfrak{N}, \mathfrak{M}^e) = \mathfrak{R}$$

from the theorem which will be given in § 11.

$$\therefore \quad (\mathfrak{N}, \mathfrak{A}_n) = \mathfrak{R} \quad [\because \ \mathfrak{M}^e \equiv 0 \ (\mathfrak{A}_n)],$$

contradictory to the assumption that $\mathfrak{A}_n \equiv 0 \ (\mathfrak{N})$. Therefore, $\mathfrak{N} = \mathfrak{M}$, i.e. $\mathfrak{M}$ is the only maximal ideal of the first kind which divides $\mathfrak{A}_n$; so that set (1) contains only one field.

N. B. Throughout this paper we denote by $\mathfrak{R}$ the ring in which ideals are treated.

§ 10. Definition. An ideal which is divisible by only one maximal ideal $\mathfrak{M}$ of the first kind is called a *primary ideal* belonging to $\mathfrak{M}$.

A primary ideal belonging to $\mathfrak{M}$ is of the first kind and divides a power of $\mathfrak{M}$, as immediately follows from the last two theorems, and conversely an ideal of the first kind which divides a power of a maximal ideal of the first kind is primary.

THEOREM: *Let $\mathfrak{P}$ be a primary ideal belonging to the maximal ideal $\mathfrak{M}$. If the product of two ideals $\mathfrak{A}$, $\mathfrak{B}$*

$$\mathfrak{A}\mathfrak{B} \equiv 0 \ (\mathfrak{P}),$$

a power of $\mathfrak{A}$ or $\mathfrak{B}$ (or both) is divisible by $\mathfrak{P}$.

Let $\mathfrak{M}^e \equiv 0 \ (\mathfrak{P})$. If $\mathfrak{A} \equiv 0 \ (\mathfrak{M})$, $\mathfrak{A}^e \equiv 0 \ (\mathfrak{M}^e)$ and consequently $\mathfrak{A}^e \equiv 0 \ (\mathfrak{P})$.

If, on the contrary, $\mathfrak{A} \not\equiv 0 \ (\mathfrak{M})$, we have $(\mathfrak{A}, \mathfrak{M}) = \mathfrak{R}$, whence it follows that

$$(\mathfrak{A}\mathfrak{R}^{e-1}, \mathfrak{M}^e) = \mathfrak{R}^e.$$

For, $\quad \mathfrak{R}^2 = (\mathfrak{A}, \mathfrak{M})\mathfrak{R} = (\mathfrak{A}\mathfrak{R}, \mathfrak{M}(\mathfrak{A}, \mathfrak{M}))$

$$= (\mathfrak{A}\mathfrak{R}, \mathfrak{A}\mathfrak{M}, \mathfrak{M}^2) = (\mathfrak{A}\mathfrak{R}, \mathfrak{M}^2).$$

$$\mathfrak{R}^3 = (\mathfrak{A}\mathfrak{R}, \mathfrak{M}^2)\mathfrak{R} = (\mathfrak{A}\mathfrak{R}^2, \mathfrak{M}^2(\mathfrak{A}, \mathfrak{M}))$$

$$=(\mathfrak{A}\mathfrak{R}^2, \mathfrak{A}\mathfrak{M}^2, \mathfrak{M}^3)=(\mathfrak{A}\mathfrak{R}^2, \mathfrak{M}^3).$$

. . . .

$$\mathfrak{R}^e=(\mathfrak{A}\mathfrak{R}^{e-1}, \mathfrak{M}^e).$$

It follows from $\mathfrak{A}\mathfrak{B}\equiv 0\ (\mathfrak{P})$ that $\mathfrak{A}\mathfrak{B}\mathfrak{R}^{e-1}\equiv 0\ (\mathfrak{P})$, while $\mathfrak{B}\mathfrak{M}^e\equiv 0\ (\mathfrak{P})$. Hencc, we have

$(\mathfrak{A}\mathfrak{R}^{e-1}, \mathfrak{M}^e)\mathfrak{B}\equiv 0\ (\mathfrak{P})$, or $\mathfrak{R}^e\mathfrak{B}=0\ (\mathfrak{M})$, and consequently $\mathfrak{B}^{e+1}\equiv 0\ (\mathfrak{P})$.

