ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT

Journal of Number Theory 116 (2006) 311–323

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

The prime at infinity and the rank of the class group in global function fields

Allison M. Pacelli*

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

Received 20 September 2004; revised 1 April 2005

Available online 21 July 2005

Communicated by D. Goss

Abstract

In this paper we construct, for any integers m and n, and $2 \leqslant g \leqslant m-1$, infinitely many function fields K of degree m over $\mathbb{F}(T)$ such that the prime at infinity splits into exactly g primes in K and the ideal class group of K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{m-g}$. This extends previous results of the author and Lee for the cases $g=1$ and $g=m$.

Keywords: Class group; Class number; Function field

1. Introduction

The study of class numbers dates back to Gauss who determined the exact power of 2 dividing the class number of a quadratic number field. In particular, he proved that infinitely many quadratic fields have class number divisible by 2. Nagell [5], Yamamoto [9], and Friesen [2] have shown that there are infinitely many quadratic fields (imaginary number field, real number field, real function field, respectively) with class number divisible by an arbitrary integer n. In fact, given any integers m and n, there are infinitely many number fields and function fields of fixed degree m with class number divisible by n (see, for example, [1,6] for number fields and [7] for function

* Fax: +1 413 597 4061.
E-mail address: apacelli@williams.edu.

0022-314X/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2005.04.014

fields). This is a consequence of stronger results about the structure of the class group, specifically the rank of a subgroup of the class group.

In 1983, Azhuhata and Ichimura [1] constructed infinitely many number fields K of degree m over $\mathbb{Q}$ such that the class group of K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{r_2}$ for any integers m and n. Here r_2 denotes half the number of complex embeddings of K into $\mathbb{C}$. Nakano [6] soon improved this result, constructing infinitely many number fields K of degree m over $\mathbb{Q}$ such that the class group of K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{r_2+1}$ for any integers m and n. In 1999, Ichimura [3] 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 $\mathbb{F}[X]$. More general function field results have been proven by the author and Lee. Recall that a function field is said to be *real* if the prime at infinity splits completely and *imaginary* if the prime at infinity is totally ramified or inert. In [7], the author proved that for any integers m and n, there are infinitely many real function fields K of degree m over $\mathbb{F}(T)$ whose ideal class group contains a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z}$. For m and n relatively prime, there are infinitely many imaginary function fields K of degree m such that the prime at infinity is totally ramified and the ideal class group of K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{m-1}$. For the case when the infinite prime is inert, subject to a few restrictions on m, Lee and the author proved in [4] that there are infinitely many function fields K of degree m whose ideal class groups contain subgroups isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{m-1}$. It should be noted that the constant field is fixed in each of these extensions.

In all the results mentioned above, we see that the rank of the subgroup of the class group is closely related to the rank of the unit group; the more units in K, the smaller the rank of the class group. In a number field of degree $m = r_1 + 2r_2$, the rank of the unit group is $r_1 + r_2 - 1$, so Azuhata and Ichimura's result shows that the rank of the unit group plus the rank of the subgroup of the class group is $r_1 + 2r_2 - 1 = m - 1$. For function fields, the rank of the unit group is one less than the number of primes lying above infinity. So for imaginary function fields, the rank of the unit group plus the rank of the subgroup of the class group is again $m - 1$, and for real function fields the sum is m.

In this paper, we extend the results above to show that the rank of the unit group plus the rank of the subgroup of the class group is at least equal to one less than the degree of the extension, regardless of the number of primes lying above infinity.

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 result is as follows:

Theorem 1. *Let m and n be any positive integers, not both even, not divisible by the characteristic of $\mathbb{F}(T)$, with $m, n > 1$. If g is an integer with $2 \leqslant g \leqslant m - 1$, then there are infinitely many function fields K of degree m over k such that*

(1) *the prime at infinity in k splits into exactly g primes in K, one with ramification index $m - g + 1$, the rest unramified, all with relative degree 1, and*
(2) *Cl_K contains an abelian subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{m-g}$.*

As in [7], 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 $\mathbb{F}[T]$. If θ is a root of $f(X)$, then $K = k(\theta)$ satisfies the conditions of the theorem.

