49. On the Class Groups of Pure Function Fields

By Humio ICHIMURA
Department of Mathematics, Faculty of Science, University of Tokyo

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 1988)

§1. **Introduction.** It was proved by Nagell [5] that there exist infinitely many quadratic number fields whose class numbers are divisible by a given integer. Similar results for quadratic number fields were obtained by several other authors. Since quadratic number fields are "pure" extensions (in the sense of Ishida [2]) over the rationals $\boldsymbol{Q}$ of degree 2, these results tempt us to ask:

For any integers $n(>2)$ and $m(>1)$, do there exist infinitely many pure extensions over $\boldsymbol{Q}$ of degree n whose class numbers are divisible by m?
When each prime factor of m divides n, "genus theory" (cf. Roquette and Zassenhause [8]) solves this problem (affirmatively). See also Ishida [1] and Madan [4, p. 117]. In other cases, it has been solved, so far, only when $2|n$ (by using the above result for quadratic fields) and when $3|n$ or $m=2$ by Nakano [6, 7], and the problem seems very difficult for general n and m.

The purpose of this note is to solve a function field analogue of the above problem. Let ℓ be a fixed prime number, $\boldsymbol{F}_\ell$ be the prime field of ℓ elements and X be a fixed indeterminate. We deal with pure extensions over the rational function field $\boldsymbol{F}_\ell(X)$, i.e., extensions of the form $\boldsymbol{F}_\ell(X, f(X)^{1/n})/\boldsymbol{F}_\ell(X)$ with $(n, \ell)=1$ and $f(X)\in \boldsymbol{F}_\ell(X)$. But, for the sake of simplicity, we consider only those for which the degree (over $\boldsymbol{F}_\ell(X)$) is an odd prime number p. In view of "genus theory" for function fields (cf. Madan [3] or §2.1), we confine ourselves to the case in which the *non p* part of the class group is "large". We shall prove

Theorem 1. *Let p be an odd prime number different from ℓ, and r_p be the number of the irreducible factors of X^p-1 in the polynomial ring $\boldsymbol{F}_\ell[X]$. For any finite abelian group A of rank $2(r_p-1)$ with exponent relatively prime to ℓp, there exist infinitely many pure extensions over $\boldsymbol{F}_\ell(X)$ of degree p for which the divisor class group of degree zero contains a subgroup isomorphic to A.*
Here, we need the assumption that the exponent of the abelian group A is relatively prime to ℓ for a technical reason.

Further, we shall prove a similar theorem concerning the ideal class groups of "imaginary" and "real" pure extensions over $\boldsymbol{F}_\ell(X)$ which is an analogue of a result of Yamamoto [10] on those of imaginary and real quadratic number fields.

The point of the proofs of our theorems is that a certain type of pure extensions over $\boldsymbol{F}_\ell(X)$ of degree p (those in §2.2) allow the use of "genus theory" for studying the *non p* part of their class groups.

§2. Proof of Theorem 1.

§2.1. "Genus theory". Let K be a function field of one variable over a finite field k, E be a finite separable geometric[1] extension over K and C_E be the divisor class group of degree zero of E. For any natural number a and any prime number p, we put

$R_{p^a}(C_E)$:=the p^a-rank of the finite abelian group C_E,

$\rho_{p^a}(E/K)$:=the number of prime divisors of K for which each of the ramification indices in E is divisible by p^a,

$\omega_{p^a}(E/K)$:=the largest integer n such that $(p^a)^n$ divides the degree of E over K.

Then, we have

Lemma 1. $R_{p^a}(C_E) \geq \rho_{p^a}(E/K) - 1 - \omega_{p^a}(E/K)$.

When $a=1$, this assertion was proved by Madan [3]. The proof of the general case goes through similarly, and we shall not give it here.

§2.2. Proof of Theorem 1. Let p be an odd prime number different from ℓ, r_p be the number of irreducible factors of X^p-1 in $\boldsymbol{F}_\ell[X]$ and N be a natural number relatively prime to ℓp. Consider the function field

$$K=K_{N,p}=\boldsymbol{F}_\ell(X, (X^{pN}-1)^{1/p}).$$

This is a pure extension over $\boldsymbol{F}_\ell(X)$ of degree p.

Proposition. *The divisor class group of degree zero of the function field $K_{N,p}$ contains a subgroup isomorphic to the $2(r_p-1)$-fold direct product of the cyclic group of order N.*

Proof. Put $Y=(X^{pN}-1)^{1/p}$. Consider the following subfields of the function field $K=K_{N,p}$;

$$K_1=\boldsymbol{F}_\ell(Y, (Y^p+1)^{1/p}) \quad \text{and} \quad K_2=\boldsymbol{F}_\ell(Y, (Y^p+1)^{1/N}).$$

Since $(p, N)=1$, we see that $K_1 \cap K_2 = \boldsymbol{F}_\ell(Y)$ and $K_1 \cdot K_2 = K$. Since p is odd, the polynomial Y^p+1 splits into r_p prime factors in the ring $\boldsymbol{F}_\ell[Y]$. Clearly, these r_p prime divisors are fully ramified in the extension $K/\boldsymbol{F}_\ell(Y)$. On the other hand, we easily see that the prime divisor of $\boldsymbol{F}_\ell(Y)$ corresponding to the zero of $1/Y$ is unramified and splits into r_p prime divisors in the extension $K_1/\boldsymbol{F}_\ell(Y)$, and that it is fully ramified in $K_2/\boldsymbol{F}_\ell(Y)$. From these, we see that at least $2r_p$ prime divisors of K_1 are fully ramified in the extension K/K_1 of degree N. Hence, we obtain our assertion from Lemma 1.

