L'Enseignement Mathematique, 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 Cebotarev'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 $p \bmod n$ 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 Wojcik [15], who finally showed [16] that for arbitrary n one can take for S a non-empty difference $H_2 \backslash H_1$ 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 $H_2 \backslash H_1$*

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

2 THE SEPARABLE CASE

In this section we will prove the theorems 1 and 2. The proof will depend on the fact that the extension of fields under consideration is separable. In section 3 we will construct examples of inseparable extensions for which the conclusion of theorem 1 does not hold.

Suppose that we are in the situation of theorem 1. As we assume L/K to be separable, there is an element $\alpha \in B$ such that $L = K(\alpha)$. Moreover, there exists $d \neq 0$ in A such that the subring $A[\alpha]$ of B satisfies $dB \subset A[\alpha] \subset B$. For instance, one can take for d the discriminant of the irreducible polynomial of α over K. One has $B_{\mathfrak{p}} = A_{\mathfrak{p}}[\alpha]$ for the localizations at all primes $\mathfrak{p} \nmid dA$, and for a prime $\mathfrak{q}$ in B that lies over such a $\mathfrak{p}$, the element $\alpha \bmod \mathfrak{q}$ generates the residue class field $B/\mathfrak{q}$ over $A/\mathfrak{p}$.

Both theorem 1 and 2 are easy consequences of the following lemma.

LEMMA. *Choose $d \neq 0$ in A such that $dB \subset A[\alpha]$, and let $\mathfrak{q}$ be a prime of B that does not divide dB. If $\deg_A \mathfrak{q} = f > 1$, then there exists a non-zero element $x \in B$ satisfying*

(a) $x \equiv 1 \bmod dB$

(b) $Bx = \mathfrak{q} \cdot \prod_{i=1}^{t} \mathfrak{b}_i$, *where $\mathfrak{b}_1, \ldots, \mathfrak{b}_t$ are primes of B of degree $< f$ that are coprime to dB.*

If, in addition, a finite number of embeddings ϕ of B into the field of real numbers are given, then the element $x \in B$ can be chosen such that $\phi(x) > 0$ for each of these embeddings.

Proof. Let $\mathfrak{p} = \mathfrak{q} \cap A$, and set $\beta = d\alpha$. As $\mathfrak{q} \nmid dB$, one has $B_{\mathfrak{p}} = A_{\mathfrak{p}}[\beta]$ and Kummer's theorem [12, Ch. I §8] implies that there exist $u_0, u_1, \ldots, u_{f-1} \in A$ such that

$$\mathfrak{q} = \mathfrak{p}B + (\beta^f + u_{f-1}\beta^{f-1} + \cdots + u_1\beta + u_0)B \tag{1}$$

We may assume that

$$x' = \beta^f + u_{f-1}\beta^{f-1} + \cdots + u_1\beta + u_0 \in \mathfrak{q} - \mathfrak{q}^2 \tag{2}$$

This follows from (1) if $\mathfrak{p} \subset \mathfrak{q}^2$, and can otherwise be achieved by adding an element of $\mathfrak{p} - \mathfrak{q}^2$ to u_0, if necessary. We shall obtain the required element

$$\begin{aligned} x = \beta^f + v_{f-1}\beta^{f-1} + u_{f-2}\beta^{f-2} + u_{f-3}\beta^{f-3} + \cdots + u_3\beta^3 \\ + u_2\beta^2 + u_1\beta + v_0 \end{aligned} \tag{3}$$

by modifying the "coefficients" u_{f-1} and u_0 of x'. Our first condition

$$v_0 \equiv 1 \bmod dA \tag{4}$$

will guarantee that $x \in \beta B + v_0 \subset d\alpha B + dA + 1 \subset dB + 1$, as required in (a). The second condition

$$\begin{aligned} v_0 &\equiv u_0 \bmod \mathfrak{p}^2 \\ v_{f-1} &\equiv u_{f-1} \bmod \mathfrak{p}^2 \end{aligned} \tag{5}$$

implies that $x \in \mathfrak{q} - \mathfrak{q}^2$, so $x \neq 0$ and we have

$$xB = \mathfrak{q} \cdot \prod_{i=1}^{t} \mathfrak{b}_i$$

for certain prime ideals $\mathfrak{b}_i \neq \mathfrak{q}$ that do not divide dB. Note also that we cannot have $\mathfrak{b}_i \mid \mathfrak{p}B$, since this would imply that $\mathfrak{b}_i \supset \mathfrak{p}B + xB = \mathfrak{q}$.