2. Preliminaries

Let $\mathcal{L}$ be the set of all prime divisors of n, and define $n_0 = \prod_{l \in \mathcal{L}} l$. 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 irreducible polynomials $p_1, \ldots, p_{m-1}$ with $|p_i| \equiv 1 \pmod{m_0 n_0}$ and polynomials $B_0, \ldots, B_{m-1}$, and D in $\mathbb{F}[T]$ such that*

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

Then for each $l \in \mathcal{L}$, the subgroup of $K^\times / W K^{\times l}$ 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. The proof is the same as in [7]. □

The following lemma is well known.

Lemma 2. *Suppose A is a finite abelian group of exponent n, and $\dim_{\mathbb{Z}/l\mathbb{Z}} A^{n/l} \geqslant r$ for all l dividing n. Then A 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, and*
(2.5) *the prime at infinity in* k *splits into exactly* g *primes in* K.

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

Proof. Let $Cl_K[n]$ 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 $Cl_K[n]^{n/l}$ has dimension at least $m - g$ over $\mathbb{Z}/l\mathbb{Z}$ for all l in $\mathcal{L}$. Consider the following sequence:

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

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 $Cl_K[n]$. If $\bar{\mathfrak{a}} \in Cl_K[n]$, then $\mathfrak{a}^n = (\alpha)$ for some $\alpha \in \mathcal{O}_K$. Set $h(\bar{\mathfrak{a}}) = [\alpha]_l$, 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 sequence above is exact.

Let $S \subset K^\times / WK^{\times l}$ be the subgroup generated by the classes of $\theta - B_1, \ldots, \theta - B_{m-1}$, 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,

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

By Lemma 1, $\dim_{\mathbb{Z}/l\mathbb{Z}}(S) = m - 1$, and by condition (2.5), we know that the rank of the unit group in K is $g - 1$. Thus

$$\dim_{\mathbb{Z}/l\mathbb{Z}}(S') = m - 1 - (g - 1) = m - g.$$

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

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

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

It remains to show that $S' \subset Im(h)$. 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. Say $(\theta - B_i) = D_i^n$ for some ideal $D_i \subset \mathcal{O}_K$, $1 \leqslant i \leqslant m-1$. It follows that $h(\bar{D}_i) = [\theta - B_i]_l$, so $S' \subset Im(h)$. This completes the proof. □

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. See [7] for the proof of this assertion.

3. Choosing polynomials

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

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

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

Note that there are infinitely many such primes p_i and s since 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 $l \in \mathcal{L}$. Let g_i, $1 \leqslant i \leqslant m-1$, be a primitive root mod p_i that satisfies the congruence

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

for all i, $1 \leqslant i \leqslant m-1$. 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 $1 \leqslant i \leqslant m-1$. Given positive integer parameters t and v with $t, v > m$, we choose polynomials $B_0, \ldots, B_{m-1}$, and D so that their degrees depend on t and v. Choose B_0 such that

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

and $\deg(B_0) = t - m$. Choose B_i, $1 \leqslant i \leqslant m-1$, so that

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

(ii) $\deg(B_i) = t - m + i + \deg(p_1 \cdots p_{m-1} s)$ for $1 \leqslant i \leqslant m - g - 1$,

(iii) $\deg(B_{m-g}) = t + \deg(p_1 \cdots p_{m-1} s)$,

(iv) $\deg(B_{m-g+1}) = t + v + \deg(p_1 \cdots p_{m-1} s)$,

(v) $\deg(B_i) = t + v + i - m + g + \deg(p_1 \cdots p_{m-1} s)$ for $m - g + 2 \leqslant i \leqslant m - 2$, and

(vi) $\deg(B_{m-1}) = t + v + g - 2 + \deg(p_1 \cdots p_{m-1} s) + X$,

where X is an integer, $1 \leqslant X \leqslant n$, chosen so that

$$\frac{(g-1)(g-2)}{2} + g - 2 + m[t + \deg(p_1 \cdots p_{m-1} s)] + (g-1)v + X \equiv 0 \pmod{n}. \quad (2)$$

Note that choosing B_i's with the desired degrees is possible for sufficiently large t and v by the strong version of Dirichlet's Theorem on primes in an arithmetic progression given below.

