A NOTE ON UNITS OF ALGEBRAIC NUMBER FIELDS

TOMIO KUBOTA

We shall prove in the present note a theorem on units of algebraic number fields, applying one of the strongest formulations, be Hasse [3], of Grunwald's existence theorem.

THEOREM. *Let k be an algebraic number field, l a prime number, E_k the group of units of k and H a subgroup of E_k containing all l-th powers of elements of E_k. Assume that, for every $\eta \in H$, $k(\sqrt[l]{\eta})$ is always ramified over k whenever k contains an l-th root ζ_l ($\neq 1$) of unity. Then there are infinitely many cyclic extentions K/k of degree l with following properties:*

a) $N_{K/k}E_K = H$, where E_K is the group of units of K.

b) if an ideal $\mathfrak{a}$ of k is principal in K, then $\mathfrak{a}$ is principal in k.

Proof. Denote by B the group of elements β of $k^{\times}$[1)] such that (β) is an l-th power of some ideal in k, and denote by $\mathfrak{C}$ the group of ideal classes of k. Let W be the group generated by H and all l-th powers of elements of $k^{\times}$, and let

$$B = B_0 \supset B_1 \supset \ldots \supset B_{s-1} \supset B_s = W \tag{1}$$

be a sequence of subgroups of B such that $(B_{i-1} : B_i) = l$ for every $i\,(1 \leqq i \leqq s)$. As preliminaries, we shall prove that, for every i, there is a prime ideal $\mathfrak{p}_i$ of k which satisfies the following conditions: i) an element γ of B_{i-1} is an l-th power of some element in the $\mathfrak{p}_i$-adic field $k_{\mathfrak{p}_i}$ if and only if γ belongs to B_i. ii) The set of ideal classes of $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ contains an independent base of $\mathfrak{C}/\mathfrak{C}^l$. Assume first that $k \not\ni \zeta_l$. Set $k_l = k(\zeta_l)$. Let $\Lambda = k_l(\sqrt[l]{B})$ be the field obtained from k_l by adjoining all l-th roots of elements of B. Then Λ contains no cyclic extention of degree l over k. For, if L/k is cyclic of degree l, and $L \subset \Lambda$, then k_lL/k is abelian, k_lL/k_l is cyclic of degree l and therefore $k_lL = k_l(\sqrt[l]{\beta})$, where

Received March 3, 1955.

1) We shall use this notation to stand for the multiplicative group of non-zero elements of a field.

β is an element of B. But this is impossible because $k_l(\sqrt[l]{\beta})/k$ is apparently non-abelian. Thus we see that, if Z_l is the class field over $\mathfrak{C}^l$, then

$$k_l(\sqrt[l]{B}) \cap Z_l = k. \tag{2}$$

Let β_i $(1 \leqq i \leqq s)$ be an element of B_{i-1} which does not belong to B_i. Set $k_l(\sqrt[l]{\beta_i}) = k_i$, $k_l(\sqrt[l]{B_i}) = k_i'$. Then since W contains all l-th powers of elements of $k^\times$ and since every element of k, being an l-th power of some element in k_l, is already an l-th power of some element in k,[2] we have $k_i \cap k_i' = k_l$. Therefore it gives infinitely many prime ideals $\mathfrak{q}_i$ of k_l which are of degree 1 over k and such that

$$\left(\frac{k_i/k_l}{\mathfrak{q}_i}\right) \neq 1, \qquad \left(\frac{k_i'/k_l}{\mathfrak{q}_i}\right) = 1. \tag{3}$$

Let $\mathfrak{F}_i$ be the set of prime ideals $\mathfrak{p}_i$ of k divisible by some $\mathfrak{q}_i$. Then since $k_{\mathfrak{p}_i} = k_{l,\mathfrak{q}_i}$, the condition i) is an immediate consequence of (3) and the theory of Kummer extentions. On the other hand, it is easily seen that $\mathfrak{F}_i$ contains a *prime ideal clase*[3] of k with respect to A. To prove the condition ii), it is sufficient to show that every class of ideals of k modulo $\mathfrak{C}^l$ contains a prime ideal of $\mathfrak{F}_i$. But this is actually the case because it follows from (2) that every *prime ideal class* of k with respect to A intersets with every class of ideals modulo $\mathfrak{C}^l$. Now, assume that $k \ni \zeta_l$. Then every cyclic subfield over k of Z_l is of the form $k(\sqrt[l]{\beta})$, where $\beta \in B$. But the assumption in the theorem implies $\beta \notin W$. Therefore the elements $\beta_1, \ldots, \beta_s$ $(\beta_i \in B_{i-1}, \notin B_i)$ can be so chosen that we have $Z_l \subset k(\sqrt[l]{\beta_1}, \ldots, \sqrt[l]{\beta_s})$. Set, as before, $k_i = k(\sqrt[l]{\beta_i})$, $k_i' = k(\sqrt[l]{B_i})$. Then our assertion follows immediately whenever we take $\mathfrak{p}_i$ with $\left(\frac{k_i/k}{\mathfrak{p}_i}\right) \neq 1$, $\left(\frac{k_i'/k}{\mathfrak{p}_i}\right) = 1$.

