

## CLASS GROUPS OF IMAGINARY FUNCTION FIELDS: THE INERT CASE

YOONJIN LEE AND ALLISON M. PACELLI

(Communicated by Wen-Ching Winnie Li)

ABSTRACT. Let  $\mathbb{F}$  be a finite field and  $T$  a transcendental element over  $\mathbb{F}$ . An imaginary function field is defined to be a function field such that the prime at infinity is inert or totally ramified. For the totally imaginary case, in a recent paper the second author constructed infinitely many function fields of any fixed degree over  $\mathbb{F}(T)$  in which the prime at infinity is totally ramified and with ideal class numbers divisible by any given positive integer greater than 1. In this paper, we complete the imaginary case by proving the corresponding result for function fields in which the prime at infinity is inert. Specifically, we show that for relatively prime integers  $m$  and  $n$ , there are infinitely many function fields  $K$  of fixed degree  $m$  such that the class group of  $K$  contains a subgroup isomorphic to  $(\mathbb{Z}/n\mathbb{Z})^{m-1}$  and the prime at infinity is inert.

### 1. INTRODUCTION

Determining the class number and class group of a number field or function field is a problem that dates back to Gauss who studied class numbers of quadratic number fields, albeit in the language of equivalence classes of binary quadratic forms. It is known that given an integer  $n$ , infinitely many number fields and function fields have class number divisible by  $n$  (see for example, Nagell [5] for imaginary quadratic number fields, Yamamoto [9] for real quadratic number fields, and Friesen [2] for real quadratic function fields). In fact, given integers  $m$  and  $n$ , it is known that 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 [6] for number fields and the second author [7] for function fields). This is a consequence of stronger results, not merely on the divisibility of the class number, but on the structure of the class group.

In 1983, Azuhata and Ichimura [1] constructed, for arbitrary integers  $m$  and  $n$ , infinitely many number fields  $K$  of degree  $m$  over  $\mathbb{Q}$  such that the ideal class group of  $K$  contains a subgroup isomorphic to  $(\mathbb{Z}/n\mathbb{Z})^{r_2}$ , where  $r_2$  as usual denotes half the number of complex embeddings of  $K$  into  $\mathbb{C}$ . Nakano [6] extended this result three years later to the case of totally real number fields, and increased the rank of the subgroup in the general case from  $r_2$  to  $r_2 + 1$ . Recently, the second author [7] proved an analogous statement for function fields in which the prime at

---

Received by the editors May 1, 2004 and, in revised form, June 8, 2004.

2000 *Mathematics Subject Classification*. Primary 11R29; Secondary 11R58.

*Key words and phrases*. Class group, class number, rank of class group, imaginary function field.

infinity is totally ramified or splits completely. If  $m$  and  $n$  are relatively prime and not divisible by the characteristic of  $\mathbb{F}$ , then we get infinitely many function fields  $K$  of degree  $m$  over  $\mathbb{F}(T)$  with the ideal class group of  $K$  containing a subgroup isomorphic to  $(\mathbb{Z}/n\mathbb{Z})^{m-1}$  and the prime at infinity of  $K$  totally ramified. For any integers  $m$  and  $n$  not divisible by the characteristic of  $\mathbb{F}$ , we get infinitely many function fields  $K$  of degree  $m$  over  $\mathbb{F}(T)$  such that the ideal class group of  $K$  contains a subgroup isomorphic to  $\mathbb{Z}/n\mathbb{Z}$  and the prime at infinity splits completely.

Although it no longer makes sense to describe a function field as real or imaginary according to whether it embeds into  $\mathbb{R}$ , it is possible to characterize function fields as real or imaginary. We define a function field to be *real* if the prime at infinity splits completely; the rank of the unit group in this case is maximal as it is for totally real number fields. We call a function field *imaginary* if the prime at infinity is inert or totally ramified; then the rank of the unit group is minimal as it is for purely imaginary number fields. The results in [7] mentioned above, then, address the case of real function fields, but the case of imaginary function fields is incomplete. In this paper, we complete the imaginary case by proving an analogous result for the case of function fields in which the prime at infinity is inert.

