Paper Communicated.

On the Classes of Congruent Integers in an Algebraic Körper.*

By Tanzo Takenouchi, *Rigakushi.*

(Communicated by Prof. R. Fujisawa, October 12, 1913)

Let $\mathfrak{m}$ be an ideal in an algebraic *körper*. All the integers in the *körper* can be classified into classes of congruent integers with respect to the modulus $\mathfrak{m}$. If α and α' be any two integers of class A, and β and β' be those of class B, the products $\alpha\beta$ and $\alpha'\beta'$ always belong to one and the same class. Let it be called C. In this sense these classes can be composed by multiplication, and we write $AB=C$. If we consider only those classes which consist of integers relatively prime to $\mathfrak{m}$, then these reduced system of classes form an Abelian group, which we shall call $\mathfrak{M}$.

Since $\mathfrak{M}$ is Abelian, it contains a system of elements (classes) called bases, say $A_1, A_2, \ldots\ldots, A_s$, such that each element of $\mathfrak{M}$ can be represented uniquely in the form

$$S=A_1^{\alpha_1} A_2^{\alpha_2} \ldots\ldots A_s^{\alpha_s}, \qquad \begin{matrix} \alpha_i=0, 1, 2, \ldots\ldots, a_i-1, \\ (i=1, 2, \ldots\ldots, s) \end{matrix}$$

where a_i denotes the order of the element A_i. Systems of bases may be constructed in different ways, and the orders of the bases, of course, vary according to different systems of bases But, if we decompose the orders into powers of distinct prime

* Since this paper was read, my attention was called to Georg Wolff's inaugural dissertation "Ueber Gruppen der Reste eines beliebigen Moduls im algebraischen Zahlkörper" (Giessen, 1905), which seems to have escaped the notice of the writers referred to in the present paper. In Wolff's paper, the results obtained in the first half of the present paper are derived in a quite different manner. Moreover, as the chief interest of the present paper lies in its second half, the knowledge of the existence of Wolff's paper will not in the least detract the merit of the present communication. R. Fujisawa.

factors, then these powers as a whole remain conserved independently of the choice of bases. Following H. Weber (Lehrbuch der Algebra, Bd. II), we call these powers the invariants of group $\mathfrak{M}$.

The chief object of the present paper is the determination of the number of the invariants of $\mathfrak{M}$.

General considerations.—First of all, it is evident that we may confine ourselves to the case, where the modulus is a a power of a single prime ideal. Hence, hereafter, we shall always suppose that $\mathfrak{m}=\mathfrak{p}^n$, $\mathfrak{p}$ being a prime ideal, and n a positive integer.

The norm of $\mathfrak{p}$ is p^f, p being a natural prime divisible by $\mathfrak{p}$, and f the degree of $\mathfrak{p}$. Then the order of group $\mathfrak{M}$ is given by $p^{f(n-1)}(p^f-1)$.

Now, since $p^{f(n-1)}$ and p^f-1 are relatively prime to each other, there are in $\mathfrak{M}$ $p^{f(n-1)}$ elements, whose orders are divisors of $p^{f(n-1)}$, forming a subgroup of $\mathfrak{M}$, say $\mathfrak{A}$; and also p^{f-1} elements, whose orders are divisors of p^{f-1}, forming another subgroup $\mathfrak{B}$; and $\mathfrak{M}=\mathfrak{A}\mathfrak{B}$.

As for the subgroup $\mathfrak{B}$, we obtain the following result:

$\mathfrak{B}$ *is a cyclic group. If*

$$p^f-1=p_1^{n_1}p_2^{n_2}\cdots\cdots p_h^{n_h},$$

where $p_1, p_2, \ldots\ldots, p_h$ *are distinct prime factors, then the invariants of* $\mathfrak{B}$ *are*

$$p_1^{n_1}, p_2^{n_2}, \ldots\ldots, p_h^{n_h}$$

As for the other subgroup $\mathfrak{A}$, let $\mathfrak{p}^d$ be the highest power of $\mathfrak{p}$ contained in p. For the sake of convenience we distinguish the following four cases:

$$d\not\equiv 0\ (mod.\ p-1)\begin{cases} f=1\begin{cases} d<p-1 \ldots\ldots & \text{I.} \\ d>p-1 \ldots\ldots & \text{II.} \end{cases} \\ f>1 \ldots\ldots & \text{III.} \end{cases}$$

$$d\equiv 0\ (mod.\ p-1) \quad \ldots\ldots \quad \text{IV.}$$

Case I.—In this case, the order of $\mathfrak{A}$ is p^{r-1}. Let π be an integer which is divisible dy p, but not by p^2; and consider d numbers

$$1+\pi^a, \qquad a=1, 2, \ldots\ldots, d.$$

The classes represented by these numbers are the elements of $\mathfrak{A}$. If e_a denotes the exponent to which $1+\pi^a$ belongs (*mod.* p^n), then we can prove that

$$\prod_{1,d}^{a} e_a = p^{n-1},$$

and also

$$\prod_{1,d}^{a} (1+\pi^a)^{e'_a} \not\equiv 1, \qquad (mod.\ p^n),$$

$$e'_a=0, 1, 2, \ldots, e_a-1, \qquad \text{excepting the combination } e'_1=e'_2=\ldots=e'_d=0.$$

Hence, we conclude that the above defined classes form a system of bases of $\mathfrak{A}$.

