Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 37 (1991)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: PRIMES OF DEGREE ONE AND ALGEBRAIC CASES OF EBOTAREV'S THEOREM
Autor: Lenstra, H. W. / Stevenhagen, P.
Kapitel: 4. Algebraic proofs
DOI: https://doi.org/10.5169/seals-58727

4. ALGEBRAIC PROOFS

In this section, we will restrict our attention to number fields, i.e. finite extensions of the field of rational numbers $\mathbf{Q}$. The degree of a prime in a number field will be the degree with respect to $\mathbf{Z}$.

Let F be a number field, $\mathfrak{f}$ a cycle of F and $Cl_{\mathfrak{f}}$ the ray class group of conductor $\mathfrak{f}$ of F, and C_F the idele class group of F. For each prime $\mathfrak{p}$ of F, we fix an element $\pi_{\mathfrak{p}} \in C_F$ that is the residue class of a prime element at $\mathfrak{p}$. There is a natural surjection $\phi_{\mathfrak{f}}: C_F \twoheadrightarrow Cl_{\mathfrak{f}}$ that maps $\pi_{\mathfrak{p}}$ to the class of the prime ideal $\mathfrak{p}$ for each $\mathfrak{p}$ not dividing $\mathfrak{f}$. A subgroup of C_F is open if and only if it contains $\ker \phi_{\mathfrak{f}}$ for some conductor $\mathfrak{f}$ of F. Our theorem 2 may now be reformulated as follows.

THEOREM 2′. *Any open subgroup of C_F that contains all but finitely many of the elements $\pi_{\mathfrak{p}}$ with $\mathfrak{p}$ of degree one is equal to C_F itself.*

If E is a finite extension of F, then the norm subgroup $N_{E/F}C_E$ is open and of finite index in C_F. If E/F is cyclic, the *first inequality* from class field theory states that $[C_F : N_{E/F}C_E] \geqslant [E:F]$.

LEMMA. *Let E/F be an extension of number fields, and suppose that almost all primes of degree one of F split completely in E. Then $E = F$.*

Proof. All primes of F that split completely in E split completely in the normal closure E' of E over F, so the assumption also holds for E'/F. If $E' \neq F$, then there exists a subextension $F \subset F' \subset E'$ for which E'/F' is cyclic of degree $[E':F'] > 1$. By the first inequality, this implies that $N_{E'/F'}C_{E'} \neq C_{F'}$. On the other hand, $N_{E'/F'}C_{E'}$ contains $\pi_{\mathfrak{p}}$ for each prime $\mathfrak{p}$ of F' that splits completely in E'. This contradicts theorem 2′. □

As a corollary, we obtain a theorem of Bauer (1916). Bauer's original proof [1] is based on the Frobenius density theorem [8].

COROLLARY 1 (Bauer [1]). *Let F be a finite normal extension of $\mathbf{Q}$, and suppose that E is a number field such that all but finitely many of the primes p that have an extension of degree one to E split completely in F. Then F is contained in E.*

Proof. All but finitely many primes of degree one of E split completely in FE/E, so $FE = E$ by the lemma.

Our lemma also shows that ray class fields are characterized by a weak form of their original definition as abelian extensions of a number field characterized by a certain set of primes splitting completely in the extension.

COROLLARY 2 (Deuring [5]). *Let F be any number field, $\mathfrak{f}$ a cycle of F and E an extension of F in which almost all primes $\mathfrak{p}$ of F satisfying $\mathfrak{p} \equiv 1 \bmod^* \mathfrak{f}$ split completely. Then E is contained in the ray class field modulo $\mathfrak{f}$ of F.*

Proof. Let R be the ray class field modulo $\mathfrak{f}$ of F. Almost all primes of degree one of R lie over a prime $\mathfrak{p}$ of F that is $1 \bmod^* \mathfrak{f}$, so they split completely in RE/R. It follows that $RE = R$. □

Proof of theorem 3. Let E' and F' be the fields corresponding to H_1 and H_2. Then $[E':F'] > 1$, so by the lemma there are infinitely many prime ideals $\mathfrak{p}$ of degree one in F' that have an extension $\mathfrak{p}'$ to E' for which $\deg \mathfrak{p}' > 1$. Let $\mathfrak{q}$ be an extension of such a prime $\mathfrak{p}'$ to E. Then the Frobenius element of $\mathfrak{q}$ in G lies in H_2 but not in H_1. Note that we obtain as additional information that the restriction of $\mathfrak{q}$ to F is of degree one. □

As a consequence we have Wójcik's result [17] mentioned in the introduction.

