If, on the other hand,

$$| A_n - A_{n+p} | < S_n$$

$$\begin{aligned}(A_n + A_{n+1} + \cdots + A_{n+p}) &- A_nA_{n+1}\cdots A_{n+p}\\ &= | A_n - A_{n+1} | + | A_n - A_{n+2} | + \cdots + | A_n - A_{n+p} |\\ &< S_n + S_n + \cdots + S_n\\ &< S_n.\end{aligned}$$

In the limit when p increases indefinitely

$$(A_n + A_{n+1} + \cdots) - A_nA_{n+1}\cdots < S_n.$$

The left member is a sequence decreasing with n and it must have the limit 0 for S_n has the limit 0. Consequently the sequence A_n has a limit according to Borel.

RICE INSTITUTE,
HOUSTON, TEXAS.

ON THE PRINCIPAL UNITS OF AN ALGEBRAIC DOMAIN $k(\mathfrak{p}, \alpha)$.

BY DR. G. E. WAHLIN.

(Read before the American Mathematical Society, April 10, 1914.)

Introduction.

THE following paper is the result of an investigation of a problem connected with the representation of the algebraic numbers in the form $\pi^\alpha\omega^\beta e^\gamma$.*

Throughout the discussion I shall use the following notation. By p I mean a rational prime and by $\mathfrak{p}$ any prime divisor of p. f is the degree of $\mathfrak{p}$, i. e., $N(\mathfrak{p}) = p^f$ and $\mathfrak{p}^\sigma$ is the highest power of $\mathfrak{p}$ contained in p. By π I mean a prime number of the domain $k(\mathfrak{p}, \alpha)$, where α is an arbitrary algebraic number. The numbers of $k(\mathfrak{p}, \alpha)$ are then of the form $a_\rho\pi^\rho + a_{\rho+1}\pi^{\rho+1} + \cdots$. A number in which $\rho = 0$ and a_ρ is relatively prime to $\mathfrak{p}$ is called a unit and in particular if $a_\rho = 1$ it is called a principal unit.

* Hensel, *Crelle's Journal*, vol. 145.

The Equation $x^{p^n} - E = 0(\mathfrak{p})$.

For the present we shall let E be any unit of $k(\mathfrak{p}, \alpha)$. From the general theory of algebraic numbers* we know that there exists a certain rational integer μ such that the equation

$$(1) \qquad x^{p^n} - E = 0(\mathfrak{p})$$

has a solution in $k(\mathfrak{p}, \alpha)$ if the congruence

$$(2) \qquad x^{p^n} - E \equiv 0 \bmod \mathfrak{p}^{\mu+1}$$

has a solution in this domain. The present section is devoted to the computation of the value of μ.

This determination of μ can be accomplished by making use of a known theorem.†

Since E is a unit, it follows that any solution E_1 of (2) is also relatively prime to $\mathfrak{p}$. Therefore if we put $F(x) = x^{p^n} - E$ and denote its ith derivative by $F^{(i)}(x)$ we see that the order of

$$F^{(i)}(E_1)/i! = \frac{p^n(p^n - 1)\cdots(p^n - i + 1)}{i!} E_1^{p^n - i}$$

is the same as the order of $C^{(i)} = p^n!/i!(p^n - i)!$.

The order of $m!$ in $k(p)$ is $(m - S_m)/(p - 1)$‡ where S_m is the sum of the coefficients in the reduced p-adic representation of m. Hence since $S_{p^n} = 1$ we know that in $k(p)$ the order of $C^{(i)}$ is

$$\frac{p^n - 1}{p - 1} - \frac{i - S_i}{p - 1} - \frac{p^n - i - S_{p^n - i}}{p - 1} = \frac{S_i + S_{p^n - i} - 1}{p - 1}.$$

Let us denote the order of i by ρ and suppose that in its reduced p-adic representation $i = a_\rho p^\rho + a_{\rho+1}p^{\rho+1} + \ldots + a_{n-1}p^{n-1}$. Since $i \leqq p^n$ the representation cannot have a term containing a higher power of p than p^{n-1}, excepting in the case where $i = p^n$ and then the order of $C^{(i)}$ is zero. The number p^n can be written in the form $p \cdot p^\rho + (p - 1)p^{\rho+1} + \ldots + (p - 1)p^{n-1}$, and hence

$$p^n - i = (p - a_\rho)p^\rho + (p - a_{\rho+1} - 1)p^{\rho+1} + \ldots + (p - a_{n-1} - 1)p^{n-1},$$

* Hensel, Theorie der algebraischen Zahlen, Kap. 4, § 4. (The method there used by Professor Hensel can be extended to any domain.)

