Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Number Theory 106 (2004) 26–49
JOURNAL OF Number Theory
http://www.elsevier.com/locate/jnt

Abelian subgroups of any order in class groups of global function fields

Allison M. Pacelli*

Department of Mathematics, Williams College, Bronfman Science Center, Room 200, Williamstown, MA 01267, USA

Received 14 December 2002; revised 27 August 2003

Communicated by D. Goss

Abstract

Let $\mathbb{F}$ be a finite field with q elements, and T a transcendental element over $\mathbb{F}$. In this paper, we construct infinitely many real function fields of any fixed degree over $\mathbb{F}(T)$ with ideal class numbers divisible by any given positive integer greater than 1. For imaginary function fields, we obtain a stronger result which shows that for any relatively prime integers m and n with $m, n > 1$ and relatively prime to the characteristic of $\mathbb{F}$, there are infinitely many imaginary fields of fixed degree m such that the class group contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{m-1}$.
© 2004 Elsevier Inc. All rights reserved.

Keywords: Class group; Class number; Function field

1. Introduction

Determining the structure of the class group is a difficult problem in both number fields and function fields that has been studied since Gauss first considered class groups of quadratic fields. Although class groups can only be computed in special cases at present, there are many interesting questions that one can ask: for example, how many class groups have class numbers divisible by a given integer n? Nagell [6] answered a special case of this question in 1922 by showing the existence of infinitely many imaginary quadratic number fields with class number divisible by a given

*Fax: +413-597-2438.
E-mail address: apacelli@williams.edu.

0022-314X/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2003.12.003

integer n. Yamamoto [10] proved the same result for real quadratic number fields in 1969. Cohen and Lenstra [3] gave a heuristic argument in 1983 predicting, as $x \to \infty$, a positive fraction of quadratic number fields with discriminant $< x$ having class number divisible by a given integer n. Their argument has been generalized to number fields of any degree and to function fields, but has not been proven yet in any of these cases.

In 1983, Azuhata and Ichimura [1] proved a result not only about the divisibility of the class number but also about the structure of the class group in the number field situation. They constructed infinitely many number fields K of degree m over $\mathbb{Q}$ such that the class group of K contains an abelian subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{r_2}$ in the special case that $r_2 > 1$. As usual, r_2 denotes half the number of complex embeddings of K into $\mathbb{C}$. Unfortunately their result says nothing about the class group of a totally real number field. In 1985, however, Shin Nakano [7] was able to extend this result to the totally real case, constructing a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$ in the class group of a totally real number field and increasing the rank of the subgroup from r_2 to $r_2 + 1$ in class groups of non-totally real fields. The smaller rank of the subgroup for totally real fields is a consequence of the extra units present.

The results above describe the class groups of number fields. Less is known about the analogous question of class groups of global function fields. In 1992, Friesen [4] constructed infinitely many real quadratic function fields with class number divisible by a given integer n. Murty and Cardon [2] proved a stronger result about quadratic function fields in 2001, giving a lower bound on the number of such fields with class number divisible by a given integer $n > 3$. Their results have been generalized to cyclic function fields of prime degree l over the rational function field in a forthcoming paper [8]. In 1999, Ichimura [5] gave a partial function field analogue to his and Azuhata's results in [1] for the special case that m is prime. In this case, the size of the subgroup constructed depends on the factorization of $X^m - 1$ in $\mathbb{F}[X]$. In this paper, we give more general function field analogues of the results of Azuhata, Ichimura, and Nakano, above, which imply the existence of infinitely many function fields of any fixed degree with ideal class numbers divisible by any given positive integer greater than 1.

Let q be a power of an odd prime, and let $\mathbb{F}$ be the field with q elements. Let k be the rational function field, and fix a transcendental element T of k so that $k = \mathbb{F}(T)$. If K is an extension of k, then denote by $\mathcal{O}_K$ the integral closure of $\mathbb{F}[T]$ in K. We write Cl_K to denote the ideal class group of $\mathcal{O}_K$. The main results are as follows:

Theorem 1. *For any relatively prime integers $m, n \in \mathbb{Z}$, not divisible by the characteristic of $\mathbb{F}(T)$, with $m, n > 1$, there exist infinitely many function fields K of degree m over $k = \mathbb{F}(T)$ such that*

(1) *the prime at infinity is totally ramified in K, and*
(2) Cl_K *contains an abelian subgroup isomorphic to* $(\mathbb{Z}/n\mathbb{Z})^{m-1}$.

Theorem 2. *For any integers $m, n \in \mathbb{Z}$, not divisible by the characteristic of $\mathbb{F}(T)$, with $m, n > 1$, there exist infinitely many function fields K of degree m over $k = \mathbb{F}(T)$ such that*

(1) *the prime at infinity splits completely in K, and*
(2) Cl_K *contains an abelian subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$.*

For the proofs of both theorems, we construct a polynomial

$$f(X) = \prod_{i=0}^{m-1} (X - B_i) + D^n,$$

where $B_0, \ldots, B_{m-1}$ and D are certain polynomials in $\mathbb{F}[T]$. The method by which we choose the B_i's and D will be different for each case in order to force the behavior of the prime at infinity. If θ is a root of $f(X)$, then $K = k(\theta)$ satisfies the conditions of the theorems.

2. Imaginary case

In the function field situation, we no longer have the quantities r_1 and r_2, so we cannot refer to a function field as real or imaginary depending on whether or not r_2 is 0. The analogue is to consider the prime at infinity in k. If the infinite prime is totally ramified in K, then we say that K is imaginary, and if the infinite prime splits completely, we say that K is totally real. In this section, we prove Theorem 1, which deals with the imaginary case.

Let $\mathscr{L}$ be the set of all prime divisors of n, and define $n_0 = \prod_{l \in \mathscr{L}} l$. Let m_0 be the least common multiple of the orders of all roots of unity contained in any function field of degree m. Let E and W denote, respectively, the group of units and the group of roots of unity in the field K. For an element r in $\mathbb{F}[T]$, let $|r| = q^{\deg(r)}$. Given polynomials $B_0, \ldots, B_{m-1}, D \in \mathbb{F}[T]$, define

$$f(X) = \prod_{i=0}^{m-1} (X - B_i) + D^n,$$

and let θ be a root. Set $K = k(\theta)$. The next two lemmas and proposition show that with an appropriate choice of $B_0, \ldots, B_{m-1}$, and D, the field K satisfies the conditions of Theorem 1.

Lemma 1. *Suppose there exist monic, irreducible polynomials $p_1, \ldots, p_{m-1}$ with $|p_i| \equiv 1 \pmod{m_0 n_0}$ and polynomials $B_1, \ldots, B_{m-1}$, and D in $\mathbb{F}[T]$ such that*

(2.1) $f(0) \equiv 0 \pmod{p_1 \cdots p_{m-1}}$,
(2.2) $(f'(0), p_1 \cdots p_{m-1}) = 1$, *and*
(2.3) $\left(\frac{B_i}{p_i}\right)_l \neq 1$, $\left(\frac{B_i}{p_j}\right)_l = 1$ *for* $i \neq j$, $1 \leqslant i,\ j \leqslant m-1$, *and for each* $l \in \mathscr{L}$.

For each $l \in \mathscr{L}$, the subgroup of $K^\times / WK^{\times l}$ generated by the classes of $\theta - B_1$, $\theta - B_2, \ldots, \theta - B_{m-1}$ is an elementary abelian group of rank $m-1$.

Proof. Let p denote one of the primes $p_1, \ldots, p_{m-1}$, and set $P = (p)$. Let $\hat{k}_P$ be the completion of k at P. Notice that

$$K \otimes_k \hat{k}_P \cong \prod_{j=1}^{t} L_j,$$

where $[L_j : \hat{k}_P] = e_j f_j$, and e_j, f_j denote, respectively, the ramification index and relative degree of the prime in L_j lying over $\hat{P} \in \hat{k}_P$. Since $K = k(\theta)$, and f is the minimal polynomial for θ over k, we have $K \cong k[x]/(f(X))$. If $f_1(X), f_2(X), \ldots, f_t(X)$ are the irreducible factors of f over $\hat{k}_P$, then

$$\begin{aligned} K \otimes_k \hat{k}_P &\cong k[x]/(f(X)) \otimes_k \hat{k}_P \\ &\cong \hat{k}[x]/(f_1(X) f_2(X) \cdots f_t(X)) \\ &\cong \bigoplus_{j=1}^{t} \hat{k}_P[x]/(f_j(X)) \\ &\cong \bigoplus_{j=1}^{t} \hat{k}_P(\theta_j), \end{aligned}$$

where each θ_j is a root of $f_j(X)$ in $\hat{k}_P$.