Making use of the condition i), we can conclude that, for every i $(1 \leqq i \leqq s)$, there is a character χ_i of $k_{\mathfrak{p}_i}^\times$ which is of order l and such that

$$\chi_i(\beta_i) \neq 1, \qquad \chi_i(\beta_i) = 1. \tag{4}$$

Now, it follows from Grunwald's theorem that there are infinitely many cyclic extention K/k of degree l with following properties: I) Besides the prime ideals $\mathfrak{p}_i$, it gives one and only one prime ideal and no infinite place of

[2] See Hasse [3], § 1, Satz 1.

[3] See Hasse [2], II, § 24.

k which ramifies in K.[4] ii) There is an isomorphism φ between the Galois group of K/k and the group of all l-th roots of unity such that

$$(5) \qquad \left(\frac{\alpha,\ K/k}{\mathfrak{p}_i}\right)^{\varphi} = \chi_i(\alpha),$$

where α is an arbitrary element of $k^{\times}$. We propose to prove that the field K has the required properties.

Let $\mathfrak{a}$ be an ideal of k. Assume that $\mathfrak{a} = (A)$, where $A \in K$. Then we have $\mathfrak{a}^l = N_{K/k}\mathfrak{a} = (N_{K/k}A)$. On the other hand, it follows from (4), (5) that $N_{K/k}A \in W$. This means that $(N_{K/k}A) = (\alpha)^l$ for an element α of k, whence $\mathfrak{a} = (\alpha)$ and the property b) is verified. To prove a), we make the following observation. Since from (4) and (5) follows, as before, $H \supseteqq N_{K/k}E_K$, it suffices to prove that

$$(6) \qquad (E_k : N_{K/k}E_K) \leqq (E_k : H)$$

Denote by $\mathfrak{a}$ the group of ideals of k, by (α) the group of principal ideals of k, by $\mathfrak{A}_0$ the group of ambiguous ideals of K/k and by (A_0) the group of principal, ambiguous ideals of K/k. Let further E_0 be the group of units E_0 of K such that $N_{K/k}E_0 = 1$, and let σ be a generator of the Galois group of K/k. Then we obtain easily the following relations:

$$(7) \qquad (\mathfrak{A}_0 : \mathfrak{a})/(\mathfrak{A}_0 : (A_0)\mathfrak{a}) = ((A_0) : (\alpha))/((A_0) \cap \mathfrak{a} : (\alpha)),$$

$$(8) \qquad (\mathfrak{A}_0 : \mathfrak{a}) = l^{s+1},$$

$$(9) \qquad (A_0)/(\alpha) \cong E_0/E_K^{1-\sigma}.$$

Since the condition ii) is satisfied, we may assume that the set of ideal classes of $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ is an independent base of $\mathfrak{C}/\mathfrak{C}^l$, where t is determined by $l^t = (\mathfrak{C} : \mathfrak{C}^l)$. Now assume that $\mathfrak{p}_i = \mathfrak{P}_i^l$ in K and that $\mathfrak{P}_1^{\nu_1} \ldots \mathfrak{P}_t^{\nu_t} \in (A_0)\mathfrak{a}$. Then we have $\mathfrak{P}_1^{l\nu_1} \ldots \mathfrak{P}_t^{l\nu_t} = \mathfrak{p}_1^{\nu_1} \ldots \mathfrak{p}_t^{\nu_t} \in (A_0)^l\mathfrak{a}^l \subset (\alpha)\mathfrak{a}^l$; therefore every $\mathfrak{p}_i^{\nu_i}$ belongs to an ideal class of $\mathfrak{C}^l$. Thus we have

$$(10) \qquad (\mathfrak{A}_0 : (A_0)\mathfrak{a}) \geqq l^t.$$

Furthermore, the property b) implies

$$(11) \qquad ((A_0) \cap \mathfrak{a} : (\alpha)) = 1$$

[4] See Hasse [3], "Starker Existenzsatz (zykilscher Fall mit Primzahlpotenzordnung)" at p. 45, especially its "Genauer"-part. In the case of prime degree l, this theorem is applicable without any extention of the set $\mathfrak{O}$, as we learn from its proof.

and finally we can conclude by means of Herbrand's lemma[5] that

$$(E_0 : E_K^{1-\sigma}) = l(E_k : N_{K/k}E_K). \tag{12}$$

It follows from (7), (8), (9), (10), (11) and (12) that $l^{s+1}/l^t \geqq l(E_k : N_{K/k}E_K)$, whence $(E_k : N_{K/k}E_K) \leqq l^{s-t}$, which shows that (6) is true. The theorem is thereby completely proved.

COROLLARY. *k and E_k being the same as in the theorem, let l be a prime number which does not divide either the class number of k or the number of roots of unity in k, and let H be any subgroup of E_k containing all l-th powers of elements of E_k. Then there are infinitely many cyclic extentions K/k of degree l with the properties a) and b).*

REFERENCES

[1] Chevalley, C., Class field theory, Nagoya University (1953/54).
[2] Hasse, H., Bericht, I (1926), I *a* (1927) and II (1930).
[3] Hasse, H., Zum Existenzsatz von Grunwald in der Klassenkörpertheorie, J. Reine Angew. Math., **188** (1950), 40-64.
[4] Whaples, G., Non-analytic class field theory and Grunwald's theorem, Duke Math. J., vol. **9** (1942), 455-473.

Mathematical Institute,
Nagoya University

5) See Chevalley [1], § 10.