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  $K$ . Let  $P_\infty$  be the prime at infinity (or the infinite place) of  $K$  defined by the negative degree valuation, i.e.  $\text{ord}_\infty(g) = \deg(g)$  for  $g \in K^\times$ . We write  $Cl_K$  to denote the ideal class group of  $\mathcal{O}_K$ . The main result is the following:

**Theorem 1.1.** *Let  $m$  and  $n$  be any relatively prime positive integers with  $m > 1$  and  $P_i \mid (q-1)$  for all primes  $P_i$  dividing  $m$ . Let  $q$  be a power of an odd prime with  $q \equiv 1 \pmod{4}$  if  $m$  is exactly divisible by 2 and  $q \equiv 1 \pmod{8}$  if  $4 \mid m$ . If  $\mathbb{F}$  is the field with  $q$  elements, and  $m$  and  $n$  are not divisible by the characteristic of  $\mathbb{F}$ , then there exist infinitely many function fields  $K$  of degree  $m$  over  $k = \mathbb{F}(T)$  such that*

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

The proof of Theorem 1.1 is similar to that of the case where the prime at infinity is totally ramified in [7]. The main difference is the use of an alternate method to control the behavior of the prime at infinity. Rather than using Newton polygons, we instead use *Kummer's criterion*. Let

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

where  $B_0, \dots, B_{m-1}$  and  $D$  are polynomials in  $\mathbb{F}[T]$  with certain conditions given in Section 2. If  $\theta$  is a root of  $f(X)$ , then we will show that  $K = k(\theta)$  satisfies the conditions of Theorem 1.1.

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, see [7].

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

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

and let  $\theta$  be a root of  $f(X)$ . Set  $K = k(\theta)$ . The next two lemmas and proposition show that with an appropriate choice of  $B_0, \dots, B_{m-1}$ , and  $D$ , the field  $K$  satisfies the conditions of Theorem 1.1.

**Lemma 2.1.** *Suppose there exist monic irreducible polynomials  $p_1, \dots, p_{m-1}$  with  $|p_i| \equiv 1 \pmod{m_0 n_0}$  and polynomials  $B_1, \dots, B_{m-1}$ , 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  $\theta - B_1, \theta - B_2, \dots, \theta - B_{m-1}$  is an elementary abelian group of rank  $m - 1$ .

*Proof.* The proof is the same as in [7]. □

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

**Lemma 2.2.** *Suppose  $G$  is a finite abelian group of exponent  $n$ , and  $\dim_{\mathbb{Z}/l\mathbb{Z}} G^{n/l} \geq r$  for all  $l$  dividing  $n$ . Then  $G$  contains a subgroup isomorphic to  $\mathbb{Z}/n\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/n\mathbb{Z}$  of rank  $r$ .*

**Proposition 2.3.** *Suppose that the polynomials  $B_0, \dots, B_{m-1}$  and  $D$  further satisfy the following two conditions:*

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

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

*Proof.* Since the prime at infinity is inert, we know that the rank of the unit group in  $K$  is 0; therefore the only units in  $K$  are the roots of unity. The result therefore follows by the same proof as in [7, Proposition 1]. □

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

3. CHOOSING POLYNOMIALS

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

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

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  $\zeta_m$  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

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

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

$$(2) \quad X^m - 1 \equiv \prod_{i=0}^{m-1} (X - C_i) \pmod{s},$$

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

Choose  $B_i, 1 \leq i \leq m - 1$ , such that

$$(3) \quad B_i \equiv \begin{cases} 1 & \pmod{p_j} \text{ if } i \neq j, \\ g_i & \pmod{p_i}, \\ C_i & \pmod{s}. \end{cases}$$

Choose an irreducible polynomial  $D'$  so that

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

$$(5) \quad (B_i - B_j, D') = 1 \text{ for } 1 \leq i, j \leq m - 1, i \neq j.$$

Infinitely many  $D'$  satisfying the conditions in (4) exist by the strong version of Dirichlet's Theorem for function fields [8, p. 40] which asserts that in any arithmetic progression, there exist polynomials of each large degree. We need only discard finitely many not satisfying (5). Next choose  $B_0$  such that

$$(6) \quad \left\{ \begin{array}{l} (i) \quad B_0 \equiv \begin{cases} g_i^{-1} & \pmod{p_i} \text{ for } 1 \leq i \leq m - 1, \\ C_0 & \pmod{s}, \end{cases} \\ (ii) \quad \deg(B_0) > \deg(B_i) - 1 \text{ for } 1 \leq i \leq m - 1, \\ (iii) \quad (B_0 - B_j, D') = 1 \text{ for } 1 \leq j \leq m - 1, \\ (iv) \quad \deg(B_0) \equiv -1 \pmod{n}, \\ (v) \quad \frac{m}{n}(\deg(B_0) + 1) > \deg(s^2 p_1 \cdots p_{m-1} \prod_{i \neq j, 0 \leq i, j \leq m-1} (B_i - B_j)), \\ (vi) \quad \frac{m}{n}(\deg(B_0) + 1) > \deg(D'), \\ (vii) \quad (D')^n + (-1)^m B_0 B_1 \cdots B_{m-1} \not\equiv 0 \pmod{s^2}. \end{array} \right.$$

