Journal of Number Theory **77**, 27–35 (1999)
Article ID jnth.1998.2366, available online at http://www.idealibrary.com on IDEAL®

On the Ideal Class Group Problem for Global Fields

Marc Perret

Unité de Mathématiques Pures et Appliquées, École Normale Supérieure de Lyon, 46 Allée d'Italie, 69 364 Lyon Cedex 7, France
E-mail: perret@umpa.ens-lyon.fr

Communicated by D. Goss

Received May 1, 1998

We prove that any finite abelian group is the ideal class group of the ring of S-integers of some global field of given characteristic. © 1999 Academic Press

Nous prouvons que tout groupe abélien fini est groupe des classes d'idéaux de l'anneau des S-entiers d'un corps global de caractéristique donné. © 1999 Academic Press

I. INTRODUCTION

The following is a classical question in number theory [7, p. 540]:

IDEAL CLASS GROUP PROBLEM. *Given a finite abelian group G, does there exist a number field K having G as ideal class group $\mathcal{C}\ell_K$?*

At this time, the following is known:

THEOREM. *Let G be a finite abelian group. Then,*

(1) (*Cornell*, 1979 [4]) *There exists a number field K_1 such that G is a quotient of $\mathcal{C}\ell_{K_1}$.*

(2) (*Yahagi*, 1978 [16]) *If G is an ℓ-group for some prime number ℓ, then there exists another field K_2 such that G is the ℓ-Sylow subgroup of $\mathcal{C}\ell_{K_2}$.*

Note that a theorem of Claborn states (in [3]) that all (not necessary finite) abelian groups arise as the ideal class group of a Krull domain. The aim of this paper is twofold. First, we prove in Section II a weak form of the problem:

THEOREM 1. *Let G be a finite abelian group. Then there exist a number field K and a finite set S of places containing the archimedian one, such that G is equal to the ideal class group $\mathcal{C}\ell(\mathcal{O}_{K,S})$ of the ring of S-integers $\mathcal{O}_S$ of K.*

0022-314X/99 $30.00

Then, after discussing some possible analogous questions in the global fields of finite characteristic setting, we will prove in Section III that the closest analogous problem has an affirmative answer:

THEOREM 2. *Let $\mathbf{F}_q$ be a finite field and let T be an indeterminate over $\mathbf{F}_q$. Let G be a finite abelian group. Then there exist infinitely many finite separable extensions $K/\mathbf{F}_q(T)$ such that $\mathbf{F}_q$ is the exact constants field of K, the g.c.d. of the degrees of the places of K above $1/T$ is one, and the integral closure $\mathcal{O}_K$ in K of the polynomial ring $\mathbf{F}_q[T]$ has ideal class group $\mathcal{C}\ell(\mathcal{O}_K) \simeq G$.*

For $G = \{1\}$, this says that there are infinitely many finite separable function field extensions $K/\mathbf{F}_q(T)$, such that G_K is principal. This is far from the analogue of Gauss conjecture, which states that there must be infinitely many quadratic separable function field extensions $K/\mathbf{F}_q(T)$, in which $1/T$ splits totally, such that G_K is principal.

The geometric interpretation of the g.c.d. condition will be explained in Section III. Both proofs of Theorems 1 and 2 follows from a common lemma, which will be stated and proved in Section II. Finally, we will make in Section IV some remarks and ask some open problems raised by Theorem 2.

II. CLASS GROUP PROBLEM FOR NUMBER FIELDS: PROOF OF THEOREM 1

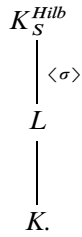
We will use the following lemma, valid for global fields of any characteristic. If S is a set of places (containing the archimedian one if there are) of a global field K (of any characteristic), we denote by K_S^{Hilb} the S-Hilbert class field of K. This is the maximal unramified abelian extension of K, in which all places of S split totally. By class field theory, the ideal class group $\mathcal{C}\ell(\mathcal{O}_{K,S})$ of the ring of S-integers of K is canonically isomorphic, via the Artin map sending an unramified finite place $\mathcal{P}$ of K to the Frobenius element $(\mathcal{P}; K_S^{Hilb}/K)$, to the Galois group $Gal(K_S^{Hilb}/K)$.