We will impose an extra condition on each of v_0 and v_{f-1} to ensure that

$$\deg_A \mathfrak{b}_i < f \qquad (i = 1, \ldots, t) .$$

Let $g \in A[X]$ be the irreducible polynomial of β over K, and M the splitting field of g over K. Denote by C the integral closure of A in M. Then g splits completely as a product $\prod_{j=1}^{n}(X - \beta_j)$ in $C[X]$. Let the finite set $W \subset C$ consist of all sums of f distinct terms from $\beta_1, \beta_2, \ldots, \beta_n$:

$$W = \{ \textstyle\sum_{j \in J} \beta_j : J \subset \{1, 2, \ldots, n\} , \ \# J = f \} .$$

Our condition on v_{f-1} reads

$$-v_{f-1} \notin W . \tag{6}$$

The ring A is infinite, so we can find v_{f-1} satisfying (5) and (6). Given such an element v_{f-1}, we define a non-zero element

$$y = \prod_{w \in W} (w + v_{f-1}) ,$$

which lies in A as it is a symmetric expression in the roots of g, and require that

(7) $v_0 \equiv 0 \bmod \mathfrak{a}$ for each prime $\mathfrak{a} \mid yA$ of A that does not divide $d\mathfrak{p}$.

There are only finitely many prime divisors of yA, so there exists v_0 satisfying (4), (5) and (7) by the Chinese remainder theorem.

We will now show that our conditions on v_0 and v_{f-1} imply $\deg_A \mathfrak{b}_i < f$ for each prime $\mathfrak{b}_i$ occurring in the decomposition of xB. Fix such a prime,

and put $\mathfrak{a}_l = A \cap \mathfrak{b}_l$ and $\bar{\beta} = \beta \bmod \mathfrak{b}_l$. We have $B/\mathfrak{b}_l = (A/\mathfrak{a}_l)[\bar{\beta}]$ because $\mathfrak{b}_l \nmid dB$. Reduction of (3) modulo $\mathfrak{b}_l$ shows that $\bar{\beta}$ satisfies an f-th degree equation

$$0 = \bar{\beta}^f + \bar{v}_{f-1}\bar{\beta}^{f-1} + \bar{u}_{f-2}\bar{\beta}^{f-2} + \bar{u}_{f-3}\bar{\beta}^{f-3} + \ldots + \bar{u}_3\bar{\beta}^3 + \bar{u}_2\bar{\beta}^2 + \bar{u}_1\bar{\beta} + \bar{v}_0 , \tag{8}$$

so we certainly have $\deg_A \mathfrak{b}_l \leqslant f$. In order to arrive at a contradiction, suppose that equality occurs for our prime $\mathfrak{b}_l$. Then the polynomial

$$\bar{h} = X^f + \bar{v}_{f-1}X^{f-1} + \bar{u}_{f-2}X^{f-2} + \bar{u}_{f-3}X^{f-3} + \ldots + \bar{u}_3X^3 + \bar{u}_2X^2 + \bar{u}_1X + \bar{v}_0$$

is the irreducible polynomial of $\bar{\beta}$ in $(A/\mathfrak{a}_l)[X]$. Since $\bar{\beta}$ is also a zero of $\bar{g} = g \bmod \mathfrak{a}_l[X]$, $\bar{h}$ divides $\bar{g}$ in $(A/\mathfrak{a}_l)[X]$, hence also in $(C/\mathfrak{c}_l)[X]$, where $\mathfrak{c}_l$ is a prime in C lying over $\mathfrak{b}_l$. In $(C/\mathfrak{c}_l)[X]$, the polynomial $\bar{g}$ splits completely as a product $\prod_{j=1}^{n}(X - \bar{\beta}_j)$, with $\bar{\beta}_j = \beta_j \bmod \mathfrak{c}_l$. It follows that $\bar{h} = \prod_{j\in J}(X - \bar{\beta}_j)$, with $J \subset \{1, 2, \ldots, n\}$ of cardinality f. Comparing coefficients at X^{f-1}, we find that $\bar{v}_{f-1} = -\sum_{j\in J}\bar{\beta}_j$. By definition of y, we now have

$$y = \prod_{w\in W}(w + v_{f-1}) \in \mathfrak{c}_l \cap A = \mathfrak{a}_l .$$

As $\mathfrak{a}_l \nmid d\mathfrak{p}$, we have $v_0 \equiv 0 \bmod \mathfrak{a}_l$ by (7). It follows that the irreducible polynomial $\bar{h} \in (A/\mathfrak{a}_l)[X]$ is divisible by X. This contradicts the fact that $\deg h = f > 1$.