Theorem 2 (*Dirichlet's Theorem*). *Let a and M be relatively prime polynomials in $\mathbb{F}[T]$ with $\deg(M) > 0$. If S_d is the number of monic irreducibles primes P in $\mathbb{F}[T]$ with $P \equiv a \pmod{M}$ and $\deg(P) = d$, then*

$$\#S_d = \frac{1}{\Phi(M)} \frac{q^d}{d} + O\left(\frac{q^{\frac{d}{2}}}{d}\right). \quad (3)$$

Proof. See [8, p. 40]. □

Notice that

$$\deg(B_0) < \cdots < \deg(B_{m-1}). \quad (4)$$

Define

$$d = \frac{1}{n}\left(\frac{(g-1)(g-2)}{2} + g - 2 + m[t + \deg(p_1 \cdots p_{m-1} s)] + (g-1)v + X\right). \quad (5)$$

Choose a monic irreducible polynomial D so that

$$D \equiv \begin{cases} 1 \pmod{s}, \\ 1 \pmod{p_i} \text{ if } m \text{ and } n \text{ are odd}, \\ -1 \pmod{p_i} \text{ otherwise}. \end{cases} \quad (6)$$

$$\deg(D) = d.$$

We claim that it is possible to choose parameters t and v so that the following condition is also met:

$$\text{(vii)}\ \ (B_i - B_j, D) = 1 \quad \text{for all } 0 \leqslant i, j \leqslant m-1,\ \ i \neq j.$$

To show that (vii) can be satisfied, note that since D is irreducible, it is enough to show that D does not divide the polynomial R, where

$$R = \prod_{\substack{i \neq j \\ 0 \leqslant i < j \leqslant m-1}} (B_i - B_j).$$

But R has at most $\deg(R)$ monic irreducible factors, where

$$\deg(R) < \binom{m}{2} \deg(B_{m-1}) = \frac{m(m-1)}{2}\,(t + v + g - 2 + X + \deg(p_1 \cdots p_{m-1} s)).$$

This upper bound is linear in both t and v. By Dirichlet's Theorem, however, the number of irreducible D that satisfy the two conditions in Eq. (6) is

$$\frac{1}{\Phi(p_1 \cdots p_{m-1} s)} \frac{q^d}{d} + O\left(\frac{q^{\frac{d}{2}}}{d}\right),$$

which is exponential in t and v (see Eq. (5)). For t and v large enough, therefore, there are more D satisfying the necessary conditions in (6) than there are irreducible factors of R. Thus it is possible to choose an irreducible polynomial D not dividing R, that satisfies the conditions in Eq. (6), so (vii) is satisfied.

Finally notice that with the above choices, we have

$$(m - g + 1)\deg(B_{m-g}) + \deg(B_{m-g+1}) + \cdots + \deg(B_{m-1}) < nd, \quad \text{and} \tag{7}$$

$$nd < (m - g + 2)\deg(B_{m-g+1}) + \deg(B_{m-g+2}) + \cdots + \deg(B_{m-1}). \tag{8}$$

This follows since

$$\begin{aligned}
&(m - g + 1)\deg(B_{m-g}) + \deg(B_{m-g+1}) + \cdots + \deg(B_{m-1}) \\
&\quad = m[t + \deg(p_1 \cdots p_{m-1} s)] + g - 2 + (g-1)v + X + \frac{(g-1)(g-2)}{2} - 1 \\
&\quad = nd - 1 \\
&\quad < nd
\end{aligned}$$

and

$$\begin{aligned}
&(m-g+2)\deg(B_{m-g+1})+\deg(B_{m-g+2})+\cdots+\deg(B_{m-1})\\
&\quad= m[t+\deg(p_1\cdots p_{m-1}s)]+mv+g-2+X+\tfrac{1}{2}(g-1)(g-2)-1\\
&\quad= nd-1+(m-g+1)v\\
&\quad\geqslant nd-1+2\\
&\quad> nd.
\end{aligned}$$

