On Congruences. IV.

By

Masazo Sono.

(Received Nov. 25, 1918.)

The present paper is intended, in the main, to discuss the ideals of a proper ring which contains at least two elements, distinct from 0, whose product is equal to 0, under the assumption that corresponding to any ideal, distinct from the 0-ideal, the ring possesses a chief-composition-series containing the ideal for the last term. In § 2 we show that in such a ring the maximal ideals are finite in number and that $\mathfrak{P}^e = \mathfrak{P}^{e+1}$ for each maximal ideal $\mathfrak{P}$, and for a certain exponent e, in § 3 we treat the converse, in § 5 we consider the resolution of ideals in such a ring, in § 6 we add a word about the product of the ideals of a quotient ring, and in §§ 7, 8 we give examples of resolvability. The result obtained in § 3 requires the correction of the theorems of Congr. II, § 28 and Congr. III, § 8: so that it is given in § 4.

For the sake of brevity the previous papers[1] on congruences are here denoted by Congr., Congr. II and Congr. III respectively.

A Proper Ring which contains at least Two Elements whose Product is Equal to 0.

§ 1. Let $\mathfrak{R}$ be a proper ring; suppose that corresponding to an ideal $\mathfrak{A}$ of $\mathfrak{R}$, there exists a chief-composition-series of $\mathfrak{R}$ which contains $\mathfrak{A}$ for the last term. Then, as shown in §§ 4, 5 of Congr. III, the maximal ideals containing $\mathfrak{A}$ are finite in number. If $\mathfrak{A}$ is contained in a single maximal ideal, say $\mathfrak{P}$, $\mathfrak{A}$ contains a power of $\mathfrak{P}$. If, on the contrary, $\mathfrak{A}$ is contained in just ν maximal ideals, $\mathfrak{A}$ is resolvable into ν factors prime to one another, each of which contains

[1] On Congruences, these Memoirs, **2**, 203 (1917);
On Congrsences, II, these Memoirs, **3**, 113 (1918 ;
On Congruences, III, these Memoirs, **3**, 189 (1918).

a power of one of the maximal ideals; and this can be done in one way only.

But in the present paper our discussion is limited to the ideals of such a proper ring as, corresponding to any given ideal distinct from the o-ideal, possesses a chief-composition-series containing the ideal for the last term: so that the result above described is always applicable.

§ 2. We now suppose that a proper ring $\mathfrak{R}$ contains at least two elements, distinct from 0, whose product is equal to 0.

Let A, B be such elements, i.e.

$$AB = 0,$$

while both are distinct from 0. Then the principal idea (A) is distinct from $\mathfrak{R}$. For, otherwise, an element R could be so chosen that $AR = 1$; and hence we should have $B = B \cdot AR = 0$, contrary to our assumption. Similarly the ideal (B) is also distinct from $\mathfrak{R}$. Therefore, as stated in § 1, (A) and (B) either contain powers of maximal ideals or are resolvable into factors which respectively contain powers of distinct maximal ideals. So that, while $AB = 0$, the product (AB) either contains a power of a maximal ideal, say $\mathfrak{P}^e$, or may be expressed in the form:

$$(AB) = \mathfrak{L}_1 \mathfrak{L}_2 \dots \mathfrak{L}_\nu,$$

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

In the former case, the power $\mathfrak{P}^e$ must be the o-ideal; hence $\mathfrak{R}$ has no other maximal ideals distinct from $\mathfrak{P}$ [Congr. II, § 4]. It will be seen in §§ 7, 8 that this case is existent.

In the latter, no powers of the $\mathfrak{P}$'s are the o-ideal; because otherwise $\mathfrak{R}$ might have a single maximal ideal only. Therefore all of the following: $\mathfrak{L}_1, \mathfrak{L}_2, \dots \mathfrak{L}_\nu$ are distinct from the o-ideal. If $\mathfrak{P}$ were another maximal ideal distinct from $\mathfrak{P}_1, \mathfrak{P}_2, \dots \mathfrak{P}_\nu$, then $\mathfrak{P}$ would be prime to all of $\mathfrak{L}_1, \mathfrak{L}_2, \dots \mathfrak{L}_\nu$, and consequently to their product $\mathfrak{L}_1 \mathfrak{L}_2 \dots \mathfrak{L}_\nu$ [Congr. II, § 4], while $\mathfrak{L}_1 \mathfrak{L}_2 \dots \mathfrak{L}_\nu = 0$. Therefore there are no other maximal ideals distinct from $\mathfrak{P}_1, \mathfrak{P}_2, \dots \mathfrak{P}_\nu$.