REDUCTION LEMMA. *Let K be a global field of any characteristic, S a finite set of places of K (containing the archimedian one if there are), and L be an intermediate field $K \subset L \subset K_S^{Hilb}$. Then, there exists a finite set S' of places of K such that $L = K_{S \cup S'}^{Hilb}$. Moreover, S' can be chosen with cardinality $\sharp S' \leqslant r(Gal(K_S^{Hilb}/L))$.*

In this statement, the rank $r(G)$ of an abelian group G is the number of factors in its canonical decomposition as a product of cyclic groups. This is also its minimal number of generators.

Proof. Suppose first that $Gal(K_S^{Hilb}/L) = \langle \sigma \rangle$ is cyclic. Denote by

$(\cdot; M/K)$ the Artin symbol under some unramified Galois extension M of K. By the Tchebotarev density theorem, there exists a finite place $\mathscr{P}$ of K, such that the corresponding Frobenius element $(\mathscr{P}; K_S^{Hilb}/K) = \sigma \in Gal(K_S^{Hilb}/K)$,



(i) L is an abelian unramified extension of K where the places of S split totally, because K_S^{Hilb} does.

(ii) $\mathscr{P}$ splits totally in L, because

$$(\mathscr{P}; L/K) = (\mathscr{P}; K_S^{Hilb}/K)_{|_L} = \sigma_{|_L}$$

is the identity on L.

(iii) If M is any intermediate field between L and K_S^{Hilb}, distinct to L, then $\mathscr{P}$ doesn't split in M, since

$$(\mathscr{P}; M/K) = \sigma_{|_M}$$

is not the identity on M.

These three points say that L is a maximal unramified abelian extension of K, in which $S \cup \{P\}$ splits totally, so that $L = K_{S\cup\{\mathscr{P}\}}^{Hilb}$. The general case follows from this one by induction on the rank of $Gal(K_S^{Hilb}/L)$, which completes the proof of the reduction lemma.

Proof of Theorem 1. Now, Theorem 1 follows easily from Cornell's theorem stated in the Introduction and the reduction lemma.

III. THE IDEAL CLASS GROUP PROBLEM FOR GLOBAL FUNCTION FIELDS

These are several analogous questions in the global fields of finite characteristic setting. The most naive of them is the divisor class-group of degree zero problem. Unfortunately,

THEOREM (Stichtenoth, 1979 [11]). *Let G be a finite abelian group of exponent n. If $\sharp G \geqslant n^{2(48n/e)^4}$, then* there does not exist *any smooth projective*

irreducible algebraic curve X, defined over any finite field, having G as its divisor class group of degree zero $Div^0(X)/P(X)$.

A simple argument, proving a Stichtenoth-type theorem, will be given in Subsection IV.5. Now, let us consider a second analogous problem:

Let G be a finite abelian group and $\mathbf{F}_q$ be a finite field. Do there exist a smooth projective irreducible algebraic curve X defined over $\mathbf{F}_q$ and a non-empty finite set S of closed points of X (whose degrees are greater than 1), such that $G \simeq \mathscr{C}\ell(\mathscr{O}_{X,S})$?

Recall that in this situation, the ring $\mathscr{O}_{X,S} = \bigcap_{P \notin S} \mathscr{O}_P$ of regular functions outside S is a Dedekind domain, whose ideal class group $\mathscr{C}\ell(\mathscr{O}_{X,S})$ is finite. Please note that by the Tchebotarev density theorem, there always exists a non-empty set S, such that $\mathscr{C}\ell(\mathscr{O}_{X,S}) = Div^0(X)/P(X)$.