We finally have to show that the element $x \in B$ constructed above can be made positive at a finite number of real embeddings $B \rightarrowtail \mathbf{R}$. This follows immediately from the fact that (4), (5) and (7) remain valid when we replace x by $x + k^2$, where k is a suitable element in $yd\mathfrak{p}$. This finishes the proof of the lemma.

Proof of theorem 1. By the approximation theorem, the class group of B is generated by the primes outside S. Thus, let $\mathfrak{q}$ be an ideal of B of degree $\deg_A \mathfrak{q} = f$ that is not in S. We are done if we can show that $[\mathfrak{q}]$ is in the subgroup C of Cl_B that is generated by the classes of primes of degree one that are not in S.

Use induction on f. For $f = 1$ there is nothing to prove, so take $f > 1$. If we choose the element d in the lemma divisible by all primes in S it follows that there exist primes $\mathfrak{b}_l$ outside S with $\deg_A \mathfrak{b}_l < f$ such that $[\mathfrak{q}]$

$= \prod_{i=1}^{l} [\mathfrak{b}_i]^{-1} \in Cl_B$. By our induction hypothesis, all $[\mathfrak{b}_i]$ are in C. It follows that $[\mathfrak{q}]$ is in C. □

By applying the first half of the proof of the lemma to a prime $\mathfrak{q}$ of degree $f = 1$, one can obtain an element $x = \beta + v_0 \in B$ whose ideal factorization reads $xB = \mathfrak{q} \cdot \prod_{i=1}^{l} \mathfrak{b}_i$ for certain primes $\mathfrak{b}_i$ of degree one outside S. It follows that the inverse class $[\mathfrak{q}]^{-1} \in Cl_B$ is a product of classes of primes of degree one outside S. Thus the classes of the primes of degree one outside S generate Cl_B already as a *monoid*, i.e. without using their inverse classes.

It is not true that every ideal class of B necessarily contains a prime of degree one with respect to A. As a trivial counterexample, with $A = B$, one can a take a Dedekind domain that is not principal and invert all prime ideals in the principal class. There are no prime ideals in the principal class of the resulting Dedekind domain. Less trivial examples are found in [6, Ch. III § 15].

Proof of theorem 2. We now take $A = \mathbf{Z}$ and B the ring of integers of F. The possibility of choosing the element x in the lemma in such a way that it is positive under certain embeddings in the field of real numbers and congruent to 1 modulo any given ideal of A shows that the lemma can also be used to generate relations in $Cl_{\mathfrak{f}}$. The proof is further analogous to that of theorem 1. □

Remark. Theorem 2 can be generalized to the case that F is a function field over a finite field. In that case, there is neither a canonical choice for a ring of integers $A \subset F$ nor an absolute degree of the primes of A with respect to a base ring $\mathbf{Z}$. For each non-empty finite set of primes T of F, one can take A to be the intersection of valuation rings $\bigcap_{\mathfrak{p} \notin T} A_{\mathfrak{p}} \subset F$. One defines a *conductor* of A to be a pair consisting of an integral ideal $\mathfrak{f}$ of A and an open subgroup H of finite index in the product of the completions $\prod_{\mathfrak{p} \in T} F_{\mathfrak{p}}^*$ of F. The ray *class group* of A modulo such a conductor is defined as the group of fractional A-ideals that is generated by all primes $\mathfrak{p} \nmid \mathfrak{f}$ of A modulo the subgroup of principal ideals $A\alpha$ for which $\alpha \equiv 1 \bmod^* \mathfrak{f}$ and $\alpha \in H$ under the natural embedding. If k is the field of constants of F and x is an element of $F \setminus k$, one can consider the degree of primes of A with respect to $k(x)$ and show that ray class groups of A are generated by the classes of primes that are of degree one in this sense. The details are left to the reader.

3. The inseparable case

In this section we will show that the separability assumption in theorem 1 cannot be omitted. As we need examples of Dedekind domains having a non-

trivial class group in order to create situations in which the conclusion of theorem 1 fails, we will first recall an explicit construction of such examples. There does not seem to be an adequate reference to the literature for this result, so we formulate it as a proposition and supply a proof.

