CHARACTERS WITH PREASSIGNED VALUES

W. H. MILLS

Let k and t be positive integers; let $q_1, q_2, \ldots, q_t$ be distinct prime numbers; and let $\zeta_1, \zeta_2, \ldots, \zeta_t$ be kth roots of unity, not necessarily primitive. Recent investigations on consecutive kth power residues have led to the following question: Under what conditions do there exist primes p that have a kth power character χ such that

$$\chi(q_i) = \zeta_i, 1 \leqslant i \leqslant t? \tag{1}$$

It has been known for a long time that if k is a prime, then for any $q_1, \ldots, q_t, \zeta_1, \ldots, \zeta_t$ there exist an infinite number of such primes p (**4**; **3**, p. 426; or **5**). However, for most even values of k there are certain restrictions. If p is a prime, $p \equiv 1 \pmod{k}$, then it follows from the quadratic reciprocity law that:

(i) If $m|k$, $m \equiv 1 \pmod 4$, then m is a square modulo p.

(ii) If $4m|k$, then m is a square modulo p.

Now (i) and (ii) impose certain restrictions on the ζ_i in order that χ satisfy (1). The object of this paper is to show that if these conditions are satisfied, then there exist primes p that have a kth power character χ that satisfies (1). In particular this is always the case if k is odd, if $k = 2$, if $k = 4$, or if $k = 2Q$ where Q is a prime of the form $4N + 3$. Moreover, if there is one such prime p, then there are an infinite number of them.

1. Let k be a positive integer, let R be the field of rational numbers, let ζ be a primitive kth root of unity, and let $F = R(\zeta)$. Let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be non-zero elements of F, and let $\zeta_1, \zeta_2, \ldots, \zeta_t$ be kth roots of unity, not necessarily primitive. Let β_i be a root of $x^k = \alpha_i$, $1 \leqslant i \leqslant t$, and let $E = F(\beta_1, \beta_2, \ldots, \beta_t)$. Then E is normal over F. Let G be the Galois group of E over F. Our starting point is the following special case of the Tschebotareff density theorem (**2**, p. 133):

THEOREM 1. *If there is a σ in G such that*

$$\sigma\beta_i = \zeta_i\beta_i, 1 \leqslant i \leqslant t, \tag{2}$$

then there exist an infinite number of prime ideals $\mathfrak{p}$ of the first degree in F such that

$$\left(\frac{\alpha_i}{\mathfrak{p}}\right) = \zeta_i, \qquad 1 \leqslant i \leqslant t, \tag{3}$$

Received January 19, 1962.

https://doi.org/10.4153/CJM-1963-019-3 Published online by Cambridge University Press

where $(\alpha/\mathfrak{p})$ is the kth power residue symbol. If there are no σ in G satisfying (2), then there are no prime ideals $\mathfrak{p}$ in F satisfying (3).

Let F^k denote the set of all elements of the form α^k, $\alpha \in F$. It follows from the theory of Kummer extensions (see, for example, **(1)**) that the existence of a σ in G satisfying (2) is equivalent to the following condition:

(I) If $m_1, m_2, \ldots, m_t$ are rational integers such that $\prod \alpha_i^{m_i} \in F^k$, then $\prod \zeta_i^{m_i} = 1$.

If $\alpha_1, \alpha_2, \ldots, \alpha_t$ are rational then (I) is equivalent to the following:

(II) If $m_1, m_2, \ldots, m_t$ are non-negative rational integers such that $\prod \alpha_i^{m_i} \in R \cap F^k$, then $\prod \zeta_i^{m_i} = 1$.

By a kth power character modulo a prime p we mean a homomorphism of the multiplicative group of integers modulo p *onto* the group of kth roots of unity. This implies that p is of the form $kN + 1$. For such a prime p the kth power characters modulo p are the mappings χ of the form

$$\chi(n) = \left(\frac{n}{\mathfrak{p}}\right),$$

where $\mathfrak{p}$ is a prime ideal in F that divides p. Now every prime ideal $\mathfrak{p}$ of the first degree in F either divides k or divides a prime p of the form $kN + 1$. Therefore we have the following result:

THEOREM 2. *Let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be non-zero rational integers, and let $\zeta_1, \zeta_2, \ldots, \zeta_t$ be kth roots of unity. If* (II) *holds, then there exist an infinite number of rational primes, p, for each of which there is a kth power character χ* modulo *p, such that $\chi(\alpha_i) = \zeta_i$, $1 \leqslant i \leqslant t$. If* (II) *does not hold, then there are no such primes p.*

2. If k is odd let S be the set of all elements of the form a^k, $a \in R$. If k is even let S be the set of all elements of the form $\epsilon a^k d^{k/2}$, where $a \in R$, d is a positive square free integer, $d | \frac{1}{2}k$, and

$$\epsilon = \begin{cases} -1 \text{ if } k \equiv 4 \pmod 8 \text{ and } 2|d, \\ -1 \text{ if } k \equiv 2 \pmod 4 \text{ and } d \equiv -1 \pmod 4, \\ 1 \text{ otherwise.} \end{cases} \tag{4}$$

LEMMA. $R \cap F^k = S$.

