PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 2, February 2009, Pages 415–424
S 0002-9939(08)09581-6
Article electronically published on October 6, 2008

CLASS GROUPS OF GLOBAL FUNCTION FIELDS WITH CERTAIN SPLITTING BEHAVIORS OF THE INFINITE PRIME

YOONJIN LEE

(Communicated by Wen-Ching Winnie Li)

Abstract. For certain two cases of splitting behaviors of the prime at infinity with unit rank r, given positive integers m, n, we construct infinitely many global function fields K such that the ideal class group of K of degree m over $\mathbb{F}(T)$ has n-rank at least $m-r-1$ and the prime at infinity splits in K as given, where $\mathbb{F}$ denotes a finite field and T a transcendental element over $\mathbb{F}$. In detail, for positive integers m, n and r with $0 \le r \le m-1$ and a given signature $(e_i, \mathfrak{f}_i)$, $1 \le i \le r+1$, such that $\sum_{i=1}^{r+1} e_i\mathfrak{f}_i = m$, in the following two cases where e_i is arbitrary and $\mathfrak{f}_i = 1$ for each i, or $e_i = 1$ and $\mathfrak{f}_i$'s are the same for each i, we construct infinitely many global function fields K of degree m over $\mathbb{F}(T)$ such that the ideal class group of K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{m-r-1}$ and the prime at infinity $\wp_\infty$ splits into $r+1$ primes $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_{r+1}$ in K with $e(\mathfrak{P}_i/\wp_\infty) = e_i$ and $\mathfrak{f}(\mathfrak{P}_i/\wp_\infty) = \mathfrak{f}_i$ for $1 \le i \le r+1$ (so, K is of unit rank r).

1. Introduction

Since Gauss, the problem of determining the structure of the class group of a number field or function field has been one of the central problems in number theory. In fact, given an integer n, infinitely many number fields and function fields have class number divisible by n (see for example Nagell [8] for imaginary quadratic number fields, Yamamoto [14] for real quadratic number fields, and Friesen [2] for real quadratic function fields). It is known that given integers m and n, infinitely many number fields and function fields of fixed degree m have class number divisible by n (see for example Azuhata and Ichimura [1] and Nakano [9] for number fields, and the author and Pacelli [5, 6, 7, 11, 12] for function fields).

For a better understanding of the structure of the class group, we need to study the n-rank of the class group, not only the divisibility of the class number by n; *n-rank* denotes the largest integer r for which the class group contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^r$. Azuhata and Ichimura [1] proved in 1984 that for any integers m and n, infinitely many number fields K of degree m over $\mathbb{Q}$ have class groups containing subgroups isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{r_2}$, where $r_2 > 0$ is half the number of complex embeddings of K into $\mathbb{C}$ (i.e., the n-rank of the class group of

Received by the editors April 26, 2007.
2000 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R58.
Key words and phrases. Class group, class number, rank of class group, imaginary function field.
This work was supported by the Ewha Womans University Research Grant of 2007.

$K \geq r_2$; we simply call r_2 the guaranteed class group n-rank). Nakano [9] improved Azuhata and Ichimura's result a year later, increasing the guaranteed n-rank from r_2 to r_2+1. Although the increase in rank is quite small, the techniques required for the proof are much more delicate than in [1].

Recently, more general function field analogues of these results developed in number fields have been proved by Pacelli and the author in several papers such as [5, 6, 7, 11, 12]. In detail, [11] works on the cases where the prime at infinity splits completely (with the guaranteed class group n-rank 1) or is totally ramified (with the guaranteed class group n-rank $m-1$), [6] works on the case in which the prime at infinity is inert (also with the guaranteed class group n-rank $m-1$), and this result is improved in [7] by increasing the guaranteed class group n-rank from $m-1$ to m. The results in [6, 7, 11] are the unit rank 0 (minimum possible unit rank) or the unit rank $m-1$ (maximum possible unit rank). The arbitrary unit rank case is proved in [12] for the guaranteed class group rank $m-r-1$, and this is improved in [5] by increasing the guaranteed class group n-rank from $m-r-1$ to $m-r$. However, these two results in [5, 12] assume specific splitting behaviors of the prime at infinity. Therefore, other cases of splitting behaviors of the prime at infinity are still missing.

In this paper, we work on certain two cases of splitting behaviors of the prime at infinity of the unit rank r with the guaranteed class group n-rank $m-r-1$. In more detail, for given splitting behaviors of the prime at infinity with the unit rank r in certain two cases, we construct infinitely many global function fields K such that the prime at infinity splits in K as given and the ideal class group of K contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{m-r-1}$. We use the *Newton polygon* method and *Kummer's criterion* to control the splitting behavior of the prime at infinity as used in [5].