It may happen in the case where $\mathfrak{A}\equiv 0\ (\mathfrak{M})$ that $\mathfrak{B}^\lambda \not\equiv 0\ (\mathfrak{P})$ for every index λ even if $\mathfrak{A}\not\equiv 0\ (\mathfrak{P})$. In this respect the primary ideal above defined is different from what has been defined by Noether[1].

§ 11. THEOREM: *Let $\mathfrak{M}$ be a maximal ideal of the first kind. Then from* $(\mathfrak{A}, \mathfrak{M})=\mathfrak{R}$ *and* $(\mathfrak{B}, \mathfrak{M})=\mathfrak{R}$, *it follows that* $(\mathfrak{A}\mathfrak{B}, \mathfrak{M})=\mathfrak{R}$.

(As already stated, $\mathfrak{R}$ always denotes the ring in which ideals are treated.)

$$\mathfrak{R}^2=(\mathfrak{A}, \mathfrak{M})(\mathfrak{B}, \mathfrak{M})=(\mathfrak{A}\mathfrak{B}, \mathfrak{A}\mathfrak{M}, \mathfrak{B}\mathfrak{M}, \mathfrak{M}^2).$$

But $\qquad \mathfrak{R}^2\not\equiv 0\ (\mathfrak{M})$,

since $\mathfrak{M}$ is of the first kind.

$$\therefore\quad \mathfrak{R}=(\mathfrak{R}^2, \mathfrak{M})=(\mathfrak{A}\mathfrak{B}, \mathfrak{A}\mathfrak{M}, \mathfrak{B}\mathfrak{M}, \mathfrak{M}^2, \mathfrak{M}) = (\mathfrak{A}\mathfrak{B}, \mathfrak{M}).$$

§ 12. THEOREM: *If an ideal $\mathfrak{A}$ of the first kind is not primary, it is capable of representation as the cross-cut of two ideals $\mathfrak{L}$ and $\mathfrak{P}$ subject to the following conditions:*

(i) $\mathfrak{L}^2\not\equiv 0\ (\mathfrak{A})$.

(ii) *$\mathfrak{P}$ consists of the elements P of the ring $\mathfrak{R}$, which satisfy the congruence*

$$\mathfrak{L}P\equiv 0\ (\mathfrak{A}).$$

(iii) *$\mathfrak{P}$ is primary.*

Proof. 1° Let $\mathfrak{A}_i$, $\mathfrak{A}_{i+1}$ be two consecutive terms of a chief-series, of which $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ is no field, i.e. $\mathfrak{A}_i^2\equiv 0\ (\mathfrak{A}_{i+1})$. And suppose that $\mathfrak{A}_i$ may be represented as the cross-cut of two ideals $\mathfrak{L}$ and $\mathfrak{P}$ subject to the following conditions:

(i) There exists an element λ in $\mathfrak{L}$ such that $\lambda^2\not\equiv 0\ (\mathfrak{A}_i)$.

(ii) $\mathfrak{P}$ is the ideal which consists of the elements P for which

---

1 Math. Ann., **83**, 37 (1921).

$\lambda P \equiv 0 \ (\mathfrak{A}_i)$.

(iii) $\mathfrak{P}$ is primary and belongs to a maximal ideal $\mathfrak{M}$, i.e. $\mathfrak{M}^e \equiv 0 \ (\mathfrak{P})$.

Consider the ideal $\mathfrak{Q}$ consisting of the elemnts Q for which $\lambda Q \equiv 0 \ (\mathfrak{A}_{i+1})$, λ being the element taken above. Then evidently

$$\mathfrak{A}_{i+1} \equiv 0 \ (\mathfrak{Q}), \ \mathfrak{Q} \equiv 0 (\mathfrak{P}),$$

and, by our assumption, $\mathfrak{A}_i$ and $\mathfrak{A}_{i+1}$ are consecutive terms of a chief-series. Therefore we have the following three cases :

(*a*) The case where $\mathfrak{Q} = \mathfrak{A}_{i+1}$, i.e. $\lambda R \equiv 0 \ (\mathfrak{A}_{i+1})$ when and only when $R \equiv 0 \ (\mathfrak{A}_{i+1})$.