† Ibid., Kap. 4, § 4, pp. 72–74.

‡ Ibid., p. 111.

which as is easily seen is also in the reduced form. Hence

$$S_i = a_\rho + a_{\rho+1} + \dots + a_{n-1}$$

and

$$S_{p^n-i} = p - a_\rho + p - a_{\rho+1} - 1 + \dots + p - a_{n-1} - 1$$

and

$$S_i + S_{p^n-i} = (n - \rho)p - (n - \rho - 1),$$

whence we have

$$(S_i + S_{p^n-i} - 1)/(p - 1) = n - \rho.$$

Since $\mathfrak{p}^\sigma$ is the highest power of $\mathfrak{p}$ in p we see now that $\rho^{(i)}$, the order of $C^{(i)}$ in $k(\mathfrak{p}, \alpha)$, is equal to $\sigma(n - \rho)$.

If we now form the expression $(i\rho' - \rho^{(i)})/(i - 1)$* we see that this is equal to

$$\sigma \frac{ni - (n + \rho)}{i - 1} = \sigma \left(n + \frac{\rho}{i - 1} \right)$$

since $\rho' = n\sigma$. The value of μ sought is the largest integer which is less than or equal to

$$\max \sigma \left(n + \frac{\rho}{i - 1} \right) \text{for } i = 2, 3, \dots, p^n.$$

Since n and σ are independent of i, it is evident that this maximum occurs when $\rho/(i - 1)$ is maximum and we shall therefore determine the value of i for which such is the case.

If we first consider the values of i of a given order ρ it is clear that $\rho/(i - 1)$ is maximum when i is minimum and hence when $i = p^\rho$ and the maximum value of $\rho/(p^\rho - 1)$ as ρ varies over the numbers $1, 2, \dots n$ is therefore the same as the maximum value of $\rho/(i - 1)$ as i varies over the numbers $2, 3, \dots p^n$. We note here that for $1 < i < p$, $\rho = 0$ and $\rho/(i - 1) = 0$.

Let us now turn our attention to the expression

$$\psi(\rho) = \rho/(p^\rho - 1).$$

Differentiating, we have

$$\psi'(\rho) = \frac{p^\rho - 1 - \rho p^\rho \log p}{(p^\rho - 1)^2} = \frac{p^\rho(1 - \rho \log p) - 1}{(p^\rho - 1)^2}.$$

* Hensel, Theorie der algebraischen Zahlen, Kap. 4, § 4.

If $p > 2$, $\log p > 1$ and hence, since $\rho \geqq 1$, $\psi'(\rho) < 0$. The function $\psi(\rho)$ is therefore a decreasing function for $\rho \geqq 1$ and the maximum value in the required interval therefore occurs when $\rho = 1$. This maximum value is $1/(p-1) > 0$ and since for $1 < i < p$, $\rho/(i-1) = 0$, $1/(p-1)$ is the maximum value of $\rho/(i-1)$. If $p = 2 < e < 4$, since $e^{1/2} < 2$ we have $\frac{1}{2} < \log 2 < 1$ and hence for $\rho \geqq 2$ we have $\rho \log 2 > 1$ and as before $\psi'(\rho) < 0$. Therefore for $\rho \geqq 2$, $\psi(\rho)$ is decreasing and must be maximum, in the given interval, when $\rho = 2$. Hence when ρ takes the values $1, 2, \ldots, n$, $\psi(\rho)$ must be maximum either at $\rho = 1$ or $\rho = 2$.

$$\text{For } \rho = 1,\ \psi(\rho) = \frac{1}{2-1} = 1.$$

$$\text{For } \rho = 2,\ \psi(\rho) = \frac{2}{4-1} = \tfrac{2}{3}$$

and hence, as in the preceding case, the maximum value occurs when $\rho = 1$ and again the maximum is $1/(p-1)$. Therefore

$$\max\left(\frac{i\rho' - \rho^{(i)}}{i-1}\right) = \sigma\left\{n + \frac{1}{p-1}\right\}$$

and if we put $k = [\sigma/(p-1)]$ we have

$$\mu = n\sigma + k.$$

A Certain Residue Group in $k(\mathfrak{p}, \alpha)$.