Let q be a power of an odd prime p, 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 a finite algebraic extension field of k, then we denote by $\mathcal{O}_K$ the integral closure of $\mathbb{F}[T]$ in K. Let $\wp_\infty$ be the prime at infinity (or the infinite place) of K defined by the negative degree valuation, $\mathrm{ord}_\infty(g) = -\deg(g)$ for $g \in K^\times$. For a prime $\mathfrak{P}$ lying above $\wp_\infty$, we denote the *ramification index* of $\mathfrak{P}$ by $e(\mathfrak{P}/\wp_\infty)$ and the *relative degree* of $\mathfrak{P}$ by $\mathfrak{f}(\mathfrak{P}/\wp_\infty)$, and Cl_K denotes the ideal class group of $\mathcal{O}_K$. If K/k is an extension of degree n, then for some positive integer t, $\wp_\infty$ splits in K as

$$\wp_\infty \mathcal{O}_K = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_t^{e_t},$$

where $\mathfrak{P}_i$ is a place in K of relative degree $\mathfrak{f}_i$ and ramification index e_i with $\sum_{i=1}^{t} e_i\mathfrak{f}_i = n$. Sorting the pairs $(e_i, \mathfrak{f}_i), 1 \leq i \leq t$, in lexicographical order, the $2t$-tuple $(e_1, \mathfrak{f}_1, e_2, \mathfrak{f}_2, \cdots, e_t, \mathfrak{f}_t)$ is called the *signature* of K/k.

The main results are the following two theorems:

Theorem 1.1. *Let m, n be any positive integers, not both even, let r be any integer, $0 \leq r \leq m-1$, and let $(e_i, \mathfrak{f}_i)$, $1 \leq i \leq r+1$, be a given signature, where $\sum_{i=1}^{r+1} e_i\mathfrak{f}_i = m$, e_i is arbitrary and $\mathfrak{f}_i = 1$ for each i. Let q be a power of an odd prime relatively prime to m and n with $q > r$. Let $\mathbb{F}$ be the finite field of q elements.*

For the given m, n as above and signature $(e_i, \mathfrak{f}_i), 1 \leq i \leq r+1$, there exist infinitely many global function fields K of degree m over $k = \mathbb{F}(T)$ such that

1) *the prime at infinity* $\wp_\infty$ *splits into* $r+1$ *primes* $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_{r+1}$ *in* K *with* $e(\mathfrak{P}_i/\wp_\infty) = e_i$ *and* $\mathfrak{f}(\mathfrak{P}_i/\wp_\infty) = 1$ *for* $1 \le i \le r+1$ (*thus,* K *is of unit rank* r) *and*

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

Theorem 1.2. *Let* m, n *be any positive integers, not both even, let* r *be any integer,* $0 \le r \le m-1$, *and let* $(e_i, \mathfrak{f}_i)$, $1 \le i \le r+1$, *be a given signature where* $\sum_{i=1}^{r+1} e_i\mathfrak{f}_i = m$, $e_i = 1$ *and the* $\mathfrak{f}_i$*'s are the same for each* i, $\mathfrak{f}_i = \mathfrak{f}$ (*so,* $m = \mathfrak{f}(r+1)$). *Let* q *be a power of an odd prime relatively prime to* m *and* n *such that* $q > \mathfrak{f}$, $(n, q-1) = 1$, *for any prime divisor* P *of* $\mathfrak{f}$, $P \mid (q-1)$ *and* $(r+1) \mid \frac{q-1}{P}$, *and if* $4 \mid \mathfrak{f}$, *then* $q \equiv 1 \pmod 8$ *and* $(r+1) \mid \frac{q-1}{4}$. *Let* $\mathbb{F}$ *be the finite field of* q *elements.*

For given m, n *as above and signature* $(e_i, \mathfrak{f}_i), 1 \le i \le r+1$, *there exist infinitely many global function fields* K *of degree* m *over* $k = \mathbb{F}(T)$ *such that*

1) *the prime at infinity* $\wp_\infty$ *splits into* $r+1$ *primes* $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_{r+1}$ *in* K *with* $e(\mathfrak{P}_i/\wp_\infty) = 1$ *and* $\mathfrak{f}(\mathfrak{P}_i/\wp_\infty) = \mathfrak{f}$ *for* $1 \le i \le r+1$ (*so,* K *is of unit rank* r) *and*

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

Notice that for given m and n, there are infinitely many q satisfying the conditions of Theorem 1.2. For instance, for given m and n, let q be one of the infinitely many primes such that $q \equiv 1 \pmod{mn(n-1)}$ (Dirichlet's Theorem) and $q > \mathfrak{f}$; then q satisfies all the conditions of Theorem 1.2. In detail, if $q \equiv 1 \pmod{mn(n-1)}$, then $(q, m) = 1, (q, n) = 1$ and $(q, n-1) = 1$. As $m = \mathfrak{f}(r+1) \mid (q-1)$, for any prime divisor P of $\mathfrak{f}$, $P \mid (q-1)$ and $(r+1) \mid \frac{q-1}{P}$, and $(r+1) \mid \frac{q-1}{4}$ if $4 \mid \mathfrak{f}$. If $4 \mid \mathfrak{f}$, then $4 \mid m$, so $q \equiv 1 \pmod 8$ since $2 \mid n(n-1)$ and $q \equiv 1 \pmod{mn(n-1)}$.