Let $g \in Z[t]$ be a non-constant polynomial with coefficients in a field Z, and define the ring $R \subset Z(t)$ by

$$R = \left\{ \frac{a}{b} : a, b \in Z[t] : b = g^m \text{ for some } m \geqslant 0, \text{ and } \deg a \leqslant \deg b \right\}.$$

For this ring the following holds.

PROPOSITION. *The ring R is a Dedekind domain with class group $Cl(R) = \mathbf{Z}/h\mathbf{Z}$, where $h = \gcd\{\deg f : f \mid g\}$.*

Proof. We will give a quick geometric proof using a theorem on class groups from [9] and a completely elementary ring theoretic proof.

For the first proof, let X be the projective line over Z. Each of the distinct irreducible factors $f_1, f_2, \ldots, f_r$ of g corresponds to a closed point P_i of X that is contained in the open affine subset $\operatorname{Spec} Z[t]$ of X. The variety $X \setminus \{P_1, P_2, \ldots, P_r\}$ is affine with coordinate ring R. It is a normal variety of dimension one, so R is a Dedekind domain. By repeated application of proposition II.6.5(c) in [9], it follows that the natural map from $Cl(X)$ to $Cl(R) = Cl(\operatorname{Spec} R)$ is a surjection, and that the kernel is generated by the classes of the prime divisors $\{P_i\}$ in $Cl(X)$. As $Cl(X) \cong \mathbf{Z}$ under the degree map [9, proposition II.6.4], the proposition follows immediately.

For the second proof, we define for each $k \in \mathbf{Z}$ the fractional R-ideal

$$\mathfrak{c}_k = \left\{ \frac{a}{b} : a, b \in Z[t] : b = g^m \text{ for some } m \geqslant 0 \text{ and } \deg a + k \leqslant \deg b \right\}.$$

One easily checks that $\mathfrak{c}_k \cdot \mathfrak{c}_l = \mathfrak{c}_{k+l}$ for $k, l \in \mathbf{Z}$. In particular, one has $\mathfrak{c}_k = \mathfrak{c}^k$ with $\mathfrak{c} = \mathfrak{c}_1$ for $k \geqslant 0$, and since $\mathfrak{c}_0 = R$ the ideal $\mathfrak{c}$ is invertible. As $R = \mathfrak{c} + Z$, one has $\dim_Z(R/\mathfrak{c}) = 1$. The invertibility of $\mathfrak{c}$ implies that $\dim_Z(\mathfrak{a}/\mathfrak{b}) = \dim_Z(\mathfrak{c}\mathfrak{a}/\mathfrak{c}\mathfrak{b})$ for any pair $\mathfrak{a} \supset \mathfrak{b}$ of fractional R-ideals of finite relative Z-dimension, so $\dim_Z(R/\mathfrak{c}^k) = k$ for any $k \geqslant 0$.

For any non-zero element $x \in R$, we set $d(x) = \dim_Z(R/Rx)$. We will prove that $d(x)$ is always finite, and that it is given by the formula

$$d(x) = -\sum_{f \mid g \text{ irred}} \operatorname{ord}_f(x) \cdot \deg f, \tag{9}$$

where $\operatorname{ord}_f(x)$ denotes the number of factors f in x.

We first prove formula (9) in two special cases. If $x = f^{-1}$ for some irreducible divisor f of degree k of g, then x generates $\mathfrak{c}^k$, so $d(f^{-1}) = k = \deg f$ and (9) holds. Next, suppose $x = a/b \in R$ with $a, b \in Z[t]$ of equal degree and $\gcd(a, g) = 1$. The natural map $Z[t] \to Z[t]/aZ[t]$ maps g to a unit, so it has an extension to the localized ring $Z[t]_g$, which contains R. An element $y \in R$ is in the kernel if and only if it is of the form $y = ahg^{-k}$ with $k \geqslant 0$ and $h \in Z[t]$ of degree at most $k \deg g - \deg a$. Writing $y = x(bh/g^k) \in xR$ one sees that an isomorphism $R/xR \xrightarrow{\sim} Z[t]/aZ[t]$ is induced, so $d(x) = \deg a = \deg b$ and formula (9) holds again. For the general case one writes an arbitrary non-zero element $x \in R$ in the form $x = (a_1 a_2)/b$ with $a_1, a_2, b \in Z[t]$ and $\gcd(a_1, a_2) = \gcd(a_1, g) = \gcd(a_1 a_2, b) = 1$, and notes that all factors except $x^{\deg g}$ in the equation

