On Congruences. II.

By

Masazo Sono.

(Received Dec. 26, 1917).

CONTENTS.

In the paper[1] entitled "On Congruences", the author has shown in the case of groups and rings the possibility and the way of changing the definition of equality, a given group or a given ring always remaining the same after the change; and a fundamental conception of congruences has thereby been established. Further the author has attacked some of the properties of rings and of ideals, which are necessarily introduced in a discussion of congruence in a ring.

The present paper presents a further investigation of the pro-

---

[1] These Memoirs, **2**, 203 (1917).

perties of rings and ideals, and of certain important relations existing among the ideals of a ring.

For the sake of brevity the former paper is herein denoted by " Congr."

Proper Ring.

§ 1. Definition. If a ring $\mathfrak{R}$ contains an element U such that $R \cdot U = R$ for every element R of $\mathfrak{R}$, it is called a *proper* ring.

In the usual definition of a number-ring, such as a ring of an algebraic number-field defined by Hilbert,[1] an "*Ordnung*" by Dedekind[2] or an "*Integritätsbereich*" by Kronecker,[3] unity is an element. So that it seems proper that an abstract ring also should be defined so as to contain an element corresponding to 1 of a number-ring. The author, however, in defining a ring abstractly in the former paper[4], omitted this condition, because, as seen there, it was more advantageous in several respects, and in particular called a ring which contained an element corresponding to 1 a *proper* ring.

The present paper is limited in the main to a discussion of the ideals of proper rings.

Let $RU = R$ and $RU' = R$ for every element R of a ring $\mathfrak{R}$. Then if we put $R = U'$ in the first equation and $R = U$ in the second, we have

$$U' U = U', \quad UU' = U;$$

whence

$$U = U'.$$

This element U is called the *unit element*[5] of the proper ring.

Let U be an unit element of $\mathfrak{R}$. Then

$$(U + U + \dots n \text{ terms})\, R = UR + UR + \dots (n \text{ terms})$$
$$= R + R + \dots (n \text{ terms}).$$

Putting

$$U + U + \dots (n \text{ terms}) = n$$

we have

$$n \cdot R = R + R + \dots (n \text{ terms}).$$

---

1 Hilbert, Jahresber. D. Math. Ver. **4**, 237 (1894/95). The word *field* here is used to mean the German *Körper*.

2 Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 4ed., § 170.

3 Kronecker, Grundzüge einer arithmetischen Theorie der algebraischen Grössen, § 5.

4 Congr., § 1.

5 Thus named because of corresponding to 1 of a number-ring.

Therefore, without misunderstanding, we may denote the unit element by "1," and moreover may treat the elements

$$1, 2, 3, \ldots$$

like ordinary integers.

§ 2. Let $\mathfrak{A}$ be a maximal ideal[1] of a ring $\mathfrak{R}$. If $\mathfrak{R}$ is proper, the quotient ring[2] $\mathfrak{R}/\mathfrak{A}$ is a field.[3] If, especially, the order of $\mathfrak{R}/\mathfrak{A}$ is finite, it is a power of prime.[4]

N.B. The number of different elements of a ring, in this paper, is called the *order* of the ring.

Multiplication of Ideals.
Ideals Prime to Each Other.

§ 3. The concept of multiplication of ideals is introduced for the further investigation of important relations existing among the ideals of a ring.

Definition.[5] By the product $\mathfrak{A}\mathfrak{B}$ of two ideals, $\mathfrak{A}$ and $\mathfrak{B}$, of a ring is meant the aggregate of all possible elements, which are obtained, if we multiply an element A of $\mathfrak{A}$ by an element B of $\mathfrak{B}$ and add an arbitrary number of such products, i.e. the aggregate of all possible elements of the form $\Sigma\, AB$.

As immediate consequence of the definition we have the following propositions:

The product of two ideals of a ring $\mathfrak{R}$ is also an ideal of $\mathfrak{R}$.

If $\mathfrak{A}=\mathfrak{A}'$ and $\mathfrak{B}=\mathfrak{B}'$, then $\mathfrak{A}\mathfrak{B}=\mathfrak{A}'\mathfrak{B}'$.

The three laws, commutative, associative and distributive, hold, viz.

$$\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A},$$
$$(\mathfrak{A}\mathfrak{B})\,\mathfrak{C} = \mathfrak{A}\,(\mathfrak{B}\mathfrak{C}),$$
$$(\mathfrak{A}, \mathfrak{B})\,\mathfrak{C} = (\mathfrak{A}\mathfrak{C}, \mathfrak{B}\mathfrak{C}),$$

where $(\mathfrak{A}, \mathfrak{B})$ denotes the ideal derived from $\mathfrak{A}$ and $\mathfrak{B}$.[6]

The product $\mathfrak{A}\mathfrak{B}$ is contained in both $\mathfrak{A}$ and $\mathfrak{B}$, and consequently in their cross-cut.[7]

1 Congr., § 9, p. 214.
2 *Loc. cit.* p. 213.
3 *Loc. cit.* § 15.
4 *Loc. cit.* § 18.
5 We adopted the definition as usually given for multiplication of ideals in a number-ring.
6 Congr., § 10, p. 214.
7 *Loc. cit.* p. 215.

If $\mathfrak{A}$ is an ideal of a proper ring $\mathfrak{R}$, then $\mathfrak{A}\mathfrak{R}=\mathfrak{A}$.

An ideal $\mathfrak{A}$ is said to be *divisible* by another ideal $\mathfrak{B}$, if an ideal $\mathfrak{C}$ can be chosen so that $\mathfrak{A}=\mathfrak{B}\mathfrak{C}$.

This ideal $\mathfrak{C}$ is usually called the quotient of $\mathfrak{A}$ by $\mathfrak{B}$, but it is entirely different from the quotient ring defined by the author,[1] and of course the notation $\dfrac{\mathfrak{A}}{\mathfrak{B}}$ never denotes the result of division (the inverse operation of multiplication) of $\mathfrak{A}$ by $\mathfrak{B}$. In this paper to avoid ambiguity the word "quotient" is used to denote the quotient ring, as defined, but never the result of division.

§ 4. Definition.[2] Let $\mathfrak{A}$ and $\mathfrak{B}$ be two ideals of a proper ring $\mathfrak{R}$. If $(\mathfrak{A}, \mathfrak{B})=\mathfrak{R}$, the ideals $\mathfrak{A}$ and $\mathfrak{B}$ are said to be *prime to each other.*

THEOREM: *If ideals* $\mathfrak{A}_1, \mathfrak{A}_2, \ldots\ldots, \mathfrak{A}_n$ *of a proper ring* $\mathfrak{R}$ *are all prime to another ideal* $\mathfrak{B}$ *of* $\mathfrak{R}$, *their product* $\mathfrak{A}_1\mathfrak{A}_2\ldots\ldots\mathfrak{A}_n$ *is also prime to* $\mathfrak{B}$. (Some of the $\mathfrak{A}$'s may be equal.)

For, since $(\mathfrak{A}_1, \mathfrak{B})=\mathfrak{R}$ and $(\mathfrak{A}_2, \mathfrak{B})=\mathfrak{R}$, we have

$$\begin{aligned}(\mathfrak{A}_1\mathfrak{A}_2, \mathfrak{B}) &= (\mathfrak{A}_1\mathfrak{A}_2, \mathfrak{R}\mathfrak{B}) = (\mathfrak{A}_1\mathfrak{A}_2, (\mathfrak{A}_1, \mathfrak{B})\,\mathfrak{B})\\ &= (\mathfrak{A}_1\mathfrak{A}_2, \mathfrak{A}_1\mathfrak{B}, \mathfrak{B}^2) = (\mathfrak{A}_1(\mathfrak{A}_2, \mathfrak{B}), \mathfrak{B}^2)\\ &= (\mathfrak{A}_1\mathfrak{R}, \mathfrak{B}^2) = (\mathfrak{A}_1, \mathfrak{B}^2),\end{aligned}$$

which shows that $(\mathfrak{A}_1\mathfrak{A}_2, \mathfrak{B})$ contains $\mathfrak{A}_1$, while containing $\mathfrak{B}$. Therefore $(\mathfrak{A}_1\mathfrak{A}_2, \mathfrak{B})=\mathfrak{R}$, viz. the product $\mathfrak{A}_1\mathfrak{A}_2$ is prime to $\mathfrak{B}$.

Since $\mathfrak{A}_3$ is prime to $\mathfrak{B}$, similarly we can show that the product $\mathfrak{A}_1\mathfrak{A}_2\cdot\mathfrak{A}_3$ is also prime to $\mathfrak{B}$; and so on. Finally we have the theorem.

Cor. If two ideals $\mathfrak{A}$ and $\mathfrak{B}$ of a proper ring are prime to each other, their powers are also prime to each other.

For, from $(\mathfrak{A}, \mathfrak{B})=\mathfrak{R}$ it follows that $(\mathfrak{A}^m, \mathfrak{B})=\mathfrak{R}$, whence $(\mathfrak{A}^m, \mathfrak{B}^n)=\mathfrak{R}$.

THEOREM: *If* $\mathfrak{P}$ *is a maximal ideal*[3] *of a proper ring* $\mathfrak{R}$, *it contains every ideal, except* $\mathfrak{R}$, *which contains a power of* $\mathfrak{P}$.

For, if an ideal $\mathfrak{B}$ of a proper ring $\mathfrak{R}$ is not contained in $\mathfrak{P}$, then $(\mathfrak{P}, \mathfrak{B})=\mathfrak{R}$ and hence $(\mathfrak{P}^e, \mathfrak{B})=\mathfrak{R}$ for every index e. Therefore $\mathfrak{B}$ can not contain a power of $\mathfrak{P}$ unless $\mathfrak{B}=\mathfrak{R}$; and the theorem holds true.

If, particularly, for a certain index e the power $\mathfrak{P}^e$ becomes the

1 Congr., § 9.

2 If $(\mathfrak{A}, \mathfrak{B})=\mathfrak{R}$, $\mathfrak{A}$ and $\mathfrak{B}$ have no common divisor except $\mathfrak{R}$, but the converse is not necessarily true, as will be seen later. Hence the definition in this respect is somewhat extended.

3 Congr., § 9, p. 214.

o-ideal, the ideal consisting of the element o alone, $\mathfrak{P}$ contains all ideals of $\mathfrak{R}$; because every ideal contains the element o.

§ 5. THEOREM: *If two ideals of a proper ring are prime to each other, their product is equal to their cross-cut.*[1]

Proof. Let $\mathfrak{A}$ and $\mathfrak{B}$ be two ideals of a proper ring $\mathfrak{R}$, and $\mathfrak{D}$ the cross-cut of $\mathfrak{A}$ and $\mathfrak{B}$. And moreover $(\mathfrak{A}, \mathfrak{B})=\mathfrak{R}$. Then the product $\mathfrak{A}\mathfrak{D}$ is contained in the product $\mathfrak{A}\mathfrak{B}$, and the product $\mathfrak{B}\mathfrak{D}$ also in $\mathfrak{A}\mathfrak{B}$. Consequently the ideal $(\mathfrak{A}\mathfrak{D}, \mathfrak{B}\mathfrak{D})$ derived from the products $\mathfrak{A}\mathfrak{D}$ and $\mathfrak{B}\mathfrak{D}$ is contained in $\mathfrak{A}\mathfrak{B}$. But

$$(\mathfrak{A}\mathfrak{D}, \mathfrak{B}\mathfrak{D}) = (\mathfrak{A}, \mathfrak{B})\,\mathfrak{D} = \mathfrak{R}\mathfrak{D} = \mathfrak{D}.$$

Hence $\mathfrak{D}$ is contained in $\mathfrak{A}\mathfrak{B}$, while containing $\mathfrak{A}\mathfrak{B}$: so that we have $\mathfrak{A}\mathfrak{B}=\mathfrak{D}$.

N.B. The last theorem evidently holds good also when one of the ideals is the ring itself.

Cor. If two ideals $\mathfrak{A}$ and $\mathfrak{B}$ of a proper ring $\mathfrak{R}$ are prime to each other and moreover if their norms[2] under $\mathfrak{R}$ are both finite, then the norm of their product is equal to the product of their norms, viz.

$$n(\mathfrak{A}\mathfrak{B}) = n(\mathfrak{A}) \cdot n(\mathfrak{B}).$$

For, let $\mathfrak{D}$ be the cross-cut of $\mathfrak{A}$ and $\mathfrak{B}$, then $\mathfrak{A}\mathfrak{B}=\mathfrak{D}$, and the norm of $\mathfrak{D}$ is equal to the product of the orders of the quotient rings $\frac{\mathfrak{R}}{\mathfrak{A}}$ and $\frac{\mathfrak{A}}{\mathfrak{D}}$. But $\frac{\mathfrak{A}}{\mathfrak{D}}$ is of the same type as $\frac{\mathfrak{R}}{\mathfrak{B}}$, since $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{R}$ [Congr., § 11, Theorem]. Therefore the order of $\frac{\mathfrak{A}}{\mathfrak{D}}$ is equal to that of $\frac{\mathfrak{R}}{\mathfrak{B}}$, which is the norm of $\mathfrak{B}$. Hence we have

$$n(\mathfrak{A}\mathfrak{B}) = n(\mathfrak{D}) = n(\mathfrak{A}) \cdot n(\mathfrak{B}).$$

THEOREM: *Let* $\mathfrak{A}_1, \mathfrak{A}_2, \ldots\ldots, \mathfrak{A}_n$ *be* n *ideals of a proper ring* $\mathfrak{R}$ *which are prime to one another. Then their product* $\mathfrak{A}_1\mathfrak{A}_2\ldots\ldots\mathfrak{A}_n$ *is equal to their cross-cut.*

Assume that the theorem holds true for any given value $n-1$. Let $\mathfrak{D}'$ be the cross-cut of $n-1$ ideals $\mathfrak{A}_1, \mathfrak{A}_2, \ldots\ldots, \mathfrak{A}_{n-1}$, then we have

$$\mathfrak{D}' = \mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{n-1},$$

which is prime to $\mathfrak{A}_n$ [§ 4, theorem]. Therefore the product $\mathfrak{A}_1\mathfrak{A}_2\ldots\ldots\mathfrak{A}_n=\mathfrak{D}'\mathfrak{A}_n$ is equal to the cross-cut of $\mathfrak{D}'$ and $\mathfrak{A}_n$ [by the last

1 Congr., § 10, p. 215.

2 *Loc. cit.* § 9, p. 213.

theorem], which is evidently the cross-cut of the n ideals. Thus the theorem must hold true also for n. But it holds true for two ideals prime to each other; therefore it is universally true.

Cor. The product of distinct maximal ideals of a proper ring is equal to their cross-cut.

Cor. If ideals $\mathfrak{A}_1, \mathfrak{A}_2, \ldots\ldots, \mathfrak{A}_n$ of a proper ring are prime to one another, the product $\mathfrak{A}_1^{e_1}\mathfrak{A}_1^{e_2}\ldots\ldots\mathfrak{A}_n^{e_n}$ is equal to the cross-cut of $\mathfrak{A}_1^{e_1}, \mathfrak{A}_2^{e_2}, \ldots\ldots\mathfrak{A}_n^{e_n}$.

For, since the $\mathfrak{A}$'s are prime to one another, their powers are also prime to one another: so that the Cor. follows from the last theorem.

§ 6. THEOREM: *If two ideals $\mathfrak{A}$ and $\mathfrak{B}$ of a proper ring $\mathfrak{R}$ are prime to each other, then*

$$(\mathfrak{C}, \mathfrak{A})(\mathfrak{C}, \mathfrak{B}) = (\mathfrak{C}, \mathfrak{A}\mathfrak{B}),$$

where $\mathfrak{C}$ is an ideal of $\mathfrak{R}$.