Again, infinitely many  $B_0$  satisfying the conditions in (6) exist by the strong version of Dirichlet's Theorem mentioned above. Finally, let  $r$  be a primitive  $(q - 1)$ st root of unity in  $\mathbb{F}$ , and define

$$D = D' + rT^z s^2 p_1 \cdots p_{m-1} \prod_{i \neq j, 0 \leq i, j \leq m-1} (B_i - B_j),$$

where  $z = \frac{m}{n}(\deg(B_0) + 1) - \deg(s^2 p_1 \cdots p_{m-1} \prod_{i \neq j, 0 \leq i, j \leq m-1} (B_i - B_j))$ . Note that  $z$  is a positive integer by (v) of (6), and  $\deg(D) = \frac{m}{n}(\deg(B_0) + 1)$  by (vi) of (6). Note that since  $(B_i - B_j, D') = 1$  for all  $i \neq j$  with  $0 \leq i, j \leq m - 1$  by (5) and (iii) of (6), 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 (4) as did  $D'$ . It is easy to verify that  $D$  also satisfies the condition (vii) of (6).

4. VERIFICATION OF DIVISIBILITY CONDITIONS

**Lemma 4.1.** *With polynomials  $B_0, \dots, B_{m-1}$  and  $D$  in  $\mathbb{F}[T]$  chosen as above, conditions (2.1)–(2.3) in Lemma 2.1 are satisfied.*

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

**Lemma 4.2.**  *$\theta - B_0, \theta - B_1, \dots, \theta - B_{m-1}$  are pairwise relatively prime, that is, condition (2.4) in Proposition 2.3 is satisfied.*

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

**Lemma 4.3.** *With the conditions on  $B_0, \dots, B_{m-1}$ , and  $D$  given above,  $f(X)$  is irreducible.*

*Proof.* We show that  $f(X)$  is an Eisenstein polynomial with respect to  $s$ . It is easy to check that  $s|(D^n + (-1)^m B_0 B_1 \cdots B_{m-1})$ , the constant term of  $f(X)$ . Furthermore, from (vii) of (6) we have  $s^2 \nmid (D^n + (-1)^m B_0 B_1 \cdots B_{m-1})$ .

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  $0 \leq i \leq m - 1$ , then

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

Therefore, 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

It remains only to prove that the prime at infinity is inert in  $K$ . We need the following lemmas. Lemma 5.1 is in [4, Ch VIII, Theorem 9.1], and Lemma 5.2 can be verified easily.

**Lemma 5.1.** *Let  $k$  be a field,  $l$  an integer  $\geq 2$ , and  $a \in k, a \neq 0$ . 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 5.2.** *For a given positive integer  $d$ ,  $a \in \mathbb{F}^*$  is a  $d$ th power of some element in  $\mathbb{F}$  if and only if  $a^{\frac{q-1}{g}} = 1$  in  $\mathbb{F}$ , where  $g = (q - 1, d)$ .*

**Proposition 5.3.** *The prime at infinity is inert in  $K$ , that is, condition (2.5) in Proposition 2.3 is satisfied.*

*Proof.* Write

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

where

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

is the  $j$ th elementary symmetric polynomial in the indeterminates  $B_0, B_1, \dots, B_{m-1}$ .

Let  $d$  denote the degree of  $D$ , and recall that  $d = \frac{m}{n}(\deg(B_0) + 1)$ . Let  $\alpha = \frac{dn}{m}$ , that is,  $\alpha = \deg(B_0) + 1$ . We then note that  $\deg(\sigma_i) < i\alpha$  from (ii) of (6) for  $i = 1, 2, \dots, m$ . Substituting  $XT^\alpha$  for  $X$  in  $f(X) = 0$ , we have that

$$(7) \quad \begin{aligned} f(XT^\alpha) &= T^{m\alpha} X^m - \sigma_1 T^{(m-1)\alpha} X^{m-1} + \sigma_2 T^{(m-2)\alpha} X^{m-2} \\ &+ \dots + (-1)^{m-1} \sigma_{m-1} T^\alpha X + ((-1)^m \sigma_m + D^n) = 0. \end{aligned}$$

Dividing both sides of (7) by  $T^{m\alpha}$ , we have that

$$\begin{aligned} \tilde{f}(X) &= X^m - \left(\frac{\sigma_1}{T^\alpha}\right) X^{m-1} + \left(\frac{\sigma_2}{T^{2\alpha}}\right) X^{m-2} \\ &+ \dots + (-1)^{m-1} \left(\frac{\sigma_{m-1}}{T^{(m-1)\alpha}}\right) X + \frac{((-1)^m \sigma_m + D^n)}{T^{m\alpha}} = 0. \end{aligned}$$