For the proof of Theorem 1.1 and Theorem 1.2, we construct a polynomial

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

where $B_0, \cdots, B_{m-1}$ and D are polynomials in $\mathbb{F}[T]$ with certain conditions given in Section 2. The same type of polynomial $f(X)$ was also used in [5, 6, 11, 12]. If θ is a root of $f(X)$, then we will show that $K = k(\theta)$ satisfies the conditions of Theorem 1.1 and Theorem 1.2.

Finally, we 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 (for details, refer to [11]).

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 the 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 $B_0, \cdots, B_{m-1}, D \in \mathbb{F}[T]$, define

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

and let θ be a root of $f(X)$. Set $K = k(\theta)$. The next two lemmas and proposition show that with an appropriate choice of $B_0, \cdots, B_{m-1}$ and D, the field K satisfies the conditions of Theorem 1.1 and Theorem 1.2. The proof of the following lemma is in [11, Lemma 7].

Lemma 2.1. *Suppose there exist monic irreducible polynomials $p_1, \cdots, p_{m-1}$ with $|p_i| \equiv 1 \pmod{m_0 n_0}$ and polynomials $B_1, \cdots, B_{m-1}$, 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* $i \neq j$, $1 \leq i, j \leq m-1$, *for each* $l \in \mathcal{L}$.

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

The following standard lemma is used for the proof of Proposition 2.3.

Lemma 2.2. *Let G be a finite abelian group of exponent n such that $\dim_{\mathbb{Z}/l\mathbb{Z}} G^{n/l} \geq r$ 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 2.3. *Suppose that the polynomials $B_0, \cdots, B_{m-1}$ and D further satisfy the following two conditions:*

(2.4) *$\theta - B_0, \theta - B_1, \cdots, \theta - B_{m-1}$ are pairwise relatively prime.*

(2.5) *The unit rank of K is r (equivalently, the prime at infinity splits into $r+1$ primes in K).*

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

Proof. The proof is very similar to [11, Proposition 1]. □

To prove Theorem 1.1 and Theorem 1.2, we will show that it is possible to choose irreducible polynomials $p_1, \cdots, p_{m-1}$, polynomials $B_0, \cdots, B_{m-1}$, and $D \in \mathbb{F}[T]$ so that conditions (2.1) - (2.5) are satisfied and $f(X)$ is irreducible.

3. Choosing polynomials

In this section, we explain how to choose polynomials for each case of Theorem 1.1 and Theorem 1.2.

Choosing polynomials: Theorem 1.1. We choose distinct irreducible polynomials p_i, s in $\mathbb{F}[T]$, $1 \leq i \leq m-1$, such that

$$|p_i| \equiv 1 \pmod{m_0 n_0}, \quad \text{for } 1 \leq i \leq m-1, \text{ and } \quad |s| \equiv 1 \pmod{m}. \tag{1}$$

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 m-th 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, $1 \leq i \leq m-1$, 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

$$X^m - 1 \equiv \prod_{i=0}^{m-1} (X - a_i) \pmod{s}, \tag{3}$$

where the a_i's are distinct mod s for $1 \leq i \leq m-1$.

We choose an irreducible polynomial D in $\mathbb{F}[T]$ so that

$$(4)\qquad D \equiv \begin{cases} 1 & \pmod{s}, \\ (-1)^{m+1} & \pmod{p_i} \ \text{ for } 1 \leq i \leq m-1. \end{cases}$$

We have $q > r$, so let $\tau_1, \tau_2, \cdots, \tau_{r+1}$ be distinct elements in $\mathbb{F}$, and let

$$(5)\qquad c_j = \begin{cases} \tau_1 & \text{if} \quad 0 \leq j \leq e_1 - 1, \\ \quad\vdots & \\ \tau_i & \text{if} \quad \sum_{k=1}^{i-1} e_k \leq j \leq \sum_{k=1}^{i} e_k - 1, \\ \quad\vdots & \\ \tau_{r+1} & \text{if} \quad \sum_{k=1}^{r} e_k \leq j \leq \sum_{k=1}^{r+1} e_k - 1 = m-1. \end{cases}$$