Proof. The field of the qth roots of unity contains $\sqrt{q}$ if $q \equiv 1 \pmod 4$, and it contains $\sqrt{-q}$ if $q \equiv -1 \pmod 4$. Moreover the field of the fourth roots of unity contains $(-4)^{\frac{1}{4}}$. It follows from these facts that $S \subseteq R \cap F^k$.

Suppose $m \in R \cap F^k$ and that k is odd. Then there is a real number α in F such that $m = \alpha^k$. Since F is an abelian extension of R, it follows that $R(\alpha)$ is a normal extension of R. Hence every conjugate of α is real. Since $x^k = m$ has only one real root, it follows that α is rational, and hence $m \in S$.

Finally, suppose that $m \in R \cap F^k$ and that k is even. Without loss of generality we suppose that m is a kth power-free integer. Furthermore $m = \alpha^k$ for some $\alpha \in F$. Since α^k is real, it follows that there exists a $2k$th root of unity ω such that $\omega\alpha$ is a positive real number. Then $(\omega\alpha)^k = |m|$. Put $K = F(\omega)$. Then K is an abelian extension of R and $\omega\alpha \in K$. Hence $R(\omega\alpha)$ is a normal extension of R. Therefore every conjugate of $\omega\alpha$ is real. Since the only real roots of $x^k = |m|$ are $\pm\omega\alpha$ it follows that $(\omega\alpha)^2$ is rational. Put $d = (\omega\alpha)^2$. Then d is a positive rational integer and $|m| = d^{k/2}$. Therefore $m = \epsilon_0 d^{k/2}$, where $\epsilon_0 = \pm 1$. Since m is kth power free, it follows that d is square free. If q is a prime number and if $q|d$, then q is ramified in the extension $R(\alpha)$ and hence in F. This implies $q|\frac{1}{2}k$. Hence $d|\frac{1}{2}k$. Therefore $\epsilon d^{k/2} \in S \subseteq R \cap F^k$, where ϵ is given by (4). Thus $\epsilon\epsilon_0 m \in R \cap F^k$. Now m and $-m$ cannot both belong to F^k since -1 does not. Hence $\epsilon\epsilon_0 = 1$, $\epsilon_0 = \epsilon$, and $m = \epsilon d^{k/2} \in S$.

We have proved that $R \cap F^k \subseteq S$ in all cases. Hence $R \cap F^k = S$, and the proof of the lemma is complete.

3. Using the lemma we now apply Theorem 2 to the case where the α_i are distinct primes. This gives us our final result:

THEOREM 3. *Let $q_1, q_2, \ldots, q_t$ be distinct positive rational prime numbers. Let $\zeta_1, \zeta_2, \ldots, \zeta_t$ be* kth *roots of unity. Let P be the set of all rational prime numbers p such that there exists a* kth *power character χ* modulo *p satisfying*

$$\chi(q_i) = \zeta_i, 1 \leqslant i \leqslant t.$$

If k is odd, then P is infinite, If $k \equiv 2 \pmod 4$; if $\zeta_i^{k/2} = 1$ for all i such that $q_i|k$, $q_i \equiv 1 \pmod 4$; and if $\zeta_j^{k/2} = \zeta_j^{k/2}$ for all pairs i, j such that $q_i q_j|k$, $q_i \equiv q_j \pmod 4$; then P is infinite. If $4|k$, and if $\zeta_i^{k/2} = 1$ for all i such that $4q_i|k$, then P is infinite. In all other cases P is empty.

In particular P is always infinite if k is odd, if $k = 2$ or 4, or if $k = 2Q$ where Q is a prime of the form $4N + 3$.

The primes p in P are all of the form $kN + 1$.

REFERENCES

1. E. Artin, *Galois theory*, Notre Dame (1946).
2. H. Hasse, Jber. Deutsch. Math. Verein. Ergänzungsbände, VI (1930).
3. D. Hilbert, Jber. Deutsch. Math. Verein., *4* (1897), 175–546.
4. E. Kummer, Abh. der K. Akad. der Wiss. zu Berlin (1859).
5. N. Tschebotareff, Math. Ann., *95* (1926), 191–228.

Yale University