And moreover we have

$$\begin{aligned} \mathfrak{P}_1 \mathfrak{L}_1 &= (\mathfrak{P}_1 \mathfrak{L}_1, \mathfrak{L}_1 \mathfrak{L}_2 \dots \mathfrak{L}_\nu) \\ &= \mathfrak{L}_1 (\mathfrak{P}_1, \mathfrak{L}_2 \dots \mathfrak{L}_\nu) \\ &= \mathfrak{L}_1 \mathfrak{R} = \mathfrak{L}_1. \end{aligned}$$

But $\mathfrak{L}_1$ contains a power of $\mathfrak{P}_1$, say $\mathfrak{P}_1^{e_1}$: so that $\mathfrak{P}_1$ contains $\mathfrak{L}_1$ [Congr. II, § 4]. Hence $\mathfrak{P}_1^{e_1}$ contains $\mathfrak{L}_1\mathfrak{P}_1^{-1}$, which is equal to $\mathfrak{L}_1$. Therefore $\mathfrak{L}_1=\mathfrak{P}_1^{e_1}$, and hence

$$\mathfrak{P}_1^{e_1} = \mathfrak{P}_1^{e_1+1}.$$

Similarly we have, for a certain exponent e_i,

$$\mathfrak{P}_i^{e_i} = \mathfrak{P}_i^{e_i+1} \qquad (i=2, 3, \ldots \nu).$$

and

$$\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\ldots\mathfrak{P}_\nu^{e_\nu}=0.$$

It has already been shown by the example in Congr. II, § 9 that this case is also existent. And we have the

THEOREM: *If a proper ring $\mathfrak{R}$ contains at least two elements, distinct from 0, whose product is equal to 0, then (i) the maximal ideals of $\mathfrak{R}$ are finite in number, (ii) if the number is one, a certain power of the maximal ideal is the 0-ideal, and (iii) if it is more than one,*

$$\mathfrak{P}^e = \mathfrak{P}^{e+1} \neq 0,$$

for each maximal ideal $\mathfrak{P}$ and for a certain exponent e.

N. B. Herein it is assumed that, corresponding to a given ideal, distinct from the 0-ideal, there exists a chief-composition-series which contains the ideal for the last term.

§ 3. To treat the converse, assume that a proper ring $\mathfrak{R}$ contains a maximal ideal $\mathfrak{P}$ for which $\mathfrak{P}^e=\mathfrak{P}^{e+1}$ for a certain exponent e.

If $\mathfrak{P}^e=0$, evidently $\mathfrak{R}$ contains two elements, distinct from 0, whose product is equal to 0, and moreover $\mathfrak{P}$ is the only maximal ideal of $\mathfrak{R}$ [Congr. II, § 4].

Next, to consider the case in which $\mathfrak{P}^e \neq 0$, take an element A, distinct from 0, of $\mathfrak{P}^e$. Then the principal ideal (A) either contains a power of $\mathfrak{P}$ or is resolvable into factors prime to each other:

$$(A) = \mathfrak{A}\mathfrak{M},$$

where $\mathfrak{A}$ is an ideal containing a power of $\mathfrak{P}$.

In the former case, evidently (A) must contain $\mathfrak{P}^e$, and consequently coincides with $\mathfrak{P}^e$: so that

$$A\mathfrak{P}=\mathfrak{P}^{e+1}=\mathfrak{P}^e=(A).$$

Hence we have

$$AP = A,$$

P being an element of $\mathfrak{P}$, or

$$A(P-1)=0,$$

while $P-1$ is distinct from 0; because P belongs to $\mathfrak{P}$, and consequently may not be equal to 1.

In the latter, $\mathfrak{A}$ must contain $\mathfrak{P}^e$, and hence $\mathfrak{A}\mathfrak{M}$ contains $\mathfrak{P}^e\mathfrak{M}$. But $\mathfrak{P}^e\mathfrak{M}$ contains (A); because, since $(\mathfrak{P}^e, \mathfrak{M})=\mathfrak{R}$, the product $\mathfrak{P}^e\mathfrak{M}$ is the cross-cut of $\mathfrak{P}^e$ and $\mathfrak{M}$, both of which contain A [Congr. II, § 5]. Therefore (A) and $\mathfrak{P}^e\mathfrak{M}$ are identical: so that

$$A\mathfrak{P}=\mathfrak{P}^{e+1}\mathfrak{M}=\mathfrak{P}^e\mathfrak{M}=(A),$$

whence, as above, we have

$$A(P-1)=0,$$

where P is an element of $\mathfrak{P}$.