Next, let β_i be positive integers such that $\frac{\deg(D^n)}{m} < \beta_1 < \beta_2 < \cdots < \beta_{r+1}$, and choose $B_i \in \mathbb{F}_q[T]$ for $0 \leq i \leq m-1$ such that

$$(6)\qquad \begin{cases} (i) \quad B_0 \equiv \begin{cases} g_i^{-1} & \pmod{p_i} \ \text{ for } 1 \leq i \leq m-1 \\ a_0 & \pmod{s}, \end{cases} \\ (ii) \quad \text{for } \ 1 \leq i \leq m-1, \\ \qquad\qquad B_i \equiv \begin{cases} 1 & \pmod{p_j} \ \text{ if } i \neq j \\ g_i & \pmod{p_i} \\ a_i & \pmod{s}, \end{cases} \\ (iii) \quad \deg(B_j) = \begin{cases} \beta_1 & \text{if } 0 \leq j \leq e_1 - 1 \\ \vdots & \\ \beta_{i+1} & \text{if } \sum_{k=1}^{i} e_k \leq j \leq \sum_{k=1}^{i+1} e_k - 1 \\ \vdots & \\ \beta_{r+1} & \text{if } \sum_{k=1}^{r} e_k \leq i \leq \sum_{k=1}^{r+1} e_k - 1 = m-1, \end{cases} \\ (iv) \quad \text{the leading coefficient of } B_i \text{ is } c_i \text{ for each } i, 0 \leq i \leq m-1, \\ (v) \quad D^n + (-1)^m B_0 B_1 \cdots B_{m-1} \not\equiv 0 \pmod{s^2}, \\ (vi) \quad (B_i - B_j, D) = 1 \ \text{ for } \ 0 \leq i, j \leq m-1, \ i \neq j. \end{cases}$$

Infinitely many B_i's satisfying the conditions (i) through (iv) in Eq. (6) exist by the strong version of Dirichlet's Theorem for function fields [13, p. 40], which asserts that in any arithmetic progression, there exist irreducible polynomials of each large degree. For (v) in Eq. (6), it is easy to see that $D^n + (-1)^m B_0 B_1 \cdots B_{m-1} \equiv 0 \pmod{s}$; so if $s \nmid (D^n + (-1)^m B_0 B_1 \cdots B_{m-1})/s$, then we have (v), but if not, for a fixed D there are only finitely many B_i's such that $s \mid (D^n + (-1)^m B_0 B_1 \cdots B_{m-1})/s$, so we need only discard those finitely many B_i's. For a fixed D, there are also only finitely many B_i's which do not satisfy (vi) in Eq. (6); thus those finitely many B_i's need to be discarded.

Choosing polynomials: Theorem 1.2. We choose polynomials p_i, s in $\mathbb{F}[T]$ as in Eq. (1), a primitive root g_i mod p_i as in Eq. (2) and hence get a_i as in Eq. (3),

$1 \leq i \leq m-1$. We also choose monic polynomials B_i for $1 \leq i \leq m-1$ such that

$$B_i \equiv \begin{cases} 1 & \pmod{p_j} \ \text{ if } i \neq j \\ g_i & \pmod{p_i} \\ a_i & \pmod{s}. \end{cases} \tag{7}$$

We choose an irreducible monic polynomial D' so that

$$D' \equiv \begin{cases} 1 & \pmod{s}, \\ (-1)^{m+1} & \pmod{p_i} \ \text{ for } 1 \leq i \leq m-1, \end{cases} \tag{8}$$

$$(B_i - B_j, D') = 1 \ \text{ for } \ 1 \leq i, j \leq m-1, i \neq j. \tag{9}$$

Infinitely many D' satisfying the conditions in (8) exist by the strong version of Dirichlet's Theorem for function fields [13, p. 40], which asserts that in any arithmetic progression, there exist polynomials of each large degree. We need only discard finitely many not satisfying (9).

Then we choose B_0 in $\mathbb{F}[T]$ such that

(10)

$$\begin{cases} (i) \quad B_0 \equiv \begin{cases} g_i^{-1} & \pmod{p_i} \text{ for } 1 \leq i \leq m-1 \\ C_0 & \pmod{s} \end{cases} \\ (ii) \quad \deg(B_0) > \deg(B_i) - 1 \text{ for } 1 \leq i \leq m-1 \\ (iii) \quad \deg(B_0) \equiv -1 \pmod{n} \\ (iv) \quad \frac{m}{n}(\deg(B_0)+1) \\ \qquad\qquad > max\{\deg(D'),\ \deg(s^2 p_1 \cdots p_{m-1} \prod_{i\neq j, 0\leq i,j\leq m-1} (B_i - B_j))\} \\ (v) \quad (B_0 - B_j, D') = 1 \ \text{ for } \ 1 \leq j \leq m-1 \\ (vi) \quad (D')^n + (-1)^m B_0 B_1 \cdots B_{m-1} \not\equiv 0 \pmod{s^2}. \end{cases}$$

Again, infinitely many B_0 satisfying conditions (i) through (iv) in Eq. (10) exist by the strong version of Dirichlet's Theorem mentioned above, and we need only discard finitely many not satisfying (v) and (vi) by the exact same reason as in Eq. (6).

We choose γ in $\mathbb{F}$ such that $x^{\mathfrak{f}} - \gamma$ is irreducible in $\mathbb{F}[x]$; such a γ can always be found, which will be shown later in Lemma 5.4 and Corollary 5.5. Furthermore, since $(n, q-1) = 1$, there exists α in $\mathbb{F}$ such that $\alpha^n = (-\gamma)^{r+1}$.