For
$$\begin{aligned}(\mathfrak{C}, \mathfrak{A})(\mathfrak{C}, \mathfrak{B}) &= (\mathfrak{C}^2, \mathfrak{C}\mathfrak{A}, \mathfrak{C}\mathfrak{B}, \mathfrak{A}\mathfrak{B})\\ &= (\mathfrak{C}^2, \mathfrak{C}(\mathfrak{A}, \mathfrak{B}), \mathfrak{A}\mathfrak{B}) = (\mathfrak{C}^2, \mathfrak{C}\mathfrak{R}, \mathfrak{A}\mathfrak{B}) \qquad [\because (\mathfrak{A}, \mathfrak{B}) = \mathfrak{R}]\\ &= (\mathfrak{C}, \mathfrak{A}\mathfrak{B}),\end{aligned}$$

since $\mathfrak{C}\mathfrak{R} = \mathfrak{C}$, and $\mathfrak{C}^2$ is contained in $\mathfrak{C}$.

The aggregate of all possible products which are obtained by multiplying a given element ρ of a ring $\mathfrak{R}$ by an element of $\mathfrak{R}$ is an ideal of $\mathfrak{R}$, which is completely determined by the element ρ. When $\mathfrak{R}$ is proper, according to the usual nomenclature and notation, we call this ideal a *principal ideal* and denote it by (ρ). Moreover, the product of two ideals (ρ) and $\mathfrak{A}$ is denoted by $\rho\mathfrak{A}$.

Cor. If two ideals $\mathfrak{A}$ and $\mathfrak{B}$ of a proper ring $\mathfrak{R}$ are prime to each other, then

$$((\rho), \mathfrak{A})((\rho), \mathfrak{B}) = ((\rho), \mathfrak{A}\mathfrak{B}),$$

where ρ is an element of $\mathfrak{R}$.

It follows, from the theorem, that, if an ideal $\mathfrak{M}$ of a proper ring $\mathfrak{R}$ contains the product of two ideals, $\mathfrak{A}$ and $\mathfrak{B}$, of $\mathfrak{R}$ prime to each other, $\mathfrak{M}$ also contains the product of two ideals $((M), \mathfrak{A})$ and $((M), \mathfrak{B})$, where M is an element of $\mathfrak{M}$ arbitrarily chosen. But the product of two ideals prime to each other is equal to their cross-cut [§ 5, Theorem]; therefore the proposition may be rewritten as follows:

If an ideal $\mathfrak{M}$ of a proper ring $\mathfrak{R}$ contains the cross-cut of two ideals, $\mathfrak{A}$ and $\mathfrak{B}$, of $\mathfrak{R}$ prime to each other, $\mathfrak{M}$ also contains the cross-cut of two ideals $((M), \mathfrak{A})$ and $((M), \mathfrak{B})$, where M is an element of $\mathfrak{M}$.

Ideals Containing the Square of a Maximal Ideal.

§ 7. Let $\mathfrak{P}$ be a maximal ideal of a proper ring $\mathfrak{R}$. Then, as shown in § 4, $\mathfrak{P}$ contains every ideal containing a power of $\mathfrak{P}$; and hence evidently a chief-composition-series of $\mathfrak{R}$ containing a power of $\mathfrak{P}$ as a term has $\mathfrak{P}$ for the second term.

As may be easily shown, there are two existent cases wherein $\mathfrak{P}^2$ either does or does not coincide with $\mathfrak{P}$; but we now suppose that $\mathfrak{P}^2$ is not equal to $\mathfrak{P}$.

Let $\mathfrak{A}$ be an ideal of $\mathfrak{R}$, distinct from $\mathfrak{P}$, which contains $\mathfrak{P}^2$ and consequently is contained in $\mathfrak{P}$. (Of course $\mathfrak{A}$ may be $\mathfrak{P}^2$; if there is no ideal, except $\mathfrak{P}$ and $\mathfrak{P}^2$, containing $\mathfrak{P}^2$, we need only take $\mathfrak{A}=\mathfrak{P}^2$.) Then the product of any two elements of $\mathfrak{P}$ must belong to $\mathfrak{A}$; because it belongs to $\mathfrak{P}^2$, which is contained in $\mathfrak{A}$.

We now proceed to find a complete set[1] of incongruent (mod. $\mathfrak{A}$) elements of the ideal $((\pi), \mathfrak{A})$, where π is an element of $\mathfrak{P}$ which does not belong to $\mathfrak{A}$.

Every element of $((\pi), \mathfrak{A})$ is given by the form $\pi R+A$, where R and A are elements of $\mathfrak{R}$ and $\mathfrak{A}$ respectively.

If an element $\pi R+A$ of $((\pi), \mathfrak{A})$, and consequently πR, belongs to $\mathfrak{A}$, R must belong to $\mathfrak{P}$; and conversely. For if it were $R\not\equiv 0$ (mod. $\mathfrak{P}$), then, since $\mathfrak{R}$ is proper and $\mathfrak{P}$ is a maximal ideal of $\mathfrak{R}$, we should have

$$((R), \mathfrak{P})=\mathfrak{R};$$

consequently two elements R_1 and P could be chosen from $\mathfrak{R}$ and $\mathfrak{P}$ respectively so that

$$RR_1+P=1.$$

Multiplying both sides of the last equation by π we have

$$\pi=\pi RR_1+\pi P\equiv 0 \quad (\text{mod. } \mathfrak{A});$$

because $\pi R\equiv 0$ (mod. $\mathfrak{A}$) by hypothesis, and $\pi P\equiv 0$ (mod. $\mathfrak{A}$). This contradicts the assumption that $\pi\not\equiv 0$ (mod. $\mathfrak{A}$); therefore if $\pi R+A\equiv 0$ (mod. $\mathfrak{A}$), $R\equiv 0$ (mod. $\mathfrak{P}$). And the converse is evidently true.

---

[1] Let $\mathfrak{S}$ be a subring of a ring $\mathfrak{R}$ [*cf.* Congr., § 6], and $\mathfrak{M}$ an ideal of $\mathfrak{R}$ which is contained in $\mathfrak{S}$. A set of elements of $\mathfrak{S}$ is called a complete set of incongruent (mod. $\mathfrak{M}$) elements of $\mathfrak{S}$, when the elements of the set are all incongruent (mod. $\mathfrak{M}$) and every element of $\mathfrak{S}$ is congruent (mod. $\mathfrak{M}$) to one element of the set. In other words, it is a set of distinct elements of the quotient ring $\frac{\mathfrak{S}}{\mathfrak{M}}$ [*cf.* Congr., § 9].

Next, if two elements $\pi R+A$ and $\pi R'+A'$ of $((\pi), \mathfrak{A})$, are congruent (mod. $\mathfrak{A}$) to each other, viz.

$$\pi R+A \equiv \pi R'+A' \quad (\text{mod. } \mathfrak{A}),$$

then
$$\pi(R-R') \equiv 0 \quad (\text{mod. } \mathfrak{A});$$

whence
$$R-R' \equiv 0 \quad (\text{mod. } \mathfrak{P}).$$

or
$$R \equiv R' \quad (\text{mod. } \mathfrak{P}).$$

Conversely, from $R\equiv R'$ (mod. $\mathfrak{P}$) it evidently follows that $\pi R+A\equiv\pi R'+A'$ (mod. $\mathfrak{A}$). Therefore we have the

THEOREM: *Let*

$$\rho_1, \rho_2, \cdots$$

be a complete set of incongruent (mod. $\mathfrak{P}$*) elements of* $\mathfrak{R}$. *Then the products*

$$\pi\rho_1, \pi\rho_2, \ldots,$$

being taken modulo $\mathfrak{A}$, *form a complete set of incongruent (mod.* $\mathfrak{A}$*) elements of* $((\pi), \mathfrak{A})$, *that is, give the quotient ring* $((\pi), \mathfrak{A})/\mathfrak{A}$. ($\mathfrak{A}$ and π are the said ideal and element).

Cor. There is no ideal of $\mathfrak{R}$, except $((\pi), \mathfrak{A})$ and $\mathfrak{A}$, which is contained in $((\pi), \mathfrak{A})$ and contains $\mathfrak{A}$.

For, if β is an element of $((\pi), \mathfrak{A})$ which does not belong to $\mathfrak{A}$, then

$$\beta \equiv \pi\rho \quad (\text{mod. } \mathfrak{A}),$$

where ρ is a certain element of the set $\rho_1, \rho_2, \ldots\ldots$, which is not congruent (mod. $\mathfrak{P}$) to 0. Since $\rho\not\equiv 0$ (mod. $\mathfrak{P}$), we have

$$((\rho), \mathfrak{P}) = \mathfrak{R}.$$

Choosing two elements R and P from $\mathfrak{R}$ and $\mathfrak{P}$ respectively so that $\rho R+P=1$, we get

$$\pi = \pi\rho R+\pi P \equiv \beta R \quad (\text{mod. } \mathfrak{A}).$$

Therefore the element π, and consequently the ideal $((\pi), \mathfrak{A})$, is contained in the ideal $((\beta), \mathfrak{A})$; and hence we have the Cor.

Particularly if the quotient ring $\mathfrak{R}/\mathfrak{P}$ is of finite order, the two quotient rings $\mathfrak{R}/\mathfrak{P}$ and $((\pi), \mathfrak{A})/\mathfrak{A}$ are of the same order.

§ 8. Let

$$\mathfrak{R}, \mathfrak{P}, \mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n, \mathfrak{P}^2$$

be a chief-composition-series[1] of a proper ring $\mathfrak{R}$ with the last term $\mathfrak{P}^2$.

And let ρ be an element of $\mathfrak{R}$ which does not belong to $\mathfrak{P}$;

$$\begin{array}{llllllll} ,, & \pi & ,, & \mathfrak{P} & ,, & \mathfrak{A}_1; \\ ,, & a_1 & ,, & \mathfrak{A}_1 & ,, & \mathfrak{A}_2; \\ ,, & a_2 & ,, & \mathfrak{A}_2 & ,, & \mathfrak{A}_3; \\ \multicolumn{6}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\ ,, & a_n & ,, & \mathfrak{A}_n & ,, & \mathfrak{P}^2. \end{array}$$

Then, by the last theorem, we have

$$\mathfrak{A}_n = ((a_n), \mathfrak{P}^2),$$
$$\mathfrak{A}_{n-1} = ((a_{n-1}), \mathfrak{A}_n) = ((a_{n-1}), (a_n), \mathfrak{P}^2),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\mathfrak{A}_1 = ((a_1), \mathfrak{A}_2) = ((a_1), (a_2), \ldots, (a_n), \mathfrak{P}^2),$$
$$\mathfrak{P} = ((\pi), \mathfrak{A}_1) = ((\pi), (a_1), (a_2), \ldots, (a_n), \mathfrak{P}^2),$$
$$\mathfrak{R} = ((\rho), \mathfrak{P}) = ((\rho), (\pi), (a_1), \ldots, (a_n), \mathfrak{P}^2),$$

And the quotient rings

$$\frac{\mathfrak{P}}{\mathfrak{A}_1}, \frac{\mathfrak{A}_1}{\mathfrak{A}_2}, \ldots, \frac{\mathfrak{A}_n}{\mathfrak{P}^2}$$

are of the same type, being no field [*cf.* Congr., § 20].

If, especially, the quotient $\mathfrak{R}/\mathfrak{P}$ is of finite order, the above quotient rings are all of the same order as $\mathfrak{R}/\mathfrak{P}$; and the norm[2] of $\mathfrak{P}^2$ is equal to $[n(\mathfrak{P})]^{n+2}$.

Therefore *if* $n(\mathfrak{P}^2) = [n(\mathfrak{P})]^2$, *an ideal of* $\mathfrak{R}$ *which contains* $\mathfrak{P}^2$ *is either* $\mathfrak{P}$ *or* $\mathfrak{P}^2$.

Powers of Maximal Ideals.

§ 9. Let $\mathfrak{P}$ be a maximal ideal of a proper ring $\mathfrak{R}$; and again suppose that $\mathfrak{P}^2$ is distinct from $\mathfrak{P}$. Then there are two existent cases wherein $\mathfrak{R}$ either does or does not possess an ideal containing $\mathfrak{P}^2$ and distinct from both $\mathfrak{P}$ and $\mathfrak{P}^2$.

In the second case we have

$$\mathfrak{P} = ((\pi), \mathfrak{P}^2),$$

and
$$\mathfrak{P}^n = ((\pi^n), \mathfrak{P}^{n+1}),$$

1 Congr. §13. p. 220.

2 *Loc. cit.* §9.

where π is an element of $\mathfrak{P}$ which does not belong to $\mathfrak{P}^2$, and n is a positive integer.

For, as seen in § 6,

$$\mathfrak{P} = ((\pi), \mathfrak{P}^2),$$

and

$$\begin{aligned}\mathfrak{P}^2 &= ((\pi), \mathfrak{P}^2)\,\mathfrak{P} = (\pi\mathfrak{P}, \mathfrak{P}^3)\\ &= (\pi((\pi), \mathfrak{P}^2), \mathfrak{P}^3) = ((\pi^2), \pi\mathfrak{P}^2, \mathfrak{P}^3)\\ &= ((\pi^2), \mathfrak{P}^3),\end{aligned}$$

since $\pi\mathfrak{P}^2$ is contained in $\mathfrak{P}^3 = ((\pi), \mathfrak{P}^2)\mathfrak{P}^2 = (\pi\mathfrak{P}^2, \mathfrak{P}^4)$. Next

$$\begin{aligned}\mathfrak{P}^3 &= ((\pi^2), \mathfrak{P}^3)\,\mathfrak{P} = (\pi^2\mathfrak{P}, \mathfrak{P}^4)\\ &= (\pi^2((\pi), \mathfrak{P}^2), \mathfrak{P}^4) = ((\pi^3), \mathfrak{P}^4),\end{aligned}$$

since $\pi^2\mathfrak{P}^2$ is contained in $\mathfrak{P}^4 = ((\pi^2), \mathfrak{P}^3)\,\mathfrak{P}^2 = (\pi^2\mathfrak{P}^2\ \mathfrak{P}^5)$; and so on.

It may happen that among the powers

$$\mathfrak{P},\ \mathfrak{P}^2,\ \mathfrak{P}^3,\ \dots$$

there exist equal ones.

For example, let p and q be two distinct prime numbers. Then the p^2q integers

$$0,\ 1,\ 2,\ \dots,\ (p^2q-1),$$

being taken modulo p^2q, form a ring, say called $\mathfrak{R}$. And the pq integers in $\mathfrak{R}$

$$0,\ p,\ 2p,\ \dots,\ (pq-1)p,$$

also being taken modulo p^2q, form a maximal ideal of $\mathfrak{R}$, say called $\mathfrak{P}$. It is easily seen that $\mathfrak{P}^2$ consists of the q integers

$$0,\ p^2,\ 2p^2,\ \dots,\ (q-1)\,p^2$$

taken modulo p^2q, and that $\mathfrak{P}^3$ coincides with $\mathfrak{P}^2$.

If, on the contrary, for every index n

$$\mathfrak{P}^n \neq \mathfrak{P}^{n+1},$$

the successive powers

$$\mathfrak{R}, \mathfrak{P}, \mathfrak{P}^2, \mathfrak{P}^3 \dots$$

give a chief-composition-series of $\mathfrak{R}$, in the present case.

For, let a be an element of $\mathfrak{P}^n$ which does not belong to $\mathfrak{P}^{n+1}$, then

$$a = \pi^n R + P^{(n+1)},$$

where $P^{(n+1)}$ is an element of $\mathfrak{P}^{n+1}$, and R an element of $\mathfrak{R}$ which does not belong to $\mathfrak{P}$. Choose an element R_1 of $\mathfrak{R}$ so that $RR_1 \equiv 1$ (mod. $\mathfrak{P}$), and we have

$$aR_1 \equiv (\pi^n R + P^{(n+1)}) R_1 \equiv \pi^n \pmod{\mathfrak{P}^{n+1}},$$

Therefore the element π^n, and consequently the ideal $\mathfrak{P}^n$, is contained in the ideal $((a), \mathfrak{P}^{n+1})$, a being an arbitrarily taken element of $\mathfrak{P}^n$ which is not contained in $\mathfrak{P}^{n+1}$. So that there is no ideal of $\mathfrak{R}$ containing $\mathfrak{P}^{n+1}$ and contained in $\mathfrak{P}^n$; and hence the series is a chief-composition-series of $\mathfrak{R}$.