Let us now introduce the following notation:

$(x)=0$, when $x \leqq 0$,
$=x$, when x is a natural number,
$=$the smallest natural number greater than x, when x is positive but not a natural number.

Making use of this notation, we can express the invariants of $\mathfrak{A}$ as follows:

$$p^{\left(\frac{n-a}{d}\right)}, \quad \text{where} \quad \begin{cases} a=1, 2, \ldots\ldots, d, & \text{if } d<n, \\ a=1, 2, \ldots\ldots, n-1, & \text{if } 1<n \leqq d, \\ a=1, & \text{if } n=1. \end{cases}$$

If we denote by r the number of invariants or the *rank* of $\mathfrak{A}$ according to Frobenius and Stickelberger (Crelle's Journal, Bd. 86), we get

$$\left.\begin{array}{ll} r=d, & \text{if } d<n, \\ r=n-1, & \text{if } 1<n \leqq d, \\ r=1, & \text{if } n=1. \end{array}\right\} \qquad (1)$$

Case II.—In this case, putting $\left(\frac{d}{p-1}\right)=k$, we can prove, as in the preceding case, that the classes represented by the numbers

$1+\pi^a$, $a=1, 2, 3,\ldots, d+k-1$, excluding the multiples of p, form a system of bases for $\mathfrak{A}$.

Hence, the invariants consists of powers of p, whose exponents are

$$\text{when } n>k,\begin{cases} j_b+\left[\frac{n-bp^{j_b}}{d}\right] & \text{where } j_b=\left[log_p\frac{k}{b}\right], \\ & b=1, 2,\ldots\ldots k-1, \quad b\not\equiv 0 \ (mod.\ p), \\ \text{and } \left[\frac{n-c}{d}\right] & c=k, k+1,\ldots\ldots, k+d-1, \\ & \qquad \text{if } n\geqq k+d, \\ & \text{or } c=k, k+1,\ldots\ldots, n-1, \\ & \qquad \text{if } n<k+d, \end{cases} c\not\equiv 0 \ (mod.\ p);$$

$$\text{when } n\leqq k\begin{cases} \left[log_p\frac{n}{a}\right], & a=1, 2, \ldots\ldots, n-1, \\ & \qquad \text{if } n>1, \\ & a=1, \quad \text{if } n=1, \end{cases} a\not\equiv 0 (mod.\ p).$$

The *rank* is given by

$$\left.\begin{array}{lll} r=d, & \text{if} & k+d\leqq n, \\ r=n-\left[\frac{n}{p}\right], & \text{if} & 1<n<k+d, \\ r=1, & \text{if} & n=1. \end{array}\right\} \quad (2)$$

It is to be observed that the preceding result (1) is included in (2).

Case III.—In this case, we take as a system of the representative bases the following fd numbers:

$$\left.\begin{array}{ll} & a=1, 2, 3,\ldots\ldots, d+k-1, \quad k=\left[\frac{d}{p-1}\right], \\ 1+\xi_i\pi^a, & a\not\equiv 0 \ (mod.\ p.), \\ & i=1, 2,\ldots\ldots, f, \end{array}\right\} \quad (3)$$

where ξ's are integers such that

$$c_1\xi_1+c_2\xi_2+\ldots\ldots+c_f\xi_f\not\equiv o \quad (mod.\ p),$$

for all combinations of c's, $\quad c_i\equiv 0, 1, 2,\ldots\ldots, p-1 \quad (mod.\ p),$

$$(i=1, 2,\ldots\ldots, f)$$

$$\text{excluding } c_1\equiv c_2\equiv\ldots\ldots\equiv c_f\equiv 0 \quad (mod.\ p).$$

That the above defined fd numbers really represent a system

of bases can be shewn by the same reasoning as in the preceding cases.

If we wish to get the invariants of $\mathfrak{A}$, we have only to write down the invariants given in case I or II (according as $d<p-1$ or $d>p-1$), each being repeated f times; only when $n=1$ no repetition is needed.

Hence, the *rank* is given by

$$\begin{aligned} &r=fd, && \text{if } d+k\leqq n,\\ &r=f\left(n-\left[\frac{n}{p}\right]\right), && \text{if } 1<n<d+k,\\ &r=1, && \text{if } n=1, \end{aligned}$$

This result clearly includes both (1) and (2).

Case IV.—Firstly, we confine ourselves to the case $k\not\equiv o$ (*mod. p*).

If $n\leqq d+k$, we can proceed in the same manner and arrive at the same conclusion as in the preceding case.

If, on the contrary, $n>d+k$, then we distinguish two cases, according as the congruence

$$p+\pi^d x^{p-1}\equiv 0 \qquad (mod.\ \mathfrak{p}^{d+1}),$$

has a solution or not. If we determine an integer ρ from

$$p\equiv\pi^d\rho \qquad (mod.\ \mathfrak{p}^{d+1}),$$

we may replace the above congruence by

$$\rho+x^{p-1}\equiv 0 \qquad (mod.\ \mathfrak{p}). \qquad (4)$$

If (4) has no solution, then following exactly the same reasoning as in the last case, we can shew that the fd numbers (3) represent a system of bases, and consequently $r=fd$.