We claim that one of the irreducible factors of f over $\hat{k}_P$ is linear. By condition (2.1), $f(0) \equiv 0 \pmod{p}$, so we have

$$f(X) \equiv Xg(X) \pmod{p}$$

for some $g(X) \in \hat{k}_P[X]$. Then

$$f'(X) \equiv Xg'(X) + g(X) \pmod{p}.$$

By condition (2.2),

$$g(0) \equiv f'(0) \not\equiv 0 \pmod{p}.$$

By Hensel's Lemma, then

$$f(X) \equiv (X - \tilde{\theta}) h(X) \in \hat{k}_p[X],$$

where $X - \tilde{\theta} \equiv X \pmod{p}$, and $h(X) \equiv g(X) \pmod{p}$. In particular, this implies that $\tilde{\theta} \in p\mathbb{F}[T]_P$, where $\mathbb{F}[T]_P$ is the completion of $\mathbb{F}[T]$ at P.

Let λ denote the embedding from $K = k(\theta)$ to $\hat{k_P}$ which takes θ to $\tilde{\theta}$. Given such an embedding, there is a corresponding prime ideal $\mathfrak{p}_\lambda$ in $\mathcal{O}_K$ lying over P:

$$\mathfrak{p}_\lambda = \{\alpha \in \mathcal{O}_K \mid \mathrm{ord}_P(\lambda(\alpha)) > 0\}.$$

Notice that $\theta \in \mathfrak{p}_\lambda$ since $\lambda(\theta) = \tilde{\theta} \in p\mathbb{F}[T]_P$. Furthermore, if e_λ and f_λ denote the ramification index and relative degree, respectively, of $\mathfrak{p}_\lambda$ over P, then

$$e_\lambda f_\lambda = \deg(X - \tilde{\theta}) = 1.$$

Thus $e_\lambda = f_\lambda = 1$, and so, for each prime p_i, $1 \leqslant i \leqslant m-1$, there exists some prime ideal $\mathfrak{p}_i \subset \mathcal{O}_K$ over $P = (p_i) \subset \mathbb{F}[T]$ of relative degree 1 and such that $\theta \equiv 0 \pmod{\mathfrak{p}_i}$.

Fix $l \in \mathscr{L}$. To prove the lemma, suppose that

$$(\theta - B_1)^{b_1} \cdots (\theta - B_{m-1})^{b_{m-1}} \in WK^{\times l},$$

for some $b_1, \ldots, b_{m-1} \in \mathbb{Z}$. Since $|p_i| \equiv 1 \pmod{m_0 n_0}$, then $\frac{|p_i|-1}{l} = m_0 z$ for some integer z. It follows that any root of unity in K is an lth power residue mod $\mathfrak{p}_i$ because if $\zeta \in W$, then

$$\left(\frac{\zeta}{\mathfrak{p}_i}\right)_l \equiv \zeta^{\frac{|p_i|-1}{l}} \equiv \zeta^{m_0 z} = 1 \pmod{p_i}.$$

Thus

$$\left(\frac{\theta - B_1}{\mathfrak{p}_i}\right)_l^{b_1} \cdots \left(\frac{\theta - B_{m-1}}{\mathfrak{p}_i}\right)_l^{b_{m-1}} = 1.$$

Since $\theta - B_i \equiv -B_i \pmod{\mathfrak{p}_i}$,

$$\left(\frac{-1}{\mathfrak{p}_i}\right)_l^{b_1+\cdots+b_{m-1}} \left(\frac{B_1}{\mathfrak{p}_i}\right)_l^{b_1} \cdots \left(\frac{B_{m-1}}{\mathfrak{p}_i}\right)_l^{b_{m-1}} = 1.$$

By condition (2.3) then,

$$\left(\frac{-1}{\mathfrak{p}_i}\right)_l^{b_1+\cdots+b_{m-1}} \left(\frac{B_i}{\mathfrak{p}_i}\right)_l^{b_i} = 1.$$

If l is odd, then clearly $(\frac{-1}{\mathfrak{p}_i})_l = 1$. If l is even, then n_0 is also even, so $|p_i| \equiv 1 \pmod 4$; say $|p_i| - 1 = 4z$ for some integer z. In this case, it is also true that $(\frac{-1}{\mathfrak{p}_i})_l = 1$ since $(\frac{-1}{\mathfrak{p}_i})_l \equiv (-1)^{\frac{|p_i|-1}{l}} \equiv (-1)^{\frac{4z}{l}} \equiv 1 \pmod{p_i}$. Thus

$$\left(\frac{B_i}{\mathfrak{p}_i}\right)_l^{b_i} = 1.$$

But again by condition (2.3), this implies $l | b_i$.

Repeating the argument above for each prime p_i, $1 \leqslant i \leqslant m-1$, we see that $l|b_i$ for each i, $1 \leqslant i \leqslant m-1$. It follows that the $m-1$ elements $\theta - B_1, \theta - B_2, \ldots, \theta - B_{m-1}$ are linearly independent over $WK^{\times l}$. $\square$

The following standard lemma will be used to construct the desired subgroup of Cl_K.

Lemma 2. *Suppose G is a finite abelian group of exponent n, and $\dim_{\mathbb{Z}/l\mathbb{Z}} G^{n/l} \geqslant r$ for all l dividing n. Then G contains a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n\mathbb{Z}$ of rank r.*

Proposition 1. *Suppose that the polynomials $B_0, \ldots, B_{m-1}$ and D further satisfy the following two conditions*:

(2.4) *$\theta - B_0, \theta - B_1, \ldots, \theta - B_{m-1}$ are pairwise relatively prime,*
(2.5) *the prime at infinity is totally ramified in K.*

Then Cl_K contains an abelian subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{m-1}$.

Proof. Let $\mathrm{Cl}_K[n]$ denote the set of all elements of the class group of $\mathcal{O}_K$ whose orders divide n. By the previous lemma, we need only show that $\mathrm{Cl}_K[n]^{n/l}$ has dimension at least $m-1$ over $\mathbb{Z}/l\mathbb{Z}$ for all l in $\mathscr{L}$. Consider the following sequence:

$$(1) \to \mathrm{Cl}_K\left[\frac{n}{l}\right] \xrightarrow{i} \mathrm{Cl}_K[n] \xrightarrow{h} K^{\times}/EK^{\times l},$$

where i is just inclusion, and the map h is defined as follows. Let $\bar{\mathfrak{a}}$ denote the class of the ideal $\mathfrak{a}$ in $\mathrm{Cl}_K[n]$. If $\bar{\mathfrak{a}} \in \mathrm{Cl}_K[n]$, then $\mathfrak{a}^n = (\alpha)$ for some $\alpha \in \mathcal{O}_K$. Set $h(\mathfrak{a}) = [\alpha]_l$, where $[\alpha]_l$ denotes the class of α in $K^{\times}/EK^{\times l}$. One can show that h is a well-defined homomorphism, and the above sequence is exact.

Since the prime at infinity is totally ramified, we know that the rank of the unit group in K is 0; therefore the only units in K are the roots of unity. Replacing E by W in the sequence above yields the following exact sequence:

$$(1) \to \mathrm{Cl}_K\left[\frac{n}{l}\right] \xrightarrow{i} \mathrm{Cl}_K[n] \xrightarrow{h} K^{\times}/WK^{\times l}. \tag{1}$$

Recall that

$$\prod_{i=0}^{m-1} (\theta - B_i) = -D^n,$$

since θ is a root of $f(X)$. By condition (2.4) then, each ideal $(\theta - B_i)$ is an nth power. Set $D_i^n = (\theta - B_i)$ for $1 \leqslant i \leqslant m-1$. It follows that $h(\overline{D_i}) = [\theta - B_i]_l$. As a vector space over $\mathbb{Z}/l\mathbb{Z}$, then, $\mathrm{Im}(h)$ has dimension at least $m-1$ by Lemma 1. Since the

sequence in Eq. (1) is exact,

$$\mathrm{Im}(h) \cong \mathrm{Cl}_K[n]/\mathrm{Cl}_K\left[\frac{n}{l}\right] \cong \mathrm{Cl}_K[n]^{n/l},$$

and so, $\mathrm{Cl}_K[n]^{n/l}$ has dimension at least $m-1$ over $\mathbb{Z}/l\mathbb{Z}$.