We shall suppose that the domain $k(\mathfrak{p}, \alpha)$ contains all the p^rth roots of unity while no primitive p^{r+1}th root of unity is contained in it. We shall in this discussion need the number μ of the preceding section for the special case when $n = r + 1$ and shall therefore put $\mu = r\sigma + \sigma + k \geqq 1 + k$.

Every principal unit E of our domain is, modulo $\mathfrak{p}^{\mu+1}$, congruent to one and only one of the $p^{\mu f}$ units $1 + a_1\pi + a_2\pi^2 + \cdots + a_\mu\pi^\mu$ where the a_i vary independently over the p^f numbers of a complete residual system modulo $\mathfrak{p}$. Since the product and quotient of two principal units are principal units it is evident that these residues and hence the E's themselves form an abelian group of order $p^{\mu f}$ with respect to the modulus $\mathfrak{p}^{\mu+1}$. This group we shall denote by G. Since G is an abelian group we know that it is the product of cyclic groups. These cyclic groups we shall denote by $C_1, C_2, \cdots C_h$, and the order of C_i we shall denote by p^{r_i}. (The order must be a power of p since it is a divisor of $p^{\mu f}$.) We shall moreover assume that $r_1 \geqq r_2 \geqq r_3 \geqq \cdots \geqq r_h$.

Let m be that one of the numbers $1, 2, \cdots, h$ such that $r_m > r \geqq r_{m+1}$ or if $r_h > r$, $h = m$. We shall first see that r cannot be greater than r_1. G cannot contain an element of period greater than p^{r_1} and hence if R is a primitive p^rth root of unity, it is an element of G and therefore $R^{p^{r_1}} \equiv 1 \bmod p^{\mu+1}$ and hence also modulo p^{k+1}, since $\mu \geqq k+1$. But since $R^{pr_1} \equiv 1 \bmod p^{k+1}$ it is an exponential unit* and we can therefore write $R^{p^{r_1}} = e^{\gamma}(\mathfrak{p})$. By raising both members of this equation to the power p^{r-r_1} we have $e^{\gamma p^{r-r_1}} = 1(\mathfrak{p})$ and hence $\gamma p^{r-r_1} = 0\ (\mathfrak{p})$ and $\gamma = 0\ (\mathfrak{p})$. But then $R^{p^{r_1}} = e^{\gamma} = 1(\mathfrak{p})$ and since R is a primitive p^rth root of unity this is impossible unless $r \leqq r_1$.

In the same way it follows that for $t < r$, $R^{p^t} \not\equiv 1 \bmod \mathfrak{p}^{\mu+1}$ and hence R and its powers form a cyclic subgroup of G, of order p^r.

If $r = r_1$ it is evident, from the proof of the theorem, that every abelian group can be written as the product of cyclic subgroups,† that we can put $C_1 = C$ where C is the cyclic group generated by R. If however $m > 1$ we shall next see that no power of R excepting R^{p^r} is modulo $p^{\mu+1}$ congruent to a number in the product $C_1 \cdot C_2 \cdots C_m$.