§ 10. THEOREM: *Let $\mathfrak{P}$ be a maximal ideal of a proper ring $\mathfrak{R}$, and assume that there is no ideal of $\mathfrak{R}$, distinct from both $\mathfrak{P}$ and $\mathfrak{P}^2$, which contains $\mathfrak{P}^2$ and consequently is contained in $\mathfrak{P}$. Then every ideal of $\mathfrak{R}$, except $\mathfrak{R}$, which contains a power of $\mathfrak{P}$ is a power of $\mathfrak{P}$.*

Proof. Since, if $\mathfrak{P}^2 = \mathfrak{P}$, it is evident, we prove it under the supposition that $\mathfrak{P}^2 \neq \mathfrak{P}$. Let $\mathfrak{A}$ be an ideal of $\mathfrak{R}$ containing the power $\mathfrak{P}^n$. Then $\mathfrak{A}$ is contained in $\mathfrak{P}$ [§ 4, 2nd theorem]. Therefore, if $\mathfrak{A} \neq \mathfrak{P}^n$, there must exist a power of $\mathfrak{P}$ such that it contains $\mathfrak{A}$, while the next power does not. Let it be $\mathfrak{P}^{n-i}$ ($i \geqq 1$). That is to say, we suppose that $\mathfrak{A}$ is contained in $\mathfrak{P}^{n-i}$ but not in $\mathfrak{P}^{n-i+1}$.

Take an element a of $\mathfrak{A}$, which does not belong to $\mathfrak{P}^{n-i+1}$, and we have

$$a = \pi^{n-i} R + P^{(n-i+1)}$$

where π is an element of $\mathfrak{P}$ which is not contained in $\mathfrak{P}^2$, and R, $P^{(n-i+1)}$ are elements of $\mathfrak{R}$, $\mathfrak{P}^{n-i+1}$ respectively; because $\mathfrak{P}^{n-i} = ((\pi^{n-i}), \mathfrak{P}^{n-i+1})$. And moreover the element R does not belong to $\mathfrak{P}$; because $R \equiv 0$ (mod. $\mathfrak{P}$) would involve $\pi^{n-i}R \equiv 0$ (mod. $\mathfrak{P}^{n-i+1}$) and consequently $a \equiv 0$ (mod. $\mathfrak{P}^{n-i+1}$), contrary to our assumption. Since thus $R \not\equiv 0$ (mod. $\mathfrak{P}$), we can choose two elements R' and P respectively from $\mathfrak{R}$ and $\mathfrak{P}$ so that $RR' + P = 1$. And we have

$$\begin{aligned} aR' &= \pi^{n-i} RR' + R' P^{(n-i+1)} \\ &= \pi^{n-i}(1 - P) + R' P^{(n-i+1)}, \end{aligned}$$

whence

$$\pi^{n-1} = \pi^{i-1} a R' + \pi^{n-1} P - R' \pi^{i-1} P^{(n-i+1)}.$$

But $\pi^{n-1}P$ and $R'\pi^{i-1}P^{(n-i+1)}$ are both contained in $\mathfrak{P}^n$. Therefore

$$\pi^{n-1} \equiv 0 \pmod{((a), \mathfrak{P}^n)},$$

and consequently

$$\pi^{n-1} \equiv 0 \pmod{\mathfrak{A}}.$$

Hence $\mathfrak{A}$ contains the ideal $((\pi^{n-1}), \mathfrak{P}^n) = \mathfrak{P}^{n-1}$.

Since, by supposition, $\mathfrak{A}$ is contained in $\mathfrak{P}^{n-i}$, if $i=1$, $\mathfrak{A}$ must$=$ $\mathfrak{P}^{n-1}$. If $i>1$, it is shown similarly that $\mathfrak{A}$ contains $\mathfrak{P}^{n-2}$; and if $i=2$, $\mathfrak{A}=\mathfrak{P}^{n-2}$. Repeating the process we finally have $\mathfrak{A}=\mathfrak{P}^{n-i}$, which we require.

Cor. If $n(\mathfrak{P})$ is finite and moreover $n(\mathfrak{P}^2)=[n(\mathfrak{P})]^2$, every ideal, except $\mathfrak{R}$, containing a power of $\mathfrak{P}$ is a power of $\mathfrak{P}$.

Because, if $n(\mathfrak{P}^2)=[n(\mathfrak{P})]^2$, an ideal containing $\mathfrak{P}^2$ is $\mathfrak{P}$ or $\mathfrak{P}^2$ [§ 8].

§ 11. The case where there is at least one ideal, distinct from $\mathfrak{P}$ and $\mathfrak{P}^2$, containing $\mathfrak{P}^2$. It is here treated under the condition that the ring $\mathfrak{R}$ possesses a chief-composition-series with the last term $\mathfrak{P}^2$. This again is divided into the two cases in which a chief-composition-series of $\mathfrak{R}$ with the last term $\mathfrak{P}^2$ consists either of four terms or of more than four terms.

Beginning with the former, let

$$\mathfrak{R},\ \mathfrak{P},\ \mathfrak{A},\ \mathfrak{P}^2$$

be a chief-composition-series of a proper ring $\mathfrak{R}$ with the last term $\mathfrak{P}^2$, $\mathfrak{P}$ being a maximal ideal of $\mathfrak{R}$.

Let π be an element of $\mathfrak{P}$ which does not belong to $\mathfrak{A}$, and α an element of $\mathfrak{A}$ which does not belong to $\mathfrak{P}^2$. Then, by § 8, we have

$$\mathfrak{P} = ((\pi), (\alpha), \mathfrak{P}^2).$$

And

$$\begin{aligned}\mathfrak{P}^2 &= ((\pi), (\alpha), \mathfrak{P}^2)\, \mathfrak{P} = (\pi\mathfrak{P}, \alpha\mathfrak{P}, \mathfrak{P}^3) \\ &= (\pi((\pi), (\alpha), \mathfrak{P}^2), \alpha((\pi), (\alpha), \mathfrak{P}^2), \mathfrak{P}^3) \\ &= ((\pi^2), (\pi\alpha), (\alpha^2), \mathfrak{P}^3),\end{aligned}$$

since the ideals $\pi\mathfrak{P}^2$ and $\alpha\mathfrak{P}^2$ are contained in the ideal $(\pi\mathfrak{P}^2, \alpha\mathfrak{P}^2, \mathfrak{P}^4) = ((\pi), (\alpha), \mathfrak{P}^2)\, \mathfrak{P}^2 = \mathfrak{P}^3$.

$$\begin{aligned}\mathfrak{P}^3 &= ((\pi^2), (\pi\alpha), (\alpha^2), \mathfrak{P}^3)\, \mathfrak{P} \\ &= (((\pi^2), (\alpha^2), \mathfrak{P}^3)\mathfrak{P}, \pi\alpha\mathfrak{P}).\end{aligned}$$

But

$$\pi\alpha\mathfrak{P} = \pi\alpha((\pi), (\alpha), \mathfrak{P}^2) = ((\pi^2\alpha), (\pi\alpha^2), \pi\alpha\mathfrak{P}^2),$$

and the ideals $(\pi^2\alpha)$, $(\pi\alpha^2)$ and $\pi\alpha\mathfrak{P}^2$ are contained in the ideals $\pi^2\mathfrak{P}$, $\alpha^2\mathfrak{P}$ and $\mathfrak{P}^4$ respectively. Therefore we have the formula, which is important in our theory:

(I) $$\mathfrak{P}^3 = ((\pi^2), (\alpha^2), \mathfrak{P}^3)\, \mathfrak{P}.$$

There are to be considered the two cases in which the ideal $((\pi^2), (\alpha^2), \mathfrak{P}^3)$ is either equal or not equal to $\mathfrak{P}^2$. The former will be further discussed in the next article.

§ 12. Now, we suppose that

$$((\pi^2), (\alpha^2), \mathfrak{P}^3) = \mathfrak{P}^2.$$

Then, since the product $\pi\alpha$ of the elements π and α belongs to $\mathfrak{P}^2$, we have

(a) $$\pi\alpha = \pi^2 R + \alpha^2 R_1 + P^{(3)},$$

where R, R_1 are elements of the ring $\mathfrak{R}$, and $P^{(3)}$ an element of $\mathfrak{P}^3$.

Again, there are two cases to consider.

(1) Suppose that R and R_1 both belong to $\mathfrak{P}$, viz.

$$R \equiv R_1 \equiv 0 \pmod{\mathfrak{P}}.$$

Then

$$\pi\alpha \equiv 0 \pmod{\mathfrak{P}^3},$$

and

$$\begin{aligned}((\pi), \mathfrak{P}^2)((\alpha), \mathfrak{P}^2) &= ((\pi\alpha), \pi\mathfrak{P}^2, \alpha\mathfrak{P}^2, \mathfrak{P}^4)\\ &= ((\pi\alpha), ((\pi), (\alpha), \mathfrak{P}^2)\,\mathfrak{P}^2)\\ &= ((\pi\alpha), \mathfrak{P}^3) = \mathfrak{P}^3.\end{aligned}$$

(2) The case in which at least one of R and R_1 does not belong to $\mathfrak{P}$.

(i) Suppose $R \not\equiv 0 \pmod{\mathfrak{P}}$.

Since $\mathfrak{P}$ is a maximal ideal of $\mathfrak{R}$, it follows, from supposition, that

$$((R), \mathfrak{P}) = \mathfrak{R}.$$

Hence, two elements R' and P can be chosen from $\mathfrak{R}$ and $\mathfrak{P}$ respectively so that

$$RR' + P = 1.$$

Multiplying both sides of equation (a) by the element R' we have

$$\begin{aligned}\pi\alpha R' &= \pi^2 RR' + \alpha^2 R_1 R' + P^{(3)} R'\\ &= \pi^2(1-P) + \alpha^2 R_1 R' + P^{(3)} R'\\ &\equiv \pi^2 + \alpha^2 R_1 R' \pmod{\mathfrak{P}^3},\end{aligned}$$

or

$$\pi^2 \equiv \pi\alpha R' - \alpha^2 R_1 R' \pmod{\mathfrak{P}^3}.$$

Hence π^2 is contained in the ideal $((\pi a), (a^2), \mathfrak{P}^3)$.
But

$$\mathfrak{P}^2 = ((\pi^2), (\pi a), (a^2), \mathfrak{P}^3),$$

and

$$\begin{aligned} ((a), \mathfrak{P}^2)\,\mathfrak{P} &= (a\mathfrak{P}, \mathfrak{P}^3) \\ &= (a((\pi), (a), \mathfrak{P}^2), \mathfrak{P}^3) \\ &= ((\pi a), (a^2), a\mathfrak{P}^2, \mathfrak{P}^3) \\ &= ((\pi a), (a^2), \mathfrak{P}^3), \end{aligned}$$

since $a\mathfrak{P}^2$ is contained in $\mathfrak{P}^3$. Therefore we have

$$\mathfrak{P}^2 = ((a), \mathfrak{P}^2)\,\mathfrak{P}.$$

(ii) If $R_1 \not\equiv 0 \pmod{\mathfrak{P}}$, similarly we have

$$\mathfrak{P}^2 = ((\pi), \mathfrak{P}^2)\,\mathfrak{P}.$$

The ideal $((\pi), \mathfrak{P}^2)$ is different from $\mathfrak{P}$; because otherwise $\mathfrak{P}$ would contain no ideal of $\mathfrak{R}$ containing $\mathfrak{P}^2$, except $\mathfrak{P}$ and $\mathfrak{P}^2$ [by § 7, Cor.].

SUMMARY. *If the set of ideals*

$$\mathfrak{R}, \mathfrak{P}, \mathfrak{A}, \mathfrak{P}^2$$

gives a chief-composition-series of the proper ring $\mathfrak{R}$, *then*

$$\mathfrak{P}^3 = ((\pi^2), (a^2), \mathfrak{P}^3)\,\mathfrak{P},$$

where π *is an element of* $\mathfrak{P}$ *which is not contained in* $\mathfrak{A}$, *and* a *an element of* $\mathfrak{A}$ *which is not contained in* $\mathfrak{P}^2$.

In case $$\mathfrak{P}^2 = ((\pi^2), (a^2), \mathfrak{P}^3),$$

(1) *if* $\pi a \equiv 0 \pmod{\mathfrak{P}^3}$,

$$\mathfrak{P}^3 = ((\pi), \mathfrak{P}^2)\,((a), \mathfrak{P}^2),$$

and (2) *if* $\pi a \not\equiv 0 \pmod{\mathfrak{P}^3}$,

$$\mathfrak{P}^2 = ((P), \mathfrak{P}^2)\,\mathfrak{P},$$

where P *is a certain element of* $\mathfrak{P}$ *which does not belong to* $\mathfrak{P}^2$.

§ 13. The case wherein a chief-composition-series with the last term $\mathfrak{P}^2$ consists of more than four terms. Let

$$\mathfrak{R}, \mathfrak{P}, \mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n, \mathfrak{P}^2 \qquad (n \geqq 2)$$

be a chief-composition-series of a proper ring $\mathfrak{R}$ with the last term $\mathfrak{P}^2$. And let

π be an element of $\mathfrak{P}$ which does not belong to $\mathfrak{A}_1$;

α_i „ $\mathfrak{A}_i$ „ $\mathfrak{A}_{i+1}$

$(i=1, 2, \ldots, n-1)$;

α_n „ $\mathfrak{A}_n$ „ $\mathfrak{P}^2$.

Then by § 8 we have

$$\text{(1)} \qquad \mathfrak{P} = ((\pi), (\alpha_1), (\alpha_2), \ldots, (\alpha_n), \mathfrak{P}^2),$$

and

$$\begin{aligned}\text{(2)} \qquad \mathfrak{P}^2 &= ((\pi), (\alpha_1), (\alpha_2), \ldots, (\alpha_n), \mathfrak{P}^2)\, \mathfrak{P} \\ &= (\pi\mathfrak{P}, \alpha_1\mathfrak{P}, \alpha_2\mathfrak{P}, \ldots, \alpha_n\mathfrak{P}, \mathfrak{P}^3) \\ &= ((\pi^2), (\pi\alpha_1), (\pi\alpha_2), \ldots, (\pi\alpha_n), \\ &\qquad (\alpha_1^2), (\alpha_1\alpha_2), \ldots, (\alpha_1\alpha_n), \\ &\qquad\qquad (\alpha_2^2), \ldots, (\alpha_2\alpha_n), \\ &\qquad\qquad\qquad \cdots\cdots\cdots\cdots \\ &\qquad\qquad\qquad (\alpha_n^2), \mathfrak{P}^3);\end{aligned}$$

because $\pi\mathfrak{P}^2$, $\alpha_1\mathfrak{P}^2, \ldots\ldots \alpha_n\mathfrak{P}^2$ are all contained in $\mathfrak{P}^3$.

Putting

$$\begin{aligned}\mathfrak{M} = ((\pi^2), (\alpha_1^2), (\alpha_1\alpha_2), \ldots, (\alpha_1\alpha_n), \\ (\alpha_2^2), \ldots, (\alpha_2\alpha_n), \\ \cdots\cdots\cdots\cdots \\ (\alpha_n^2), \mathfrak{P}^3)\end{aligned}$$

we have

$$\mathfrak{P}^3 = (\pi\alpha_1\mathfrak{P}, \pi\alpha_2\mathfrak{P}, \ldots, \pi\alpha_n\mathfrak{P}, \mathfrak{M}\mathfrak{P}).$$

But

$$\begin{aligned}\pi\alpha_i\mathfrak{P} &= \pi\alpha_i((\pi), (\alpha_1), \ldots, (\alpha_n), \mathfrak{P}^2) \\ &= ((\pi^2)\,\alpha_i, (\alpha_i\alpha_1)\,\pi, \ldots, (\alpha_i\alpha_n)\,\pi, \pi\alpha_i\mathfrak{P}^2);\end{aligned}$$

therefore the ideal $\pi\alpha_i\mathfrak{P}$ is contained in the product $\mathfrak{M}\mathfrak{P}$. And hence we get the second important formula:

$$\text{(II)} \qquad \mathfrak{P}^3 = \mathfrak{M}\mathfrak{P},$$

where

$$\begin{aligned}\mathfrak{M} = ((\pi^2), (\alpha_1^2), (\alpha_1\alpha_2), \ldots, (\alpha_1\alpha_n), \\ (\alpha_2^2), \ldots, (\alpha_2\alpha_n), \\ \cdots\cdots\cdots\cdots \\ (\alpha_n^2), \mathfrak{P}^3).\end{aligned}$$

In this also are to be considered the two cases in which the ideal $\mathfrak{M}$ is either equal or not equal to $\mathfrak{P}^2$. The former will be further discussed in the next article.