To prove Theorem 1, we will show that it is possible to choose irreducible polynomials $p_1, \ldots, p_{m-1}$ and polynomials $B_0, \ldots, B_{m-1}$, and $D \in \mathbb{F}[T]$ so that conditions (2.1)–(2.5) are satisfied, and $f(X)$ is irreducible. Finally, note that the existence of infinitely many such fields K is a consequence of the existence of one such field because of the finiteness of the class number. Let p be prime. If K_1 is a field of degree m whose class group contains a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{m-1}$, and h_1 is the class number of K_1, then let f_1 be any integer such that $p^{f_1} > h_1$. Next, let K_2 be a field of degree m whose class group contains a subgroup isomorphic to $(\mathbb{Z}/p^{f_1}\mathbb{Z})^{m-1}$. Since $p^{f_1} > h_1$, we know that K_1 and K_2 are distinct. Moreover, the class group of K_2 also contains a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{m-1}$. If h_2 is the class number of K_2, then next choose an integer f_2 with $p^{f_2} > h_2$, and a field K_3 of degree m whose class group contains a subgroup isomorphic to $(\mathbb{Z}/p^{f_2}\mathbb{Z})^{m-1}$. Again, K_3 is distinct from K_1 and K_2, and the class group of each field contains a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{m-1}$. Continuing in this manner, we create infinitely many function fields of degree m with class group containing a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{m-1}$. A similar argument shows that the existence of one field whose class group contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{m-1}$ for a general n implies the existence of infinitely many such fields.

2.1. Choosing polynomials

Choose distinct irreducible polynomials p_i, s in $\mathbb{F}[T]$, $1 \leqslant i \leqslant m-1$, such that

$$|p_i| \equiv 1 \pmod{m_0 n_0}, \quad 1 \leqslant i \leqslant m-1,$$

and

$$|s| \equiv 1 \pmod{m}.$$

Note that there are infinitely many such primes p_i and s. Because m and n are relatively prime to the characteristic of $\mathbb{F}$, the primes whose norms are congruent to 1 modulo an integer m are exactly those primes which split completely in $k(\zeta_m)$, where ζ_m is a primitive mth root of unity.

Since $|p_i| \equiv 1 \pmod{m_0 n_0}$, we have $l \mid (|p_i| - 1)$ for all $l \in \mathscr{L}$. Let g_i, $1 \leqslant i \leqslant m-1$, be a primitive root mod p_i that satisfies the congruence

$$g_i^2 + (m-2)g_i + 1 \not\equiv 0 \pmod{p_i}. \tag{2}$$

This is possible since $|p_i| - 1 > 3$. Since $m \mid (|s| - 1)$, we also have that

$$X^m - 1 \equiv \prod_{i=0}^{m-1} (X - C_i) \pmod{s},$$

where the C_i's are distinct mod s for $1 \leqslant i \leqslant m-1$. Choose B_i, $1 \leqslant i \leqslant m-1$ such that

$$B_i \equiv \begin{cases} 1 & (\mathrm{mod}\, p_j) \text{ if } i \neq j, \\ g_i & (\mathrm{mod}\, p_i), \\ C_i & (\mathrm{mod}\, s). \end{cases}$$

Choose B_0 such that

$$B_0 \equiv \begin{cases} g_i^{-1} & (\mathrm{mod}\, p_i) \text{ for } 1 \leqslant i \leqslant m-1, \\ C_0 & (\mathrm{mod}\, s). \end{cases}$$

Next choose an irreducible polynomial D such that the following properties hold.

$$D \equiv \begin{cases} 1 & (\mathrm{mod}\, s), \\ (-1)^{m+1} & (\mathrm{mod}\, p_i) \text{ for } 1 \leqslant i \leqslant m-1, \end{cases}$$

$$\begin{aligned} &(\deg(D), m) = 1, \\ &\deg(D^n) > m \max\{\deg(B_i)\}_{i=0}^{m-1}, \\ &(B_i - B_j, D) = 1 \text{ for } 0 \leqslant i, j \leqslant m-1,\ i \neq j. \end{aligned} \tag{3}$$

Infinitely many D satisfying the first two properties exist by a strong version of Dirichlet's Theorem for function fields [9, p. 40] which asserts that in any arithmetic progression, there exist irreducible polynomials of each large degree. We need only discard finitely many not satisfying the second two properties above.

2.2. Verification of divisibility conditions

Lemma 3. *With polynomials $B_0, \ldots, B_{m-1}$ and D in $\mathbb{F}[T]$ chosen as above, conditions* (2.1)–(2.3) *in Lemma* 1 *are satisfied.*

Proof. Condition (2.1) is satisfied because

$$\begin{aligned} D^n + (-1)^m B_0 B_1 \cdots B_{m-1} &\equiv (-1)^{(m+1)n} + (-1)^m g_i^{-1} g_i \pmod{p_i} \\ &\equiv (-1)^{m+1} + (-1)^m \pmod{p_i} \\ &\equiv 0 \pmod{p_i}. \end{aligned}$$

For condition (2.2), observe that

$$\begin{aligned} f'(0) &= \sum_{k=0}^{m-1} \prod_{\substack{j=0 \\ j\neq k}}^{m-1} (-B_j) \\ &\equiv (-1)^{m-1} \left[\prod_{j=1}^{m-1} B_j + \sum_{\substack{k=1 \\ k\neq i}}^{m-1} \prod_{\substack{j=0 \\ j\neq k}}^{m-1} B_j + \prod_{\substack{j=0 \\ j\neq k}}^{m-1} B_j \right] \pmod{p_i} \\ &\equiv (-1)^{m-1} [g_i + m - 2 + g_i^{-1}] \pmod{p_i} \\ &\not\equiv 0 \pmod{p_i} \text{ by Eq. (2).} \end{aligned}$$

Finally, condition (2.3) follows immediately from the choice of B_i for $1 \leqslant i \leqslant m-1$. □

Lemma 4. *$\theta - B_0, \theta - B_1, \ldots, \theta - B_{m-1}$ are pairwise relatively prime, that is, condition (2.4) in Proposition 1 is satisfied.*

Proof. We chose D so that $(B_i - B_j, D) = 1$ for $i \neq j$, $0 \leqslant i, j \leqslant m-1$. If there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\mathfrak{p}$ divides both $\theta - B_i$ and $\theta - B_j$ for some i and j, then $\mathfrak{p} | (B_i - B_j)$. Since $\prod_{h=0}^{m-1} (\theta - B_h) = -D^n$, we also have that $\mathfrak{p} \mid D$. Thus, $\mathfrak{p} \mid (B_i - B_j, D)$, a contradiction. □

Lemma 5. *With the conditions on $B_0, \ldots, B_{m-1}$, and D given above, $f(X)$ is irreducible.*

Proof. We show that $f(X)$ is an Eisenstein polynomial with respect to s. Notice first that $s || (D^n + (-1)^m B_0 B_1 \cdots B_{m-1})$, the constant term of $f(X)$:

$$\begin{aligned} D^n + (-1)^m B_0 B_1 \cdots B_{m-1} &\equiv 1 + (-1)^m \prod_{i=0}^{m-1} C_i \pmod{s} \\ &\equiv 1 - 1 \pmod{s} \\ &\equiv 0 \pmod{s}. \end{aligned}$$

If $s^2 \mid (D^n + (-1)^m B_0 B_1 \cdots B_{m-1})$, then replace B_0 by $B_0 + p_1 \cdots p_{m-1} s$. All the desired properties of $B_1, \ldots, B_{m-1}$ and D above still hold since $B_0 \equiv B_0 + p_1 \cdots p_{m-1} s$ modulo p_i and s. But now we also have that

$$\begin{aligned} &D^n + (-1)^m (B_0 + p_1 \cdots p_{m-1} s) B_1 \cdots B_{m-1} \\ &\quad \equiv D^n + (-1)^m B_0 \cdots B_{m-1} + (-1)^m p_1 \cdots p_{m-1} s B_1 \cdots B_{m-1} \pmod{s^2} \end{aligned}$$

$$\equiv 0 + (-1)^m p_1 \cdots p_{m-1} s B_1 \cdots B_{m-1} \pmod{s^2}$$

$$\not\equiv 0 \pmod{s^2}.$$

Because $f(X)$ is monic, we need only show that the remaining coefficients of f are divisible by s. Since $B_i \equiv C_i \pmod{s}$ for $0 \leqslant i \leqslant m-1$, then

$$\prod_{i=0}^{m-1} (X - B_i) \equiv X^m - 1 \pmod{s}.$$

So all coefficients of $\prod_{i=0}^{m-1} (X - B_i)$, excluding the leading and constant terms, are divisible by s. Since these are exactly the coefficients of $f(X)$ under consideration, this completes the proof. □

2.3. The infinite prime

Lemma 6. *The prime at infinity is totally ramified in K, that is, condition* (2.5) *in Proposition* 1 *is satisfied.*

Proof. Consider the Newton polygon for $f(X)$ with respect to the prime at ∞. In this case, it is not hard to see that the Newton Polygon consists of the single line segment from $(0, -\deg(B_0 \cdots B_{m-1} + D^n))$ to $(m, 0)$ with slope equal to $\deg(B_0 \cdots B_{m-1} + D^n)/m$. Thus $f(X)$ has m roots θ_i each with

$$\operatorname{ord}_\infty(\theta_i) = \frac{-1}{m} \deg(B_0 \cdots B_{m-1} + D^n) = -\frac{n \deg(D)}{m},$$

by Eq. (3). Since m is relatively prime to both n and $\deg(D)$, ∞ must be totally ramified in K. □

3. Real case

We now address the analogue of the totally real case for number fields, that is, the situation in which the infinite prime splits completely. As in [7], we increase the rank of the subgroup of $K^\times / WK^{\times l}$ by one in order to obtain a copy of $\mathbb{Z}/n\mathbb{Z}$ in Cl_K. In order to obtain this extra rank, we need one more linearly independent element over $WK^{\times l}$. This requires choosing a new polynomial $A \in \mathbb{F}[T]$ such that $f(A)$ is an nth power. We also choose $B_0, \ldots, B_{m-1}$ and D differently than in the last section; we use parametric representations as in [7].