4. 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. The proof is the same as in [7, Lemma 3]. □

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. Again, the proof is the same as in [7, Lemma 4]. □

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

Proof. We show that $f(X)$ is an Eisenstein polynomial with respect to s. Notice first that $s\|(D^n+(-1)^m B_0B_1\cdots B_{m-1})$, the constant term of $f(X)$:

$$\begin{aligned}
D^n+(-1)^m B_0B_1\cdots B_{m-1} &\equiv 1+(-1)^m\prod_{i=0}^{m-1}C_i \pmod s\\
&\equiv 1-1 \pmod s\\
&\equiv 0 \pmod s.
\end{aligned}$$

If $s^2|(D^n+(-1)^m B_0B_1\cdots B_{m-1})$, then replace B_0 by $B_0+p_1\cdots p_{m-1}s$. Both of the desired congruence conditions for B_0 still hold since $B_0\equiv B_0+p_1\cdots p_{m-1}s$ modulo p_i and s. By (ii), we also still have that the degrees of the B_i's are strictly increasing. But now we have that

$$\begin{aligned}
&D^n+(-1)^m(B_0+p_1\cdots p_{m-1}s)B_1\cdots B_{m-1}\\
&\quad\equiv D^n+(-1)^m B_0\cdots B_{m-1}+(-1)^m p_1\cdots p_{m-1}sB_1\cdots B_{m-1} \pmod{s^2}\\
&\quad\equiv 0+(-1)^m p_1\cdots p_{m-1}sB_1\cdots B_{m-1} \pmod{s^2}\\
&\quad\not\equiv 0 \pmod{s^2}.
\end{aligned}$$

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 $0 \leqslant i \leqslant m-1$, we have that

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

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. □

5. The infinite prime

Lemma 6. *The prime at infinity splits into g primes in K, one with ramification index $m - g + 1$, the rest unramified, all with relative degree* 1. *That is, condition* (2.5) *in Proposition* 1 *is satisfied.*

Proof. We claim that the Newton polygon for $f(X)$ (Fig. 1) with respect to the prime at infinity consists of g distinct line segments with increasing positive slopes

$$\frac{n\deg(D) - \deg(B_{m-g+1}) - \cdots - \deg(B_{m-1})}{m - g + 1} < \deg(B_{m-g+1}) < \deg(B_{m-g+2}) < \cdots < \deg(B_{m-1}).$$

The lemma follows from the claim; since the g line segments have distinct slope, there must be at least g distinct roots of f in $\bar{k}_\infty$ and therefore at least g infinite primes in K. Otherwise, if α and β are roots with $\alpha, \beta \notin k_\infty$, then there is an 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. Also notice that the numerator of the first slope is relatively prime to the denominator since

$$\begin{aligned}
&n\deg(D) - \deg(B_{m-g+1}) - \cdots - \deg(B_{m-1}) \\
&\quad = nd - 2(t + v + \deg(p_1 \cdots p_{m-1}s)) - (g - 2 + X) \\
&\qquad - \sum_{i=m-g+2}^{m-2} [t + v + i - m + g + \deg(p_1 \cdots p_{m-1}s)] \\
&\quad = nd - X - (g-2) - (g-1)[t + v + \deg(p_1 \cdots p_{m-1}s)] - \tfrac{1}{2}(g-1)(g-2) + 1 \\
&\quad = (m - g + 1)[t + \deg(p_1 \cdots p_{m-1}s)] + 1.
\end{aligned}$$

Thus, the slope of the first line segment, in reduced form, contains $m - g + 1$ in the denominator, so the primes in $\bar{k}_\infty$ corresponding to this segment have ramification index