Therefore $\mathfrak{R}$ contains at least two elements, distinct from 0, whose product is equal to 0. And we have the

THEOREM: *If there exists in a proper ring $\mathfrak{R}$ a maximal ideal $\mathfrak{P}$, for which $\mathfrak{P}^e=\mathfrak{P}^{e+1}$ for a certain exponent e, $\mathfrak{R}$ contains at least two elements, distinct from 0, whose product is equal to 0.*

If, therefore, in a proper ring $\mathfrak{R}$ the product of two elements is distinct from 0, unless at least one of the factors is equal to 0, we have

$$\mathfrak{P}^e \neq \mathfrak{P}^{e+1}$$

for any maximal ideal $\mathfrak{P}$ and for any exponent e. Hence the theorem of Congr. III, § 8 and that of Congr. II, § 28 must be corrected: the former will be given as the theorem and the latter as the corollary in the next article.

Resolvability of Ideals.

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

(1) The product of two elements of $\mathfrak{R}$ is distinct from 0, unless at least one of the factors is equal to 0;

(2) Corresponding to any given ideal $\mathfrak{A}$, distinct from the 0-ideal, of $\mathfrak{R}$, there exists a chief-composition-series of $\mathfrak{R}$ which contains $\mathfrak{A}$ for the last term.

Then we have the

THEOREM: *In order that every composite ideal of $\mathfrak{R}$ may be uniquely resolvable into prime factors, it is necessary and sufficient that*

for every maximal ideal $\mathfrak{P}$ *of* $\mathfrak{R}$ *the following condition should hold: an ideal of* $\mathfrak{R}$ *which contains* $\mathfrak{P}^2$ *is either* $\mathfrak{P}$ *or* $\mathfrak{P}^2$.

The proof here is repeated for the sake of completeness, slight as the correction is.

To prove the necessity of the condition we assume that every composite ideal is uniquely resolvable into prime factors; let $\mathfrak{P}$ be a maximal ideal of $\mathfrak{R}$. Then, by condition (1) for the ring $\mathfrak{R}$, $\mathfrak{P}^2$ is distinct from the 0-ideal, and hence, by condition (2), there is a chief-composition-series containing $\mathfrak{P}^2$ for the last term. And moreover $\mathfrak{P}^2$ is distinct from $\mathfrak{P}$, as has been already proved. Therefore the chief-composition-series consists either of three terms or of more than three terms. Namely, it is either

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

or

$$\mathfrak{R},\ \mathfrak{P},\ \mathfrak{A}_1,\ \mathfrak{A}_2, \ldots \mathfrak{A}_n,\ \mathfrak{P}^2 \qquad (n \geqq 1).$$

If the latter case happened, the $\mathfrak{A}$'s would be all prime, and hence at least one of the ideals containing $\mathfrak{P}^3$ would be resolvable into prime factors in more than one way, as seen from the results obtained in Congr. II, §§ 11–15. Therefore an ideal containing $\mathfrak{P}^2$ must be either $\mathfrak{P}$ or $\mathfrak{P}^2$ [Congr. II, § 4].

Next, to prove the sufficiency of the condition we assume that it is fulfilled. Then the maximal ideals are all prime, but the others all composite [Congr. III, § 7]; and also an ideal is resolvable into the product of the maximal ideals [Congr. III, § 6]. Therefore a composite ideal $\mathfrak{A}$ may be reduced to the form

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

where $\mathfrak{P}_1, \mathfrak{P}_2, \ldots \mathfrak{P}_\nu$ are distinct prime ideals.

It is clear that a prime ideal dividing $\mathfrak{A}$ must be one of the $\mathfrak{P}$'s, and also that if two resolutions are possible the same prime factors must occur in both: so that the only admissible supposition is

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

whence we have

$$\mathfrak{P}_i^{e_i} = \mathfrak{P}_i^{e_i'} \qquad (i = 1, 2, \ldots \nu) \qquad \text{[Congr. III, § 5]};$$

and hence

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

because otherwise $\mathfrak{P}_i^{e_i}$ and $\mathfrak{P}_i^{e_i'}$ would be distinct [§ 3]. So that the two resolutions are identical.