$$\lambda \mathfrak{P} \equiv 0 \ (\mathfrak{A}_i), \text{ while } \mathfrak{A}_i^2 \equiv 0 \ (\mathfrak{A}_{i+1}).$$

$$\therefore \ \lambda^2 \mathfrak{P}^2 \equiv 0 \ (\mathfrak{A}_{i+1}).$$

$$\therefore \ \lambda \mathfrak{P}^2 \equiv 0 \ (\mathfrak{A}_{i+1}). \ [\because \ \mathfrak{Q} = \mathfrak{A}_{i+1}]$$

$$\therefore \ \mathfrak{P}^2 \equiv 0 \ (\mathfrak{A}_{i+1}), \text{ while } \mathfrak{M}^e \equiv 0 \ (\mathfrak{P}).$$

$$\therefore \ \mathfrak{M}^{2e} \equiv 0 \ (\mathfrak{A}_{i+1}),$$

that is, $\mathfrak{A}_{i+1}$ must be a primary ideal belonging to $\mathfrak{M}$.

(*b*) The case where $\mathfrak{Q} \neq \mathfrak{A}_{i+1}$, $[\mathfrak{A}_i, \mathfrak{Q}] = \mathfrak{A}_{i+1}$.

Since $\mathfrak{Q} \equiv 0 \ (\mathfrak{P})$ and $[\mathfrak{L}, \mathfrak{P}] = \mathfrak{A}_i$, we have

$$[\mathfrak{L}, \mathfrak{Q}] \equiv 0 \ (\mathfrak{A}_i).$$

$$\therefore \ [\mathfrak{L}, \mathfrak{Q}] \equiv 0 \ ([\mathfrak{A}_i, \mathfrak{Q}]).$$

$$\therefore \ [\mathfrak{L}, \mathfrak{Q}] = [\mathfrak{A}_i, \mathfrak{Q}] = \mathfrak{A}_{i+1}.$$

And $\mathfrak{Q}$ is a primary ideal belonging to $\mathfrak{M}$. Because $\lambda^2 \mathfrak{P}^2 \equiv 0$ $(\mathfrak{A}_{i+1})$ and hence, $\lambda \mathfrak{P}^2 \equiv 0 \ (\mathfrak{Q})$, while $\lambda \equiv 0 \ (\mathfrak{L})$.

$$\therefore \ \lambda \mathfrak{P}^2 \equiv 0 \ ([\mathfrak{L}, \mathfrak{Q}]), \text{ or } \lambda \mathfrak{P}^2 \equiv 0 \ (\mathfrak{A}_{i+1}).$$

$$\therefore \ \mathfrak{P}^2 \equiv 0 \ (\mathfrak{Q}), \text{ while } \mathfrak{M}^e \equiv 0 \ (\mathfrak{P}).$$

$$\therefore \ \mathfrak{M}^{2e} \equiv 0 \ (\mathfrak{Q}).$$

Thue $\mathfrak{A}_{i+1}$ can be reduced into the cross-cut of $\mathfrak{L}$ and $\mathfrak{Q}$ which satisfy the same conditions as assumed for $\mathfrak{L}$ and $\mathfrak{P}$.

(*c*) The case where $[\mathfrak{A}_i, \mathfrak{Q}] = \mathfrak{A}_i$.

If $\lambda L \equiv 0 \ (\mathfrak{A}_i)$ for an element L of $\mathfrak{L}$, we have $L \equiv 0 \ (\mathfrak{P})$, and consequently $L \equiv 0 \ (\mathfrak{A}_i)$; hence $\lambda L \equiv 0 \ (\mathfrak{A}_{i+1})$, because $\mathfrak{A}_i \equiv 0 \ (\mathfrak{Q})$ and $\lambda \mathfrak{Q} \equiv 0 \ (\mathfrak{A}_{i+1})$. Therefore the elements of $\lambda \mathfrak{L}$, which belong to $\mathfrak{A}_i$, must belong to $\mathfrak{A}_{i+1}$. So that

$$[(\lambda \mathfrak{L}, \mathfrak{A}_{i+1}), \mathfrak{P}] = \mathfrak{A}_{i+1}.$$

The ideals $(\lambda\mathfrak{L}, \mathfrak{A}_{i+1})$ and $\mathfrak{P}$ also satisfy the three conditions.