Although the answer to this question is "yes" (which will follow from Theorem 2), this is not the best question. Indeed, following [8], this ideal class group $\mathscr{C}\ell(\mathscr{O}_{X,S})$ can be interpreted, by class field theory, as the Galois group of the maximal unramified abelian covering X_S^{Hilb} of X, where the points of S split totally. For instance, if X is the projective line $\mathbf{P}^1_{\mathbf{F}_2}$ over the finite field with 2 elements, and S is the set reduced to the unique point of X of degree 2, then X_S^{Hilb} is the projective line $\mathbf{P}^1_{\mathbf{F}_4}$ over the finite field with 4 elements (where the point of S splits into two points of degree 1). In the general case, there is an exact sequence (described in [8])

$$J_X(\mathbf{F}_q) \to \mathscr{C}\ell(\mathscr{O}_{X,S}) \to \mathbf{Z}/\delta\mathbf{Z} \to 1,$$

where δ is the g.c.d. of the degrees of the points of S. Thus, if $\mathscr{C}\ell(\mathscr{O}_{X,S})_{geom}$ denotes the quotient of $J_X(\mathbf{F}_q)$ by the kernel of the first map, one has an exact sequence

$$1 \to \mathscr{C}\ell(\mathscr{O}_{X,S})_{geom} \to \mathscr{C}\ell(\mathscr{O}_{X,S}) \to \mathbf{Z}/\delta\mathbf{Z} \to 1 \qquad (1)$$

which breaks the group $\mathscr{C}\ell(\mathscr{O}_{X,S})$ into two pieces, namely its geometric part $\mathscr{C}\ell(\mathscr{O}_{X,S})_{geom}$, and its constant field extension part $\mathbf{Z}/\delta\mathbf{Z}$.

This leads us to the final question, which we state as a theorem asserting that any G can be achieved as a fully geometric ideal class group, that is, without cheated constant field extension part.

THEOREM 3.1 (Geometric Form). *Let G be a finite abelian group and $\mathbf{F}_q$ be a finite field. Then there exist infinitely many smooth projective irreducible algebraic curves X defined over $\mathbf{F}_q$ and non-empty finite sets S of closed points of X such that $G \simeq \mathscr{C}\ell(\mathscr{O}_{X,S})_{geom} = \mathscr{C}\ell(\mathscr{O}_{X,S})$.*

Note that this theorem is equivalent to the following one:

THEOREM 3.2 (Arithmetic Form). *Let $\mathbf{F}_q$ be a finite field and let T be an indeterminate over $\mathbf{F}_q$. Let G be a finite abelian group. Then there exist infinitely many finite separable extensions $K/\mathbf{F}_q(T)$ such that $\mathbf{F}_q$ is the exact constants field of K, the g.c.d. of the degrees of the places of K above $1/T$ is one, and the integral closure O_K in K of the polynomial ring $\mathbf{F}_q[T]$ has ideal class group $\mathscr{C}\ell(\mathcal{O}_K) \simeq G$.*

The proof of the theorem relies on the fact, proved by Angles in [1], that Cornell's theorem also holds in this setting. He gave two proofs, which we omit here, the first one working as Cornell's original one, and the second working as Washington's one given in [13]. Both make an intensive use of the cyclotomic fields $\mathbf{Q}(\zeta_n)$: the given group G appears as a quotient of the Galois group of the Hilbert class field of a cyclotomic field. These proofs work in the function field case, if one uses Hayes cyclotomic function fields $\mathbf{F}_q(T)(\Lambda_M)$ (for $M \in \mathbf{F}_q[T]$, introduced in [5]) instead of classical ones. Let us state under the geometric setting the Angles theorem, originally stated under the arithmetic one. Note that in its proof, all places of S have degree one, so that the geometric condition is fulfilled.