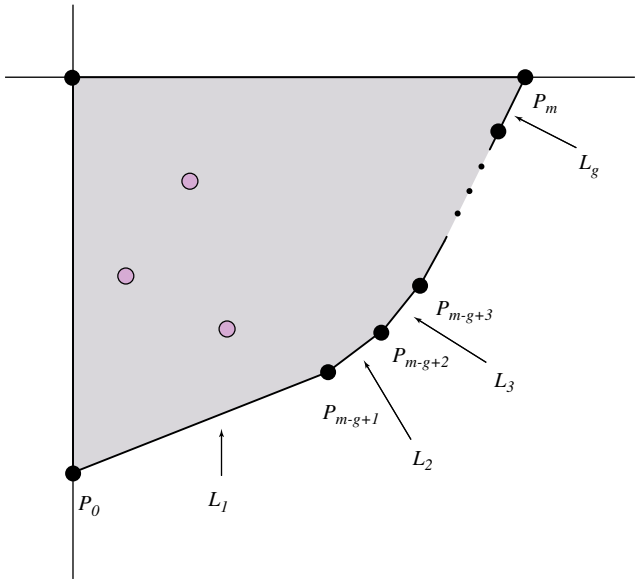

Fig. 1. Newton polygon for $f(X)$.

at least $m-g+1$. We have shown then that the prime at infinity in k decomposes into at least g primes in K, one of which has ramification index at least $m-g+1$. If e_i and f_i denote the ramification indices and relative degrees, respectively, of the infinite primes in K, then

$$m = \sum_i e_i f_i \geqslant (m-g+1)(1) + (g-1)(1)(1) = m,$$

so the infinite prime must split into exactly g primes in K, one with ramification index $m-g+1$, the rest unramified, all with relative degree 1.

To prove the claim, first notice that by Eqs. (4) and (7), $\deg((-1)^m B_0 \cdots B_{m-1} + D^n) = n \deg(D)$. From this, we see that the points to consider for the Newton polygon are the following:

$$P_0 = (0, -n \deg(D)),$$

$$P_i = (i, -\deg(B_i) - \cdots - \deg(B_{m-1})) \quad \text{for } 1 \leqslant i \leqslant m-1,$$

$$P_m = (m, 0).$$

Let M_i be the slope of the line segment from P_0 to P_i for $1 \leqslant i \leqslant m$, that is,

$$M_i = \frac{n \deg(D) - \deg(B_i) - \cdots - \deg(B_{m-1})}{i}.$$

We will show that $M = M_{m-g+1} < M_i$ for all $i \neq m-g+1$, from which it follows that the line segment L_1 from P_0 to P_{m-g+1} is part of the edge of the Newton polygon. Note that the slope of L_1 is $\frac{1}{m-g+1}(n\deg(D) - \deg(B_{m-g+1}) - \cdots - \deg(B_{m-1}))$, as desired.

If $i < m-g+1$, then $M < M_i$ if and only if

$$\begin{aligned}(m-g+1)[n\deg(D) - \deg(B_i) - \cdots - \deg(B_{m-1})] \\ > i[n\deg(D) - \deg(B_{m-g+1}) - \cdots - \deg(B_{m-1})],\end{aligned}$$

that is, if and only if

$$\begin{aligned}n\deg(D) > \deg(B_{m-g+1}) + \cdots + \deg(B_{m-1}) + \frac{m-g+1}{m-g+1-i} \\ \times[\deg(B_i) + \cdots + \deg(B_{m-g})].\end{aligned}$$

But for $i < m-g+1$, the sum on the right is strictly less than

$$\deg(B_{m-g+1}) + \cdots + \deg(B_{m-1}) + (m-g+1)\deg(B_{m-g}) < n\deg(D)$$

by Eq. (7). Thus $M < M_i$ for $i < m-g+1$.