$$(a_2^{-1})^{\deg g} \cdot (g^{-1})^{\deg a_1} \cdot x^{\deg g} = \frac{a_1^{\deg g}}{g^{\deg a_1}} \cdot (b^{-1})^{\deg g}$$

are products of factors of the special types dealt with above. It is immediate from the definition of d that if x and y are in $R \setminus \{0\}$, we have $d(xy) = d(x) + d(y)$ in the sense that if one of the sides is finite, then so is the other and the equality holds. Repeated application of this fact now shows that (9) is valid for our arbitrary element $x \in R$. As a consequence, we see that d has a unique extension to a homomorphism $d: Z(t)^* \to \mathbf{Z}$. Also, since every fractional ideal contains a principal ideal and is contained in a principal fractional ideal, we can define the integer $\dim_Z(\mathfrak{a}/\mathfrak{b})$ as $\dim_Z(\mathfrak{a}/(\mathfrak{a} \cap \mathfrak{b})) - \dim_Z(\mathfrak{b}/(\mathfrak{a} \cap \mathfrak{b}))$ for any two fractional R-ideals $\mathfrak{a}$ and $\mathfrak{b}$.

We will finish the proof of the proposition by showing that for any fractional R-ideal $\mathfrak{b} \supset R$, one has $\mathfrak{b} \sim \mathfrak{c}^{-\dim_Z(\mathfrak{b}/R)}$, where $\sim$ denotes equality up to multiplication by an element from Z^*. First of all, this implies that all fractional R-ideals are invertible, so R is a Dedekind ring. Moreover, the ideal class $[\mathfrak{c}]$ generates $Cl(R)$. The order of $[\mathfrak{c}]$ is at least h as we have $[xR] = [\mathfrak{c}^{d(x)}]$ for any $x \in Z^*$ and $d(x) \in h\mathbf{Z}$ by formula (9). We have already seen that $\mathfrak{c}^{\deg f} = f^{-1}R$ for each irreducible factor f of g, so $\mathfrak{c}^h$ is principal and we obtain the desired result $Cl(R) \cong \mathbf{Z}/h\mathbf{Z}$.

We prove the relation $\mathfrak{b} \sim \mathfrak{c}^{-\dim_Z(\mathfrak{b}/R)}$ by induction on $\dim_Z(\mathfrak{b}/R)$. If $\dim_Z(\mathfrak{b}/R) = 0$ one has $\mathfrak{b} = R$ and there is nothing to prove. Assume $\dim_Z(\mathfrak{b}/R) > 0$, so that $\mathfrak{b}\mathfrak{c} \supsetneq \mathfrak{c}$. We claim that there exists $z \in \mathfrak{b}\mathfrak{c} \setminus \mathfrak{c}$ such that $d(z) \leqslant 0$. Indeed, every element $x \in Z(t)$ has a partial fraction expansion, i.e. it can be written as the sum of an element of $Z[t]$ and a finite k-linear combination of elements of the form t^i/f^n, where $f \in Z[t]$ is an irreducible

polynomial, $n \in \mathbf{Z}_{>0}$ and $0 \leqslant t < \deg f$. Consequently, $Z = S + \mathfrak{c}$ with $S = \{x \in Z(t)^* : d(x) \leqslant 0\} \cup \{0\}$, and our claim follows. We have $\mathfrak{b}\mathfrak{c}z^{-1} \supset R$ and over R its Z-dimension $\dim(\mathfrak{b}\mathfrak{c}z^{-1}/R) = \dim(\mathfrak{b}\mathfrak{c}/\mathfrak{c}) - \dim(R/\mathfrak{c}) + \dim(R/Rz) = \dim(\mathfrak{b}/R) - 1 + d(z)$ is strictly smaller than $\dim(\mathfrak{b}/R)$. Our induction hypothesis gives $\mathfrak{b}\mathfrak{c} \sim \mathfrak{c}^{\dim(\mathfrak{b}/R)+1-d(z)}$, so $\mathfrak{b} \sim \mathfrak{c}^{-\dim(\mathfrak{b}/R)-d(z)} \sim \mathfrak{c}^{-\dim(\mathfrak{b}/R)}$ and we are done. □

If R is as in the lemma, one sees that $R = \sum_{i=0}^{\deg g - 1} Z[1/g]t^i/g$. It follows that R is the integral closure of the ring $Z[1/g]$ of polynomials in $1/g$ in the field $Z(t)$.