Lemma 7. *Suppose there exist monic, irreducible polynomials* $p_1, \ldots, p_{m-1}$ *and* s *with* $|s| \equiv 1 \bmod (m_0 n_0)$ *and polynomials* $B_1, \ldots, B_{m-1}, A, C,$ *and* D *in* $\mathbb{F}[T]$ *such that for each* $l \in \mathscr{L}$

(3.1) $f(0) \equiv 0 \pmod{p_1 \cdots p_{m-1} s}$,
(3.2) $(f'(0), p_1 \cdots p_{m-1} s) = 1$,
(3.3) $\left(\frac{B_i}{p_i}\right)_l \neq 1$, $\left(\frac{B_i}{p_j}\right)_l = 1$ *for* $i \neq j$, $1 \leqslant i \leqslant m-1$, $1 \leqslant j \leqslant m-1$, *and*
(3.4) $\left(\frac{B_i}{s}\right)_l = 1$, $\left(\frac{A}{s}\right)_l \neq 1$ *for* $1 \leqslant i \leqslant m-1$.

Then for each $l \in \mathscr{L}$, *the subgroup of* $K^\times / WK^{\times l}$ *generated by the classes of* $\theta - B_1, \theta - B_2, \ldots, \theta - B_{m-1}$, *and* $\theta - A$ *is an elementary abelian group of rank* m.

Proof. The proof is similar to that of Lemma 1 for the imaginary case. Since we also have that $f(0) \equiv 0$ and $f'(0) \not\equiv 0 \pmod{s}$ by conditions (3.1) and (3.2) above, the argument in Lemma 1 also proves that there exists a prime $\mathfrak{s}$ of K over s of relative degree 1 which contains θ.

Fix $l \in \mathscr{L}$. To prove the lemma, suppose that

$$(\theta - B_1)^{b_1} \cdots (\theta - B_{m-1})^{b_{m-1}} (\theta - A)^a \in WK^{\times l},$$

where b_i, $a \in \mathbb{Z}$. Since $|s| \equiv 1 \pmod{m_0 n_0}$, any root of unity in K is an lth power residue mod $\mathfrak{s}$, so

$$\left(\frac{\theta - B_1}{\mathfrak{s}}\right)_l^{b_1} \cdots \left(\frac{\theta - B_{m-1}}{\mathfrak{s}}\right)_l^{b_{m-1}} \left(\frac{\theta - A}{\mathfrak{s}}\right)_l^{a} = 1.$$

Since $\theta - B_i \equiv -B_i \pmod{\mathfrak{s}}$,

$$\left(\frac{-1}{\mathfrak{s}}\right)_l^{b_1 + \cdots + b_{m-1} + a} \left(\frac{B_1}{\mathfrak{s}}\right)_l^{b_1} \cdots \left(\frac{B_{m-1}}{\mathfrak{s}}\right)_l^{b_{m-1}} \left(\frac{A}{\mathfrak{s}}\right)_l^{a} = 1.$$

By condition (3.4) then,

$$\left(\frac{-1}{\mathfrak{s}}\right)_l^{b_1 + \cdots + b_{m-1} + a} \left(\frac{A}{\mathfrak{s}}\right)_l^{a} = 1.$$

If l is odd then clearly $\left(\frac{-1}{\mathfrak{s}}\right)_l = 1$.If l is even, then n_0 is also even, so $|s| \equiv 1 \pmod 4$. In this case, it is also true that $\left(\frac{-1}{\mathfrak{s}}\right)_l = 1$. Thus

$$\left(\frac{A}{\mathfrak{s}}\right)_l^{a} = 1.$$

But again by condition (3.4), this implies $l \mid a$.

The proof is now reduced to showing that $b_i \equiv 0 \pmod{l}$ for $1 \leqslant i \leqslant m-1$ which follows just as in Lemma 1. □

Proposition 2. *Suppose that the primes* $p_1, \ldots, p_{m-1}$ *and* s *and polynomials* $B_0, \ldots, B_{m-1}, A, C$, *and* D *further satisfy the following four conditions*:

(3.5) $f(A) = C^n$,
(3.6) $(f'(A), C) = 1$,
(3.7) $(f'(B_i), D) = 1$ *for* $i = 1, \ldots, m-1$, *and*
(3.8) *the prime at infinity splits completely in* K.

Then the ideal class group of $\mathcal{O}_K$ *contains an abelian subgroup isomorphic to* $\mathbb{Z}/n\mathbb{Z}$.

Proof. As before, let $\mathrm{Cl}_K[n]$ denote the set of all elements of the class group of $\mathcal{O}_K$ whose orders divide n. By Lemma 2, we need only show that $\mathrm{Cl}_K[n]^{n/l}$ has dimension at least 1 over $\mathbb{Z}/l\mathbb{Z}$ for all l in $\mathscr{L}$. The following sequence is still exact:

$$(1) \to \mathrm{Cl}_K\left[\frac{n}{l}\right] \xrightarrow{i} \mathrm{Cl}_K[n] \xrightarrow{h} K^\times / EK^{\times l}. \tag{4}$$

Because the infinite prime splits completely, however, we cannot just replace E by W in the sequence as before. Instead, let $S \subset K^\times / WK^{\times l}$ be the subgroup generated by the classes of $\theta - A, \theta - B_1, \ldots, \theta - B_{m-1}$, and let $S' \subset K^\times / EK^{\times l}$ be the image of S under the natural reduction map from $K^\times / WK^{\times l}$ to $K^\times / EK^{\times l}$. The following sequence is also exact:

$$(1) \to S \cap EK^{\times l} / WK^{\times l} \to S \to S' \to (1).$$

As a result,

$$\dim_{\mathbb{Z}/l\mathbb{Z}}(S) = \dim_{\mathbb{Z}/l\mathbb{Z}}(E/W) + \dim_{\mathbb{Z}/l\mathbb{Z}}(S').$$

By Lemma 7, $\dim_{\mathbb{Z}/l\mathbb{Z}}(S) \geqslant m$, and by condition (3.8), we know that the rank of the unit group in K is $m-1$. Thus

$$m - 1 + \dim_{\mathbb{Z}/l\mathbb{Z}}(S') \geqslant m,$$

and so, $\dim_{\mathbb{Z}/l\mathbb{Z}}(S') \geqslant 1$. We claim that S' is contained in $\mathrm{Im}(h)$, from which the proposition follows. If $S' \subset \mathrm{Im}(h)$, then $\mathrm{Im}(h)$ has dimension at least 1 over $\mathbb{Z}/l\mathbb{Z}$. Since the sequence in Eq. (4) is exact,

$$\mathrm{Im}(h) \cong \mathrm{Cl}_K[n] / \mathrm{Cl}_K\left[\frac{n}{l}\right] \cong \mathrm{Cl}_K[n]^{n/l},$$

and so, $\mathrm{Cl}_K[n]^{n/l}$ has dimension at least 1 over $\mathbb{Z}/l\mathbb{Z}$ for all primes l dividing n. Applying Lemma 2 to $\mathrm{Cl}_K[n]$ completes the proof.

It remains to show that $S' \subset \mathrm{Im}(h)$. Since $f(A) = C^n$ by condition (3.5), there exists a polynomial $g(X) \in \mathbb{F}[T][X]$ with

$$f(X) = (X - A)g(X) + C^n.$$

Then

$$(\theta - A)g(\theta) = -C^n.$$

Notice that the ideals $(\theta - A)$ and $g(\theta)$ are relatively prime. If some prime $\mathfrak{p}$ divided both, then

$$g(A) \equiv g(\theta) \equiv 0 \pmod{\mathfrak{p}},$$

and $C \equiv 0 \pmod{\mathfrak{p}}$. This would imply that $f'(A) = g(A) \equiv 0 \pmod{\mathfrak{p}}$, contradicting condition (3.6) that $f'(A)$ and C are relatively prime. Thus the ideal $(\theta - A)$ is an nth power; set $D_m^n = (\theta - A)$ for some ideal D_m.