§ 14. We now suppose that $\mathfrak{M}=\mathfrak{P}^2$. Then, since by (2)

$$\pi\alpha_i \equiv 0 \pmod{\mathfrak{P}^2} \quad (i=1, 2, \dots, n),$$

we have

$$(b) \qquad \begin{aligned} \pi\alpha_i = \pi^2 R_i &+ \alpha_1^2 R_{i11} + \alpha_1\alpha_2 R_{i12} + \dots + \alpha_1\alpha_n R_{i1n} \\ &+ \alpha_2^2 R_{i22} + \dots + \alpha_2\alpha_n R_{i2n} \\ &+ \dots\dots\dots\dots\dots\dots \\ &+ \alpha_n^2 R_{inn} + P_i^{(3)}, \end{aligned}$$

$$(i=1, 2, \dots, n),$$

where the R's are elements of the ring $\mathfrak{R}$, and the $P^{(3)}$'s are elements of $\mathfrak{P}^3$.

Again there are four cases to consider.

(1) Suppose that all the R's of (*b*) belong to $\mathfrak{P}$.

Then by (*b*)

$$\pi\alpha_i \equiv 0 \pmod{\mathfrak{P}^3} \text{ for every } i=1, 2, \dots, n;$$

and we get

$$\begin{aligned} &((\pi), \mathfrak{P}^2)((\alpha_1), (\alpha_2), \dots, (\alpha_n), \mathfrak{P}^2) \\ &= ((\pi\alpha_1), (\pi\alpha_2), \dots, (\pi\alpha_n), \pi\mathfrak{P}^2, \alpha_1\mathfrak{P}^2, \alpha_2\mathfrak{P}^2, \dots \alpha_n\mathfrak{P}^2, \mathfrak{P}^4) \\ &= ((\pi\alpha_1), (\pi\alpha_2), \dots, (\pi\alpha_n), ((\pi), (\alpha_1), (\alpha_2), \dots, (\alpha_n), \mathfrak{P}^2)\,\mathfrak{P}^2) \\ &= ((\pi\alpha_1), (\pi\alpha_2), \dots, (\pi\alpha_n), \mathfrak{P}^3) \\ &= \mathfrak{P}^3. \end{aligned}$$

The ideals $((\pi), \mathfrak{P}^2)$ and $((\alpha_1), \dots\dots, (\alpha_n), \mathfrak{P}^2)$ contain $\mathfrak{P}^2$ and are contained in $\mathfrak{P}$; but evidently both are different from $\mathfrak{P}$ and $\mathfrak{P}^2$ [*cf.* § 7, Cor.].

(2), (i) Suppose that at least one of $R_1, R_2, \dots\dots, R_n$, (say R_1), does not belong to $\mathfrak{P}$, viz. $R_1 \not\equiv 0 \pmod{\mathfrak{P}}$.

Then we have

$$((R_1), \mathfrak{P}) = \mathfrak{R};$$

and hence we can choose two elements R' and P respectively from $\mathfrak{R}$ and $\mathfrak{P}$ so that

$$R_1 R' + P = 1.$$

Multiplying both sides of equation (*b*) by this element R' we have

$$\pi\alpha_1 R' = \pi^2 R_1 R' + P_1^{(3)} R' + \sum_{i,j} \alpha_i \alpha_j R_{1ij} R'$$
$$= \pi^2(1-P) + P_1^{(3)} R' + \sum \alpha_i \alpha_j R_{1ij} R';$$

or

$$\pi^2 \equiv \pi\alpha_1 R' - \sum \alpha_i \alpha_j R_{1ij} R' \quad (\text{mod. } \mathfrak{P}^3),$$

which shows that π^2 is contained in the ideal $((\pi\alpha_1), (\alpha_1^2), (\alpha_1\alpha_2), \ldots\ldots, (\alpha_1\alpha_n), (\alpha_2^2), \ldots\ldots, (\alpha_2\alpha_n), \ldots\ldots, (\alpha_n^2), \mathfrak{P}^3)$. We obtain a similar result also when $R_i \not\equiv 0$ (mod. $\mathfrak{P}$), $i=2, 3, \ldots\ldots, n$; viz. π^2 is contained in the ideal, $((\pi\alpha_i), (\alpha_1^2), (\alpha_1\alpha_2), \ldots\ldots, (\alpha_1\alpha_n), (\alpha_2^2), \ldots\ldots, (\alpha_2\alpha_n), \ldots\ldots, (\alpha_n^2), \mathfrak{P}^3)$. Therefore, if at least one of $R_1, R_2, \ldots\ldots, R_n$ does not belong to $\mathfrak{P}$, the ideal

$$\begin{aligned} ((\pi\alpha_1), (\pi\alpha_2), \ldots\ldots, &(\pi\alpha_n), \\ (\alpha_1^2), (\alpha_1\alpha_2), \ldots, &(\alpha_1\alpha_n), \\ (\alpha_2^2), \ldots, &(\alpha_2\alpha_n), \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &(\alpha_n^2), \mathfrak{P}^3) \end{aligned}$$

contains the element π^2, and consequently becomes equal to $\mathfrak{P}^2$ [*cf.* § 13, (2)], while being equal to the product

$$((\alpha_1), (\alpha_2), \ldots, (\alpha_n), \mathfrak{P}^2)\, \mathfrak{P}.$$

So that

$$\mathfrak{P}^2 = ((\alpha_1), (\alpha_2), \ldots, (\alpha_n), \mathfrak{P}^2)\, \mathfrak{P}.$$

The first factor of the right side is equal to $\mathfrak{A}_1$, which, of course, is distinct from $\mathfrak{P}$.

(ii) If the coefficient $R_{i11} \not\equiv 0$ (mod. $\mathfrak{P}$), the element α_1^2, as is shown similarly, belongs to the ideal

$$\begin{aligned} ((\pi^2), (\pi\alpha_i), & \\ (\alpha_1\alpha_2), (\alpha_1\alpha_3), \ldots, &(\alpha_1\alpha_n), \\ (\alpha_2^2), (\alpha_2\alpha_3), \ldots, &(\alpha_2\alpha_n), \\ (\alpha_3^2), \ldots, &(\alpha_3\alpha_n), \\ &\ldots\ldots\ldots\ldots, \\ &(\alpha_n^2), \mathfrak{P}^3). \end{aligned}$$

Therefore, if at least one of the n coefficients $R_{111}, R_{211}, \ldots\ldots, R_{n11}$ does not belong to $\mathfrak{P}$, the ideal

$$\begin{aligned}((\pi^2), (\pi a_1), (\pi a_2), \ldots\ldots\ldots\ldots, (\pi a_n),\\ (a_1 a_2), (a_1 a_3), \ldots, (a_1 a_n),\\ (a_2^2), (a_2 a_3), \ldots, (a_2 a_n),\\ (a_3^2), \ldots, (a_3 a_n),\\ \ldots\ldots\ldots\ldots,\\ (a_n^2), \mathfrak{P}^3)\end{aligned}$$

must contain the element a_1^2, and consequently becomes equal to $\mathfrak{P}^2$, while being equal to the product

$$((\pi), (a_2), (a_3), \ldots, (a_n), \mathfrak{P}^2)\, \mathfrak{P}.$$

So that

$$\mathfrak{P}^2 = ((\pi), (a_2), (a_3), \ldots, (a_n), \mathfrak{P}^2)\, \mathfrak{P}.$$

The first factor of the right side is evidently distinct from $\mathfrak{P}$ [*cf.* § 7, Cor.].

Similarly, if at least one of the n coefficients $R_{1jj}, R_{2jj}, \ldots\ldots, R_{njj}$ does not belong to $\mathfrak{P}$, then

$$\mathfrak{P}^2 = ((\pi), (a_1), \ldots (a_{j-1}), (a_{j+1}), \ldots, (a_n), \mathfrak{P}^2)\, \mathfrak{P},$$

the first factor of which is also different from $\mathfrak{P}$.

(3) Lastly, suppose that all of R_i and R_{ijj} $(i, j=1, 2, \ldots\ldots, n)$ belong to $\mathfrak{P}$, but at least one of the other coefficients R_{ijk}'s $(j \neq k)$ does not belong to $\mathfrak{P}$.

Then equations (b) become

$$\begin{aligned}\pi a_i \equiv a_1 a_2 R_{i12} + a_1 a_3 R_{i13} + \ldots + a_1 a_n R_{i1n}\\ + a_2 a_3 R_{i23} + \ldots + a_2 a_n R_{i2n}\\ + \ldots\ldots\ldots\ldots\ldots\\ + a_{n-1} a_n R_{i, n-1, n} \quad (\text{mod. } \mathfrak{P}^3),\\ (i=1, 2, \ldots, n).\end{aligned}$$

And hence all the products πa_1, πa_2, ..., πa_n are contained in the ideal

$$\begin{aligned}((a_1 a_2), (a_1 a_3), \ldots, (a_1 a_n),\\ (a_2 a_3), \ldots, (a_2 a_n),\\ \ldots\ldots\ldots\ldots,\\ (a_{n-1} a_n), \mathfrak{P}^3),\end{aligned}$$

which we denote by $\mathfrak{N}$. But

$$((\pi), (a_1), (a_2), \ldots, (a_{n-1}), \mathfrak{P}^2)\, ((a_2), (a_3), \ldots, (a_n), \mathfrak{P}^2)$$

$$\begin{aligned}=\big(&(\pi a_2), (\pi a_3), \ldots\ldots\ldots\ldots, (\pi a_n), \pi\mathfrak{P}^2,\\ &(a_1 a_2), (a_1 a_3), \ldots\ldots\ldots\ldots, (a_1 a_n), a_1\mathfrak{P}^2,\\ &(a_2^2), (a_2 a_3), \ldots\ldots\ldots\ldots, (a_2 a_n), a_2\mathfrak{P}^2,\\ &\quad (a_3^2), \ldots\ldots\ldots\ldots, (a_3 a_n), a_3\mathfrak{P}^2,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\ &\qquad (a_{n-1}^2), (a_{n-1}a_n), a_{n-1}\mathfrak{P}^2,\\ &\qquad\qquad a_n\mathfrak{P}^2, \mathfrak{P}^4\big)\end{aligned}$$

$$= \big((\pi a_2), (\pi a_3), \ldots, (\pi a_n), (a_2^2), (a_3^2), \ldots, (a_{n-1}^2), \mathfrak{N}\big) \text{ [by § 13, (1)]}$$
$$= \big((a_2^2), (a_3^2), \ldots, (a_{n-1}^2), \mathfrak{N}\big),$$

since all πa_i's ($i=1, 2, \ldots\ldots, n$) are contained in $\mathfrak{N}$. And similarly

$$\begin{aligned}&\big((a_1), (a_2), \ldots, (a_{n-1}), \mathfrak{P}^2\big)\big((\pi), (a_2), (a_3), \ldots, (a_n), \mathfrak{P}^2\big)\\ =\ &((a_2^2), (a_3^2), \ldots, (a_{n-1}^2), \mathfrak{N}).\end{aligned}$$

Therefore we have

$$\begin{aligned}&\big((\pi), (a_1), (a_2), \ldots, (a_{n-1}), \mathfrak{P}^2\big)\ \big((a_2), (a_3), \ldots, (a_n), \mathfrak{P}^2\big)\\ =\ &\big((a_1), (a_2), \ldots, (a_{n-1}), \mathfrak{P}^2\big)\ \big((\pi), (a_2), (a_3), \ldots, (a_n), \mathfrak{P}^2\big).\end{aligned}$$

These four ideals are different from one another, and all are contained in $\mathfrak{P}$ and contain $\mathfrak{P}^2$.

For, since

$$((a_2), (a_3), \ldots, (a_n), \mathfrak{P}^2) = \mathfrak{A}_2$$

as shown in § 8, if we put

$$((a_1), (a_2), \ldots, (a_{n-1}), \mathfrak{P}^2) = \mathfrak{B},$$

the last equation may be rewritten as follows:

$$((\pi), \mathfrak{B})\,\mathfrak{A}_2 = \mathfrak{B}\,((\pi), \mathfrak{A}_2).$$

But $((\pi), \mathfrak{B}) = \mathfrak{A}_2$ or $\mathfrak{B}$ would involve $\mathfrak{P}=\mathfrak{A}_2$ or $\mathfrak{A}_1$ respectively; $((\pi), \mathfrak{B}) = ((\pi), \mathfrak{A}_2)$ would involve $\mathfrak{P} = ((\pi), \mathfrak{A}_2)$, and consequently $\mathfrak{A}_1 = \mathfrak{P}$ or $\mathfrak{A}_2$ [by § 7, Cor.]; $\mathfrak{A}_2 = \mathfrak{B}$ would involve $\mathfrak{A}_1 = \mathfrak{A}_2$; $\mathfrak{A}_2 \neq ((\pi), \mathfrak{A}_2)$ by hypothesis; $\mathfrak{B} = ((\pi), \mathfrak{A}_2)$ would involve $\mathfrak{P} = \mathfrak{A}_1$. Therefore the four ideals are all different from one another.

§ 15. SUMMARY. *If the set of ideals*

$$\mathfrak{N}, \mathfrak{P}, \mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n, \mathfrak{P}^2 \quad (n \geqq 2)$$

gives a chief-composition-series of a proper ring $\mathfrak{R}$ *with the last term* $\mathfrak{P}^2$, *we have*

$$\mathfrak{P}^3 = \mathfrak{M}\mathfrak{P},$$

where

$$\begin{aligned}\mathfrak{M} = ((\pi^2), (\alpha_1^2), &(\alpha_1\alpha_2), \ldots, (\alpha_1\alpha_n),\\ &(\alpha_2^2), \ldots, (\alpha_2\alpha_n),\\ &\qquad\ldots\ldots\ldots\ldots,\\ &\qquad\qquad(\alpha_n^2), \mathfrak{P}^3),\end{aligned}$$

and π *and the* α*'s denote the same as in* § *13.*

If $\mathfrak{M}=\mathfrak{P}^2$, *there holds good at least one of the following four equations :*

$$(1) \qquad \mathfrak{P}^3 = ((\pi), \mathfrak{P}^2)((\alpha_1), (\alpha_2), \ldots, (\alpha_n), \mathfrak{P}^2);$$

$$(2), \text{(i)} \qquad \mathfrak{P}^2 = ((\alpha_1), (\alpha_2), \ldots, (\alpha_n), \mathfrak{P}^2)\,\mathfrak{P};$$

$$\text{(ii)} \qquad \mathfrak{P}^2 = ((\pi), (\alpha_1), \ldots, (\alpha_{j-1}), (\alpha_{j+1}), \ldots, (\alpha_n), \mathfrak{P}^2)\,\mathfrak{P};$$

$$\begin{aligned}(3) \qquad &((\pi), (\alpha_1), (\alpha_2), \ldots, (\alpha_{n-1}), \mathfrak{P}^2)((\alpha_2), (\alpha_3), \ldots, (\alpha_n), \mathfrak{P}^2)\\ &= ((\alpha_1), (\alpha_2), \ldots, (\alpha_{n-1}), \mathfrak{P}^2)((\pi), (\alpha_2), (\alpha_3), \ldots, (\alpha_n), \mathfrak{P}^2).\end{aligned}$$

Ideals of a Proper Ring in which every Ideal, Distinct from the O-ideal, is of Finite Norm. Resolution of an Ideal into Factors Prim to Each Other.