Let us denote by E_i any generator of the cyclic group C_i and let us suppose that

$$E_1^{n_1 p^{\lambda_1}} \cdot E_2^{n_2 p^{\lambda_2}} \cdots E_m^{n_m p^{\lambda_m}} \equiv R^{n p^{\lambda}} \bmod \mathfrak{p}^{\mu+1}, \tag{3}$$

where we assume that $n, n_1, n_2, \cdots, n_m$ are rational integers relatively prime to p and $0 \leqq \lambda < r$ and $0 \leqq \lambda_i < r_i$ $(i = 1, 2, \cdots m)$. By raising both members of (3) to the power $p^{r-\lambda}$ we have

$$E_1^{n_1 p^{\lambda_1 + r - \lambda}} \cdot E_2^{n_2 p^{\lambda_2 + r - \lambda}} \cdots E_m^{n_m p^{\lambda_m + r - \lambda}} \equiv 1 \bmod \mathfrak{p}^{\mu+1} \tag{4}$$

and from the fact that G is an abelian group and $C_1, C_2, \cdots, C_h$ the base we know that this is possible when and only when the exponent of each E_i is divisible by p^{r_i}. Hence $\lambda_i + r - \lambda \geqq r_i$ and since for $i \leqq m$, $r_i > r$, we have $\lambda_i \geqq r_i - r + \lambda > \lambda$. If we now let $l = \min(\lambda_1, \lambda_2, \cdots \lambda_m)$ and put

$$E = E_1^{n_1 p^{\lambda_1 - l}} \cdot E_2^{n_2 p^{\lambda_2 - l}} \cdots E_m^{n_m p^{\lambda_m - l}}$$

* Hensel, *Crelle's Journal*, vol. 145, pp. 94–95.

† Weber, Algebra, vol. II, pp. 3, 38–45.

we can write (3) in the form

$$E^{p^l} \equiv R^{np^\lambda} \bmod \mathfrak{p}^{\mu+1}.$$

Since $\lambda_i > \lambda$ it follows that $l > \lambda$.

If we now put $t =$ minimum $(l, r+1)$ and use the result of the first part of this paper we can from the last congruence conclude that the equation

$$x^{p^t} = R^{np^\lambda}\ (\mathfrak{p}) \tag{5}$$

has a solution in $k(\mathfrak{p}, \alpha)$. Let us denote this solution by $\mathfrak{A}$. Then $\mathfrak{A}^{p^{t+r-\lambda}} = 1(\mathfrak{p})$. Since R is a primitive p^rth root of unity and n is relatively prime to p, R^n is also a primitive p^rth root of unity and hence

$$\mathfrak{A}^{p^{t+r-\lambda-1}} = (R^n)^{p^{r-1}} \mp 1(\mathfrak{p}).$$

$\mathfrak{A}$ is therefore a primitive $p^{t+r-\lambda}$th root of unity which is contained in $k(\mathfrak{p}, \alpha)$.

But we have seen that $l > \lambda$ and have assumed that $\lambda < r$ and hence $r + 1 > \lambda$ and consequently $t = \min (r+1, l) > \lambda$ and $t + r - \lambda > r$. But this contradicts our assumption that $k(\mathfrak{p}, \alpha)$ contains no primitive p^{r+1}th root of unity.

Hence (3) is impossible when $\lambda < r$ and hence no power of R excepting $R^{p^r} = R^0$ or power of R^{p^r} can be congruent, modulo $p^{\mu+1}$ to the left hand member of (3).

From this it now follows that in the construction of the base of G we can put $C_{m+1} = C$ and hence have

$$G = C_1 \cdot C_2 \cdots C_m \cdot C \cdot C_{m+2} \cdots C_h.$$

If we put $G_1 = C_1 \cdot C_2 \cdots C_m \cdot C_{m+2} \cdots C_h$, this is also an abelian group and

$$G = G_1 \cdot C. \tag{6}$$

The result may now be summed up in the following

THEOREM: *If the domain $k(\mathfrak{p}, \alpha)$ contains a primitive p^rth root of unity but no primitive p^{r+1} th root of unity, and if we denote by μ the number $r\sigma + \sigma + k$ where σ is the exponent of the prime divisor $\mathfrak{p}$ in p and $k = [\sigma/(p-1)]$, then the abelian group consisting of the principal units of $k(\mathfrak{p}, \alpha)$ modulo $\mathfrak{p}^{\mu+1}$ is the product of an abelian group G_1 and the cyclic group C whose elements are the p^rth roots of unity.*

UNIVERSITY OF ILLINOIS.