Replacing C with D above, the same argument shows that $(\theta - B_i)$ is also an nth power for $1 \leqslant i \leqslant m-1$ since $f'(B_i)$ is relatively prime to D by condition (3.7). Set $D_i^n = (\theta - B_i)$ for $1 \leqslant i \leqslant m-1$. We have $h(\overline{D}_i) = [\theta - B_i]_l$ for $1 \leqslant i \leqslant m-1$, and $h(\overline{D}_m) = [\theta - A]_l$, where $[\cdot]_l$ denotes the class of an element in $K^\times / EK^{\times l}$. This completes the proof. □

To prove Theorem 2, we will show that it is possible to choose primes $p_1, \ldots, p_{m-1}$ and s, and polynomials $B_0, \ldots, B_{m-1}, A, C$, and $D \in \mathbb{F}[T]$ so that conditions (3.1)–(3.8) are satisfied and $f(X)$ is irreducible. As in the imaginary case, the existence of infinitely many such fields K is a consequence of the existence of one such field because of the finiteness of the class number.

3.1. Choosing polynomials

Let $N = 2^m n$, and define polynomials

$$F_0(X) = X^n - 1,$$

$$F_i(X) = X^{2^i n} + 1 \text{ for } 1 \leqslant i \leqslant m-2,$$

and

$$F_{m-1}(X) = (X^n + 1)(X^{2^{m-1}n} + 1).$$

Note that $F_0(X) \cdots F_{m-1}(X) = X^N - 1$. Set $\mu_i = \deg(F_i)$, and observe that

$$\mu_0 < \cdots < \mu_{m-1},$$

and $\sum_{i=0}^{m-1} \mu_i = N$. Denote by $F_i(X, Y)$ the homogeneous polynomial defined by $F_i(X)$:

$$F_i(X, Y) = Y^{\mu_i} F_i\left(\frac{X}{Y}\right) \in \mathbb{F}[T][X, Y].$$

Lemma 8. *There exist infinitely many primes $s \in \mathbb{F}[T]$ with $|s| \equiv 1 \pmod{m_0 N}$ and for which there exists some $w \in \mathbb{F}[T]$ with*

$$\left(\frac{w}{s}\right)_l \neq 1, \quad \text{and} \quad \left(\frac{(w+1)^m - 1}{s}\right)_N = 1$$

for all primes l dividing n.

Proof. For each natural number v, let ζ_v be a fixed primitive v-th root of unity. Set $L = k(\zeta_{m_0 N}, \zeta_m)$. Choose any primes $\mathfrak{p}_1, \mathfrak{p}_2$ of L with $(\mathfrak{p}_2, mn_0) = 1$. Let π_1 and π_2 be uniformizing parameters for $\mathfrak{p}_1$ and $\mathfrak{p}_2$, respectively. Let $\beta \in L^\times$ be such that

$$\beta \equiv \begin{cases} \pi_1 & (\mathrm{mod}\ \mathfrak{p}_1^2), \\ -1 + \zeta_m + \pi_2 & (\mathrm{mod}\ \mathfrak{p}_2^2). \end{cases}$$

Because $\beta = (\beta - \pi_1) + \pi_1$, and $\beta - \pi_1$ and π_1 have different ords, then

$$\mathrm{ord}_{\mathfrak{p}_1}(\beta) = \min\{\mathrm{ord}_{\mathfrak{p}_1}(\beta - \pi_1), \mathrm{ord}_{\mathfrak{p}_1}(\pi_1)\} = 1.$$

So β is also a uniformizing parameter for $\mathfrak{p}_1$. Since $(\mathfrak{p}_2, m) = 1$ and $(\beta+1)^m - 1 \equiv m\zeta_m^{m-1}\pi_2 \pmod{\mathfrak{p}_2^2}$, we also have that

$$\mathrm{ord}_{\mathfrak{p}_2}((\beta+1)^m - 1) = \mathrm{ord}_{\mathfrak{p}_2}(m) + (m-1)\mathrm{ord}_{\mathfrak{p}_2}(\zeta_m) + \mathrm{ord}_{\mathfrak{p}_2}(\pi_2) = 1.$$

Thus $(\beta+1)^m - 1$ is a uniformizing parameter for $\mathfrak{p}_2$. It follows that $X^{n_0} - \beta$ is Eisenstein with respect to $\mathfrak{p}_1$, and $X^N - (\beta+1)^m + 1$ is Eisenstein with respect to $\mathfrak{p}_2$. If $E_1 = L(\sqrt[n_0]{\beta})$ and $E_2 = L(\sqrt[N]{(\beta+1)^m - 1})$, then $\mathfrak{p}_2$ is totally ramified in E_2. In E_1, however, $\mathfrak{p}_2$ is unramified. Recall that since $\sqrt[n_0]{\beta}$ generates E_1 over L, the different $\mathscr{D}_{E_1/L}$ contains $n_0(\sqrt[n_0]{\beta})^{n_0-1}$. If $\mathfrak{p}_2$ was ramified in E_1, that would imply that $n_0(\sqrt[n_0]{\beta})^{n_0-1} \in P$ for some P in E_1 lying over $\mathfrak{p}_2$. But then $n_0\beta$ would be contained in $P \cap L = \mathfrak{p}_2$, a contradiction since $\beta \equiv -1 + \zeta_m \not\equiv 0 \pmod{\mathfrak{p}_2}$ and $(\mathfrak{p}_2, n_0) = 1$.

Thus $E_1 \cap E_2 = L$, and so, $\mathrm{Gal}(E_1E_2/L) \cong \mathrm{Gal}(E_1/L) \times \mathrm{Gal}(E_2/L)$. Let σ be a generator of the cyclic group $\mathrm{Gal}(E_1/L)$, and let τ be the identity element of $\mathrm{Gal}(E_2/L)$. By the Chebotarev Density Theorem, there exist infinitely many primes $\mathfrak{s}$ of L, unramified in E_1E_2, for which there exists $\mathfrak{S}$ over $\mathfrak{s}$ with $\sigma\tau = (\mathfrak{S}, E_1E_2/L)$, that is, with $\mathfrak{s}$ inert in E_1 and split completely in E_2.

Let $s = \mathfrak{s} \cap \mathbb{F}[T]$, and let $w \equiv \beta \pmod{s}$. Because s is unramified in $E_1 = L(\sqrt[n_0]{\beta})$,

$$\left(\frac{w}{s}\right)_l = \left(\frac{\beta}{s}\right)_l \neq 1,$$

and since s splits completely in $E_2 = L(\sqrt[N]{(\beta+1)^m - 1})$, we also have

$$\left(\frac{(w+1)^m - 1}{s}\right)_N = \left(\frac{(\beta+1)^m - 1}{s}\right)_N = 1.$$

Finally, notice that since s splits completely in L, s must also split completely in $\mathbb{F}(T)(\zeta_{m_0N})$, so we must have $|s| \equiv 1 \pmod{m_0N}$. $\square$

By the previous lemma, we can choose $w \in \mathbb{F}[T]$ and a prime s satisfying

$$|s| \equiv 1 \pmod{m_0N},$$

$$\left(\frac{w}{s}\right)_l \neq 1,$$

and

$$\left(\frac{(w+1)^m - 1}{s}\right)_N = 1.$$

Notice that $m_0n_0 \mid m_0N$, so s satisfies the hypothesis of Lemma 7 that $|s| \equiv 1 \pmod{m_0n_0}$.

Since $\left(\frac{(w+1)^m-1}{s}\right)_N = 1$, there exists some $z \in \mathbb{F}[T]$ with

$$z^N \equiv (w+1)^m - 1 \pmod{s}. \tag{5}$$

Because $|s| \equiv 1 \pmod 4$, there also exists some $y \in \mathbb{F}[T]$ with

$$y^N \equiv -1 \pmod{s}. \tag{6}$$

Choose distinct monic, irreducible polynomials $p_1, \ldots, p_{m-1} \neq s$ such that

$$|p_i| \equiv 1 \pmod{m_0n_0}.$$

Let Φ denote the Euler phi function for polynomials. Choose primitive roots $g_i \pmod{p_i}$ such that $\Phi(p_i) > 4$ and

$$g_i^2 - (m-2)g_i - 1 \not\equiv 0 \pmod{p_i}. \tag{7}$$

Choose $A \in \mathbb{F}[T]$ with

$$A \equiv \begin{cases} g_i^{-1} & (\mathrm{mod}\, p_i), \text{ for } 1 \leqslant i \leqslant m-1, \\ w & (\mathrm{mod}\, s). \end{cases} \tag{8}$$