We define

$$D = D' + \alpha T^z s^2 p_1 \cdots p_{m-1} \prod_{i\neq j, 0\leq i,j\leq m-1} (B_i - B_j), \tag{11}$$

where $z = \frac{m}{n}(\deg(B_0)+1) - \deg(s^2 p_1 \cdots p_{m-1} \prod_{i\neq j, 0\leq i,j\leq m-1}(B_i - B_j))$. We note that from (iv) of Eq. (10), we have that z is a positive integer and $\deg(D) = \frac{m}{n}(\deg(B_0)+1)$. Notice that since $(B_i - B_j, D') = 1$ for all $i \neq j$ with $0 \leq i, j \leq m-1$ by (v) of Eq. (10), it follows that $(B_i - B_j, D) = 1$ for all $i \neq j$ with $0 \leq i, j \leq m-1$, and D satisfies the same congruences in Eq. (8) as does D'. It is easy to verify that D also satisfies the conditions $(v), (vi)$ of Eq. (10). We notice that D has the leading coefficient α.

4. Verification of divisibility conditions

Lemma 4.1. *For each case of Theorem* 1.1 *and Theorem* 1.2 *with polynomials* $B_0, \cdots, B_{m-1}$ *and* D *as chosen in Section* 3*, conditions* (2.1) - (2.3) *in Lemma* 2.1 *are satisfied.*

Proof. We use the condition that m and n are not both even for Theorem 1.1 and Theorem 1.2, and we also use conditions $(i), (ii)$ of Eq. (6), which are common to Theorem 1.1 and Theorem 1.2. The proof is the same as in [11, Lemma 3]. □

Lemma 4.2. *For each case of Theorem* 1.1 *and Theorem* 1.2*, with polynomials* $B_0, \cdots, B_{m-1}$ *and* D *as chosen in Section* 3*,* $\theta - B_0, \theta - B_1, \cdots, \theta - B_{m-1}$ *are pairwise relatively prime; that is, condition* (2.4) *in Proposition* 2.3 *is satisfied.*

Proof. The proof is the same as in [11, Lemma 4] by using condition (v) of Eq. (6), which is common to Theorem 1.1 and Theorem 1.2. □

Lemma 4.3. *For each case of Theorem* 1.1 *and Theorem* 1.2*, with polynomials* $B_0, \cdots, B_{m-1}$ *and* D *as chosen in Section* 3*,* $f(X)$ *is irreducible.*

Proof. The proof is the same as in [6, Lemma 4.3] by using conditions $(i), (ii), (v)$ of Eq. (6), which are common to Theorem 1.1 and Theorem 1.2. □

5. The infinite prime

Now, in each case of Theorem 1.1 and Theorem 1.2, it remains only to verify the splitting behaviors of the prime at infinity $\wp_\infty$ as the given signature.

Proposition 5.1. *Under the assumptions of Theorem* 1.1*, for a given signature* (e_i, f_i)*,* $1 \le i \le r+1$*, where* $\sum_{i=1}^{r+1} e_i \mathfrak{f}_i = m$*,* e_i *is arbitrary and* $\mathfrak{f}_i = 1$ *for each* i*, the prime at infinity* $\wp_\infty$ *splits into* $r+1$ *primes* $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_{r+1}$ *in* K *with* $e(\mathfrak{P}_i/\wp_\infty) = e_i$ *and* $\mathfrak{f}(\mathfrak{P}_i/\wp_\infty) = 1$ *for* $1 \le i \le r+1$*. That is, condition* 1) *of Theorem* 1.1 *and condition* (2.5) *of Proposition* 2.3 *are satisfied.*

Proof. Let

(12)

$$f(X) = \prod_{i=0}^{m-1}(X - B_i) + D^n = X^m - \sigma_1 X^{m-1} + \cdots + (-1)^{m-1}\sigma_{m-1}X + (-1)^m \sigma_m + D^n,$$

where

$$\sigma_j = \sigma_j(B_0, B_1, \cdots, B_{m-1}) = \sum_{0 \le i_1 < i_2 < \cdots < i_j \le m-1} B_{i_1} B_{i_2} \cdots B_{i_j}$$

is the jth *elementary symmetric polynomial* in the indeterminates $B_0, B_1, \cdots, B_{m-1}$ for $1 \le j \le m$. Let $k_\infty = \mathbb{F}((\frac{1}{T}))$ be the completion field of k at $\wp_\infty$.

Using the *Newton Polygon* method, we show that there are at least $r+1$ primes lying above $\wp_\infty$ in K.

