COLLOQUIUM MATHEMATICUM

VOL. XX 1969 FASC. 2

ON PRIME IDEALS WITH PRESCRIBED VALUES OF CHARACTERS OF PRIME DEGREE

BY

JAN WÓJCIK (WARSZAWA)

Kummer proved in 1859 the following

THEOREM. *Let k be an algebraic number field containing a primitive l-th root of unity, and l a prime. Let $a_1, \dots, a_t$ be integers of k such that $a_1^{m_1} a_2^{m_2} \dots a_t^{m_t}$ is an l-th power in k only if all m_i's are divisible by l. For any given l-th roots of unity $\gamma_1, \gamma_2, \dots, \gamma_t$ there exist infinitely many prime ideals $\mathfrak{P}$ in k satisfying for some rational integer $m = m(\mathfrak{P})$ prime to l the relations*

$$\left\{\frac{a_1}{\mathfrak{P}}\right\}^m = \gamma_1, \quad \left\{\frac{a_2}{\mathfrak{P}}\right\}^m = \gamma_2, \quad \dots, \quad \left\{\frac{a_t}{\mathfrak{P}}\right\}^m = \gamma_t,$$

where $\{a/\mathfrak{P}\}$ is the l-th power residue symbol.

An analytical proof of this theorem is given in [3] (Satz 152), a proof using p-adic analysis can be obtained from the modern class field theory (see [4], Corollary 8.8).

The aim of this paper is to give a short and elementary proof. In the sequel residue means an l-th power residue.

LEMMA 1. *Let $a_1, \dots, a_s$ satisfy the assumption of the theorem. There exists a prime ideal $\mathfrak{P}$ in k such that $\mathfrak{P} \nmid l a_1 a_2 \dots a_s$ and that $a_1, a_2, \dots, a_{s-1}$ are residues while a_s is a non-residue.*

Proof. Let $K = k(\sqrt[l]{a_1}, \sqrt[l]{a_2}, \dots, \sqrt[l]{a_{s-1}})$, and $L = k(\sqrt[l]{a_1}, \sqrt[l]{a_2}, \dots, \sqrt[l]{a_s})$. Clearly,

$$L = K(\sqrt[l]{a_s}). \tag{1}$$

By the assumption of the theorem we have $(K : k) = l^{s-1}$, $(L : k) = l^s$, $(L : K) = l$ (see [2], p. 87-88). The extension L/K is thus cyclic of prime degree. Let δ be its discriminant. It is well known that $\delta = f^{l-1}$, where f is an ideal in K. Let A be the group of all ideal classes in K mod$f$ prime to f, H_f the group of these ideal classes in K mod$f$ which contain the relative norm of an ideal in L, finally, H_1 the group of these ideal classes

in K mod$f$ which contain the norm of a principal ideal in L. The well known inequality (see [2], p. 22-24)

$$(H_f : H_1) \leqslant a \leqslant \frac{1}{l}(A : H_1),$$

where a is the number of ambiguous classes, implies

$$|H_f| \leqslant \frac{1}{l}|A|. \tag{2}$$

Suppose that the assertion of Lemma 1 does not hold. Let $\mathfrak{P}$ be any prime ideal in K not dividing $la_1a_2\ldots a_s$, $\mathfrak{p}$ the prime ideal in k divisible by $\mathfrak{P}$. We distinguish two cases:

Case 1: $\{a_s/\mathfrak{p}\} = 1$. Then a_s is a residue mod $\mathfrak{P}$ and by (1) and the decomposition law in a cyclic field of prime degree we have $\mathfrak{P} = N_{L/K}Q$, where Q is a prime ideal in L.

Case 2: $\{a_s/\mathfrak{p}\} \neq 1$. Hence by the assumption $\{a_i/\mathfrak{p}\} \neq 1$ for some $i < s$.

Clearly, $\{a_i/\mathfrak{p}\}^c = \{a_s/\mathfrak{p}\}$ for some integer c. This implies the solvability of the congruences $a_i^c x^l \equiv a_s \bmod \mathfrak{p}$, $x \in k$, and $y^l \equiv a_s \bmod \mathfrak{P}$, $y = x\sqrt[l]{a_i^c} \in K$.

As before, we have $\mathfrak{P} = N_{L/K}Q$, where Q is a prime ideal in L. On the other hand, each ideal class mod$f$ contains an ideal $\mathfrak{a}$ prime to $la_1a_2\ldots a_s$ (see [2], p. 63). By factorizing $\mathfrak{a}$ into prime ideals we get $\mathfrak{a} = N_{L/K}(\Pi Q)$, where Q are prime ideals in L. It follows that each ideal class mod$f$ contains a relative norm of an ideal in L, thus $H_f = A$ contrary to (2). The obtained contradiction completes the proof of Lemma 1.