Choose irreducible polynomials $h_1, \ldots, h_{m-1}$ with

$$h_j \equiv \begin{cases} \dfrac{F_j(1)}{g_i^{-1}+1} & (\mathrm{mod}\, p_i),\ j \neq i, \\ \dfrac{F_j(1)}{g_i^{-1}+g_i} & (\mathrm{mod}\, p_i),\ j = i, \\ \dfrac{F_j(z,y)}{w+1} & (\mathrm{mod}\, s), \end{cases} \tag{9}$$

$$|h_j| \equiv 1 \pmod{N}.$$

Note that the denominators above are relatively prime to the moduli because $\Phi(p_i) > 4$ for each i with $1 \leqslant i \leqslant m-1$ and $\left(\frac{w}{s}\right)_l \neq 1$. Also note that there are infinitely many choices for each h_i by the strong version of Dirichlet's Theorem for function fields mentioned above in Section 2.1. Let $h_0 = (h_1 \cdots h_{m-1})^{-1}$. Let $\mathscr{S}, \mathscr{V}, \mathscr{U}$ be the sets of primes S, V, and U, respectively, which satisfy:

$$\begin{aligned} &S \equiv V \equiv U \equiv 1 \pmod{p_1 \cdots p_{m-1}}, \\ &S \equiv 1,\ V \equiv y,\ U \equiv z \pmod{s}, \\ &S \not\equiv 0,\ V \equiv 1,\ F_i(U) \equiv 0 \pmod{h_i},\ 1 \leqslant i \leqslant m-1. \end{aligned} \tag{10}$$

By Dirichlet's Theorem, $\mathscr{S}$ and $\mathscr{V}$ are infinite. To see that $\mathscr{U}$ is also infinite, we just need to show that $F_i(U) \equiv 0$ is solvable modulo h_i. But this follows from the fact that $|h_i| \equiv 1 \pmod{N}$. Because all the Nth roots of unity are contained in $\mathbb{F}[T]/h_i\mathbb{F}[T]$, $X^N - 1$ factors into linear factors mod h_i, and therefore so does $F_i(X)$.

Now we are ready to define $B_0, \ldots, B_{m-1}, D$, and C. Take integers $v_0, \ldots, v_{m-1}$, multiples of n, with

$$v_0 < v_1 < \cdots < v_{m-1}.$$

Given any $S_0, \ldots, S_{m-1} \in \mathscr{S}$, $V \in \mathscr{V}$, and $U \in \mathscr{U}$, set

$$\begin{aligned} B_i &= A - h_i^{-1} S_i^{v_i} F_i(U, V), \\ D &= V^{N/n} \prod_{i=0}^{m-1} S_i^{v_i/n}, \\ C &= U^{N/n} \prod_{i=0}^{m-1} S_i^{v_i/n}. \end{aligned} \tag{11}$$

It is clear that B_0, C, and D are in $\mathbb{F}[T]$. To see that B_i is as well for $1 \leqslant i \leqslant m-1$, note that by Eq. (10), $h_i \mid F_i(U, V)$:

$$F_i(U, V) = V^{\mu_i} F_i\left(\frac{U}{V}\right) \equiv F_i(U) \equiv 0 \pmod{h_i}. \qquad \square$$

3.2. Verification of divisibility conditions

Lemma 9. *For any $S_0, \ldots, S_{m-1} \in \mathscr{S}, V \in \mathscr{V}$, and $U \in \mathscr{U}$, conditions* (3.1)–(3.5) *in Lemma* 7 *and Proposition* 2 *are satisfied.*

Proof. For (3.5), notice that

$$f(A) = \prod_{i=0}^{m-1} (A - B_i) + D^n$$

$$
\begin{aligned}
&= \prod_{i=0}^{m-1} h_i^{-1} S_i^{v_i} F_i(U,V) + D^n \\
&= \left(\prod_{i=0}^{m-1} S_i^{v_i} \right) (U^n - V^n) + D^n \\
&= C^n - D^n + D^n \\
&= C^n.
\end{aligned}
$$

For (3.1)–(3.4), first observe that the following congruences follow from Eqs. (5), (6), and (8)–(11) and the definition of h_0:

$$
B_0 \equiv \begin{cases} g_i^{-1} & (\mathrm{mod}\, p_i), \\ -1 & (\mathrm{mod}\, s), \end{cases}
$$

$$
B_j \equiv \begin{cases} -g_i & (\mathrm{mod}\, p_i), \ i = j, \\ -1 & (\mathrm{mod}\, p_i), \ i \neq j, \\ -1 & (\mathrm{mod}\, s), \end{cases} \tag{12}
$$

$$
D^n \equiv \begin{cases} 1 & (\mathrm{mod}\, p_i), \\ -1 & (\mathrm{mod}\, s). \end{cases}
$$

It is now not hard to see that conditions (3.1)–(3.4) in Lemma 7 hold. For example, (3.1) is satisfied since

$$
\begin{aligned}
f(0) &\equiv (-1)^m B_0 B_1 \cdots B_{m-1} + D^n \\
&\equiv \begin{cases} (-1)^m (g_i^{-1})(-g_i)(-1)^{m-2} + 1 \equiv -1 + 1 \equiv 0 & (\mathrm{mod}\, p_i), \\ (-1)^m (-1)^m - 1 \equiv 1 - 1 \equiv 0 & (\mathrm{mod}\, s). \end{cases}
\end{aligned}
$$

Condition (3.2) follows from Eqs. (7) and (12):

$$
\begin{aligned}
f'(0) &= \sum_{k=0}^{m-1} \prod_{\substack{j=0 \\ j \neq k}}^{m-1} (-B_k) \\
&\equiv (-1)^{m-1} \left[\prod_{j=1}^{m-1} B_j + \prod_{\substack{j=0 \\ j \neq k}} B_j + \sum_{\substack{k=1 \\ k \neq i}}^{m-1} \prod_{j \neq k} B_k \right] (\mathrm{mod}\, p_i)
\end{aligned}
$$

$$\equiv (-1)^{m-1}\left[(-1)^{m-2}(-g_i)+(-1)^{m-2}g_i^{-1}+\sum_{\substack{k=1\\k\neq j}}^{m-1}(-1)^{m-2}\right] \pmod{p_i}$$

$$\equiv (-1)^{m-1}(-1)^{m-2}[-g_i+g_i^{-1}+m-2] \pmod{p_i}$$

$$\not\equiv 0 \pmod{p_i},$$

$$f'(0)=\sum_{k=0}^{m-1}\prod_{\substack{j=0\\j\neq k}}^{m-1}(-B_k)\equiv(-1)^{m-1}\sum_{k=0}^{m-1}(-1)^{m-1}\equiv m\not\equiv 0 \pmod{s}.$$

The first part of condition (3.3) follows from Eq. (12) since clearly $-g_i$ is not an lth power. The second part holds because Eq. (12) implies that for $i\neq j$, $\left(\frac{B_i}{p_j}\right)_l=\left(\frac{-1}{p_j}\right)_l=1$. Finally, for condition (3.4), $\left(\frac{B_i}{s}\right)_l=\left(\frac{-1}{s}\right)_l=1$ by Eq. (12). The fact that $\left(\frac{A}{s}\right)_l\neq 1$ follows from Eq. (8) and Lemma 8. □

We can choose $S_0,\ldots,S_{m-1}$, V and U more specifically so that conditions (3.6) and (3.7) are also satisfied. For ease of notation, let

$$s_i=h_i^{-1}S_i^{v_i},$$

for $0\leqslant i\leqslant m-1$. Define polynomials

$$G_i(X,Y)=\prod_{\substack{j=0\\j\neq i}}^{m-1}s_jF_j(X,Y)\prod_{\substack{0\leqslant j<k\leqslant m-1\\j,k\neq i}}^{m-1}\left[s_kF_k(X,Y)-s_jF_j(X,Y)\right]$$

for $1\leqslant i\leqslant m-1$,

$$H_1(X)=\prod_{0\leqslant i<j\leqslant m-1}[(s_jF_j(X,0)-s_iF_i(X,0)]$$

$$\prod_{\substack{0\leqslant e_j\leqslant v_j(0\leqslant j\leqslant m-1)\\\emptyset\neq I\subset\{1,\ldots,m-1\}}}\left[\prod_{i\in I}[s_1F_1(X,0)-s_0F_0(X,0)]^2-\prod_{j=0}^{m-1}S_j^{2e_j}\right],$$

$$H_2(X)=\sum_{i=0}^{m-1}\prod_{\substack{j=0\\j\neq i}}^{m-1}s_jF_j(0,X).$$

Lemma 10. *If for $S_0,\ldots,S_{m-1}\in\mathscr{S}$, $V\in\mathscr{V}$, and $U\in\mathscr{U}$, we further have that*

$$G_i(U,V)\not\equiv 0 \pmod{S_i},$$

$$H_1(U) \not\equiv 0 \pmod{V},$$

$$\text{and } H_2(V) \not\equiv 0 \pmod{U}, \tag{13}$$

then $B_0, \ldots, B_{m-1}, C$, *and* D *parametrized by* $S_0, \ldots, S_{m-1}, V$, *and* U *also satisfy conditions* (3.6) *and* (3.7) *in Proposition* 2, *and* $f(X)$ *is irreducible.*