For, take the element λ^2 of $(\lambda\mathfrak{L}, \mathfrak{A}_{i+1})$, then $\lambda^4 \not\equiv 0\ (\mathfrak{A}_{i+1})$. Indeed, if $\lambda^4 \equiv 0\ (\mathfrak{A}_{i+1})$, λ^3 would $\equiv 0\ (\mathfrak{A}_i)$ and consequently, λ^2 would $\equiv 0\ (\mathfrak{P})$, while $\lambda \equiv 0\ (\mathfrak{L})$ and $[\mathfrak{L}, \mathfrak{P}] \equiv \mathfrak{A}_i$. Hence, λ^2 would $\equiv 0\ (\mathfrak{A}_i)$, contradictory to assumption (i).

Next, if $\lambda^2 R \equiv 0\ (\mathfrak{A}_{i+1})$, we have $\lambda R \equiv 0\ (\mathfrak{Q})$, and hence, $\lambda R \equiv 0\ ([\mathfrak{L}, \mathfrak{Q}])$, while $[\mathfrak{L}, \mathfrak{Q}] \equiv 0\ (\mathfrak{A}_i)$. Therefore, $R \equiv 0\ (\mathfrak{P})$.

Moreover $\lambda^2\mathfrak{P} = \lambda.\lambda\mathfrak{P} \equiv 0\ (\lambda\mathfrak{A}_i)$ and $\lambda\mathfrak{A}_i \equiv 0\ (\mathfrak{A}_{i+1})$, as already shown above. Therefore, $\lambda^2\mathfrak{P} \equiv 0\ (\mathfrak{A}_{i+1})$. Thus the elements X for which $\lambda^2 X \equiv 0\ (\mathfrak{A}_{i+1})$ form the ideal $\mathfrak{P}$.

Lastly $\mathfrak{P}$ is primary as has been assumed.

We can conclude from (*a*), (*b*) and (*c*) that if $\mathfrak{A}_i$ may be represented as the cross-cut of two ideals subject to the conditions (i), (ii), (iii), it is also for $\mathfrak{A}_{i+1}$, unless $\mathfrak{A}_{i+1}$ is primary.

2° Let

$$\mathfrak{A}_{i-1},\ \mathfrak{A}_i,\ \mathfrak{A}_{i+1}, \cdots\cdots\cdots \mathfrak{A}_n$$

be consecutive terms of a chief-series, and suppose that the quotient-ring $\mathfrak{A}_{i-1}/\mathfrak{A}_i$ is a field, but not the others $\mathfrak{A}_i/\mathfrak{A}_{i+1}, \cdots\cdots\cdots \mathfrak{A}_{n-1}/\mathfrak{A}_n$. Then

$$\mathfrak{A}_i = [\mathfrak{A}_{i-1}, \mathfrak{M}],$$

where $\mathfrak{M}$ is a maximal ideal of the first kind, so that the three conditions in 1° are satisfied in this representation.

If $\mathfrak{A}_n$ is not primary, it is also for $\mathfrak{A}_{i+1}, \mathfrak{A}_{i+2}, \cdots\cdots \mathfrak{A}_{n-1}$ [by § 7, theorem]. Therefore, by the repeated use of the result obtained in 1°, $\mathfrak{A}_n$ must be reduced into the cross-cut of two ideals satisfying the same conditions as assumed for $\mathfrak{L}$ and $\mathfrak{P}$ in 1°.

3° Again, returning to the reduction of $\mathfrak{A}_i$ in 1°, we have $\mathfrak{L}\mathfrak{P} \equiv 0\ (\mathfrak{A}_i)$. But if $\mathfrak{L}X \equiv 0\ (\mathfrak{A}_i)$, evidently $\lambda X \equiv 0\ (\mathfrak{A}_i)$ and consequently, $X \equiv 0\ (\mathfrak{P})$. Therefore, $\mathfrak{P}$ consists of the elements X for which $\mathfrak{L}X \equiv 0\ (\mathfrak{A}_i)$. And the three conditions given in the theorem are satisfied.

The results in 1°, 2°, 3° furnish a proof of the theorem.