Cor. Let $\mathfrak{R}$ be a proper ring such that the product of two elements, distinct from 0, is not equal to 0, and moreover every ideal distinct from the 0-ideal is of finite norm. Then in order that every composite ideal of $\mathfrak{R}$ may be uniquely resolvable into prime factors, it is necessary and sufficient that for every maximal ideal $\mathfrak{P}$ the equation

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

should hold.

This follows from the above theorem and the result obtained in Congr. II, § 8.

§ 5. The resolvability of an ideal of a proper ring which contains at least two elements, distinct from 0, whose product is equal to 0. *If $\mathfrak{R}$ is such a ring, the maximal ideals are finite in number; and if $\mathfrak{P}$ is one of them, for a certain exponent e, the power $\mathfrak{P}^e$ coincides either with the 0-ideal or with $\mathfrak{P}^{e+1}$, while $\mathfrak{P}^e$ is not the 0-ideal.*

(1) First taking the former case, we treat it under the assumption that $e > 2$; because, if $e=2$, the ideals of $\mathfrak{R}$ are all prime.

(i) If a chief-composition-series with the last term $\mathfrak{P}^2$ consists of three terms:

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

we have

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

and consequently

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

where π is an element of $\mathfrak{P}$, which does not belong to $\mathfrak{P}^2$ [Congr. II, § 9]. But, in the present case, $\mathfrak{P}^e=0$; therefore $\mathfrak{P}=(\pi)$, and $\pi^e=0$. And moreover the ideals of $\mathfrak{R}$ are given by the following $e-1$:

$$(\pi),\ (\pi)^2,\ \ldots\ (\pi)^{e-1};$$

because all the ideals must be contained in $\mathfrak{P}$.

(ii) If, on the contrary, the series consists of more than three terms, taking an element P of $\mathfrak{P}$ which does not belong to $\mathfrak{P}^2$ we have

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

But, when $\mathfrak{P}^e=0$, an ideal which is not contained in $\mathfrak{P}^2$ is prime; because, when $\mathfrak{P}^e=0$, the ideals of $\mathfrak{R}$ are contained in $\mathfrak{P}$, and hence the product of the ideals must be contained in $\mathfrak{P}^2$. Therefore, both $(\,(P),\ \mathfrak{P}^2)$ and (P) are prime; if these two are distinct, the resolution

of $P\mathfrak{P}^{e-2}$ is not unique. If, on the contrary, $((P), \mathfrak{P}^2)=(P)$, the elements of $\mathfrak{P}^2$ are contained in (P), and consequently may be expresssed in the form PR. In this, R must belong to $\mathfrak{P}$; because, otherwise, the ideal (PR) would coincide with (P), contrary to our assumption that P does not belong to $\mathfrak{P}^2$. If, conversely, R belongs to $\mathfrak{P}$, the product PR is an element of $\mathfrak{P}^2$. Therefore, if $((P), \mathfrak{P}^2) = (P)$, we have

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

which shows that the resolution of $\mathfrak{P}^2$ is not unique.

(2) Next, to consider the case in which the number of the maximal ideals is more than one, let $\mathfrak{P}$ be one of them. Then, as stated above, $\mathfrak{P}^e=\mathfrak{P}^{e+1}$ for a certain exponent e. If $e=1$, an ideal containing a power of $\mathfrak{P}$ is $\mathfrak{P}$ itself; therefore we need only consider the case in which $e>1$.

(i) If there are no ideals, distinct from $\mathfrak{P}$ and $\mathfrak{P}^2$, which contain $\mathfrak{P}^2$, an ideal containing a power of $\mathfrak{P}$ is a power of $\mathfrak{P}$ [Congr. II, § 10], and hence is divisible by no other prime ideals distinct from $\mathfrak{P}$.

(ii) In the opposite case, taking an element P of $\mathfrak{P}$ which does not belong to $\mathfrak{P}^2$ we have

$$((P), \mathfrak{P}^2)\ \mathfrak{P}^{e-1} = \mathfrak{P}^e,$$

showing that $\mathfrak{P}^e$ is divisible by the prime ideal $((P), \mathfrak{P}^2)$ distinct from $\mathfrak{P}$.

§ 6. Before giving examples which show the existence of the cases discussed in the last article, we add a word about the product of the ideals of a quotient ring.