If $m > i > m-g+1$, then $M < M_i$ if and only if

$$\begin{aligned}(m-g+1)[n\deg(D) - \deg(B_i) - \cdots - \deg(B_{m-1})] \\ > i[n\deg(D) - \deg(B_{m-g+1}) - \cdots - \deg(B_{m-1})],\end{aligned}$$

that is, if and only if

$$\begin{aligned}(i+g-m-1)n\deg(D) < i[\deg(B_{m-g+1}) + \cdots + \deg(B_{i-1})] \\ + (i+g-m-1)[\deg(B_i) + \cdots + \deg(B_{m-1})],\end{aligned}$$

that is,

$$\begin{aligned}n\deg(D) < \deg(B_i) + \cdots + \deg(B_{m-1}) + \frac{i}{i+g-m-1} \\ \times[\deg(B_{m-g+1}) + \cdots + \deg(B_{i-1})].\end{aligned}$$

Since $i > i+g-m-1$, the sum on the right is smallest when $i = m-g+2$. So it is enough that

$$\deg(B_{m-g+2}) + \cdots + \deg(B_{m-1}) + (m-g+2)\deg(B_{m-g+1}) > n\deg(D)$$

which holds by Eq. (8). Thus $M < M_i$ for $m > i > m-g+1$.

Finally, $M > M_m$ if and only if

$$m[n\deg(D) - \deg(B_{m-g+1}) - \cdots - \deg(B_{m-1})] < (m-g+1)n\deg(D),$$

that is, if and only if

$$(g-1)n\deg(D) < m[\deg(B_{m-g+1}) + \cdots + \deg(B_{m-1})]. \tag{9}$$

Notice that Eq. (9) holds if and only if

$$\begin{aligned} 0 &< m[\deg(B_{m-g+1}) + \cdots + \deg(B_{m-1})] - (g-1)n\deg(D) \\ &= m[g-2+X+(g-1)(t+v+\deg(p_1\cdots p_{m-1})) \\ &\quad + \tfrac{1}{2}(g-1)(g-2)-1] - (g-1)nd \\ &= (m-g+1)[g-2+X+\tfrac{1}{2}(g-1)(g-2)] + m(g-1)v \\ &\quad - m - (g-1)^2 v. \end{aligned} \tag{10}$$

The first term in the last sum is non-negative since $2 \leqslant g \leqslant m-1$. The remaining sum is positive since $v > m$:

$$\begin{aligned} m(g-1)v - m - (g-1)^2 v &\geqslant (g+1)(g-1)v - v - (g-1)^2 \\ &= v(2g-3) \\ &> 0. \end{aligned} \tag{11}$$

Thus $M > M_m$, so the line segment L_1 connecting P_0 and P_{m-g+1} is part of the Newton polygon for f.

Next, let L_i be the line segment from $P_{m-g+i-1}$ to P_{m-g+i} for $2 \leqslant i \leqslant g$. Notice that the slope of L_i is $\deg(B_{m-g+i})$, so the slopes of the L_i's are strictly increasing. It follows that these $g-1$ line segments, $L_2, \ldots, L_g$ constitute the rest of the Newton polygon for f. □

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] C. Friesen, Class number divisibility in real quadratic function fields, Canad. Math. Bull. 35 (1992) 361–370.
[3] H. Ichimura, On the class groups of pure function fields, Proc. Japan Acad. 64 (1988) 170–173; H. Ichimura, On the class groups of pure function fields, Proc. Japan. Acad. 75 (1999) 22.
[4] Y. Lee, A. Pacelli, Subgroups of the class groups of global function fields: the inert case, Proc. Amer. Math. Soc. 133 (2005) 2883–2889.

[5] T. Nagell, Uber die Klassenzahl imaginar quadratischer Zahlkorper, Abh. Math. Sem. Univ. Hamburg 1 (1922) 140–150.
[6] S. Nakano, On ideal class groups of algebraic number fields, J. Reine Angew. Math. 358 (1985) 61–75.
[7] A. Pacelli, Abelian subgroups of any order in class groups of global function fields, J. Number Theory 106 (2004) 29–49.
[8] M. Rosen, Number Theory in Function Fields, Springer, Berlin, 2002.
[9] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, Osaka J. Math. 7 (1970) 57–76.