§ 16. Throughout the present and the subsequent articles (§§ 16—30) we assume that a ring to be treated is such that the norm of every ideal of it, which is not the o-ideal[1], is finite.

THEOREM : *Let*

$$\mathfrak{R},\ \mathfrak{A}_1,\ \mathfrak{A}_2,\ \ldots,\ \mathfrak{A}_n \quad (n \geqq 2)$$

be a chief-composition-series[2] *of a proper ring* $\mathfrak{R}$ *with the last term* $\mathfrak{A}_n$. *If any one of the quotient rings*

$$\frac{\mathfrak{A}_1}{\mathfrak{A}_2},\ \frac{\mathfrak{A}_2}{\mathfrak{A}_3},\ \ldots,\ \frac{\mathfrak{A}_{n-1}}{\mathfrak{A}_n}$$

derived from the series is a field[3], *the ideal* $\mathfrak{A}_n$ *may be expressed as the product of two ideals prime to each other.*

---

1 The ideal consisting of the element o alone.

2 *Cf.* Congr. § 13,

3 The term *field* is used to denote the German *Körper.*

LEMMA 1. If in a ring $\mathfrak{F}$ of finite order the product of any two elements of it is not 0, unless at least one of the factors is 0, the ring $\mathfrak{F}$ must be a field.

For, let

$$(1) \qquad F_1, F_2, \ldots, F_s$$

be the distinct elements of $\mathfrak{F}$. Taking out an element F, not equal to 0, of $\mathfrak{F}$ and multiplying each one of the series (1) by it, we get

$$(2) \qquad F_1F, F_2F, \ldots, F_sF.$$

These products are all distinct, while belonging to $\mathfrak{F}$. For, since $F \neq 0$, $F_iF = F_jF$ would involve $F_i = F_j$, contrary to our assumption. Therefore, series (1) and (2) are identical, except as regards the sequence in which the terms occur. And, corresponding to every element F_i of (1), there exists in $\mathfrak{F}$ one and only one element F_j such that

$$F_jF = F_i.$$

Therefore $\mathfrak{F}$ is a field [Congr., p. 205].

LEMMA 2. Let $\mathfrak{B}$ be an ideal of a proper ring $\mathfrak{R}$ which is contained in another ideal $\mathfrak{A}$. If the quotient $\mathfrak{A}/\mathfrak{B}$ is a field, $\mathfrak{B}$ is equal to the product of $\mathfrak{A}$ and an ideal prime to $\mathfrak{A}$.

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

Since the quotient $\mathfrak{R}/\mathfrak{B}$ is never a field,[1] there exist in $\mathfrak{R}$ at least two elements (say, called R_1 and R_2), such that their product is congruent (mod. $\mathfrak{B}$) to 0, while they are both incongruent (mod. $\mathfrak{B}$) to 0 [by lemma]. If it happen that one, say R_1, of the elements R_1, R_2 belongs to $\mathfrak{A}$, we take R_1 and denote it by S. Since $\mathfrak{A}/\mathfrak{B}$ is a field, R_2 does not belong to $\mathfrak{A}$. On the contrary if every product which we obtain by multiplying an element, not belonging to $\mathfrak{B}$, of $\mathfrak{A}$ by an element, not belonging to $\mathfrak{B}$, of $\mathfrak{R}$ is incongruent (mod. $\mathfrak{B}$) to 0, we take any one of R_1, R_2 and denote it by S. Then the elements X of $\mathfrak{R}$ which satisfy the condition

$$SX \equiv 0 \pmod{\mathfrak{B}}$$

form an ideal (say, called $\mathfrak{K}$) of $\mathfrak{R}$. $\mathfrak{K}$ necessarily contains all the elements of $\mathfrak{B}$ and also contains certain elements not belonging to $\mathfrak{A}$, while containing no element, not belonging to $\mathfrak{B}$, of $\mathfrak{A}$; because $\mathfrak{A}/\mathfrak{B}$ is assumed to be a field. Therefore the ideal $\mathfrak{K}$ is distinct from $\mathfrak{B}$ and contains $\mathfrak{B}$ for the cross-cut with $\mathfrak{A}$.

---

[1] Congr., § 9.

If $\mathfrak{K}$ is prime to $\mathfrak{A}$, our theorem has already been proved. On the contrary, if not, the process may be repeated with the ideals $(\mathfrak{A}, \mathfrak{K})$ and $\mathfrak{K}$ as follows:

Since the cross-cut of $\mathfrak{A}$ and $\mathfrak{K}$ is $\mathfrak{B}$, the quotient $(\mathfrak{A}, \mathfrak{K})/\mathfrak{K}$ is simply isomorphic with the quotient $\mathfrak{A}/\mathfrak{B}$ [Congr., § 11, Theorem] and consequently is a field. Therefore it can be proved similarly that there exists an ideal (say, called $\mathfrak{K}_1$) such that $\mathfrak{K}_1$ is distinct from $\mathfrak{K}$ and contains $\mathfrak{K}$ for the cross-cut with $(\mathfrak{A}, \mathfrak{K})$. But the cross-cut of $\mathfrak{K}_1$ and $(\mathfrak{A}, \mathfrak{K})$ is $\mathfrak{K}$, and that of $\mathfrak{K}$ and $\mathfrak{A}$ is $\mathfrak{B}$; hence the cross-cut of $\mathfrak{K}_1$ and $\mathfrak{A}$ is $\mathfrak{B}$. If, therefore, $\mathfrak{K}_1$ is prime to $(\mathfrak{A}, \mathfrak{K})$ and consequently to $\mathfrak{A}$, the theorem has already been proved. If $\mathfrak{K}_1$ is not yet prime to $(\mathfrak{A}, \mathfrak{K})$, the process may be repeated with the ideals $(\mathfrak{A}, \mathfrak{K}_1)$ and $\mathfrak{K}_1$, viz. there may be obtained an ideal $\mathfrak{K}_2$, distinct from $\mathfrak{K}_1$, such that the cross-cut of $\mathfrak{K}_2$ and $(\mathfrak{A}, \mathfrak{K}_1)$ is $\mathfrak{K}_1$, and consequently that of $\mathfrak{K}_2$ and $\mathfrak{A}$ is $\mathfrak{B}$; and so on. Then, since the norm of every ideal $(\neq 0)$ of $\mathfrak{R}$ is assumed to be finite, eventually we shall obtain an ideal (say, called $\mathfrak{M}$) which is prime to $\mathfrak{A}$ and contains $\mathfrak{B}$ as the cross-cut with $\mathfrak{A}$. And then $\mathfrak{B}=\mathfrak{A}\mathfrak{M}$ [by § 5, 1st theorem].

Returning to the subject in question, if $\mathfrak{A}_{n-1}/\mathfrak{A}_n$ is a field, by lemma 2 we have

$$\mathfrak{A}_n = \mathfrak{A}_{n-1}\mathfrak{M},$$

$\mathfrak{M}$ being an ideal prime to $\mathfrak{A}_{n-1}$, what is to be proved.

We now suppose that $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ is a field, but all of

$$\frac{\mathfrak{A}_{i+1}}{\mathfrak{A}_{i+2}}, \ \frac{\mathfrak{A}_{i+2}}{\mathfrak{A}_{i+3}}, \ \dots \ \frac{\mathfrak{A}_{n-1}}{\mathfrak{A}_n} \quad (i < n-1)$$

are not fields. Then the product of two elements of $\mathfrak{A}_{i+j}$ is contained in $\mathfrak{A}_{i+j+1}$ $(j \geqq 1)$ [*cf.* Congr., § 20].

First we prove that $\mathfrak{A}_{i+2}$ may be resolved into the product of two ideals prime to each other. Since $\mathfrak{A}_i/\mathfrak{A}_{i+1}$ is a field, by lemma 2 $\mathfrak{A}_{i+1}$ may be expressed as the product of $\mathfrak{A}_i$ and an ideal, say $\mathfrak{M}$, prime to $\mathfrak{A}_i$, viz.

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

where $(\mathfrak{A}_i, \mathfrak{M})=\mathfrak{R}$. But $\mathfrak{A}^2_{i+1}$ is contained in $\mathfrak{A}_{i+2}$. If $\mathfrak{A}_{i+2}=\mathfrak{A}^2_{i+1}=\mathfrak{A}^2_i\mathfrak{M}^2$, $\mathfrak{A}_{i+2}$ has already been resolved into two factors prime to each other; because from $(\mathfrak{A}_i, \mathfrak{M})=\mathfrak{R}$ follows $(\mathfrak{A}^2_i, \mathfrak{M}^2)=\mathfrak{R}$, none of $\mathfrak{A}^2_i$ and $\mathfrak{M}^2$ being $\mathfrak{R}$ [§ 4, theorem].

If not, a finite number of elements

$$P_1,\ P_2,\ \ldots,\ P_\mu$$

can be so chosen that

$$\mathfrak{A}_{i+2} = (\mathfrak{A}^2_{i+1},\ (P_1), (P_2),\ \ldots,\ (P_\mu)) = (\mathfrak{A}^2_i\mathfrak{M}^2,\ \mathfrak{C}),$$

where

$$\mathfrak{C} = ((P_1),\ (P_2),\ \ldots,\ (P_\mu))\,;$$

because, since the norm of every ideal ($\neq 0$) of $\mathfrak{R}$ is finite and $(\mathfrak{A}^2_i, \mathfrak{M}^2)=\mathfrak{R}$, neither of $\mathfrak{A}^2_i$, $\mathfrak{M}^2$ being the o-ideal, we have $n(\mathfrak{A}^2_{i+1})= n(\mathfrak{A}^2_i)\, n(\mathfrak{M}^2)$ [§ 5, Cor.], and hence the order of the quotient $\mathfrak{A}_{i+2}/\mathfrak{A}^2_{i+1}$ is, of course, finite. And, since $(\mathfrak{A}^2_i, \mathfrak{M}^2)=\mathfrak{R}$, we have

$$\mathfrak{A}_{i+2} = (\mathfrak{A}^2_i\mathfrak{M}^2, \mathfrak{C}) = (\mathfrak{A}^2_i, \mathfrak{C})(\mathfrak{M}^2, \mathfrak{C}) \quad \text{[by § 6, theorem].}$$

But since the ideal $\mathfrak{C}$ is contained in $\mathfrak{A}_{i+2}$, evidently it is contained in $\mathfrak{A}_i$ and $\mathfrak{M}$; hence the ideal $(\mathfrak{A}^2_i, \mathfrak{C})$ is contained in $\mathfrak{A}_i$, and the ideal $(\mathfrak{M}^2, \mathfrak{C})$ in $\mathfrak{M}$. Therefore $\mathfrak{A}_{i+2}$ can be resolved into factors prime to each other, none of which is $\mathfrak{R}$; and, if $i+2=n$, the theorem has been thereby proved.

If $i+2 < n$, put

$$(\mathfrak{A}^2_i, \mathfrak{C}) = \mathfrak{L}_1,$$
$$(\mathfrak{M}^2, \mathfrak{C}) = \mathfrak{M}_1.$$

But $\mathfrak{A}_{i+3}$ contains $\mathfrak{A}^2_{i+2}$, which is the product of the two ideals $\mathfrak{L}_1^2$ and $\mathfrak{M}_1^2$ prime to each other. If $\mathfrak{A}_{i+3}=\mathfrak{A}^2_{i+2}=\mathfrak{L}_1^2\mathfrak{M}_1^2$, $\mathfrak{A}_{i+3}$ is equal to the product of two ideals $\mathfrak{L}_1^2$ and $\mathfrak{M}_1^2$ which are prime to each other and none of which is $\mathfrak{R}$; because $(\mathfrak{L}_1, \mathfrak{M}_1)=\mathfrak{R}$, and $\mathfrak{L}_1$, $\mathfrak{M}_1$ are contained in $\mathfrak{A}_i$ and $\mathfrak{M}$ respectively. If not, in the same way as before we have

$$\mathfrak{A}_{i+3} = (\mathfrak{A}^2_{i+2}, \mathfrak{C}_1) = (\mathfrak{L}_1^2\mathfrak{M}_1^2, \mathfrak{C}_1)\,;$$

because the quotient $\mathfrak{A}_{i+3}/\mathfrak{A}^2_{i+2}$ is of finite order. And then

$$\mathfrak{A}_{i+3} = (\mathfrak{L}_1^2, \mathfrak{C}_1)(\mathfrak{M}_1^2, \mathfrak{C}_1).$$

Since $\mathfrak{C}_1$ is contained in $\mathfrak{A}_{i+3}$, evidently the ideals $(\mathfrak{L}_1^2, \mathfrak{C}_1)$ and $(\mathfrak{M}_1^2, \mathfrak{C}_1)$ are contained in $\mathfrak{L}_1$ and $\mathfrak{M}_1$ respectively. And, moreover, these are prime to each other; because $(\mathfrak{L}_1, \mathfrak{M}_1)=\mathfrak{R}$. Therefore $\mathfrak{A}_{i+3}$ can be resolved into factors which are prime to each other and none of which is $\mathfrak{R}$: so that, if $i+3=n$, the theorem has already been proved. If $i+3$ is not yet equal n, repeat the process, and eventually we shall reach the result which we require.

§ 17. The converse of the theorem also holds true, viz.

THEOREM: *If an ideal $\mathfrak{A}$ of a proper ring $\mathfrak{R}$ may be resolved into the product of two ideals prime to each other, the set of quotient rings derived from a chief-composition-series of $\mathfrak{R}$ with the last term $\mathfrak{A}$ contains at least one field besides the first quotient.*

For, suppose that

$$\mathfrak{A} = \mathfrak{L}\mathfrak{M}$$

where $\mathfrak{L}$ and $\mathfrak{M}$ are two ideals prime to each other. Let $\mathfrak{P}$ and $\mathfrak{Q}$ be maximal ideals of $\mathfrak{R}$, respectively containing $\mathfrak{L}$ and $\mathfrak{M}$. Then $\mathfrak{P}$ and $\mathfrak{Q}$ must be distinct; because otherwise the ideal $(\mathfrak{L}, \mathfrak{M})$ would be contained in $\mathfrak{P}$, contrary to the assumption $(\mathfrak{L}, \mathfrak{M})=\mathfrak{R}$. Since $n(\mathfrak{A})$ is finite and the product $\mathfrak{P}\mathfrak{Q}$, being the cross-cut of $\mathfrak{P}$ and $\mathfrak{Q}$, contains $\mathfrak{A}$, we can choose a chief-composition-series of $\mathfrak{R}$ containing $\mathfrak{P}$ and $\mathfrak{P}\mathfrak{Q}$, and having $\mathfrak{A}$ as the last term. Let

$$\mathfrak{R},\ \mathfrak{P},\ \mathfrak{P}\mathfrak{Q},\ \dots,\ \mathfrak{A}$$

be such one. Then the quotient $\mathfrak{P}/\mathfrak{P}\mathfrak{Q}$ is of the same type as $\mathfrak{R}/\mathfrak{Q}$ [Congr., § 11, Theorem], which is a field [§ 2].

