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: 1. Introduction
DOI: https://doi.org/10.5169/seals-58727

L'Enseignement Mathématique, t. 37 (1991), p. 17-30

PRIMES OF DEGREE ONE AND ALGEBRAIC CASES OF ČEBOTAREV'S THEOREM

by H. W. LENSTRA, JR. and P. STEVENHAGEN

ABSTRACT. Let $A \subset B$ be an extension of Dedekind domains for which the corresponding extension of fields of fractions is finite and separable. It is shown that the class group of B is then generated by classes of primes of degree one with respect to A. When the main argument of the proof is applied to the situation of the ray class groups occurring in class field theory, it leads to purely algebraic proofs of special cases of Čebotarev's density theorem.

1. INTRODUCTION

Let A be a Dedekind domain with field of fractions K, and suppose L is a finite field extension of K. Then the integral closure of A in L is a Dedekind domain B, and for each non-zero prime ideal $\mathfrak{q}$ of B we define its *degree* over A as the degree of the residue class field extension at $\mathfrak{q}$, i.e.

$$\deg_A \mathfrak{q} = [B/\mathfrak{q} : A/(A \cap \mathfrak{q})] .$$

We write Cl_B for the ideal class group of B and denote the class of $\mathfrak{q}$ in Cl_B by $[\mathfrak{q}]$. Using this notation, we prove the following theorem.

THEOREM 1. *If L/K is a separable field extension and S is a finite set of primes of B, one has*

$$Cl_B = \langle [\mathfrak{q}] : \deg_A \mathfrak{q} = 1 \quad \text{and} \quad \mathfrak{q} \notin S \rangle .$$

In case B is not a principal ideal domain, it follows that B has infinitely many primes that are of degree one over A. We will see in section 3 that the hypothesis that L/K be separable cannot be omitted.

1980 Mathematics subject classification (1985): 11R44, 13F05.

Acknowledgements: The authors are supported by the National Science Foundation under grants No. DMS-8706176 and 9002939 and by the Netherlands Organisation for Scientific Research (NWO).

As a special case of theorem 1, taking $A = \mathbf{Z}$, we obtain a well known result: the class group of the ring of integers of a number field is generated by the classes of the primes of degree one. Our approach is sufficiently general to yield the corresponding result for the ray class groups of a number field. Thus, let $\mathfrak{f}$ be a cycle of a number field F and $Cl_{\mathfrak{f}}$ the ray class group modulo $\mathfrak{f}$ (cf. [12]). We then have the following analogue of theorem 1.

THEOREM 2. *Let $\mathfrak{f}$ be a cycle of the number field F and S a finite set of primes of F containing the finite primes dividing $\mathfrak{f}$. Then the ray class group $Cl_{\mathfrak{f}}$ satisfies*

$$Cl_{\mathfrak{f}} = \langle [\mathfrak{p}] : \deg_{\mathbf{Z}} \mathfrak{p} = 1 \text{ and } \mathfrak{p} \notin S \rangle .$$

The statement of theorem 2 is not very striking in view of a much stronger theorem of Čebotarev from 1926 [4], which implies that the primes of F that do not divide $\mathfrak{f}$ are equidistributed over the classes of $Cl_{\mathfrak{f}}$. More precisely, the Dirichlet density of the set of primes lying in a given class of $Cl_{\mathfrak{f}}$ is the same for all classes, and these densities already come from the primes of degree one because the set of primes of degree one has Dirichlet density 1 (cf. [12, Ch. VIII §4]). A weak form of this theorem had already been proved by Frobenius [8] in 1896. Like Frobenius' proof, the proof of the Čebotarev density theorem depends on the properties of L-functions and makes use of complex analysis. Our theorem 1 is purely algebraic in its statement and proof. The idea goes back to Kummer [11, p. 241-243], who proved already in 1847 by an algebraic argument that the class group of the cyclotomic field $\mathbf{Q}(\zeta_p)$ for a prime number p is generated by the classes of the primes of degree one. Generalizations of Kummer's argument in the direction of theorem 2 are found in Hilbert's Zahlbericht [10, Kap. 14, sec. 53] and in Deuring's lecture notes on class field theory [5].

The algebraic nature of theorem 2 makes it a legitimate tool in so-called algebraic proofs of special cases of Čebotarev's theorem. For abelian extensions of the rational number field, where the theorem reduces to Dirichlet's theorem on primes in arithmetic progressions, many algebraic proofs of special cases are known to exist. Here the typical statement of a special case is that for an integer $n > 1$ and a subset S of the multiplicative group $(\mathbf{Z}/n\mathbf{Z})^*$, there are infinitely many primes p for which p mod n is in S.

When $S = \{1\}$ there is an easy argument using the n-th cyclotomic polynomial [14, p. 13]. In fact, the stronger statement that every number field has infinitely many primes of degree one is not very deep and follows from an algebraic argument, as Bianchi already points out in [2] (*"La proposizione*

si stabilisce in generale col sussidio dell'aritmetica analitica. Qui vogliamo dimonstrarla... con mezzi puramente aritmetici."). The statement follows immediately from our theorem 2, since any number field has non-trivial ray class groups for $\mathfrak{f}$ sufficiently large. Schur [13] gave elementary proofs for special values of n and S consisting of an element of order 2. They were generalized to other values of n by Wójcik [15], who finally showed [16] that for arbitrary n one can take for S a non-empty difference $H_2 \setminus H_1$ of two subgroups $H_1 \subset H_2$ of $(\mathbf{Z}/n\mathbf{Z})^*$. The proof goes through for the ray class groups of an arbitrary number field [17].

All of the results above are restricted to abelian cases of Čebotarev's theorem. These are described by class field theory, and the main theorems of this theory can be obtained by "algebraic means". In fact, much of the above is already implicit in the so-called first inequality from class field theory, which states that for a cyclic extension of number fields E/F, the norm index $[C_F : N_{E/F} C_E]$ of the idele classes is at least equal to the degree $[E:F]$ (cf. section 4). It implies that in any extension E/F with $E \neq F$, there are infinitely many primes of F that do not split completely in E. Even though the requirements for a proof to be "algebraic" may depend on taste, they are certainly met by the Herbrand quotient argument that one usually encounters as the proof of the first inequality [12, Ch. IX § 5]. If one combines only the first inequality with theorem 2, one obtains a theorem that does not only apply to abelian extensions.

THEOREM 3. *Let E/F be a Galois extension of number fields with group G, and let H_1 and H_2 be subgroups of G such that $H_1 \subset H_2$ and $H_1 \neq H_2$. Then there are infinitely many primes $\mathfrak{q}$ of E for which the Frobenius symbol of $\mathfrak{q}$ in G lies in $H_2 \setminus H_1$.*

The proof of theorem 3 will show that the restriction of $\mathfrak{q}$ to F can even be required to be of degree one. By enlarging E, one sees that the theorem is also true for H_1 the empty set. This case follows also from Bianchi's result mentioned above.

The attempt to construct algebraic proofs for certain corollaries of Čebotarev's theorem can lead to amusing situations. We give an example in which the theorem above gives the desired result only when one assumes the classification of finite simple groups.

It seems that in order to improve upon theorem 3, one would have to distinguish by algebraic means between primes whose Frobenius elements generate the same subgroup.