THEOREM (Angles, 1997 [1]). *Let G be a finite abelian group and $\mathbf{F}_q$ be a finite field. Then there exist infinitely many smooth projective irreducible algebraic curves X defined over $\mathbf{F}_q$, finite non-empty sets S of closed points of degree* 1 *of X, and geometric unramified coverings Y of X where S splits totally, having G as a Galois group. This means that G appears as a* quotient *of $\mathscr{C}\ell(\mathcal{O}_{X,S})$ as the Galois group of a* geometric *covering of X.*

Proof of Theorems 3.1 *and* 3.2. Of course, the Angles theorem, together with the reduction lemma, implies Theorem 3.1. Now, both forms of Theorem 3 are equivalent. First, let $K/\mathbf{F}_q(T)$ be a field extension as in the arithmetic form statement. Then K appears as the rational function field of an (unique) algebraic projective irreducible curve X defined over $\mathbf{F}_q$, in such a way that $\mathcal{O} = \mathcal{O}_{X,S}$ for the set S of primes lying over $1/T$. Conversely, let (X, S) be a pair as in the geometric form theorem. If g denotes the genus of X, and $S = \{P_1, ..., P_k\}$ where P_i is a closed point of degree d_i, let n be a positive integer, such that $(n-1)(\sum_{i=1}^{k} d_i) \geqslant 2g-1$. If $H = L(nP_1 + \cdots + nP_k)$ and $H_i = L(nP_1 + \cdots + nP_{i-1} + (n-1)P_i + \cdots + nP_k)$, then the Riemann–Roch theorem gives $\dim H = n(\sum_{i=1}^{k} d_i) + 1 - g$, and $\dim H_i = n(\sum_{i=1}^{k} d_i) - nd_i + 1 - g = \dim H - nd_i$, hence the codimension of H_i is H and is proportional to n. It implies that H is not the union of its subspaces H_i for sufficiently large n. Let $f \in H$, $f \notin \bigcup_{i=1}^{k} H_i$. This is a rational function on X having exactly S as support of the divisor of poles. This yields a covering $f: X \to \mathbf{P}^1_{\mathbf{F}_q}$, where the ramification indexes of the

points $P_1, ..., P_k$ above ∞ all equal n. If n is chosen prime to p, this corresponds to a *separable* field extension of the rational functions fields $\mathbf{F}_q(\mathbf{P}^1) = \mathbf{F}_q(T) \subset K = \mathbf{F}_q(X)$, under which the integral closure of $\mathbf{F}_q[T]$ is nothing else than $\mathcal{O}_{X,S}$. Finally, both conditions $\mathcal{C}\ell(\mathcal{O}_{X,S})_{geom} = \mathcal{C}\ell(\mathcal{O}_{X,S})$ and $\delta = 1$ are equivalent from the exact sequence (1).

Note that a Yahagi theorem in this setting follows easily in the same way from the Angles theorem and the reduction lemma. This was also proved by Angles in [1], but the proof, using a previous work [2] of the author, is more complicated.

IV. SOME REMARKS AND QUESTIONS

If X is an algebraic smooth projective irreducible curve defined over $\mathbf{F}_q$ whose Jacobian is denoted by J_X, let $\mathcal{C}\ell_{X,S} = \mathcal{C}\ell(\mathcal{O}_{X,S})$ and $\mathcal{C}\ell_{X,S,geom} = \mathcal{C}\ell(\mathcal{O}_{X,S})_{geom}$ if $S \neq \varnothing$, and $\mathcal{C}\ell_{X,\varnothing} = \mathcal{C}\ell_{X,\varnothing,geom} = Div^0(X)/P(X) = J_X(\mathbf{F}_q)$.