§ 13. In the representation of an ideal : $\mathfrak{A} = [\mathfrak{L}, \mathfrak{P}]$ given in the last section, $\mathfrak{L}$ is prime to $\mathfrak{P}$ according to Noether's definition[1]; because if $\mathfrak{L}\mathfrak{N}\equiv 0\ (\mathfrak{P})$, we have immediately $\mathfrak{L}\mathfrak{N}\equiv 0\ (\mathfrak{A})$ and consequently $\mathfrak{N}\equiv 0\ (\mathfrak{P})$. But $\mathfrak{P}$ is not necessarily prime to $\mathfrak{L}$.

Let $\mathfrak{Z}$ be the aggregate of such elements Z that ZR$=0$ for every element R of the ring. Then it follows from the definition by Noether that, if an ideal $\mathfrak{H}$ is prime to another $\mathfrak{K}$, $\mathfrak{K}$ must be a divisor of $\mathfrak{Z}$, and that if $\mathfrak{H}$ and $\mathfrak{K}$ are mutually prime[2], both divide $\mathfrak{Z}$. In other words, the ideals which do not divide $\mathfrak{Z}$ are relatively-prime-irreducible[3].

§ 14. THEOREM : *If an ideal of the first kind is divisible by ν maximal ideals of the first kind, it is representable as the cross-cut of ν primary ideals belonging to the respective maximal ideals.*

Let $\mathfrak{A}$ be an ideal of the first kind and not primary. Then $\mathfrak{A}$ can be so reduced that $\mathfrak{A}=[\mathfrak{L}, \mathfrak{P}]$, where $\mathfrak{P}$ is primary.

And $\mathfrak{L}$ is also of the first kind. For otherwise, $\mathfrak{P}^d$ would $\equiv 0$ $(\mathfrak{L})$ for a certain exponent d, and consequently $\mathfrak{P}^d$ would $\equiv 0\ (\mathfrak{A})$. But $\mathfrak{M}^e\equiv 0\ (\mathfrak{P})$, $\mathfrak{M}$ being the maximal ideal to which $\mathfrak{P}$ belongs. Therefore, $\mathfrak{M}^{de}$ would $\equiv 0\ (\mathfrak{A})$, contrary to our assumption that $\mathfrak{A}$ is of the first kind and not primary.

If $\mathfrak{L}$ is not primary, reduce $\mathfrak{L}$ so that one of the components is primary. But the number of maximal ideals of the first kind which divide $\mathfrak{A}$ is finite. Therefore, after a finite number of reductions, $\mathfrak{A}$ can be represented as the cross-cut of the primary ideals :

$$\mathfrak{A}=[\mathfrak{P},\mathfrak{P}_1,\ldots\ldots\mathfrak{P}_r],$$

where $\mathfrak{P}$, $\mathfrak{P}_1,\ldots\ldots\mathfrak{P}_r$ are primary ideals respectively belonging to the maximal ideals $\mathfrak{M}$, $\mathfrak{M}_1,\ldots\ldots\mathfrak{M}_r$.

If $\mathfrak{N}$ is a maximal ideal, distinct from $\mathfrak{M}$, $\mathfrak{M}_1,\ldots\ldots\mathfrak{M}_r$, of the first kind, we have

$$(\mathfrak{P}, \mathfrak{N})=(\mathfrak{P}_1, \mathfrak{N})=\ldots\ldots=(\mathfrak{P}_r, \mathfrak{N})=\mathfrak{N}$$

---

1 Math. Ann., **83**, 45 (1921).

2, 3 For these nomenclatures, see Loc. cit. p. 51.

and consequently

$$(\mathfrak{P}\mathfrak{P}_1\cdots\cdots\mathfrak{P}_r,\ \mathfrak{N})=\mathfrak{N} \text{ [by § 11, theorem].}$$

$$\therefore\quad ([\mathfrak{P},\mathfrak{P}_1,\cdots\cdots\mathfrak{P}_r],\ \mathfrak{N})=\mathfrak{N},\ \text{or}\ (\mathfrak{A},\ \mathfrak{N})=\mathfrak{N}.$$

Therefore, the maximal ideals which divide $\mathfrak{A}$ are $\mathfrak{M}, \mathfrak{M}_1, \ldots \mathfrak{M}_r$; so that $r+1=\nu$.

By the above theorem the study of the representation of ideals as the cross-cut of their divisors is reduced to that of primary ideals and of ideals of the secend kind.

December, 9, 1923.