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: 3. THE INSEPARABLE CASE
DOI: https://doi.org/10.5169/seals-58727

$= \prod_{i=1}^{t} [\mathfrak{b}_i]^{-1} \in Cl_B$. 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 $xB = \mathfrak{q} \cdot \prod_{i=1}^{t} \mathfrak{b}_i$ 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 $\mathfrak{b}\mathfrak{c} \supseteq \mathfrak{c}$. 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 $0 \leqslant i < \deg f$. 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.