If G is a finite abelian group, it can be interesting to investigate the minimal genus of a curve, and the minimal cardinality of a set S, such that $G \simeq \mathcal{C}\ell_{X,S} = \mathcal{C}\ell_{X,S,geom}$. In this order, let us define

$$g_q(G) = \mathrm{Inf}\{\, g(X) \mid X \text{ genus } g \text{ curve over } \mathbf{F}_q;\ \exists S;\ G \simeq \mathcal{C}\ell_{X,S} = \mathcal{C}\ell_{X,S,geom}\}$$

and

$$s_q(G) = \mathrm{Inf}\{\sharp S \mid \exists X \text{ curve of genus } g_q(G) \text{ over } \mathbf{F}_q;\ \exists S;\ G \simeq \mathcal{C}\ell_{X,S} = \mathcal{C}\ell_{X,S,geom}\}.$$

1. Note that the theorem says that $g_q(G)$ and $s_q(G)$ are defined. Moreover, one has always $g_q(G) \geqslant 1$ (provided $G \neq \{1\}$) since the projective line has no geometric unramified covering. Papers [9, 10, 12] are devoted to the determination of group G, for which $s_q(G) = 0$ and $g_q(G) = 1$.

2. It follows from the reduction lemma that if H is a subgroup of G, then

$$\begin{cases} g_q(H) \leqslant g_q(G), \\ s_q(H) \leqslant s_q(G) + r(G/H). \end{cases}$$

3. If p denotes the characteristic of $\mathbf{F}_q$, let G_p be the p-Sylow subgroup of G. Then

$$g_q(G) \geqslant g_q(G)_{exp.} = \mathrm{Max}\left(r(G_p), \frac{r(G/G_p)}{2}\right).$$

How far from this expected value $g_q(G)_{exp.}$ can the number $g_q(G)$ be? For instance, is it true that given an odd prime number p and an integer r, then $g_p((\mathbf{Z}/2\mathbf{Z})^r) = r/2$ if r is even, and $(r+1)/2$ if r is odd? On the other side, given a prime number p, is it true that $g_p((\mathbf{Z}/p\mathbf{Z})^2) = 2$? Note that a theorem of Waterhouse in [14] implies that $g_p(\mathbf{Z}/p\mathbf{Z}) = 1$.

4. The Weil inequality implies $s_q(G) \geqslant 1$, provided that $\sharp G \leqslant (\sqrt{q}-1)^2$ (for instance, $s_q(\mathbf{Z}/4\mathbf{Z}) = 0$ only if $q \leqslant 9$). Lachaud and Martin-Deschamps established in [6] a better lower bound for the number of rational points of the Jacobian of a curve. It implies that $s_q(G) \geqslant 1$ whether

$$\sharp G \leqslant \frac{q^{g_q(G)-1}(q-1)^2}{(q+1)(g_q(G)+1)}.$$

5. A simple argument proves the following claim, easier than Stichtenoth's theorem stated above:

CLAIM. *Let $\mathbf{F}_q$ be a finite field and ℓ be a prime number, prime to q. Suppose that $\ell < \sqrt{q}-1$. Then an elementary abelian ℓ-group G (of any rank) cannot be isomorphic to the divisor class group of degree zero $Div^0(X)/P(X)$ of any smooth projective irreducible algebraic curve X, defined over $\mathbf{F}_q$.*

For instance, an elementary abelian 2-group can be the divisor class group of degree zero only on the finite fields with less than 9 elements. What Stichtenoth's theorem says is that it is possible only perhaps for elementary 2-groups of rank $\leqslant 3$, 111, 265.