If (4) has a solution, say $x\equiv x_o$, then f rational integers a_i $(i=1, 2, \ldots\ldots, f)$, such that

$$x_o\equiv a_1\xi_1+a_2\xi_2+\ldots\ldots+a_f\xi_f \qquad (mod.\ \mathfrak{p}),$$

can be uniquely determined with respect to *mod. p*. Hereby, without losing generality, we may suppose $a_1\not\equiv 0$ (*mod. p*). Then, we can determine an integer ξ_0, such that

$$\rho\left(\sum_{2,f}^{i} c_i\xi_i\right)+\left(\sum_{2,f}^{i} c_i\xi_i\right)^p+c_o\xi_o\not\equiv 0 \qquad (mod.\ \mathfrak{p}),$$

$$c_o,\ c_i\equiv 0,\ 1,\ 2,\ \ldots\ldots,\ p-1 \qquad (mod.\ p),$$

excluding the combination $c_o\equiv c_2\equiv c_3\equiv\ldots\ldots\equiv c_f\equiv 0 \quad (mod.\ p)$.

This premised, let us consider the product

$$R=(1+\xi_o\pi^{d+k})^{e'}\prod_{a}\prod_{i}(1+\xi_i\pi^{a})^{e'_{ai}},$$

$$a=1,\ 2,\ \ldots\ldots,\ d+k-1, \quad a\not\equiv 0\ (mod.\ p),$$

$$i=1,\ 2,\ \ldots\ldots,\ f,$$

$$e'_{ai}=0,\ 1,\ 2,\ \ldots\ldots,\ e_{ai}-1,$$

$$e'=0,\ 1,\ 2,\ \ldots\ldots,\ e_{d+k}-1,$$

where e_{ai} and e_{d+k} denote the exponents, to which $1+\xi_i\pi^a$ and $1+\xi_o\pi^{d+k}$ belong $(mod.\ \mathfrak{p}^n)$.

In R there are $fd+1$ different numbers of the form $1+\xi\pi^a$, and it can be shewn that all the elements of $\mathfrak{A}$ are represented by R, each being repeated $\frac{e_{k1}}{p}$ times. Hence we conclude that $r\leqq fd+1$.

Next, we can proceed a step further and shew that $r=fd+1$ exactly. This is done by shewing that, if we reject any one of the $fd+1$ numbers in R, the number of elements of $\mathfrak{A}$ represented by means of the remaining fd numbers is always less than the order of $\mathfrak{A}$.

The same reasoning as above, with but slight modification, also applies to the case $k\equiv 0$ $(mod.\ p)$, giving exactly the same result.

Lastly, it can be shewn that the congruence (4) can be replaced by

$$p+x^{p-1}\equiv 0 \qquad (mod.\ \mathfrak{p}^{d+1}),$$

and that d is necessarily divisible by $p-1$, if this congruence has a solution.

Thus, including all the results hitherto obtained concerning the group $\mathfrak{A}$, we can state our final result as follows:

$\mathfrak{A}$ is an Abelian group, whose invariants consist of powers of p, and whose rank is given by

$$\left.\begin{array}{lll} r=fd+1 \text{ or } fd, & \text{if} & d+k<n, \\ \quad \text{according as the congruence } p+x^{p-1}\equiv 0 & & \\ \quad (\text{mod. } \mathfrak{p}^{d+1}) \text{ has a solution or not,} & & \\ r=fd, & \text{if} & n=d+k, \\ r=f\left(n-\left[\frac{n}{p}\right]\right) & \text{if} & 1<n<d+k, \\ r=1, & \text{if} & n=1. \end{array}\right\} \quad (5)$$

Application.—The problem of determining all the ideals that admit of primitive roots was solved by A. Wiman (Öfversigt af Svenska Vetenskapsakademiens Förhandlingar, 56) and by J. Westlund (Mathematische Annalen, Bd. 71). Here, we can solve the same problem as an application of the above result.

Now, it can easily be seen that the necessary and sufficient condition in order that $\mathfrak{p}^n$ may admit of primitive roots is $r=1$. Applying the result (5) in this condition, we arrive at the following conclusions:

Unless $\mathfrak{p}$ *be a prime ideal of the first degree, there exists no primitive root of* $\mathfrak{p}^n$ *when* $n>1$.

Let $\mathfrak{p}$ *be a prime ideal of the first degree and suppose that its norm* p *is divisible by* $\mathfrak{p}^d$ *but not by* $\mathfrak{p}^{d+1}$, *then there exist primitive roots of* $\mathfrak{p}^n$, *when*

(1) $p>2$, $d=1$, $n\geqq 1$,
(2) $p>2$, $d>1$, $n=1, 2$,
(3) $p=2$, $d=1$, $n=1, 2$,
(4) $p=2$, $d>1$, $n=1, 2, 3$,

but in no other cases.