The points to consider in the construction of the Newton polygon of $f(X)$ are $P_0 = (0, -\deg((-1)^m \sigma_m + D^n))$, $P_i = (i, -\deg(\sigma_{m-i}))$ for $1 \le i \le m-1$, and $P_m = (m, 0)$. From the degree conditions of B_i given in (iii) of Eq. (6), it follows that for every i with $1 \le i \le e_1$, the line segment $\overline{P_0 P_i}$ has the slope $\frac{\deg(\sigma_m) - \deg(\sigma_{m-i})}{i} = \frac{i\beta_1}{i} = \beta_1$. The line segment $\overline{P_0 P_m}$ has the slope

$$\frac{e_1\beta_1 + e_2\beta_2 + \cdots + e_{r+1}\beta_{r+1}}{m} > \frac{(e_1 + e_2 + \cdots + e_{r+1})\beta_1}{m} = \beta_1,$$

and this implies that the line segment $\overline{P_0P_i}$ for $1 \le i \le e_1$ lies strictly below the secant line $\overline{P_0P_m}$, and so $\overline{P_0P_{e_1}}$ with slope β_1 forms one edge of the Newton polygon. Furthermore, for every i with $e_1 \le i \le e_1 + e_2$, the line segment $\overline{P_{e_1}P_i}$ has the slope $\frac{\deg(\sigma_m)-\deg(\sigma_{m-i})}{i} = \frac{i\beta_2}{i} = \beta_2$. Similarly, we can see that the Newton polygon for $f(X)$ with respect to $\wp_\infty$ consists of strictly increasing $r+1$ distinct line segments, where the slope of each line segment is β_i for $1 \le i \le r+1$ with $\beta_1 < \beta_2 < \cdots < \beta_{r+1}$, and the x-increment of each slope is e_i, $1 \le i \le r+1$. It thus follows that at least $r+1$ roots of $f(X)$ in $\bar{k}_\infty$ have distinct ord_∞, which implies that those $r+1$ distinct roots are in k_∞. Hence, there exist at least $r+1$ infinite primes $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_{r+1}$ lying above $\wp_\infty$.

According to the Newton Polygon obtained as above, by *Kummer's Criterion* [10, Proposition 8.2] or [3, Theorem 23], we know that $\bar{f}(X) \bmod (\frac{1}{T})$ can be factored in the completion field $k(\theta)_\infty$ as follows:

$$\bar{f}(X) \equiv \bar{f}_1(X)\bar{f}_2(X)\cdots\bar{f}_{r+1}(X) \mod (1/T). \tag{13}$$

Since the x-increment of each slope of the Newton polygon is e_i, $\bar{f}_i(X)$ is of degree e_i for each $i = 1, 2, \cdots, r+1$, and $\sum_{i=1}^{r+1} e_i = m$.

Since $\frac{\deg(D^n)}{m} < \beta_1 < \beta_2 < \cdots < \beta_{r+1}$, we have $\deg(D^n) < \deg(\sigma_m)$. Hence, substituting XT^{β_1} for X in $f(X) = 0$ and dividing both sides by $T^{m\beta_1}$, we can see that

$$\bar{f}(X) \equiv \prod_{i=0}^{m-1}(X - B_i) \mod \left(\frac{1}{T}\right).$$

For each i, all the roots of $\bar{f}_i(X)$ in Eq. (13) have the same valuations as the slope β_i of each line segment of the Newton polygon. Furthermore, $ord_\infty(B_j) = -\beta_i$ for $\sum_{k=1}^{i-1} e_k \le j \le \sum_{k=1}^{i} e_k - 1$. Therefore, we have

$$\bar{f}_i(X) \equiv \prod_{\sum_{k=1}^{i-1} e_k \le j \le \sum_{k=1}^{i} e_k - 1} (X - B_j) \mod \left(\frac{1}{T}\right)$$

for $i = 1, 2, \cdots, r+1$.

Let $\mathfrak{P}_i$ be the prime corresponding to each $\bar{f}_i(X)$. We claim that the ramification index of $\mathfrak{P}_i$ is e_i and the relative degree of $\mathfrak{P}_i$ is 1 for each $i = 1, 2, \cdots, r+1$. For each f_i with $i = 1, 2, \cdots, r+1$, substituting XT^{β_i} for X in $\bar{f}_i(X) = 0$, we have that

$$\begin{aligned} \bar{f}_i(XT^{\beta_i}) &\equiv \prod_{\sum_{k=1}^{i-1} e_k \le j \le \sum_{k=1}^{i} e_k - 1} (XT^{\beta_i} - B_j) \mod \left(\frac{1}{T}\right) \\ &= T^{e_i\beta_i} \prod_{\sum_{k=1}^{i-1} e_k \le j \le \sum_{k=1}^{i} e_k - 1} (X - \frac{B_j}{T^{\beta_i}}) = 0. \end{aligned} \tag{14}$$

Dividing both sides of Eq. (14) by $T^{e_i\beta_i}$, since $\dfrac{B_j}{T^{\beta_i}} \equiv c_j \bmod (\frac{1}{T})$ for j with $\sum_{k=1}^{i-1} e_k \le j \le \sum_{k=1}^{i} e_k - 1$, we have that

$$\begin{aligned} \bar{f}_i(X) &\equiv \prod_{\sum_{k=1}^{i-1} e_k \le j \le \sum_{k=1}^{i} e_k - 1} (X - c_j) \mod \left(\frac{1}{T}\right) \\ &= (X - \tau_i)^{e_i}. \end{aligned} \tag{15}$$

According to *Kummer's Criterion*, it thus follows that $\wp_\infty$ splits into $r+1$ primes, $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_{r+1}$ in K with $e(\mathfrak{P}_i/\wp_\infty) = e_i$ and $\mathfrak{f}(\mathfrak{P}_i/\wp_\infty) = 1$ for $1 \le i \le r+1$ as asserted. □

Lemma 5.4 shows that we can choose γ in $\mathbb{F}$ such that $x^{\mathfrak{f}} - \gamma$ is irreducible in $\mathbb{F}[x]$. For details, we need the following lemmas. Lemma 5.2 is in [4, Ch VIII, Theorem 9.1], and Lemma 5.3 can be verified easily.