§ 18. Let

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

be a chief-composition-series of a proper ring $\mathfrak{R}$. If none of the quotient rings

$$\frac{\mathfrak{A}_1}{\mathfrak{A}_2},\ \frac{\mathfrak{A}_2}{\mathfrak{A}_3},\ \dots,\ \frac{\mathfrak{A}_{n-1}}{\mathfrak{A}_n}$$

is a field, $\mathfrak{A}_n$ contains a power of the maximal ideal $\mathfrak{A}_1$. Conversely if $\mathfrak{A}_n$ contains a power of $\mathfrak{A}_1$ (say, $\mathfrak{A}_1^e$), none of the quotient rings is a field. For, if any one of the quotient rings were a field, $\mathfrak{A}_n$ would be resolvable into two factors prime to each other. Suppose that $\mathfrak{A}_n=\mathfrak{L}\mathfrak{M}$, where $(\mathfrak{L}, \mathfrak{M})=\mathfrak{R}$. Since $(\mathfrak{L}, \mathfrak{M})=\mathfrak{R}$, the maximal ideal $\mathfrak{A}_1$ would be prime to at least one of $\mathfrak{L}$ and $\mathfrak{M}$; suppose $(\mathfrak{A}_1, \mathfrak{L})=\mathfrak{R}$. Then $(\mathfrak{A}_1, \mathfrak{L})=\mathfrak{R}$ would involve $(\mathfrak{A}_1^e, \mathfrak{L})=\mathfrak{R}$ [§ 4], and consequently $(\mathfrak{A}_n, \mathfrak{L})=\mathfrak{R}$, while $\mathfrak{A}_n=\mathfrak{L}\mathfrak{M}$ would involve $(\mathfrak{A}_n, \mathfrak{L})=\mathfrak{L}$. Therefore $\mathfrak{A}_n$ can not be resolved into two factors prime to each other; hence none of the quotient rings is a field. Therefore the last two theorems, being summed up, may be rewritten as follows:

An ideal of a proper ring can or can not be resolved into two factors prime to each other, according as it does not or does contain a power of maximal ideal.

It is clear that no ideal can contain two powers of distinct maximal ideals; because powers of distinct maximal ideals are prime to each other; and also that no ideal containing a power of maximal ideal is contained in two distinct maximal ideals. [*cf.* § 4].

§ 19 THEOREM: *Every ideal which contains no power of maximal ideal may be expressed as the product of a finite number of ideals which contain powers of distinct maximal ideals respectively; and this can be done in only one way.*

Let $\mathfrak{A}$ be an ideal of a proper ring $\mathfrak{R}$, which contains no power of maximal ideal of $\mathfrak{R}$. Then by the last proposition $\mathfrak{A}$ can be resolved into two factors prime to each other. Suppose that $\mathfrak{A}=\mathfrak{L}\mathfrak{M}$, where $(\mathfrak{L}, \mathfrak{M})=\mathfrak{R}$. If both factors $\mathfrak{L}$ and $\mathfrak{M}$ contain powers of maximal ideals, these two maximal ideals must be distinct; because otherwise $\mathfrak{L}$ and $\mathfrak{M}$ would be contained in the same maximal ideal [§ 4, 2nd theorem], contrary to $(\mathfrak{L}, \mathfrak{M})=\mathfrak{R}$. And hence the resolution has already been effected. If not, the process may be repeated, viz. either $\mathfrak{L}$ or $\mathfrak{M}$ or both may be resolved into two factors prime to each other, and so on. It is clear that eventually no further resolution will be possible; because if $\mathfrak{A}$ could be resolved into the product of an infinite number of ideals prime to one another, none of which is $\mathfrak{R}$, the norm of $\mathfrak{A}$ would be infinitely great, contrary to our assumption [*cf.* § 5, 1st Cor.]. And $\mathfrak{A}$ is finally reduced to the form

$$\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2 \dots \mathfrak{A}_\nu,$$

where $\mathfrak{A}_1, \mathfrak{A}_2, \dots\dots, \mathfrak{A}_\nu$ are ideals respectively containing powers of distinct maximal ideals.

Next a maximal ideal containing $\mathfrak{A}$ must contain one of $\mathfrak{A}_1, \mathfrak{A}_2, \dots\dots, \mathfrak{A}_\nu$. For, let $\mathfrak{P}$ be a maximal ideal containing $\mathfrak{A}$. If $\mathfrak{P}$ contained none of $\mathfrak{A}_1, \mathfrak{A}_2, \dots\dots, \mathfrak{A}_\nu$, it would be prime to all of them and consequently to their product $\mathfrak{A}_1 \mathfrak{A}_2 \dots\dots \mathfrak{A}_\nu=\mathfrak{A}$ [§ 4], contrary to the assumption that $\mathfrak{P}$ contains $\mathfrak{A}$. Therefore $\mathfrak{P}$ must contain one of $\mathfrak{A}_1, \mathfrak{A}_2, \dots\dots, \mathfrak{A}_\nu$.

So that if two resolutions are possible, the maximal ideals, each of which contains one of the factors, are the same in both. And hence the only admissible supposition is

$$\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2 \dots \mathfrak{A}_\nu = \mathfrak{A}_1' \mathfrak{A}_2' \dots \mathfrak{A}_\nu',$$

where $\mathfrak{A}_i$ and $\mathfrak{A}_i'$ are ideals containing powers of the same maximal ideal $\mathfrak{P}_i$, $(i=1, 2, \ldots\ldots, \nu)$. Since $\mathfrak{A}_1'$ contains a power of $\mathfrak{P}_1$, it is prime to all of $\mathfrak{A}_2, \mathfrak{A}_3 \ldots\ldots, \mathfrak{A}_\nu$ and consequently to their product [§ 4]; similarly $\mathfrak{A}_1$ is prime to the product $\mathfrak{A}_2' \mathfrak{A}_3' \ldots\ldots \mathfrak{A}_\nu'$. Therefore

$$(\mathfrak{A}_1\mathfrak{A}_1', \mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_\nu) = \mathfrak{A}_1(\mathfrak{A}_1', \mathfrak{A}_2\mathfrak{A}_3\ldots\mathfrak{A}_\nu) = \mathfrak{A}_1,$$
$$(\mathfrak{A}_1'\mathfrak{A}_1, \mathfrak{A}_1'\mathfrak{A}_2'\ldots\mathfrak{A}_\nu') = \mathfrak{A}_1'(\mathfrak{A}_1, \mathfrak{A}_2'\mathfrak{A}_3'\ldots\mathfrak{A}_\nu') = \mathfrak{A}_1',$$

while $\mathfrak{A}_1\mathfrak{A}_2 \ldots\ldots \mathfrak{A}_\nu = \mathfrak{A}_1'\mathfrak{A}_2' \ldots\ldots \mathfrak{A}_\nu'$. So that $\mathfrak{A}_1 = \mathfrak{A}_1'$. Taking $\mathfrak{A}_i$ for $\mathfrak{A}_1$, similarly we can prove $\mathfrak{A}_i = \mathfrak{A}_i'$: so that the two resolutions are identical.

§ 20. Let $\mathfrak{P}_1, \mathfrak{P}_2, \ldots\ldots, \mathfrak{P}_\nu$ be the distinct maximal ideals of a proper ring $\mathfrak{R}$ which contain a given ideal $\mathfrak{A}$ of $\mathfrak{R}$. Then $\mathfrak{A}$ can be resolved into factors as follows:

$$\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_\nu,$$

where $\mathfrak{A}_1, \mathfrak{A}_2, \ldots\ldots, \mathfrak{A}_\nu$ are ideals containing powers of $\mathfrak{P}_1, \mathfrak{P}_2, \ldots\ldots, \mathfrak{P}_\nu$ respectively.

Now take a chief-composition-series of $\mathfrak{R}$

$$\mathfrak{R}, \mathfrak{P}_i, \mathfrak{P}_{i1}, \mathfrak{P}_{i2}, \ldots, \mathfrak{A}_i$$

having $\mathfrak{A}_i$ for the last term, and the quotient $\mathfrak{R}/\mathfrak{P}_i$ is a field, but the others $\mathfrak{P}_i/\mathfrak{P}_{i1}, \mathfrak{P}_{i1}/\mathfrak{P}_{i2}, \ldots\ldots$ are not fields, viz. $\mathfrak{P}^2_i, \mathfrak{P}^2_{i1}, \ldots\ldots$ are contained in $\mathfrak{P}_{i1}, \mathfrak{P}_{i2}, \ldots\ldots$ respectively [§ 18]. Multiplying each term of the series by the product $\mathfrak{A}_1\mathfrak{A}_2 \ldots\ldots \mathfrak{A}_{i-1}$ we have the series of ideals

$$\mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{i-1}, \quad \mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{i-1}\mathfrak{P}_i, \quad \mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{i-1}\mathfrak{P}_{i1}, \quad \mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{i-1}\mathfrak{P}_{i2},$$
$$\ldots, \mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_{i-1}\mathfrak{A}_i.$$

The quotient $\mathfrak{A}_1\mathfrak{A}_2 \ldots\ldots \mathfrak{A}_{i-1}/\mathfrak{A}_1\mathfrak{A}_2 \ldots\ldots \mathfrak{A}_{i-1}\mathfrak{P}_i$ is a field; because it follows from $(\mathfrak{A}_1\mathfrak{A}_2 \ldots\ldots \mathfrak{A}_{i-1}, \mathfrak{P}_i) = \mathfrak{R}$ [by Congr., § 11, theorem]. But $(\mathfrak{A}_1\mathfrak{A}_2 \ldots\ldots \mathfrak{A}_{i-1}\mathfrak{P}_i)^2$, $(\mathfrak{A}_1\mathfrak{A}_2 \ldots\ldots \mathfrak{A}_{i-1}\mathfrak{P}_{i1})^2$, …… evidently are contained in $\mathfrak{A}_1\mathfrak{A}_2 \ldots\ldots \mathfrak{A}_{i-1}\mathfrak{P}_{i1}$, $\mathfrak{A}_1\mathfrak{A}_2 \ldots\ldots \mathfrak{A}_{i-1}\mathfrak{P}_{i2}$, …… respectively.

Therefore if we take a chief-composition-series[1] of $\mathfrak{R}$ such that it contains the ideals

$$\mathfrak{P}_1, \quad \mathfrak{P}_{11}, \quad \mathfrak{P}_{12}, \ldots, \mathfrak{A}_1,$$
$$\mathfrak{A}_1\mathfrak{P}_2, \quad \mathfrak{A}_1\mathfrak{P}_{21}, \quad \mathfrak{A}_1\mathfrak{P}_{22}, \ldots, \mathfrak{A}_1\mathfrak{A}_2,$$
$$\mathfrak{A}_1\mathfrak{A}_2\mathfrak{P}_3, \quad \mathfrak{A}_1\mathfrak{A}_2\mathfrak{P}_{31}, \quad \mathfrak{A}_1\mathfrak{A}_2\mathfrak{P}_{32}, \ldots, \mathfrak{A}_1\mathfrak{A}_2\mathfrak{A}_3,$$

1 Such a series evidently exists.

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$

$$\mathfrak{A}_1 \ldots \mathfrak{A}_{\nu-1}\mathfrak{P}_\nu,\quad \mathfrak{A}_1 \ldots \mathfrak{A}_{\nu-1}\mathfrak{P}_{\nu 1},\quad \mathfrak{A}_1 \ldots \mathfrak{A}_{\nu-1}\mathfrak{P}_{\nu 2}, \ldots, \mathfrak{A}_1 \ldots \mathfrak{A}_{\nu-1}\mathfrak{A}_\nu,$$

and has $\mathfrak{A}$ for the last term, then the set of quotient rings derived from it contains just ν fields

$$\mathfrak{R}/\mathfrak{P}_1,\quad \mathfrak{A}_1/\mathfrak{A}_1\mathfrak{P}_2,\quad \mathfrak{A}_1\mathfrak{A}_2/\mathfrak{A}_1\mathfrak{A}_2\mathfrak{P}_3, \ldots,$$
$$(\mathfrak{A}_1 \ldots \mathfrak{A}_{\nu-1})/(\mathfrak{A}_1 \ldots \mathfrak{A}_{\nu-1}\mathfrak{P}_\nu).$$

But two chief-composition-series with the same last term lead to two sets of quotient rings which are identical [Congr., § 13, theorem]. Therefore we have the

THEOREM: *The number of the maximal ideals of a proper ring $\mathfrak{R}$ which contain a given ideal $\mathfrak{A}$ of $\mathfrak{R}$ is equal to the number of the fields which are contained in the set of quotient rings derived from a chief-composition-series of $\mathfrak{R}$ with the last term $\mathfrak{A}$.*

Φ-Function: Fermat's Theorem.

§ 21. The function $\Phi(\mathfrak{A})$. Let $\mathfrak{A}$ be an ideal of a proper ring $\mathfrak{R}$, and

$$R_1, R_2, \ldots, R_\lambda$$

a complete set of incongruent (mod. $\mathfrak{A}$) elements of $\mathfrak{R}$. The number of the elements of the set which are prime[1] to $\mathfrak{A}$ is denoted by the symbol[2] $\Phi(\mathfrak{A})$ as a number dependent on $\mathfrak{A}$; and let $\Phi(\mathfrak{A})=1$ for $\mathfrak{A}=\mathfrak{R}$.

1.° First to determine the Φ-function of an ideal containing a power of maximal ideal, we suppose that $\mathfrak{A}$ is an ideal of a proper ring $\mathfrak{R}$ which contains a power of a maximal ideal $\mathfrak{P}$. Then $\mathfrak{P}$ contains $\mathfrak{A}$, and an element of $\mathfrak{R}$ which does not belong to $\mathfrak{P}$ is prime to $\mathfrak{A}$. [§ 4]. Now let

$$(1)\qquad \rho_1, \rho_2, \ldots, \rho_n \qquad (n=n(\mathfrak{P}))$$

be a complete set of incongruent (mod. $\mathfrak{P}$) elements of $\mathfrak{R}$, and

$$(2)\qquad \pi_1, \pi_2, \ldots, \pi_m$$

a complete set of incongruent (mod. $\mathfrak{A}$) elements of $\mathfrak{P}$. Then the nm elements

[1] The phrase that an element R is prime to $\mathfrak{A}$ is used to denote that the principal ideal (R) is prime to $\mathfrak{A}$.

[2] As in the case of ideals in algebraic number-fields.

(3) $$\rho_i+\pi_j \qquad (i=1, 2, \ldots, n; \; j=1, 2, \ldots, m)$$

evidently form a complete set of incongruent (mod. $\mathfrak{A}$) elements of $\mathfrak{R}$, and the number of the elements of (3) which do not belong to $\mathfrak{P}$ is $\Phi(\mathfrak{A})$

But if $\rho_i\equiv 0$ (mod. $\mathfrak{P}$), $\rho_i+\pi_j\equiv 0$ (mod. $\mathfrak{P}$) for every $j=1, 2, \ldots\ldots, m$; conversely if $\rho_i+\pi_j\equiv 0$ (mod. $\mathfrak{P}$), $\rho_i\equiv 0$ (mod. $\mathfrak{P}$). And there exists in (1) just one element which belongs to $\mathfrak{P}$. Therefore the number of the elements of (3) which do not belong to $\mathfrak{P}$ is

$$nm-m = nm\left(1-\frac{1}{n}\right) = n(\mathfrak{A})\left(1-\frac{1}{n(\mathfrak{P})}\right).$$

And hence we have

$$\Phi(\mathfrak{A}) = n(\mathfrak{A})\left(1-\frac{1}{n(\mathfrak{P})}\right).$$

2.° Next suppose that two ideals $\mathfrak{A}$ and $\mathfrak{B}$ are prime to each other. Then the cross-cut of $\mathfrak{A}$ and $\mathfrak{B}$ is equal to the product $\mathfrak{A}\mathfrak{B}$ [§ 5, 1st theorem], and

$$n(\mathfrak{A}\mathfrak{B}) = n(\mathfrak{A})\cdot n(\mathfrak{B}) \qquad \text{[§ 5, Cor.]}.$$

Let

(4) $$\alpha_1, \alpha_2, \ldots, \alpha_\mu,$$

(5) $$\beta_1, \beta_2, \ldots, \beta_\nu$$

be complete sets of incongruent (mod. $\mathfrak{A}\mathfrak{B}$) elements of $\mathfrak{A}$ and $\mathfrak{B}$ respectively. Then, as shown in Congr., § 11, the elements of (4) being considered for elements of $(\mathfrak{A}, \mathfrak{B})=\mathfrak{R}$ and being taken modulo $\mathfrak{B}$ form a complete set of incongruent (mod. $\mathfrak{B}$) elements of $\mathfrak{R}$. And hence the number of the elements of (4) which are prime to $\mathfrak{B}$ is $\Phi(\mathfrak{B})$. Similarly the number of the elements of (5) which are prime to $\mathfrak{A}$ is $\Phi(\mathfrak{A})$.