Proof. If either condition (3.6) or condition (3.7) is not satisfied, then at least one of the following congruences must hold:

$$\sum_{i=0}^{m-1} \prod_{\substack{j=0 \\ j\neq i}}^{m-1} (A - B_j) \equiv 0 \pmod{S_k} \text{ or } \pmod{U}, \tag{14}$$

$$B_i - B_j \equiv 0 \pmod{S_k} \text{ or } \pmod{V}. \tag{15}$$

Each of these congruences, however, implies a contradiction to one of the conditions in (13). For example, if (14) holds, then by Eq. (11)

$$\sum_{i=0}^{m-1} \prod_{j=0}^{m-1} s_j F_j(U, V) \equiv 0 \pmod{S_k} \text{ or } \pmod{U}.$$

If the modulus is U, this contradicts the assumption that $H_2(V) \not\equiv 0 \pmod{U}$, and if the modulus is S_k, the expression reduces to

$$\prod_{\substack{j=0 \\ j\neq k}}^{m-1} s_j F_j(U, V),$$

contradicting $G_k(U, V) \not\equiv 0 \pmod{S_k}$. If (15) holds, then by Eq. (11), we have

$$s_j F_j(U, V) - s_i F_i(U, V) \equiv 0 \pmod{S_k} \text{ or } \pmod{V}.$$

If the modulus is V, this contradicts the hypothesis that $H_1(U) \not\equiv 0 \pmod{V}$, and if the modulus is S_k, this contradicts the hypothesis that $G_k(U, V) \not\equiv 0 \pmod{S_k}$.

To see that $f(X)$ is irreducible, suppose for contradiction that there exists some monic polynomial $\tilde{f}(X)$ with $\tilde{f}(X) | f(X)$ and $1 \leqslant \deg(\tilde{f}) < \deg(f)$. We have

$$f(X) = \prod_{i=0}^{m-1} (X - B_i) + D^n \equiv \prod_{i=0}^{m-1} (X - B_i) \pmod{V}.$$

There must exist a nonempty set $I \subset \{0, \ldots, m-1\}$ for which

$$\tilde{f}(X) \equiv \prod_{i\in I} (X - B_i) \pmod{V}.$$

By condition (3.7) in Proposition 2, $B_0 \not\equiv B_i \pmod V$, so B_0 is not a multiple root of $f \pmod V$. We can assume, then, that $0 \notin I$, replacing $\tilde{f}$ with $f/\tilde{f}$ if necessary. It follows that $V - \tilde{f}(B_0)$. But $\tilde{f}(B_0) | f(B_0)$, where

$$f(B_0) = D^n = V^N \prod_{i=0}^{m-1} S_i^{v_i},$$

so it must be that $\tilde{f}(B_0) = \pm \prod_{i=0}^{m-1} S_i^{e_i}$ for some $0 \leqslant e_i \leqslant v_i$. Then

$$\prod_{i \in I} (B_0 - B_i) = \tilde{f}(B_0) \equiv \pm \prod_{i=0}^{m-1} S_i^{e_i} \pmod V.$$

Squaring both sides and using Eq. (11) gives that

$$\prod_{i \in I} (s_i F_i(U,0) - s_0 F_0(U,0))^2 \equiv \prod_{i=0}^{m-1} S_i^{2e_i} \pmod V,$$

which implies that $H_1(U) \equiv 0 \pmod V$, a contradiction.

It remains to show that we can, in fact, choose primes $S_0, \ldots, S_{m-1}, V$, and U with

$$G_i(U, V) \not\equiv 0 \pmod{S_i},$$

$$H_1(U) \not\equiv 0 \pmod V,$$

$$\text{and} \quad H_2(V) \not\equiv 0 \pmod U.$$

Let $P = p_1 \cdots p_{m-1} s h_1 \cdots h_{m-1}$. Given $S_0 \in \mathscr{S}$ with $\deg(S_0) > \deg(P)$, choose an irreducible polynomial S_i in $\mathscr{S}$, $1 \leqslant i \leqslant m-1$, with $\deg(S_i) = \deg(S_{i-1}) + 1$. This is possible by the strong version of Dirichlet's Theorem for function fields. Set

$$\mathscr{U}(S_0) = \{U \in \mathscr{U} \mid |S_{m-1}| < |U| < q^{m+1}|S_0|\},$$

and

$$\mathscr{V}(S_0) = \{V \in \mathscr{V} \mid q^{m+1}|S_0| < |V| < q^{m+3}|S_0|\}.$$

We claim that as $|S_0| \to \infty$, $|\mathscr{V}(S_0)|, |\mathscr{U}(S_0)| \to \infty$. By the function field version of the Tchebotarev Density Theorem,

$$\#\{V \in \mathscr{V}(S_0) \mid \deg(V) = x, V \equiv a \pmod P\} \sim \frac{q^x}{\Phi(P)x},$$

for any fixed $a \in \mathbb{F}_q[T]$ with $(a, P) = 1$. As $|S_0|$ increases, the interval containing $|V|$, which has length $|S_0|(q^{m+3} - q^{m+1})$, increases as well. It follows that $|\mathscr{V}(S_0)| \to \infty$ as $|S_0| \to \infty$. A similar argument can be used for $\mathscr{U}(S_0)$. Since $|S_{m-1}| = q^{m-1}|S_0|$, the interval containing U has length $|S_0|(q^{m+1} - q^{m-1})$ which also goes to ∞ with $|S_0|$. $\square$

Lemma 11. *For sufficiently large $S_0 \in \mathscr{S}$, there exist $V \in \mathscr{V}(S_0)$ and $U \in \mathscr{U}(S_0)$ which satisfy the conditions in Eq.* (13).

Proof. Fix $S_0 \in \mathscr{S}$, and consider S_i, G_i, $(1 \leqslant i \leqslant m-1), H_1$, and H_2 to be fixed as well. For each $V \in \mathscr{V}(S_0)$, the polynomial $G_i(X, V) \bmod S_i$ is not null, and its degree d_i is independent of the choice of S_0 and V. Since each $U \in \mathscr{U}(S_0)$ has $|S_i| < |U| < q^{m+1}|S_i|$, it follows that if $U_1, U_2 \in \mathscr{U}(S_0)$ with $U_1 \equiv U_2 \pmod{S_i}$, then $U_1 - U_2 = rS_i$ for some $r \in \mathbb{F}_q[T]$. Then $\deg(r) = \deg(U_1 - U_2) - \deg(S_i) < m+1$. Thus for a given U in $\mathscr{U}(S_0)$ with $G_i(U, V) \equiv 0 \pmod{S_i}$, there are at most q^{m+1} solutions in $\mathscr{U}(S_0)$ that are congruent to U modulo S_i. Therefore, for each $V \in \mathscr{V}(S_0)$, the number of $U \in \mathscr{U}(S_0)$ with $G_i(U, V) \equiv 0 \pmod{S_i}$ is at most $q^{m+1}d_i$. Thus at most $q^{m+1}d_i|\mathscr{V}(S_0)|$ pairs $(V, U) \in \mathscr{V}(S_0) \times \mathscr{U}(S_0)$ satisfy $G_i(U, V) \equiv 0 \pmod{S_i}$.

Next, notice that the leading term of $H_1(X)$ is

$$\prod_{i=1}^{m-1} s_i X^{\mu_i} \prod_{\emptyset \neq I \subset \{1,\ldots,m-1\}} \prod_{i \in I} (s_i X^{\mu_i})^{2(1+v_0)\cdots(1+v_{m-1})}.$$

For any $V \in \mathscr{V}(S_0)$, then, the polynomial $H_1(X)$ is not null and its degree d_1' is independent of the choice of S_0 and V. Each $U \in \mathscr{U}(S_0)$ has $|U| < |V|$ so $\mathscr{U}(S_0)$ is contained in one set of representatives modulo V. The congruence $H_1(X) \equiv 0 \pmod{V}$ then has at most d_1' solutions in $\mathscr{U}(S_0)$, and so, the number of pairs $(V, U) \in \mathscr{V}(S_0) \times \mathscr{U}(S_0)$ with $H_1(U) \equiv 0 \pmod{V}$ is at most $d_1'|\mathscr{V}(S_0)|$. Finally, if $d_2' = \deg(H_2)$, then at most $q^4 d_2'|\mathscr{U}(S_0)|$ pairs $(V, U) \in \mathscr{V}(S_0) \times \mathscr{U}(S_0)$ satisfy $H_2(V) \equiv 0 \pmod{U}$. This follows because each $V \in \mathscr{V}(S_0)$ has $|U| < |V| < q^4|U|$.