Lemma 5.2. *Let k be a field, l an integer ≥ 2, and $a \in k, a \ne 0$. Assume that for any prime p with $p \mid l$, we have $a \notin k^p$, and if $4 \mid l$, then $a \notin -4k^4$. Then $x^l - a$ is irreducible in $k[x]$.*

Lemma 5.3. *For a given positive integer d, $a \in \mathbb{F}^*$ is a dth power of some element in $\mathbb{F}$ if and only if $a^{\frac{q-1}{g}} = 1$ in $\mathbb{F}$, where $g = (q-1, d)$.*

Lemma 5.4. *Let r be any positive integer and q be a power of odd prime $> \mathfrak{f}$ such that for any prime divisor P of $\mathfrak{f}$, we have $P \mid (q-1)$ and $(r+1) \mid \frac{q-1}{P}$, and if $4 \mid \mathfrak{f}$, then we have $q \equiv 1 \pmod 8$ and $(r+1) \mid \frac{q-1}{4}$. Let γ be such that $\gamma^{\frac{q-1}{P}} \ne 1$ for any prime $P \mid \mathfrak{f}$ and $\gamma^{\frac{q-1}{4}} \ne 1$ if $4 \mid \mathfrak{f}$.*

Then $x^{\mathfrak{f}} - \zeta^i\gamma$ is irreducible in $\mathbb{F}[x]$ for each $0 \le i \le r$, where ζ denotes a primitive $(r+1)$st root of unity in $\mathbb{F}$ (since $(r+1) \mid (q-1)$, we have $(q, r+1) = 1$, so char $\mathbb{F} \nmid (r+1)$; therefore $\zeta \in \mathbb{F}$).

Proof. To show the irreducibility of $x^{\mathfrak{f}} - \zeta^i\gamma$ for each $0 \le i \le r$, by Lemma 5.2 it is enough to show that

$$(i) \quad \zeta^i\gamma \notin \mathbb{F}^P \qquad \text{for every prime } P \mid \mathfrak{f},$$
$$(ii) \quad \zeta^i\gamma \notin -4\mathbb{F}^4 \qquad \text{if } 4 \mid \mathfrak{f}.$$

Using Lemma 5.3, (i) is equivalent to $(\zeta^i\gamma)^{\frac{q-1}{P}} \ne 1$, and this follows from the following: $\zeta^{\frac{q-1}{P}} = 1$ since $(r+1) \mid \frac{q-1}{P}$, and $\gamma^{\frac{q-1}{P}} \ne 1$ for any prime $P \mid \mathfrak{f}$ by our assumption.

To show (ii), we assume that $4 \mid \mathfrak{f}$, so $q \equiv 1 \pmod 8$, which implies that -4 is a fourth power in $\mathbb{F}$. This is because -1 is a fourth power in $\mathbb{F}$ and 2 is a square in $\mathbb{F}$. It thus suffices to show that $\zeta^i\gamma$ is not a fourth power in $\mathbb{F}$. We see that ζ is a fourth power in $\mathbb{F}$ by Lemma 5.3 since $(r+1) \mid \frac{q-1}{4}$. Furthermore, γ is not a fourth power in $\mathbb{F}$ because $\gamma^{\frac{q-1}{4}} \ne 1$. Condition (ii) is thus satisfied as well. □

One explicit way to find such a γ is as follows:

Corollary 5.5. *Let γ be a primitive $(q-1)$st root of unity with the other assumptions the same as in Lemma 5.4. Then $x^{\mathfrak{f}} - \zeta^i\gamma$ is irreducible in $\mathbb{F}[x]$ for each $0 \le i \le r$.*

Proposition 5.6. *Under the assumptions of Theorem 1.2, for a given signature $(e_i, \mathfrak{f}_i)$, $1 \le i \le r+1$, with $\sum_{i=1}^{r+1} e_i\mathfrak{f}_i = m$, $e_i = 1$, and the $\mathfrak{f}_i$'s the same for each i, $\mathfrak{f}_i = \mathfrak{f}$, the prime at infinity $\wp_\infty$ splits into $r+1$ primes $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_{r+1}$ in K with $e(\mathfrak{P}_i/\wp_\infty) = 1$ and $\mathfrak{f}(\mathfrak{P}_i/\wp_\infty) = \mathfrak{f}$ for $1 \le i \le r+1$. That is, condition 1) of Theorem 1.2 and condition (2.5) of Proposition 2.3 are satisfied.*