Indeed, suppose that such a curve does exist. Then G would be isomorphic to the group $J_X(\mathbf{F}_q)$ of $\mathbf{F}_q$-rational points of the jacobian J_X of X. But one knows, from the Weil theorem (see [15]), that this group has order $\prod_{i=1}^{2g}(1-\alpha_i)$, where g is the genus of X, and the α_i are the inverse roots of the characteristic polynomial of the Frobenius endomorphism acting on the Tate module $T_\ell(J_X)$. These numbers having modulus $\sqrt{q}$, one deduces the *Weil inequality*:

$$(\sqrt{q}-1)^{2g} \leqslant \sharp G.$$

Now, $G = (\mathbf{Z}/\ell\mathbf{Z})^r = J_X(\mathbf{F}_q)$ is equal to its own ℓ-Sylow, which is a subgroup of the ℓ-Sylow of $J_X(\bar{\mathbf{F}}_q) = (\mathbf{Z}/\ell\mathbf{Z})^{2g}$, so that $r \leqslant 2g$. Thus, the Weil inequality implies $(\sqrt{q}-1)^{2g} \leqslant \sharp G = \ell^r \leqslant \ell^{2g}$. Hence $\sqrt{q}-1 \leqslant \ell$, which is a contradiction.

6. Is it true that $s_q(G) = 0$ or 1 for any G, q?

7. Of course, one can compute the genus of the curves constructed by Angles. But these are very large in regard to the real values of $g_q(G)$.

For instance, if $G = \mathbf{Z}/2\mathbf{Z}$ and q is odd, one finds a curve of genus $\frac{5}{2}(q-1)^2$, whereas the real value of $g_q(\mathbf{Z}/2\mathbf{Z})$ is 1, as indicated in the following table.

8. Here is a table for small groups G.

G	$g_q(G)$	$s_q(G)$
$\mathbf{Z}/2\mathbf{Z}$	1	$\begin{cases} 1 & \text{if } q \geqslant 7 \\ 0 & \text{if } q \leqslant 5 \end{cases}$
$\mathbf{Z}/3\mathbf{Z}$	1	$\begin{cases} 1 & \text{if } q \geqslant 8 \\ 0 & \text{if } q \leqslant 7 \end{cases}$
$\mathbf{Z}/4\mathbf{Z}$	1	$\begin{cases} 1 & \text{if } q \geqslant 9 \\ 0 & \text{if } q \leqslant 8 \end{cases}$
$(\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$	$\begin{cases} 1 & \text{if } q \text{ odd} \\ \geqslant 2 & \text{if } 2 \mid q \end{cases}$	$\begin{cases} 1 & \text{if } q \geqslant 11, q \text{ odd}, \\ 0 & \text{if } q \leqslant 9, q \text{ odd}, \\ ?? & \text{if } q \text{ even} \end{cases}$
$\mathbf{Z}/5\mathbf{Z}$	1	$\begin{cases} 1 & \text{if } q \geqslant 11 \\ 0 & \text{if } q \leqslant 9 \end{cases}$

The proof uses parts of the Waterhouse [14], Schoof [10], and Ruck and Voloch ([9, 12] for non-cyclic G's) theorems, and the reduction lemma.

Proof in Case $G = \mathbf{Z}/4\mathbf{Z}$. Recall that from Remark 4, one has $s_q(\mathbf{Z}/4\mathbf{Z}) \geqslant 1$ whenever $q \geqslant 11$. Suppose first that q is even, greater than 4. Then by the Waterhouse theorem—which states that given a rational integer $-2\sqrt{q} \leqslant t \leqslant 2\sqrt{q}$, prime to q, there exists an elliptic curve E defined over $\mathbf{F}_q$, having exactly $q+1-t$ rational points—applied with $t=1$, one gets E with q rational points. Now, by the Voloch Lemma (stated as "Lemma 1" in [12])—asserting that if there exists an elliptic curve E having N rational points and if $N \not\equiv 1 \bmod q$, then there exists another elliptic curve E', such that $E'(\mathbf{F}_q) = \mathbf{Z}/N\mathbf{Z}$—there is an E' (defined over $\mathbf{F}_q$) such that $E'(\mathbf{F}_q) = \mathbf{Z}/q\mathbf{Z}$. This proves the assertion by the reduction lemma. For $q=2$, the same argument with $t=-1$ gives E' such that $E'(\mathbf{F}_2) = \mathbf{Z}/4\mathbf{Z}$.