Since $(\mathfrak{A}, \mathfrak{B})=\mathfrak{R}$, an element of $\mathfrak{R}$ is expressed in the form $A+B$, where A and B are elements of $\mathfrak{A}$ and $\mathfrak{B}$ respectively, while A and B are given by the forms α_i+D' and β_j+D'' respectively where D', D'' denote elements of $\mathfrak{A}\mathfrak{B}$. Therefore every element of $\mathfrak{R}$ is expressed in the form $\alpha_i+\beta_j+D$, where D is an element of $\mathfrak{A}\mathfrak{B}$. But two sums $\alpha_i+\beta_j$ and $\alpha_s+\beta_t$ are congruent (mod. $\mathfrak{A}\mathfrak{B}$) when, and only when, $\alpha_i\equiv\alpha_s$ and $\beta_j\equiv\beta_t$ (mod. $\mathfrak{A}\mathfrak{B}$) simultaneously. Therefore the $\mu\nu$ sums

(6) $$\alpha_i+\beta_j \qquad (i=1, 1, \ldots, \mu; \; j=1, 2, \ldots, \nu)$$

form a complete set of incongruent (mod. $\mathfrak{A}\mathfrak{B}$) elements of $\mathfrak{R}$.

But by § 6, Cor. we have

$$((\alpha_i+\beta_j), \mathfrak{A}\mathfrak{B}) = ((\alpha_i+\beta_j), \mathfrak{A})\,((\alpha_i+\beta_j), \mathfrak{B})$$
$$= ((\beta_j), \mathfrak{A})\,((\alpha_i), \mathfrak{B}).$$

Therefore $\alpha_i+\beta_j$ is prime to $\mathfrak{A}\mathfrak{B}$ when, and only when,

$$((\beta_j), \mathfrak{A}) = \mathfrak{R}$$

and

$$((\alpha_i), \mathfrak{B}) = \mathfrak{R}$$

simultaneously. The number of the elements of (5) which are prime to $\mathfrak{A}$ is $\Phi(\mathfrak{A})$, and that of those of (4) which are prime to $\mathfrak{B}$ is $\Phi(\mathfrak{B})$, as shown above. Hence the number of the elements of (6) which are prime to $\mathfrak{A}\mathfrak{B}$ is equal to $\Phi(\mathfrak{A})\cdot\Phi(\mathfrak{B})$; so that

$$\Phi(\mathfrak{A}\mathfrak{B}) = \Phi(\mathfrak{A})\cdot\Phi(\mathfrak{B}),$$

if $(\mathfrak{A}, \mathfrak{B})=\mathfrak{R}$.

3°. Lastly let $\mathfrak{A}$ be an ideal of $\mathfrak{R}$, and let $\mathfrak{P}_1, \mathfrak{P}_2, \ldots\ldots, \mathfrak{P}_\nu$ be the different maximal ideals of $\mathfrak{R}$ which contain $\mathfrak{A}$. Then, as shown in § 19, $\mathfrak{A}$ may be resolved into the product of ideals prime to one another as follows:

$$\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2\ldots\mathfrak{A}_\nu,$$

where $\mathfrak{A}_1, \mathfrak{A}_2, \ldots\ldots, \mathfrak{A}_\nu$ are ideals containing powers of $\mathfrak{P}_1, \mathfrak{P}_2, \ldots\ldots, \mathfrak{P}_\nu$ respectively. Since the factors are prime to one another, from 1° and 2° we have

$$\Phi(\mathfrak{A}) = \Phi(\mathfrak{A}_1)\,\Phi(\mathfrak{A}_2)\ldots\Phi(\mathfrak{A}_\nu)$$
$$= n(\mathfrak{A}_1)\left(1-\frac{1}{n(\mathfrak{P}_1)}\right)n(\mathfrak{A}_2)\left(1-\frac{1}{n(\mathfrak{P}_2)}\right)\ldots n(\mathfrak{A}_\nu)\left(1-\frac{1}{n(\mathfrak{P}_\nu)}\right)$$
$$= n(\mathfrak{A})\left(1-\frac{1}{n(\mathfrak{P}_1)}\right)\left(1-\frac{1}{n(\mathfrak{P}_2)}\right)\ldots\left(1-\frac{1}{n(\mathfrak{P}_\nu)}\right),$$

since $n(\mathfrak{A}) = n(\mathfrak{A}_1)\,n(\mathfrak{A}_2)\ldots n(\mathfrak{A}_\nu)$ [§ 5, Cor.].

Thus we have the formula:

$$\Phi(\mathfrak{A}) = n(\mathfrak{A})\left(1-\frac{1}{n(\mathfrak{P}_1)}\right)\left(1-\frac{1}{n(\mathfrak{P}_2)}\right)\ldots\left(1-\frac{1}{n(\mathfrak{P}_\nu)}\right),$$

where $\mathfrak{P}_1, \mathfrak{P}_2, \ldots\ldots, \mathfrak{P}_\nu$ are all the different maximal ideals which contain $\mathfrak{A}$.

§ 22. Fermat's theorem. *Let $\mathfrak{A}$ be an ideal of a proper ring $\mathfrak{R}$, and ρ any element of $\mathfrak{R}$ which is prime to $\mathfrak{A}$, then the congruence*

$$\rho^{\Phi(\mathfrak{A})} \equiv 1 \qquad (\text{mod. } \mathfrak{A})$$

holds good.

Lemma. If an element ρ of $\mathfrak{R}$ is prime to $\mathfrak{A}$, then every element X of $\mathfrak{R}$ for which

$$\rho X \equiv 0 \qquad (\text{mod. } \mathfrak{A})$$

is congruent (mod. $\mathfrak{A}$) to 0.

For, if $\rho X = A$, A being an element of $\mathfrak{A}$, we have

$$((\rho X), X\mathfrak{A}) = ((A), X\mathfrak{A}),$$

while

$$((\rho X), X\mathfrak{A}) = X((\rho), \mathfrak{A}) = X\mathfrak{R} = (X),$$

and evidently $((A), X\mathfrak{A})$ is contained in $\mathfrak{A}$. Therefore (X) is contained in $\mathfrak{A}$.

Reterning to the theorem let

(1) $$\rho_1, \rho_2, \ldots, \rho_\mu \qquad (\mu = \Phi(\mathfrak{A}))$$

be a set of the incongruent (mod. $\mathfrak{A}$) elements of $\mathfrak{R}$ which are prime to $\mathfrak{A}$, and ρ an element of (1). Then the μ products

(2) $$\rho\rho_1, \rho\rho_2, \ldots, \rho\rho_\mu$$

are incongruent (mod. $\mathfrak{A}$) to one another; because $\rho\rho_i \equiv \rho\rho_j$ (mod. $\mathfrak{A}$) would involve $\rho_i \equiv \rho_j$ (mod. $\mathfrak{A}$) [by lemma]. Moreover they are all prime to $\mathfrak{A}$ [*cf.* § 4]. Therefore set (2), each term being taken modulo $\mathfrak{A}$, is identical with (1) except as regards the sequence. So that

$$\rho_1\rho_2 \ldots \rho_\mu\rho^\mu \equiv \rho_1\rho_2 \ldots \rho_\mu \qquad (\text{mod. } \mathfrak{A}),$$

or

$$\rho_1\rho_2 \ldots \rho_\mu(\rho^\mu - 1) \equiv 0 \qquad (\text{mod. } \mathfrak{A}).$$

Whence it follows by lemma that

$$\rho^\mu - 1 \equiv 0 \qquad (\text{mod. } \mathfrak{A}),$$

since $\rho_1, \rho_2, \ldots\ldots, \rho_\mu$ and consequently their product are prime to $\mathfrak{A}$.

Divisibity of Ideals.

§ 23. Let $\mathfrak{A}$ and $\mathfrak{B}$ be two ideals of a proper ring $\mathfrak{R}$; let $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_\nu$ be the distinct maximal ideals of $\mathfrak{R}$ which contain $\mathfrak{A}$, and $\mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_\mu$ those which contain $\mathfrak{B}$. And suppose that

$$\mathfrak{P}_1 = \mathfrak{Q}_1, \ \mathfrak{P}_2 = \mathfrak{Q}_2, \ \ldots, \ \mathfrak{P}_\lambda = \mathfrak{Q}_\lambda \qquad (\lambda \leqq \nu, \mu),$$

but that no others are equal, viz. that the λ ideals $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_\lambda$ are the maximal ideals which contain both $\mathfrak{A}$ and $\mathfrak{B}$. Then $\mathfrak{A}$ and $\mathfrak{B}$ may be expressed in the forms

$$\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_\nu,$$
$$\mathfrak{B} = \mathfrak{B}_1\mathfrak{B}_2 \ldots \mathfrak{B}_\mu,$$

where $\mathfrak{A}_1, \ldots, \mathfrak{A}_\nu, \mathfrak{B}_1, \ldots, \mathfrak{B}_\mu$ are ideals which contain powers of $\mathfrak{P}_1, \ldots, \mathfrak{P}_\nu, \mathfrak{Q}_1, \ldots, \mathfrak{Q}_\mu$ respectively. Again they may be rewritten as follows:

$$\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_\lambda\mathfrak{A}'$$
$$\mathfrak{B} = \mathfrak{B}_1\mathfrak{B}_2 \ldots \mathfrak{B}_\lambda\mathfrak{B}',$$

where

$$\mathfrak{A}' = \mathfrak{R} \quad \text{or} \quad \mathfrak{A}_{\lambda+1}\mathfrak{A}_{\lambda+2} \ldots \mathfrak{A}_\lambda$$

according as $\lambda = \nu$ or $< \nu$,

and $\mathfrak{B}' = \mathfrak{R}$ or $\mathfrak{B}_{\lambda+1}\mathfrak{B}_{\lambda+2} \ldots \mathfrak{B}_\mu$

according as $\lambda = \mu$ or $< \mu$. Then evidently

$$(\mathfrak{A}, \mathfrak{B}') = \mathfrak{R},$$

and

$$(\mathfrak{A}', \mathfrak{B}_1\mathfrak{B}_2 \ldots \mathfrak{B}_\lambda) = \mathfrak{R}.$$

By successive use of § 6, theorem we have

$$\begin{aligned}
(\mathfrak{A}, \mathfrak{B}) &= (\mathfrak{A}, \mathfrak{B}_1\mathfrak{B}_2 \ldots \mathfrak{B}_\lambda\mathfrak{B}') \\
&= (\mathfrak{A}, \mathfrak{B}_1\mathfrak{B}_2 \ldots \mathfrak{B}_\lambda)(\mathfrak{A}, \mathfrak{B}') \\
&= (\mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_\lambda\mathfrak{A}', \mathfrak{B}_1\mathfrak{B}_2 \ldots \mathfrak{B}_\lambda) \\
&= (\mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_\lambda, \mathfrak{B}_1\mathfrak{B}_2 \ldots \mathfrak{B}_\lambda)(\mathfrak{A}', \mathfrak{B}_1\mathfrak{B}_2 \ldots \mathfrak{B}_\lambda) \\
&= (\mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_\lambda, \mathfrak{B}_1\mathfrak{B}_2 \ldots \mathfrak{B}_\lambda) \\
&= (\mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_\lambda, \mathfrak{B}_1)(\mathfrak{A}_1\mathfrak{A}_2 \ldots \mathfrak{A}_\lambda, \mathfrak{B}_2\mathfrak{B}_3 \ldots \mathfrak{B}_\lambda) \\
&= (\mathfrak{A}_1, \mathfrak{B}_1)(\mathfrak{A}_2\mathfrak{A}_3 \ldots \mathfrak{A}_\lambda, \mathfrak{B}_1)(\mathfrak{A}_1, \mathfrak{B}_2\mathfrak{B}_3 \ldots \mathfrak{B}_\lambda)(\mathfrak{A}_2\mathfrak{A}_3 \ldots \mathfrak{A}_\lambda, \mathfrak{B}_2\mathfrak{B}_3 \ldots \mathfrak{B}_\lambda) \\
&= (\mathfrak{A}_1, \mathfrak{B}_1)(\mathfrak{A}_2\mathfrak{A}_3 \ldots \mathfrak{A}_\lambda, \mathfrak{B}_2\mathfrak{B}_3 \ldots \mathfrak{B}_\lambda).
\end{aligned}$$

Similarly

$$\begin{aligned}
&(\mathfrak{A}_2\mathfrak{A}_3 \ldots \mathfrak{A}_\lambda, \mathfrak{B}_2\mathfrak{B}_3 \ldots \mathfrak{B}_\lambda) \\
&= (\mathfrak{A}_2, \mathfrak{B}_2)(\mathfrak{A}_3 \ldots \mathfrak{A}_\lambda, \mathfrak{B}_3 \ldots \mathfrak{B}_\lambda);
\end{aligned}$$

and so on. Finally we have the

THEOREM:

$$(\mathfrak{A}, \mathfrak{B}) = (\mathfrak{A}_1, \mathfrak{B}_1)(\mathfrak{A}_2, \mathfrak{B}_2) \ldots (\mathfrak{A}_\lambda, \mathfrak{B}_\lambda).$$

§ 24. We now suppose that $\mathfrak{A}$ contains $\mathfrak{B}$. Then $\lambda = \nu \leqq \mu$, and

$$\mathfrak{A} = (\mathfrak{A}, \mathfrak{B}) = (\mathfrak{A}_1, \mathfrak{B}_1)(\mathfrak{A}_2, \mathfrak{B}_2) \dots (\mathfrak{A}_\nu, \mathfrak{B}_\nu),$$

while $$\mathfrak{A} = \mathfrak{A}_1\mathfrak{A}_2 \dots \mathfrak{A}_\nu.$$

Therefore by § 19, theorem we have

$$(\mathfrak{A}_1, \mathfrak{B}_1) = \mathfrak{A}_1; \ (\mathfrak{A}_2, \mathfrak{B}_2) = \mathfrak{A}_2; \dots;$$
$$(\mathfrak{A}_\nu, \mathfrak{B}_\nu) = \mathfrak{A}_\nu.$$

Namely $\mathfrak{A}_1, \mathfrak{A}_2, \dots, \mathfrak{A}_\nu$ contain $\mathfrak{B}_1, \mathfrak{B}_2, \dots, \mathfrak{B}_\nu$ respectively.

If moreover $n(\mathfrak{P}_i^2)=[n(\mathfrak{P}_i)]^2$, the ideals $\mathfrak{A}_i$ and $\mathfrak{B}_i$ are powers of $\mathfrak{P}_i$ [§ 10. Cor.], while $\mathfrak{A}_i$ contains $\mathfrak{B}_i$. And hence $\mathfrak{A}_i$ divides $\mathfrak{B}_i$. Therefore we have the

THEOREM: *Let $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_\nu$ be the maximal ideals of a proper ring $\mathfrak{R}$ which contain a given ideal $\mathfrak{A}$ of $\mathfrak{R}$.* If

$$n(\mathfrak{P}_i^2) = [n(\mathfrak{P}_i)]^2$$

for each $i=1, 2, \dots \nu$, $\mathfrak{A}$ divides every ideal of $\mathfrak{R}$ which is contained in $\mathfrak{A}$.

Cor. 1. A maximal ideal $\mathfrak{P}$ of a proper ring $\mathfrak{R}$, for which $n(\mathfrak{P}^2)=[n(\mathfrak{P})]^2$, divides every ideal of $\mathfrak{R}$ which is contained in $\mathfrak{P}$,

In other words, if an ideal $\mathfrak{A}$ of $\mathfrak{R}$ is not divisible by a maximal ideal $\mathfrak{P}$, for which $n(\mathfrak{P}^2)=[n(\mathfrak{P})]^2$, $\mathfrak{A}$ is prime to $\mathfrak{P}$, i.e, $(\mathfrak{A}, \mathfrak{P})=\mathfrak{R}$.