LEMMA 2. *Let $a_1, \ldots, a_s$ satisfy the assumptions of the theorem. For any given l-th roots of unity $\gamma_1, \gamma_2, \ldots, \gamma_s$ there exists a prime ideal $\mathfrak{p}$ in k satisfying, for some rational integer m prime to l, the relations*

$$\left\{\frac{a_1}{\mathfrak{p}}\right\}^m = \gamma_1, \quad \left\{\frac{a_2}{\mathfrak{p}}\right\}^m = \gamma_2, \quad \ldots, \quad \left\{\frac{a_s}{\mathfrak{p}}\right\}^m = \gamma_s.$$

Proof. Without loss of generality we can assume that $\gamma_j = 1$ $(1 \leqslant j \leqslant t)$, $\gamma_j \neq 1$ $(t < j \leqslant s)$.

Case 1: $t = s$. In virtue of a result of [1] there exists a prime ideal $\mathfrak{p}$ in k not dividing $la_1a_2\ldots a_s$ such that all the congruences $x_1^l \equiv a_1 \bmod \mathfrak{p}$, $x_2^l \equiv a_2 \bmod \mathfrak{p}$, $\ldots$, $x_s^l \equiv a_s \bmod \mathfrak{p}$, are solvable in k.

Case 2: $t < s$. Let

$$\gamma_s^{-1} = \gamma_j^{\xi_j}, \quad t < j < s. \tag{3}$$

Clearly, $\xi_j \not\equiv 0 \bmod l$. Hence

$$\alpha_1^{m_1} \dots \alpha_t^{m_t} (\alpha_{t+1}^{\xi_{t+1}} \alpha_s)^{m_{t+1}} \dots (\alpha_{s-1}^{\xi_{s-1}} \alpha_s)^{m_{s-1}} \alpha_s^{m_s}$$
$$= \alpha_1^{m_1} \dots \alpha_t^{m_t} \alpha_{t+1}^{\xi_{t+1} m_{t+1}} \dots \alpha_{s-1}^{\xi_{s-1} m_{s-1}} \alpha_s^{m_{t+1}+\dots+m_{s-1}+m_s}$$

is an l-th power in k only if all m are divisible by l. By Lemma 1 there exists a prime ideal $\mathfrak{P}$ in k such that $\mathfrak{P} \nmid l a_1 a_2 \dots a_s$, and $a_1, \dots, a_t$, $a_{t+1}^{\xi_{t+1}} a_s, \dots, a_{s-1}^{\xi_{s-1}} a_s$ are residues mod $\mathfrak{P}$ while a_s is not a residue mod $\mathfrak{P}$. Hence for some integer m prime to l we have

$$\left\{\frac{a_s}{\mathfrak{P}}\right\}^m = \gamma_s, \quad \left\{\frac{a_j}{\mathfrak{P}}\right\}^{\xi_j m} \left\{\frac{a_s}{\mathfrak{P}}\right\}^m = 1, \quad t < j < s.$$

Hence and from (3) we get

$$\left\{\frac{a_j}{\mathfrak{P}}\right\}^{\xi_j m} = \gamma_j^{\xi_j} \quad (t < j < s).$$

Since $\xi_j \not\equiv 0 \bmod l$, we obtain $\{a_j/\mathfrak{P}\}^m = \gamma_j$ $(t < j < s)$. The proof is complete.

Proof of the theorem. Let $\mathfrak{P}_0, \mathfrak{P}_1, \dots, \mathfrak{P}_{r-1}$ $(r \geqslant 0)$ be prime ideals in k satisfying the assertion of the theorem. We shall construct a new prime ideal $\mathfrak{P}_r$ with the same property. Let $M = (N\mathfrak{P}_0\mathfrak{P}_1 \dots \mathfrak{P}_{r-1})^l$. By Lemma 2 there exists a prime ideal $\mathfrak{P}_r$ such that for some integer m prime to l we have

$$\left\{\frac{a_1 M}{\mathfrak{P}_r}\right\}^m = \gamma_1, \quad \left\{\frac{a_2 M}{\mathfrak{P}_r}\right\}^m = \gamma_2, \quad \dots, \quad \left\{\frac{a_s M}{\mathfrak{P}_r}\right\}^m = \gamma_s.$$

Clearly $\mathfrak{P}_r$ satisfies the assertion of the theorem and is different from $\mathfrak{P}_0, \mathfrak{P}_1, \dots, \mathfrak{P}_{r-1}$. The proof is complete.

REFERENCES

[1] L. Fjellstedt, *Bemerkungen über gleichzeitige Lösbarkeit von Kongruenzen*, Arkiv för Matematik 3 (1958), p. 193-198.

[2] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I: Klassenkörpertheorie, Teil Ia: Beweise zu Teil I, Würzburg-Wien 1965.

[3] D. Hilbert, *Gesammelte Abhandlungen*, I Band, Berlin 1932.

[4] J. Tate, *Global class field theory*, Algebraic number theory, p. 162-203, London and New York 1967.

Reçu par la Rédaction le 16. 8. 1968