Let $\mathfrak{M}$ be an ideal of a ring $\mathfrak{R}$, and $\mathfrak{A}$, $\mathfrak{B}$ other ideals of $\mathfrak{R}$ which contain $\mathfrak{M}$. Then the quotients $\mathfrak{A}/\mathfrak{M}$ and $\mathfrak{B}/\mathfrak{M}$ are ideals of the quotient ring $\mathfrak{R}/\mathfrak{M}$ [*cf.* Congr. § 9], and the elements of their product are given by the form

$$\Sigma\alpha\beta \pmod{\mathfrak{M}},$$

where α, β are elements of $\mathfrak{A}/\mathfrak{M}$ and $\mathfrak{B}/\mathfrak{M}$ respectively. If $\mathfrak{C}$ denotes the ideal of $\mathfrak{R}$, whose quotient as regards $\mathfrak{M}$ is the product $\frac{\mathfrak{A}}{\mathfrak{M}} \cdot \frac{\mathfrak{B}}{\mathfrak{M}}$, the elements of $\mathfrak{C}$ are given by the form

$$M + \Sigma\alpha\beta,$$

where M is an element of $\mathfrak{M}$ [*cf.* Congr. § 9]; hence $\mathfrak{C}$ is contained in the ideal $(\mathfrak{M}, \mathfrak{AB})$. But the elements of $(\mathfrak{M}, \mathfrak{AB})$ may be expressed in the form

$$M + \Sigma AB,$$

where A, B, M are elements of $\mathfrak{A}, \mathfrak{B}, \mathfrak{M}$ respectively; and

$$\Sigma AB \equiv \Sigma a\beta \pmod{\mathfrak{M}}.$$

Therefore $(\mathfrak{M}, \mathfrak{AB})$ is contained in $\mathfrak{C}$: so that $(\mathfrak{M}, \mathfrak{AB})$ and $\mathfrak{C}$ are identical. Hence we have the

THEOREM: *Let $\mathfrak{M}$ be an ideal of a ring $\mathfrak{R}$, and $\mathfrak{A}, \mathfrak{B}$ other ideals of $\mathfrak{R}$ which contain $\mathfrak{M}$. Then*

$$\frac{\mathfrak{A}}{\mathfrak{M}} \cdot \frac{\mathfrak{B}}{\mathfrak{M}} = \frac{(\mathfrak{AB}, \mathfrak{M})}{\mathfrak{M}}.$$

If $\mathfrak{M}$ contains a power of a maximal ideal, say $\mathfrak{P}^e$ $(e>1)$, we have

$$\left(\frac{\mathfrak{P}}{\mathfrak{M}}\right)^e = \frac{(\mathfrak{P}^e, \mathfrak{M})}{\mathfrak{M}} = \frac{\mathfrak{M}}{\mathfrak{M}},$$

while $\mathfrak{M}/\mathfrak{M}$ is the o-ideal of $\mathfrak{R}/\mathfrak{M}$.

Next, suppose that

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

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

Then

$$\left(\frac{\mathfrak{P}_i}{\mathfrak{M}}\right)^n = \frac{(\mathfrak{P}_i^n, \mathfrak{M})}{\mathfrak{M}} = \frac{(\mathfrak{P}_i^n, \mathfrak{M}_i)}{\mathfrak{M}},$$

since

$$(\mathfrak{P}_i^n, \mathfrak{M}) = (\mathfrak{P}_i^n, \mathfrak{M}_1 \mathfrak{M}_2 \dots \mathfrak{M}_\nu) = (\mathfrak{P}_i^n, \mathfrak{M}_i) \qquad \text{[Congr. III, § 6]}.$$

If, therefore, $\mathfrak{P}_i^{e_i}$ is the lowest power of $\mathfrak{P}_i$ which is contained in $\mathfrak{M}_i$, we have

$$\left(\frac{\mathfrak{P}_i}{\mathfrak{M}}\right)^{e_i+n} = \frac{\mathfrak{M}_i}{\mathfrak{M}} \qquad n \geqq 0;\ i = 1, 2, \dots \nu,$$

while

$$\left(\frac{\mathfrak{P}_i}{\mathfrak{M}}\right)^{e_i-1} \neq \frac{\mathfrak{M}_i}{\mathfrak{M}}.$$

§ 7. Now let $\mathfrak{R}$ be a set of all possible polynomials of x, y, whose coefficients are numbers of a field Ω. Then evidently $\mathfrak{R}$ is a

proper ring, and the ideal[1] (x, y) derived from (x) and (y) is maximal.