Cor. 2. Under the same assumption for $\mathfrak{P}$ as in Cor. 1, if an ideal $\mathfrak{A}$ is contained in $\mathfrak{P}^e$ but not in $\mathfrak{P}^{e+1}$, then

$$\mathfrak{A} = \mathfrak{P}^e \quad \text{or} \quad \mathfrak{P}^e\mathfrak{M},$$

where $$(\mathfrak{M}, \mathfrak{P}) = \mathfrak{R}.$$

For, $\mathfrak{P}$ is the only maximal ideal containing $\mathfrak{P}^e$, and hence $\mathfrak{P}^e$ divides $\mathfrak{A}$ which is contained in it [by the theorem]: so that $\mathfrak{A}=\mathfrak{P}^e\mathfrak{M}$, If $\mathfrak{M}\neq\mathfrak{R}$, $(\mathfrak{M}, \mathfrak{P})$ must$=\mathfrak{R}$; because otherwise $\mathfrak{M}$ would be divisible by $\mathfrak{P}$ [by Cor, 1], and consequently $\mathfrak{A}$ would be divisible by $\mathfrak{P}^{e+1}$, contrary to the assumption that $\mathfrak{A}$ is not contained in $\mathfrak{P}^{e+1}$.

Cor. 3. Under the same assumption for $\mathfrak{P}$, if the product of two ideals is divisible by $\mathfrak{P}$, at least one of the factors is divisible by $\mathfrak{P}$.

For, if $\mathfrak{A}\mathfrak{B} = \mathfrak{P}\mathfrak{Q}$, then evidently

$$\mathfrak{A}(\mathfrak{B}, \mathfrak{P}) = \mathfrak{P}(\mathfrak{Q}, \mathfrak{A}).$$

Hence, if $\mathfrak{B}$ is not divisible by $\mathfrak{P}$, $(\mathfrak{B}, \mathfrak{P})=\mathfrak{R}$ [by Cor. 1], and consequently

$$\mathfrak{A} = \mathfrak{P}(\mathfrak{O}, \mathfrak{A}),$$

which shows that $\mathfrak{A}$ is divisible by $\mathfrak{P}$.

§ 25. Consider a proper ring $\mathfrak{R}$ of which every maximal ideal $\mathfrak{P}$ is subject to the condition

$$n(\mathfrak{P}^2) = [n(\mathfrak{P})]^2.$$

In $\mathfrak{R}$ an ideal divides all ideals which are contained in it [by the last theorem]. The ideal $(\mathfrak{A}, \mathfrak{B})$ derived from two ideals $\mathfrak{A}$ and $\mathfrak{B}$ divides both $\mathfrak{A}$ and $\mathfrak{B}$, while being divisible by each of the ideals which contain both $\mathfrak{A}$ and $\mathfrak{B}$: so that $(\mathfrak{A}, \mathfrak{B})$ is a common divisor of $\mathfrak{A}$ and $\mathfrak{B}$, while being divisible by any other common divisor.

Also the cross-cut $\mathfrak{D}$ of $\mathfrak{A}$ and $\mathfrak{B}$ is a common multiple of $\mathfrak{A}$ and $\mathfrak{B}$, while dividing any other common multiple of $\mathfrak{A}$ and $\mathfrak{B}$.

Moreover between $(\mathfrak{A}, \mathfrak{B})$ and $\mathfrak{D}$ the relation

$$(\mathfrak{A}, \mathfrak{B})\,\mathfrak{D} = \mathfrak{A}\mathfrak{B}$$

holds good.

For, put

$$\mathfrak{A} = (\mathfrak{A}, \mathfrak{B})\,\mathfrak{A}', \qquad \mathfrak{B} = (\mathfrak{A}, \mathfrak{B})\,\mathfrak{B}'.$$

Then

$$(\mathfrak{A}, \mathfrak{B})\,\mathfrak{A}'\,\mathfrak{B}' = \mathfrak{A}\mathfrak{B}' = \mathfrak{A}'\,\mathfrak{B},$$

and hence $(\mathfrak{A}, \mathfrak{B})\,\mathfrak{A}'\,\mathfrak{B}'$ is contained in both $\mathfrak{A}$ and $\mathfrak{B}$, and consequently in $\mathfrak{D}$. Therefore the product $\mathfrak{A}\mathfrak{B} = (\mathfrak{A}, \mathfrak{B})^2\mathfrak{A}'\,\mathfrak{B}'$ is contained in $(\mathfrak{A}, \mathfrak{B})\,\mathfrak{D}$, while containing $(\mathfrak{A}, \mathfrak{B})\,\mathfrak{D}$: so that $\mathfrak{A}\mathfrak{B} = (\mathfrak{A}, \mathfrak{B})\,\mathfrak{D}$.

Composite and Prime Ideals.

Condition for the Unique Resolvability[1] of an Ideal into Prime Factors.

§ 26. Every ideal $\mathfrak{A}$ of a proper ring $\mathfrak{R}$, which is different from $\mathfrak{R}$, has at least two distinct divisors, namely $\mathfrak{R}$ and $\mathfrak{A}$. If it has no other divisors distinct from these, it is called a *prime* ideal: if otherwise, it is said to be *composite*.

Let $\mathfrak{P}$ be a maximal ideal of a proper ring $\mathfrak{R}$. Then there are four cases to consider.

---

[1] If an ideal can be expressed as the product of a finite number of prime ideals, and moreover if this can be done in only one way, the ideal is said to be *uniquely resolvable* into prime factors.

Convention: When $\mathfrak{P}^a = \mathfrak{P}^{a+1}$, $\mathfrak{P}$ being a prime ideal, the ideal $\mathfrak{P}^a$ is considered as not uniquely resolvable, even if divisible by no other prime ideal than $\mathfrak{P}$.

(1) Suppose that $\mathfrak{P}^2 = \mathfrak{P}$. Then $\mathfrak{P}$ apparently seems composite, but here *is considered as prime*, because having no other divisors distinct from $\mathfrak{R}$ and $\mathfrak{P}$. And evidently *it divides each ideal of* $\mathfrak{R}$ *which is contained in it.* For, if an ideal $\mathfrak{A}$ is contained in $\mathfrak{P}$, $\mathfrak{A}$ is divisible by an ideal containing a power of $\mathfrak{P}$ [§ 19]. But, since $\mathfrak{P}^2=\mathfrak{P}$, the latter coincides with $\mathfrak{P}$. Therefore $\mathfrak{A}$ is divisible by $\mathfrak{P}$.

(2) The case in which $\mathfrak{P}^2 =$ the o-ideal.

In this case all ideals are contained in $\mathfrak{P}$ [§ 4, 2nd theorem], and the product of any two of them is the o-ideal. Hence *the ideals, except the o-ideal, are all prime.*

(3) Suppose that $\mathfrak{P}^2 \neq 0$, and that there are ideals of $\mathfrak{R}$, distinct from $\mathfrak{P}$ and $\mathfrak{P}^2$, which contain $\mathfrak{P}^2$, viz. that $n(\mathfrak{P}^2) > [n(\mathfrak{P})]^2$ [*cf.* § 8].

Take an ideal $\mathfrak{A}$ of $\mathfrak{R}$, which is distinct from $\mathfrak{P}^2$ and contains $\mathfrak{P}^2$. If $\mathfrak{A}$ were composite, all its divisors would contain $\mathfrak{A}$ and consequently $\mathfrak{P}^2$. So that they would be contained in $\mathfrak{P}$ [§ 4, 2nd theorem], and the ideal $\mathfrak{A}$, which is the product of them, would be contained in $\mathfrak{P}^2$, contrary to assumption. Therefore *every ideal of* $\mathfrak{R}$, *which is distinct from* $\mathfrak{P}^2$ *and contains* $\mathfrak{P}^2$ *is prime.*

Next let $\mathfrak{M}$ be an ideal contained in $\mathfrak{P}$, and

$$\mathfrak{R},\quad \mathfrak{P},\quad \mathfrak{P}_1,\quad \mathfrak{P}_2,\quad \ldots, \mathfrak{P}_n,\quad \mathfrak{M}$$

a chief-composition-series of $\mathfrak{R}$ with last term $\mathfrak{M}$. If any one of the quotient rings

$$\frac{\mathfrak{P}}{\mathfrak{P}_1}, \frac{\mathfrak{P}_1}{\mathfrak{P}_2}, \ldots, \frac{\mathfrak{P}_n}{\mathfrak{M}}$$

is a field, $\mathfrak{M}$ may be resolved into two factors prime to each other [§ 16, theorem], and hence is composite. The contrary case will be left for future investigation.

(4) Lastly we suppose that there is no ideal, distinct from $\mathfrak{P}$ and $\mathfrak{P}^2$, which contains $\mathfrak{P}^2$ and consequently is contained in $\mathfrak{P}$. This is equivalent to the supposition that $n(\mathfrak{P}^2) = [n(\mathfrak{P})]^2$, [*cf.* §8].

Then $\mathfrak{P}$ *is prime, but every ideal of* $\mathfrak{R}$ *which is contained in* $\mathfrak{P}$ *is composite.*

For, since $n(\mathfrak{P}^2)=[n(\mathfrak{P})]^2$, $\mathfrak{P}$ must be prime; and every ideal contained in $\mathfrak{P}$ is divisible by $\mathfrak{P}$ [§ 24, Cor. 1].

§ 27. THEOREM: *Let* $\mathfrak{A}$ *be a composite ideal of a proper ring* $\mathfrak{R}$,

and $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_\nu$ *the distinct maximal ideals*[1] *of* $\mathfrak{R}$ *which contain* $\mathfrak{A}$.
1° *If*

$$n(\mathfrak{P}_i^2) = [n(\mathfrak{P}_i)]^2 \quad (\textit{for every } i = 1, 2, \cdots, \nu),$$

$\mathfrak{A}$ *can be resolved into the product of a finite number of prime ideals;*
2° *if*

$$n(\mathfrak{P}_i^e) = [n(\mathfrak{P}_i)]^e \quad \begin{pmatrix} \textit{for every } i = 1, 2, \ldots, \nu; \\ \textit{for every exponent } e \end{pmatrix},$$

this can be done in only one way.

For $\mathfrak{A}$ may be expressed in the form

$$\mathfrak{A} = \mathfrak{A}_1 \mathfrak{A}_2 \ldots \mathfrak{A}_\nu,$$

where $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_\nu$ are ideals which contain powers of $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_\nu$ respectively [§ 19, theorem]. But $n(\mathfrak{P}_i^2) = [n(\mathfrak{P}_i)]^2$ for every i. Therefore the maximal ideals are all prime [§ 26] and moreover $\mathfrak{A}_i$ is equal to a power of $\mathfrak{P}_i$ [§ 10, Cor.]. And hence $\mathfrak{A}$ can be resolved into prime factors, as

$$\mathfrak{A} = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \ldots \mathfrak{P}_\nu^{e_\nu}.$$

Taking up the second it is clear that a prime ideal dividing $\mathfrak{A}$ must be one of $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_\nu$, and also clear that if two resolutions are possible the same prime factors must occur in both; otherwise Cor. 3 of § 24 would be contradicted: so that the only admissible supposition is

$$\mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \ldots \mathfrak{P}_\nu^{e_\nu} = \mathfrak{P}_1^{e_1'} \mathfrak{P}_2^{e_2'} \ldots \mathfrak{P}_\nu^{e_\nu'},$$

where none of the exponents e's and e''s is zero. Then, by § 19, theorem, we have

$$\mathfrak{P}_i^{e_i} = \mathfrak{P}_i^{e_i'} \quad (i = 1, 2, \ldots, \nu),$$

whence by hypothesis

$$[n(\mathfrak{P}_i)]^{e_i} = [n(\mathfrak{P}_i)]^{e_i'} \quad (i = 1, 2, \ldots, \nu),$$

and hence

$$e_i = e_i' \quad (i = 1, 2, \ldots, \nu);$$

because $n(\mathfrak{P}_i) > 1$. So that the two resolutions are identical.

§ 28. Let $\mathfrak{R}$ be a proper ring subject to the conditions:

[1] N.B. The number of the maximal ideals which contain a given ideal is always finite, as shown already.

1. The product of two elements of $\mathfrak{R}$ is not equal to 0, unless at least one of the factors is equal to 0;

2. Every ideal of $\mathfrak{R}$, distinct from the 0-ideal, is of finite norm.

THEOREM: *In order that every composite ideal of the ring $\mathfrak{R}$ can be resolved into prime factors always and in only one way, it is necessary and sufficient that for every maximal ideal $\mathfrak{P}$ of $\mathfrak{R}$ and for every exponent e the equation*

$$n(\mathfrak{P}^e) = [n(\mathfrak{P})]^e$$

should hold.

It is clear by the last theorem that the condition is sufficient for unique resolvability. Hence we need only show that it is necessary.

Let $\mathfrak{P}$ be a maximal ideal of $\mathfrak{R}$. Then, by condition (1), $\mathfrak{P}^2$ is never the 0-ideal, and consequently is of finite norm. And moreover $\mathfrak{P}^2$ must be distinct from $\mathfrak{P}$; because otherwise the resolution of a power of $\mathfrak{P}$ would not be unique by our convention [p. 145]. Therefore

$$n(\mathfrak{P}^2) = [n(\mathfrak{P})]^{n+2},$$

where n is 0 or a finite positive integer [*cf.* §§ 7,8].

If $n \geqq 1$, there are ideals, distinct from $\mathfrak{P}$ and $\mathfrak{P}^2$, which contain $\mathfrak{P}^2$ and consequently are contained in $\mathfrak{P}$; and they are all prime [§ 25]. And hence we see from the results obtained in §§ 11–15 that the powers $\mathfrak{P}^2$ or $\mathfrak{P}^3$ may be resolved into prime factors in at least two ways. Therefore, in order that a composite ideal may be uniquely resolvable into prime factors, it must be that $n(\mathfrak{P}^2) = [n(\mathfrak{P})]^2$, viz. there is no ideal, except $\mathfrak{P}$ and $\mathfrak{P}^2$, which contains $\mathfrak{P}^2$.

Next $\mathfrak{P}^e$ must $\neq \mathfrak{P}^{e+1}$ for every exponent e; because otherwise $\mathfrak{P}^{e}$ can be resolved into prime factors in more than one way according to our convention

Therefore, as shown in § 9, $\mathfrak{R}$ and the powers

$$\mathfrak{R},\ \mathfrak{P},\ \mathfrak{P}^2,\ \mathfrak{P}^3,\ \dots$$

must give a chief-composition-series of $\mathfrak{R}$: so that $n(\mathfrak{P}^e)$ must $=$ $[n(\mathfrak{P})]^e$ for every index e.

§ 29. Let $\mathfrak{A}$ be an ideal containing a power of a maximal ideal $\mathfrak{P}$, for which $n(\mathfrak{P}^2)=[n(\mathfrak{P})]^2$. Then $\mathfrak{A}$ is equal to a power of $\mathfrak{P}$, and therefore suppose that $\mathfrak{A}=\mathfrak{P}^n$.

If $\mathfrak{P}^e \neq \mathfrak{P}^{e+1}$ for every index $e \leqq n$, $\mathfrak{A}$ is uniquely resolvable into prime factors.

If, on the contrary, $\mathfrak{P}^e = \mathfrak{P}^{e+1}$ for a certain index $e \leqq n$, the resolution of $\mathfrak{A}$ is not unique according to our convention [*p.* 145, foot note]. If, however, we regard $\mathfrak{A}$ as uniquely resolvable also in the latter case, the condition for the unique resolvability requires to be changed and stated as follows:

$$n(\mathfrak{P}^2) \leqq [n(\mathfrak{P})]^2$$

for each maximal ideal of the ring.

§ 30. It would be of interest to find all possible resolutions of an ideal resolvable into prime factors in two or more than two ways; but this problem must be left for future investigation, with the mere statement that, by application of the theorem of § 19 and a few others, the problem may be reduced to an investigation of resolutions of ideals which contain powers of a maximal ideal $\mathfrak{P}$ for which $n(\mathfrak{P}^2) > [n(\mathfrak{P})]^2$.

November, 1917.