COROLLARY. *Let H_1 and H_2 be subgroups of the ray class group $Cl_{\mathfrak{f}}$ of a number field F such that $H_1 \subset H_2$ and $H_1 \neq H_2$. Then there are infinitely many primes $\mathfrak{p}$ of F for which the ray class $\mathfrak{p} \bmod^* \mathfrak{f}$ lies in $H_2 \setminus H_1$.*

Proof. Take for E/F the ray class field extension of conductor $\mathfrak{f}$, then $\mathrm{Gal}(E/F) \cong Cl_{\mathfrak{f}}$ and our claim follows from theorem 3. □

Using the generalization of theorem 2 discussed in the remark at the end of section 2, one can in a similar way prove the analogue of theorem 3 for the function field case. However, the somewhat intuitive distinction between algebraic and analytic proofs we accepted for the number field case becomes rather questionable here, as one may very well argue that the zeta-functions occurring in the "analytic proofs" are formal power series and therefore of an algebraic nature.

We finally describe the somewhat bizarre situation that arises when one tries to give an algebraic proof of the following well known theorem [3, p. 362].

THEOREM. *If* $f \in \mathbf{Z}[X]$ *is an irreducible polynomial that has a zero modulo almost all primes* p, *then* f *is linear.*

In order to see what is needed for a proof, assume that $\deg f > 1$, and let G be the Galois group of the splitting field of f. Then G acts transitively on the set Ω of roots of f, and the assumption that f has a root modulo p for almost all p implies that almost all Frobenius elements in G fix a root of f. If $H \subset G$ is the stabilizer of some $\omega \in \Omega$, the subset of G consisting of those elements that fix at least one element of Ω equals $\bigcup_{g \in G} gHg^{-1}$. As no finite group is the union of the conjugates of a proper subgroup, G contains elements that fix no root of f, and which therefore occur as the Frobenius of only finitely many primes in the splitting field of f. This obviously contradicts the Čebotarev density theorem.

In order to replace Čebotarev's theorem in the argument above by a weaker, algebraically provable form like our theorem 3, we need an element σ of G that fixes no element of Ω *and whose order is a power of a prime number.* Indeed, if σ has q-power order then each element of $\langle \sigma \rangle - \langle \sigma^q \rangle$ fixes no element of Ω, and we obtain a contradiction since theorem 3 implies that there are infinitely many Frobenius symbols among them. Thus, we are reduced to proving the following.

LEMMA. *Given a finite group* G *acting transitively on a finite set* Ω *of cardinality* $\#\Omega > 1$, *there exists* $\sigma \in G$ *of prime power order that fixes no element of* Ω.

Suppose G is a counterexample of minimal order to this statement, and let H be the stabilizer of some element of Ω. The set of left cosets in G of a maximal subgroup $H' \supset H$ with natural G-action now also gives a counterexample to the lemma, so we may assume that H is a maximal subgroup of G. We have $D = \bigcap_{g \in G} gHg^{-1} = \{1\}$, since otherwise the action factors via G/D and an element of prime power order fixing no element of Ω in G/D can be lifted to an element of the same sort in G. Now suppose G has a normal subgroup $N \neq \{1\}$. Then $H \cap N = \{1\}$, so $G = NH$ and N acts transitively on the set of left cosets of H in G, hence on Ω. By the minimality of G, we conclude that $N = G$, so G is simple. Now the lemma is known to hold for simple G, but the only existing proof (which, as M. Isaacs kindly pointed out to us, can be found in [7]) proceeds by checking all cases given by the classification of finite simple groups. Thus, it turns out that currently we can only eliminate the use of Čebotarev's density theorem in our proof at the cost of introducing the classification of finite simple groups.