If no pair $(V, U) \in \mathscr{V}(S_0) \times \mathscr{U}(S_0)$ satisfies all four congruence conditions, then we must have

$$|\mathscr{V}(S_0) \times \mathscr{U}(S_0)| \leqslant (q^{m+1}d_0 + \cdots + q^{m+1}d_{m-1} + d_1')|\mathscr{V}(S_0)| + q^4 d_2'|\mathscr{U}(S_0)|,$$

that is,

$$1 \leqslant (q^{m+1}d_0 + \cdots + q^{m+1}d_{m-1} + d_1')|\mathscr{U}(S_0)|^{-1} + q^4 d_2'|\mathscr{V}(S_0)|^{-1}. \tag{16}$$

Since $d_0, \ldots, d_{m-1}, d_1'$ and d_2' are independent of the choice of S_0, the right-hand side of (16) goes to 0 as $|S_0| \to \infty$. For large enough S_0 then, we can find V and U to satisfy the congruences. □

3.3. The infinite prime

Lemma 12. *The prime at infinity splits completely in K.*

Proof. We claim that the Newton polygon for $f(X)$ with respect to the prime at infinity consists of m distinct line segments. It then follows that the m roots of $f(X)$ in $\bar{k}_\infty$ have distinct ord_∞. We will show that each of these roots is actually in k_∞, and therefore, the m roots must be distinct.

First note that we can choose $|S_0|$ large enough so that

- $(v_1 - v_0)\deg(S_0) > 2\deg(h_1) + \deg(h_2) + \cdots + \deg(h_{m-1})$,
- $(v_{i+1} - v_i)\deg(S_0) > \deg(h_{i+1}) - \deg(h_i)$ for $1 \leqslant i \leqslant m-2$, and
- $v_0 \deg(S_0) + \mu_0 \deg(V) > \deg(A)$.

Also recall that $v_i < v_{i+1}$, $\mu_0 < \mu_{i+1}$, and $\deg(S_i) < \deg(S_{i+1})$ for $0 \leqslant i \leqslant m-2$. Given these conditions, we see that

$$\begin{aligned}
\deg(B_0) &= \deg(A - h_0^{-1} S_0^{v_0} F_0(U,V)) \\
&= \deg(h_1) + \cdots + \deg(h_{m-1}) + v_0 \deg(S_0) + \mu_0 \deg(V) \\
&< -\deg(h_1) + v_1 \deg(S_1) + \mu_1 \deg(V) \\
&= \deg(A - h_1^{-1} S_1^{v_1} F_1(U,V)) \\
&= \deg(B_1),
\end{aligned}$$

and

$$\begin{aligned}
\deg(B_i) &= \deg(A - h_i^{-1} S_i^{v_i} F_i(U,V)) \\
&= -\deg(h_i) + v_i \deg(S_i) + \mu_i \deg(V) \\
&< -\deg(h_{i+1}) + v_{i+1} \deg(S_{i+1}) + \mu_{i+1} \deg(V) \\
&= \deg(A - h_{i+1}^{-1} S_{i+1}^{v_{i+1}} F_{i+1}(U,V)) \\
&= \deg(B_{i+1}) \text{ for } 1 \leqslant i \leqslant m-2.
\end{aligned}$$

Thus

$$\deg(B_0) < \deg(B_1) < \cdots < \deg(B_{m-1}). \tag{17}$$

Also notice that

$$\deg(B_0) + \deg(B_1) + \cdots + \deg(B_{m-1}) = n\deg(D), \tag{18}$$

since

$$\begin{aligned}\deg(B_0)+\cdots+\deg(B_{m-1}) &= \sum_{i=0}^{m-1}\deg(A-h_i^{-1}S_i^{v_i}F_i(U,V))\\ &= \sum_{i=0}^{m-1}(\deg(h_i^{-1})+v_i\deg(S_i)+\mu_i\deg(V))\\ &= \sum_{i=0}^{m-1}v_i\deg(S_i)+N\deg(V)\\ &= n\deg(D).\end{aligned}$$

Given these conditions on the degrees of the B_i's, we see that the points to consider for the Newton polygon are

$$(0,-\deg(B_0\cdots B_{m-1}+D^n)),$$

$$(i,-\deg(B_iB_{i+1}\cdots B_{m-1})),\quad 1\leqslant i\leqslant m-1,$$

$$\text{and}\quad (m,0).$$

We must show that the line segments connecting these points do, in fact, constitute the edges of the Newton polygon, and no two segments have the same slope. Let L_0 denote the line segment between the points $(0,-\deg(B_0\cdots B_{m-1}+D^n))$ and $(1,-\deg(B_1\cdots B_{m-1}))$. From Eqs. (17) and (18), it follows that

$$\deg(B_0)<\frac{n\deg(D)}{m}.$$

Subtracting $n\deg(D)$ from both sides gives that

$$-\deg(B_1)-\cdots-\deg(B_{m-1})<\left(\frac{1}{m}-1\right)n\deg(D).$$

Because the slope of the secant line from $(0,-\deg(B_0\cdots B_{m-1}+D^n))$ to $(m,0)$ is $\frac{1}{m}n\deg(D)$, this implies that L_0 lies strictly below that secant line and is therefore one edge of the Newton polygon.

Let $L_i, 1\leqslant i\leqslant m-2$, denote the line segment connecting the points $(i,-\deg(B_iB_{i+1}\cdots B_{m-1}))$ and $(i+1,-\deg(B_{i+1}\cdots B_{m-1}))$; let L_{m-1} be the line segment between $(m-1,-\deg(B_{m-1}))$ and $(m,0)$. If m_i denotes the slope of L_i, for $0\leqslant i\leqslant m-1$, then notice that $m_i=\deg(B_i)$.

Next we show that each L_i constitutes an edge of the Newton polygon. From Eqs. (17) and (18), observe that

$$\deg(B_i)<\frac{\deg(B_iB_{i+1}\cdots B_{m-1})}{m-i}.$$

Subtracting $\deg(B_i \cdots B_{m-1})$ from each side yields:

$$-\deg(B_{i+1} \cdots B_{m-1}) < \left(\frac{1}{m-i} - 1\right) \deg(B_i B_{i+1} \cdots B_{m-1}).$$

But this is equivalent to stating that L_i lies strictly below the secant line connecting

$$(i, -\deg(B_i B_{i+1} \cdots B_{m-1})) \text{ and } (m, 0)$$

which has slope $\frac{1}{m-i}\deg(B_i \cdots B_{m-1})$. Thus L_i is one edge of the Newton polygon for $f(X)$ with respect to the infinite prime. Finally, by Eq. (17), the slopes of the line segments L_i are distinct which implies that the m roots are in k_∞. Otherwise, if α and β are roots with $\alpha, \beta \notin k_\infty$, then there must exist some isomorphism σ from $k_\infty(\alpha)$ to $k_\infty(\beta)$ which leaves k_∞ fixed. It follows that $|\beta| = |\sigma(\alpha)| = |\alpha|$, that is, $\deg(\beta) = \deg(\alpha)$, a contradiction. This completes the proof. □

Acknowledgments

I thank my advisor Michael Rosen for providing many helpful suggestions as I worked on my dissertation, of which this work is a major part. I also thank the referee for his valuable comments.

References

[1] T. Azuhata, H. Ichimura, On the divisibility problem of the class numbers of algebraic number fields, J. Fac. Sci. Univ. Tokyo 30 (1984) 579–585.
[2] D. Cardon, R. Murty, Exponents of class groups of quadratic function fields over finite fields, Canad. Math. Bull. 44 (4) (2001) 398–407.
[3] H. Cohen, H.W. Lenstra Jr., Heuristics on class groups of number fields, Number Theory, Noordwijkerhout 1983, Lecture Notes in Mathematics, Vol. 1068, Springer, Berlin, New York, 1984, pp. 33–62.
[4] C. Friesen, Class number divisibility in real quadratic function fields, Canad. Math. Bull. 35 (1992) 361–370.
[5] H. Ichimura, On the class groups of pure function fields, Proc. Japan Acad. 64 (1988) 170–173 (corrigendum Proc. Japan Acad. 75 (1999) 22).
[6] T. Nagell, Uber die Klassenzahl imaginar quadratischer Zahlkorper, Abh. Math. Sem. Univ. Hamburg 1 (1922) 140–150.
[7] S. Nakano, On ideal class groups of algebraic number fields, J. Reine Angew. Math. 358 (1985) 61–75.
[8] A. Pacelli, A lower bound on the number of cyclic function fields with class number divisible by n, preprint.
[9] M. Rosen, Number Theory in Function Fields, Springer, Berlin, 2002.
[10] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, Osaka J. Math. 7 (1970) 57–76.