Now, by taking various integers N, we obtain the assertion of Theorem 1.

Remark. By considering Artin-Schreier extensions over $\boldsymbol{F}_\ell(X)$ defined by the equations of type $Y^\ell - Y = X^N$, we can prove that for any finite abelian group A of rank $\ell-1$ and with exponent relatively prime to ℓ, there exist infinitely many cyclic extensions over $\boldsymbol{F}_\ell(X)$ of degree ℓ for which the divisor class group of degree zero contains a subgroup isomorphic to A.

§3. "Imaginary" and "real" pure function fields. Let ∞_X denote the prime divisor of the rational function field $\boldsymbol{F}_\ell(X)$ corresponding to the zero

---

1) This means that $E \cap \bar{k} = k$.

of $1/X$. We regard the prime divisor ∞_X as the "infinite" prime of $\boldsymbol{F}_\ell(X)$, and consequently, the polynomial ring $\boldsymbol{F}_\ell[X]$ as the ring of integers of the rational function field $\boldsymbol{F}_\ell(X)$. For a finite separable extension K over $\boldsymbol{F}_\ell(X)$, we denote by $C_{K,X}$ the ideal class group of the integral closure of the integer ring $\boldsymbol{F}_\ell[X]$ in K.

As before, p is a prime number different from ℓ. For the behavior of the infinite prime divisor ∞_X in a pure extension over $\boldsymbol{F}_\ell(X)$ of degree p, there are three possible types;

Type I: ∞_X is fully ramified,

Type R: ∞_X is unramified and splits into r_p prime divisors,

Type E: otherwise.

Those of Type I (resp. Type R) are called *imaginary* (resp. *real*) pure extensions. As is easily seen, pure extensions over $\boldsymbol{F}_\ell(X)$ of degree p and of Type E can exist only when $p\mid\ell-1$, and hence may be viewed as rather exceptional. So, we consider only imaginary and real ones. We prove

Theorem 2. *Let p be an odd prime number different from ℓ and r_p be as before. Then, for any finite abelian group A of rank $2(r_p-1)$ (resp. rank r_p-1) with exponent relatively prime to ℓp, there exist infinitely many imaginary (resp. real) pure extensions K over $\boldsymbol{F}_\ell(X)$ of degree p for which the ideal class group $C_{K,X}$ contains a subgroup isomorphic to A.*

To prove Theorem 2, we need the following

Lemma 2 (cf. Rosen [9, Proposition 1]). *Let K be a finite separable geometric extension over $\boldsymbol{F}_\ell(X)$, and $\mathcal{D}_X^0$ and $\mathcal{P}_X$ be, respectively, the divisor group of degree zero and the principal divisor group of K, both supported on prime divisors of K over ∞_X. Assume that at least one prime divisors of K over ∞_X are of degree 1. Then, there is an exact sequence;*

$$0\longrightarrow\mathcal{D}_X^0/\mathcal{P}_X\longrightarrow C_K\longrightarrow C_{K,X}\longrightarrow 0.$$

Proof of Theorem 2. Let N be a natural number relatively prime to ℓp, and $K=K_{N,p}$ be the pure extension as in § 2.2. We easily see that K is real and satisfies the assumption of Lemma 2. Since there are r_p prime divisors in K over ∞_X, the finite abelian group $\mathcal{D}_X^0/\mathcal{P}_X$ is generated by r_p-1 elements. Hence, we see from Proposition and Lemma 2 that the ideal class group $C_{K,X}$ contains a subgroup isomorphic to the (r_p-1)-fold direct product of the cyclic group of order N. Next, consider the function field

$$K'=K'_{N,p}=\boldsymbol{F}_\ell(X, ((X+1)^{pN}-X^{pN})^{1/p}).$$

We easily see that K' is isomorphic to K by $1+(1/X)\leftrightarrow X$. On the other hand, since the degree of the polynomial $(X+1)^{pN}-X^{pN}$ is not divisible by p, the infinite prime divisor ∞_X is fully ramified in K'. Therefore, we see from Proposition and Lemma 2 that the ideal class group $C_{K',X}$ of the imaginary pure extension K' over $\boldsymbol{F}_\ell(X)$ contains a subgroup isomorphic to the $2(r_p-1)$-fold direct product of the cyclic group of order N. Finally, by taking various integers N, we obtain Theorem 2.

References

[1] M. Ishida: Class numbers of algebraic number fields of Eisenstein type. J. Number Theory, **2**, 404–413 (1970).

[2] ——: The genus field of algebraic number fields. Lecture Notes in Math., vol. 555, Springer, Berlin-Heidelberg-New York (1976).

[3] M. L. Madan: Class numbers and ramification in fields of algebraic functions. Arch. Math., **19**, 121–124 (1968).

[4] ——: On class numbers of algebraic number fields. J. Number Theory, **2**, 116–119 (1970).

[5] T. Nagell: Über die Klassenzahl imaginär quadratischer Zahlkörper. Abh. Math. Sem. Univ. Hamburg, **1**, 140–150 (1922).

[6] S. Nakano: Class numbers of pure cubic fields. Proc. Japan Acad., **59**A, 263–265 (1983).

[7] ——: On the 2-rank of the ideal class groups of pure number fields. Arch. Math., **42**, 53–57 (1984).

[8] P. Roquette and H. Zassenhause: A class rank estimate for algebraic number fields. J. London Math. Soc., **44**, 31–38 (1969).

[9] M. Rosen: S-units and S-class group in algebraic function fields. J. Algebra, **26**, 98–108 (1973).

[10] Y. Yamamoto: On unramified Galois extensions of quadratic number fields. Osaka J. Math., **7**, 57–76 (1970).