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 \( a_1, \ldots, a_l \) be integers of \( k \) such that \( a_1^{m_1}a_2^{m_2}\cdots a_l^{m_l} \) 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 \( \gamma_1, \gamma_2, \ldots, \gamma_l \) there exist infinitely many prime ideals \( \mathfrak{p} \) in \( k \) satisfying for some rational integer \( m = m(\mathfrak{p}) \) prime to \( l \) the relations

\[
\begin{align*}
\left\{ \frac{a_1}{\mathfrak{p}} \right\}^m &= \gamma_1, \\
\left\{ \frac{a_2}{\mathfrak{p}} \right\}^m &= \gamma_2, \\
&\ldots, \\
\left\{ \frac{a_l}{\mathfrak{p}} \right\}^m &= \gamma_l,
\end{align*}
\]

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 \( a_1, \ldots, a_s \) satisfy the assumption of the theorem. There exists a prime ideal \( \mathfrak{p} \) in \( k \) such that \( \mathfrak{p} \vdash a_1a_2\cdots a_s \) and that \( a_1, a_2, \ldots, a_{s-1} \) are residues while \( a_s \) is a non-residue.

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

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

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 \( \delta \) be its discriminant. It is well known that \( \delta = f^{l-1} \), where \( f \) is an ideal in \( K \). Let \( \mathcal{A} \) be the group of all ideal classes in \( K \) mod \( f \) prime to \( f \), \( H_1 \) 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)

\[
(H_f : H_1) \leq a \leq \frac{1}{l} (A : H_1),
\]

where \( a \) is the number of ambiguous classes, implies

\[
|H_f| \leq \frac{1}{l} |A|.
\]

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

Case 1: \( \{a_s/\mathfrak{P}\} = 1 \). Then \( a_s \) is a residue mod \( \mathcal{P} \) and by (1) and the decomposition law in a cyclic field of prime degree we have \( \mathcal{P} = N_{L/K} Q \), 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, \( \{a_i/\mathfrak{P}\} = \{a_s/\mathfrak{P}\} \) for some integer \( c \). This implies the solvability of the congruences \( a_s^e x^f \equiv a_s \mod \mathfrak{P}, x \in k \), and \( y^f \equiv a_s \mod \mathcal{P}, y = x^f/a_s^c \).

As before, we have \( \mathcal{P} = N_{L/K} Q \), where \( Q \) is a prime ideal in \( L \). On the other hand, each ideal class \( \mathcal{P} \) contains an ideal a prime to \( la_1a_2\ldots a_s \) (see [2], p. 63). By factorizing \( a \) into prime ideals we get \( a = N_{L/K}(PQ) \), where \( Q \) are prime ideals in \( L \). It follows that each ideal class \( \mathcal{P} \) 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 \( \gamma_j = 1 \) \( (1 \leq j \leq t) \), \( \gamma_j \neq 1 \) \( (t < j \leq s) \).

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 \( x_1^f \equiv a_1 \mod \mathfrak{P}, x_2^f \equiv a_2 \mod \mathfrak{P}, \ldots, x_s^f \equiv a_s \mod \mathfrak{P} \), are solvable in \( k \).

Case 2: \( t < s \). Let

\[
\gamma_s^{-1} = \gamma_j^t, \quad t < j < s.
\]
Clearly, \( \xi_j \not\equiv 0 \mod l \). Hence
\[
a_1^{m_1} \cdots a_t^{m_t} (a_{t+1}^{\xi_{t+1}} a_s)^{m_{t+1}} \cdots (a_{s-1}^{\xi_{s-1}} a_s)^{m_{s-1}} a_s^{m_s}
\]
\[
= a_1^{m_1} \cdots a_t^{m_t} a_{t+1}^{\xi_{t+1} m_{t+1}} \cdots a_{s-1}^{\xi_{s-1} m_{s-1}} a_s^{m_{s-1} + \cdots + m_s - 1} a_s^{m_s}
\]
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 \( \mathfrak{p} \not| l a_1 a_2 \cdots a_s \), and \( a_1, \ldots, a_t, a_{t+1}^{\xi_{t+1}}, \ldots, a_{s-1}^{\xi_{s-1}} a_s \) 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
\[
\left\{ \frac{a_s}{\mathfrak{p}} \right\} = \gamma_s, \quad \left\{ \frac{a_j}{\mathfrak{p}} \right\}^{\xi_j m} \left\{ \frac{a_s}{\mathfrak{p}} \right\}^m = 1, \quad t < j < s.
\]

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

**Proof of the theorem.** Let \( \mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_{r-1} \) \((r \geq 0)\) 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 \( M = (N \mathfrak{p}_0 \mathfrak{p}_1 \cdots \mathfrak{p}_{r-1})^t \). By Lemma 2 there exists a prime ideal \( \mathfrak{p}_r \) such that for some integer \( m \) prime to \( l \) we have
\[
\left\{ \frac{a_1 M}{\mathfrak{p}_r} \right\}^m = \gamma_1, \quad \left\{ \frac{a_2 M}{\mathfrak{p}_r} \right\}^m = \gamma_2, \quad \cdots, \quad \left\{ \frac{a_s M}{\mathfrak{p}_r} \right\}^m = \gamma_s.
\]

Clearly \( \mathfrak{p}_r \) satisfies the assertion of the theorem and is different from \( \mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_{r-1} \). The proof is complete.

**REFERENCES**


*Reçu par la Rédaction le 16. 8. 1968*