Now suppose that k is a field of characteristic $p > 0$ and that there exist $\alpha, \beta \in k$ such that $[k(\sqrt[p]{\alpha}, \sqrt[p]{\beta}) : k] = p^2$. In order to construct a counter-example to theorem 1 for an inseparable extension L/K we choose A and L as below.

$$\begin{array}{ccccccc} k(\sqrt[p]{\beta}, t) & = & L & \supset & B & & \\ & & | & & | & & \\ k(t^p) & = & K & \supset & A & = & k\left[\dfrac{1}{t^p - \alpha}\right] \end{array}$$

The integral closure B of A in L is the integral closure of $k(\sqrt[p]{\beta})[(t^p - \alpha)^{-1}]$ in L, so the proposition applied to $Z = k(\sqrt[p]{\beta})$ and the irreducible polynomial $g = t^p - \alpha \in Z[t]$ shows that B has a class group of order p. We claim that B has no primes of degree one over A, so that its class group cannot be generated by the classes of such primes. For the degree valuation, the residue class field extension is of degree $[k(\sqrt[p]{\beta}) : k] = p$. For all other valuations of A, it is an extension of the form $k(\gamma^p) \subset k(\sqrt[p]{\beta}, \gamma)$, where γ denotes the residue class of t. If the degree of this extension is one, then $k(\gamma) = k(\gamma^p)$, so $k \subset k(\gamma)$ is a separable extension. This contradicts the fact that $\sqrt[p]{\beta} \in k(\gamma)$, and our claim is proved.

More generally, the argument above shows that for any non-perfect field k, one can construct examples of this type: if $\beta \in k \setminus k^p$ with $p = \operatorname{char} k$ and t is transcendental over k, take $L = k(\sqrt[p]{\beta})(t)$. As $k(\sqrt[p]{\beta})$ is not algebraically closed, there exist irreducible polynomials $g \in k(\sqrt[p]{\beta})[t]$ of arbitrarily high degree, so the construction above gives us infinitely many Dedekind domains $B \supset k(\sqrt[p]{\beta})[1/g]$ in L having non-trivial class group. As in our example, the rings B have no primes of degree one with respect to the subring $A = B \cap k(t^p)$ of which they are the integral closure in L.

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 Wojcik'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.

REFERENCES

[1] BAUER, M Zur Theorie der algebraischen Zahlkorper *Math Ann 77* (1916), 353-356

[2] BIANCHI, L Sugli ideali primarii assoluti in un corpo algebrico *Journ de Math (9) 1* (1922), 1 18

[3] CASSELS, J W S and A FROHLICH (eds) *Algebraic Number Theory* Academic Press, 1967

[4] CEBOTAREV, N Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehoren *Math Ann 95* (1926), 191-228

[5] DEURING, M *Klassenkorpertheorie* Lecture notes Universitat Gottingen (1966)

[6] FOSSUM, R M *The divisor class group of a Krull domain* Springer Verlag, Berlin, 1973

[7] FEIN, B , W M KANTOR and M SCHACHER Relative Brauer groups, II *J Reine Angew Math 328* (1981), 39-57

[8] FROBENIUS, G Uber die Beziehungen zwischen den Primidealen eines algebraischen Korpers und den Substitutionen seiner Gruppe *S B preuss Akad Wiss* (1896), 689-703

[9] HARTSHORNE, R *Algebraic Geometry* Springer Verlag, Berlin, 1977

[10] HILBERT, D Die Theorie der algebraischen Zahlkorper *Jber Deutsch Math Verein 4* (1894/5), 175-546

[11] KUMMER, E E *Collected Papers, vol I* Springer Verlag, Berlin, 1975

[12] LANG, S *Algebraic number theory* Addison Wesley, Reading, 1970

[13] SCHUR, I Uber die Existenz unendlich vieler Primzahlen in einigen speziellen arithmethischen Progressionen *S -B Berlin Math Ges 11* (1912)

[14] WASHINGTON, L *Introduction to cyclotomic fields* Springer Verlag, Berlin, 1982

[15] WOJCIK, J A refinement of a theorem of Schur on primes in arithmetic progressions II *Acta Arith 12* (1966), 97-109

[16] —— A refinement of a theorem of Schur on primes in arithmetic progressions III *Acta Arith 15* (1969), 193-197

[17] —— A purely algebraic proof of special cases of Tschebotarev's theorem *Acta Arith 28* (1975), 137-145

(Reçu le 25 juin 1990)

Hendrik W Lenstra Jr
Peter Stevenhagen

Department of Mathematics
University of California
Berkeley, CA 94720 (USA)