By *Kummer’s Criterion* [3, Theorem 23], to show that the prime at infinity  $P_\infty$  is inert in  $K$ , it suffices to show that  $\tilde{f}(X) \pmod{\left(\frac{1}{T}\right)}$  is irreducible over  $\mathbb{F}$ . Since  $\deg(\sigma_i) < i\alpha$  for  $i = 1, 2, \dots, m$ , it follows that  $\frac{\sigma_i}{T^{i\alpha}} \equiv 0 \pmod{\left(\frac{1}{T}\right)}$  for  $i = 1, 2, \dots, m$ . Thus  $\tilde{f}(X) \equiv X^m + r^n \pmod{\left(\frac{1}{T}\right)}$ , where  $r$  is the leading coefficient of  $D$ . Thus, it is enough to show that  $X^m + r^n$  is irreducible over  $\mathbb{F}$ . By Lemmas 5.1 and 5.2 above, we only need to show that the following two conditions hold, where  $P_1, \dots, P_t$  are the distinct primes dividing  $m$ :

- (i)  $-r^n \notin \mathbb{F}^{P_i}$  for every  $i = 1, 2, \dots, t$ .
- (ii)  $r^n \notin 4\mathbb{F}^4$  if  $4 \mid m$ .

Recall that  $r$ , the leading coefficient of  $D$ , is a primitive  $(q - 1)$ st root of unity. If  $P_i$  is odd for some  $i = 1, 2, \dots, t$ , then  $-1$  is a  $P_i$ th power of  $-1$ . Since  $P_i \mid q - 1$ , we have  $r^{\frac{q-1}{P_i}} \neq 1$ , and so  $(r^n)^{\frac{q-1}{P_i}} \neq 1$  since  $P_i \nmid n$ . Thus condition (i) is satisfied by Lemma 5.2. If  $P_i = 2$ , then we have  $q \equiv 1 \pmod{4}$ , so  $\left(\frac{-1}{q}\right) = 1$ . Then  $r^{\frac{q-1}{2}} \neq 1$ , and so,  $\left(\frac{r}{q}\right) = -1$ . Since  $(m, n) = 1$ ,  $2 \nmid n$  it follows that  $\left(\frac{r^n}{q}\right) = -1$ . Therefore we have  $\left(\frac{-r^n}{q}\right) = -1$ , so condition (i) holds for this case as well.

Now, if  $4 \mid m$ , then  $r^{\frac{q-1}{4}} \neq 1$  since  $r$  is a primitive  $(q - 1)$ st root of unity. This implies that  $(r^n)^{\frac{q-1}{4}} \neq 1$  since  $(m, n) = 1$  and so  $4 \nmid n$ . Then  $r^n$  is not a 4th power in  $\mathbb{F}$  by Lemma 5.2. Suppose, for contradiction, that  $r^n \in 4\mathbb{F}^4$ . Because  $q \equiv 1 \pmod{8}$  in this case, we know that 2 is a square in  $\mathbb{F}$ . Then 4 is a 4th power in  $\mathbb{F}$ ; this implies that  $r^n$  must be a 4th power in  $\mathbb{F}$ , a contradiction. Condition (ii) is thus satisfied as well.

It therefore follows that  $X^m + r^n$  is irreducible over  $\mathbb{F}$ , and so, the prime at infinity is inert as desired. □

#### ACKNOWLEDGMENTS

We thank Professor Michael Rosen for his valuable comments during the writing of this paper.

## REFERENCES

1. T. Azuhata and H. Ichimura, *On the divisibility problem of the class numbers of algebraic number fields*, J. Fac. Sci. Univ. Tokyo **30** (1984), 579–585. MR0731519 (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. MR0783636 (86j:00003)
5. T. Nagell, *Über die Klassenzahl imaginär quadratischer Zahlkörper*, 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. MR0797674 (86k:11063)
7. A. Pacelli, *Abelian subgroups of any order in class groups of global function fields*, J. Number Theory **106** (2004), 26–49. MR2029780 (2004m:11193)
8. M. Rosen, *Number Theory in Function Fields*, Springer, 2002. MR1876657 (2003d:11171)
9. Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76. MR0266898 (42:1800)

DEPARTMENT OF MATHEMATICS, SMITH COLLEGE, NORTHAMPTON, MASSACHUSETTS 01063  
E-mail address: yjlee@smith.edu

DEPARTMENT OF MATHEMATICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MASSACHUSETTS 01267  
E-mail address: Allison.Pacelli@williams.edu