Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 43 (1997)

Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ON CYCLOTOMIC POLYNOMIALS, POWER RESIDUES, AND RECIPROCITY LAWS

Autor: Sharifi, Romyar T.

Kapitel: 5. Homogeneous polynomials

DOI: https://doi.org/10.5169/seals-63283

5. Homogeneous polynomials

Generalizing Theorem 1 to include homogeneous polynomials introduces subtle difficulties, which we address in the following proof.

Proof of Theorem 2. Let K and L be as in the proof of Theorem 1. We set $\pi_n = y - qx\zeta_n$ and $\pi = N_{L/K}(\pi_n)$ and note $p = N_K(\pi)$ with the assumption $s > 0$. Now let a be an integer dividing x, and decompose a as $a = a'q^k$ where a' is not divisible by q. Let $y' = N_{L/K}(y) = y^{[L:K]}$. We remark that $\pi \equiv y' \mod qa$ since $\pi_n \equiv y \mod qa$.

We can now apply reciprocity. We are interested in evaluating the symbol $(a/\pi)_l$. We can use reciprocity laws (5) and (6) along with multiplicativity from Theorems 5(a) and 6(a) in the following manner. We have

$$\left(\frac{a}{\pi}\right)_l = \left(\frac{a'}{\pi}\right)_l \left(\frac{q}{\pi}\right)_l^k = \left(\frac{\pi}{a'}\right)_l (\pi, a')_l (\pi, q)_l^k = \left(\frac{\pi}{a'}\right)_l (\pi, a)_l .$$

Now $\pi \equiv y' \mod a'$ so $(\pi/a')_l = (y'/a')_l$ by Theorem 5(c). And letting $(y')^{-1}$ denote the q-adic inverse of y' in $\mathbf{Z}_q$, we have

$$(\pi, a)_l = (\pi(y')^{-1}, a)_l (y', a)_l .$$

Let $\pi' = \pi(y')^{-1}$. Now $\pi' \equiv 1 \mod qa$. So $\pi' \equiv 1 \mod q$, and if q divides a, then $\pi' \equiv 1 \mod q^2$. Thus the fact that λ_q^2 divides q implies $\pi' \equiv 1 \mod \mathfrak{f}_l(a)$ by Corollary 8. Thus $(\pi', a)_l = 1$.

We now have that

$$\left(\frac{a}{\pi}\right)_l = \left(\frac{y'}{a'}\right)_l (y', a)_l .$$

The symbol $(y'/a')_l$ is an l-th root of unity, and by Theorem 5(d) an element $\sigma \in G_K$ acts on it as follows:

$$\sigma\left(\frac{y'}{a'}\right)_l = \left(\frac{\sigma y'}{\sigma a'}\right)_l = \left(\frac{y'}{a'}\right)_l ,$$

since a' and y' are rational integers. Since l is odd, the only such root of unity fixed under the action of the Galois group is 1. In the same manner, Theorem 6(h) enables us to see that $(y', a)_l = 1$. We therefore conclude that $(a/\pi)_l = 1$. □