Suppose now $q \equiv 1 \bmod 4$. The same argument for $t=2$ gives E' over $\mathbf{F}_q$ having $E'(\mathbf{F}_q) = \mathbf{Z}/(q-1)\,\mathbf{Z}$, which proves the assertion using the reduction lemma if $q \neq 9$, for which it remains to prove that $s_9(\mathbf{Z}/4\mathbf{Z}) \neq 0$. If it were false, then there should exist an elliptic curve E over $\mathbf{F}_9$ having $4 = 9+1-6$ rational points, that is, with $t=6$. But this is impossible by the Schoof theorem—which lists all possibilities for the number of rational points of an elliptic curve over $\mathbf{F}_q$.

Finally, suppose $q \equiv 3 \bmod 4$. The above argument with $t = 4$ gives the result for $q \neq 3$. For $q = 3$, then $t = 0$ works by the Schoof theorem.

9. Of course, one can also study analogous numbers $g'_q(G)$ and $s'_q(G)$ without any geometric restriction.

ACKNOWLEDGMENTS

The author thanks Bruno Angles and Yves Aubry for helpful discussions.

Note added in proof. It has been proved recently by G. Lachaud and S. Vladut that for $q = 4, 9, 25, 49$ or 169, there are infinitely many Galois extensions $K/\mathbf{F}_q(T)$ in which $1/T$ splits totally, such that G_K is principal. See their preprint, "Gauss Problem for Function Fields."

REFERENCES

1. B. Angles, On the class group problem for function fields, *J. Number Theory* **10** (1998), 146–159.
2. B. Angles, Some results on Hilbert class field towers of global function fields, *in* "Drinfeld Modules, Modular Schemes and Applications, Alden Biesen, September 1996" (E. U. Gekeler, M. Van der Put, M. Reversat, and J. Van Geel, Eds.), pp. 261–271, World Scientific, Singapore, 1996.
3. L. Claborn, Every abelian group is a class group, *Pacific J. Math.* **18**, No. 2 (1966), 219–222.
4. G. Cornell, Abhyankar's Lemma and the class group, *in* "Lecture Notes in Math.," Vol. 751, pp. 82–88, Springer-Verlag, New York/Berlin, 1979.
5. D. R. Hayes, Explicit class field theory for rational function fields, *Trans. Amer. Math. Soc.* **189** (1974), 77–91.
6. G. Lachaud and M. Martin-Deschamps, Nombre de points des jacobiennes sur un corps fini, *Acta Arith.* **56** (1990), 329–340.
7. W. Narkiewicz, "Elementary and Analytic Theory of Algebraic Numbers," 2nd ed., Springer-Verlag, New York/Berlin, 1990.
8. M. Rosen, The Hilbert class field in function fields, *Exposition Math.* **5** (1987), 365–378.
9. H. G. Ruck, A note on elliptic curves over finite fields, *Math. Comp.* **49**, No. 179 (1987), 301–304.
10. R. Schoof, Nonsingular plane cubic curves over finite fields, *J. Combin. Theory Ser. A* **46** (1987), 183–211.
11. H. Stichtenoth, Zur Divisorklassengruppe eines Kongruenzfunktionenkorpers, *Arch. Math.* **32** (1979), 336–340.
12. J. F. Voloch, A note on elliptic curves over finite fields, *Bull. Soc. Math. France* **116** (1988), 455–458.
13. L. C. Washington, "Introduction to Cyclotomic Fields," Grad. Texts in Math., Vol. 83, Springer-Verlag, New York/Berlin, 1982.
14. W. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup. (4)* **2** (1969), 521–560.
15. A. Weil, "Courbes algébriques et variétés abéliennes," Hermann, Paris, 1948.
16. O. Yahagi, Construction of number fields with prescribed ℓ-class groups, *Tokyo J. Math.* **1**, No. 2 (1978), 275–283.