Proof. Let $f(X)$ be written as in Eq. (12), $d = \deg(D)$ and $\beta = \deg(B_0)+1$. Recall that $d = \frac{m\beta}{n}$, so $\beta = \frac{dn}{m}$. We then note that $\deg(\sigma_i) < i\beta$ for every $i = 1, 2, \cdots, m$

since $\beta > \deg(B_i)$ for every $0 \le i \le r-1$ from (ii) of Eq. (10). Substituting XT^{β} for X in $f(X) = 0$ and then dividing both sides of Eq. (12) by $T^{m\beta}$, we have that

$$\bar{f}(X) = X^m - \left(\frac{\sigma_1}{T^{\beta}}\right) X^{m-1} + \left(\frac{\sigma_2}{T^{2\beta}}\right) X^{m-2} + \cdots + \frac{((-1)^m \sigma_m + D^n)}{T^{m\beta}} = 0.$$

Since $\deg(\sigma_i) < i\beta$ for $i = 1, 2, \cdots, m$, it follows that $\frac{\sigma_i}{T^{i\beta}} \equiv 0 \bmod (\frac{1}{T})$ for $i = 1, 2, \cdots, m$. Thus $\bar{f}(X) \equiv X^m + \alpha^n \pmod{\frac{1}{T}}$, where α is the leading coefficient of D. As $\alpha^n = (-\gamma)^{r+1}$ and $m = (r+1)\mathfrak{f}$,

$$\begin{aligned}\bar{f}(X) &\equiv X^{(r+1)\mathfrak{f}} + (-\gamma)^{r+1} \\ &\equiv (X^{\mathfrak{f}} - \gamma)(X^{\mathfrak{f}} - \zeta\gamma)(X^{\mathfrak{f}} - \zeta^2\gamma)\cdots(X^{\mathfrak{f}} - \zeta^r\gamma),\end{aligned}$$

where ζ denotes a primitive $(r+1)$st root of unity.

Lemma 5.4 shows that $x^{\mathfrak{f}} - \zeta^i\gamma$ is irreducible over $\mathbb{F}$ for $1 \le i \le r+1$. According to *Kummer's Criterion*, it follows that $\wp_\infty$ splits into $r+1$ primes, $\mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_{r+1}$ in K with $e(\mathfrak{P}_i/\wp_\infty) = 1$ and $\mathfrak{f}(\mathfrak{P}_i/\wp_\infty) = \mathfrak{f}$ for $1 \le i \le r+1$ as asserted. $\square$

Acknowledgment

The author thanks the referee for very helpful comments.

References

1. T. Azuhata and H. Ichimura, *On the divisibility problem of the class numbers of algebraic number fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **30** (1984), 579–585. MR731519 (85a:11021)
2. C. Friesen, *Class number divisibility in real quadratic function fields*, Canad. Math. Bull. **35** (1992), 361–370. MR1184013 (93h:11130)
3. A. Frohlich and M.J. Taylor, *Algebraic Number Theory*, Cambridge University Press, 1993.
4. S. Lang, *Algebra*, 2nd edition, Addison-Wesley, Reading, MA, 1984. MR0197234 (33:5416)
5. Y. Lee, *The structure of the class groups of global function fields with any unit rank*, J. Ramanujan Math. Soc. **20**, No. 2 (2005), 125-145. MR2169092 (2007m:11154)
6. Y. Lee and A. Pacelli, *Class groups of imaginary function fields: The inert case*, Proc. Amer. Math. Soc. **133** (2005), 2883-2889. MR2159765 (2006e:11177)
7. Y. Lee and A. Pacelli, *Higher rank subgroups in the class groups of imaginary function fields*, J. Pure Appl. Algebra **207** (2006), 51-62. MR2244260 (2007d:11124)
8. T. Nagell, *Uber die Klassenzahl imaginar quadratischer Zahlkorper*, Abh. Math. Sem. Univ. Hamburg **1** (1922), 140–150.
9. S. Nakano, *On ideal class groups of algebraic number fields*, J. Reine Angew. Math. **358** (1985), 61–75. MR797674 (86k:11063)
10. J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999. MR1697859 (2000m:11104)
11. A. Pacelli, *Abelian subgroups of any order in class groups of global function fields*, J. Number Theory **106** (2004), 26-49. MR2029780 (2004m:11193)
12. A. Pacelli, *The prime at infinity and the rank of the class group in global function fields*, J. Number Theory **116** (2006), 311-323. MR2195928 (2006k:11228)
13. M. Rosen, *Number Theory in Function Fields*, Springer-Verlag, New York, 2002. MR1876657 (2003d:11171)
14. Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76. MR0266898 (42:1800)

Department of Mathematics, Ewha Womans University, Seoul, 120-750, Republic of Korea

E-mail address: `yoonjinl@ewha.ac.kr`