Putting $\mathfrak{P}=(x, y)$ we have

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

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

$$((x),\ \mathfrak{P}^e) = (x,\ y^e) \qquad (e > 2),$$

the last two of which are distinct. Consequently quotients $((x), \mathfrak{P}^2)/\mathfrak{P}^e$ and $((x), \mathfrak{P}^e)/\mathfrak{P}^e$ are also distinct, and are not contained in $(\mathfrak{P}/\mathfrak{P}^e)^2$. But

$$\frac{((x), \mathfrak{P}^2)}{\mathfrak{P}^e} \cdot \left(\frac{\mathfrak{P}}{\mathfrak{P}^e}\right)^{e-2} = \frac{((x), \mathfrak{P}^2)}{\mathfrak{P}^e} \cdot \frac{\mathfrak{P}^{e-2}}{\mathfrak{P}^e} = \frac{(x\,\mathfrak{P}^{e-2}, \mathfrak{P}^e)}{\mathfrak{P}^e},$$

and

$$\frac{((x), \mathfrak{P}^e)}{\mathfrak{P}^e} \cdot \left(\frac{\mathfrak{P}}{\mathfrak{P}^e}\right)^{e-2} = \frac{(x\,\mathfrak{P}^{e-2}, \mathfrak{P}^{2e-2}, \mathfrak{P}^e)}{\mathfrak{P}^e} = \frac{(x\,\mathfrak{P}^{e-2}, \mathfrak{P}^e)}{\mathfrak{P}^e}.$$

So that we have

$$\frac{((x), \mathfrak{P}^2)}{\mathfrak{P}^e} \cdot \left(\frac{\mathfrak{P}}{\mathfrak{P}^e}\right)^{e-2} = \frac{((x), \mathfrak{P}^e)}{\mathfrak{P}^e} \cdot \left(\frac{\mathfrak{P}}{\mathfrak{P}^e}\right)^{e-2},$$

while the first factors of both sides are distinct. This gives an example for the former part of § 5, (1), (ii), if we consider the quotient ring $\mathfrak{R}/\mathfrak{P}^e$.

§ 8. Let K be the quadratic field with discriminant d, Q a rational integer, and $\mathfrak{R}$ the ring, with *Führer* (Q), of K. Then it is easily shown that the elements of $\mathfrak{R}$ may be expressed in the form

$$x + y \cdot \frac{Q(d + \sqrt{d})}{2},$$

where x, y are rational integers.[2] If p is an odd prime, which divides Q, the congruence $b^2 \equiv Q^2 d \pmod{4p}$ is satisfied by $b \equiv$ either 0 or $p \pmod{2p}$. And the ideal

$$\left(p,\ \frac{-b+Q\sqrt{d}}{2}\right) \qquad [b^2 \equiv Q^2 d \pmod{4p}]$$

of $\mathfrak{R}$ is maximal. Moreover, if this ideal is denoted by $\mathfrak{P}$, it can be proved that

[1] For the sake of simplicity, the ideal derived from the principal ideals (A), (B), ... will hereafter be denoted by $(A, B, ...)$.

[2] See Weber, Lehrbuch der Algebra III, 2nd ed., § 96.

$$\mathfrak{P}^2 = \mathfrak{p}\mathfrak{P},$$

and also that the principal ideal $(\mathfrak{p})$ is distinct from $\mathfrak{P}$ and $\mathfrak{P}^2$. And, if $e > 2$, we have

$$\left(\frac{\mathfrak{P}}{\mathfrak{P}^e}\right)^2 = \frac{\mathfrak{P}^2}{\mathfrak{P}^e} = \frac{\mathfrak{p}\mathfrak{P}}{\mathfrak{P}^e} = \frac{(\mathfrak{p})}{\mathfrak{P}^e} \cdot \frac{(\mathfrak{P})}{\mathfrak{P}^e},$$

while

$$\frac{((\mathfrak{p}), \mathfrak{P}^2)}{\mathfrak{P}^e} = \frac{(\mathfrak{p})}{\mathfrak{P}^e}.$$

If we consider the quotient ring $\mathfrak{R}/\mathfrak{P}^e$, this gives an example for the latter part of § 5, (1) (ii).

Examples for case (2) of § 5 can easily be given from the ring $\mathfrak{R}$: so that here they are omitted.

November, 1918.