PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 64, Number 1, May 1977

ON HILBERT CLASS FIELDS IN CHARACTERISTIC $p > 0$ AND THEIR L-FUNCTIONS

STUART TURNER

ABSTRACT. Let k be a global field of characteristic $p > 0$ with field of constants $\mathbf{F}_q$. Let $\bar{k}$ be an algebraic closure of k. In this note we study the subfields of $\bar{k}$ which are maximal unramified abelian extensions of k with field of constants $\mathbf{F}_q$. Each of these fields may be regarded as an analogue of the Hilbert class field of algebraic number theory [1, p. 79]. In §1 we recall the construction of these class fields and in §2 we show that if k has genus one, they are all $\mathbf{F}_q$-isomorphic. In §3 we show that this is not necessarily the case if the genus of k is greater than one. The argument there is based on an observation about the L-functions of the fields.

1. Let k_A^x be the idele group of k and identify k^x with the principal ideles in k_A^x. Let k_A^1 be the ideles of module 1 and U be the maximal compact subgroup of k_A^x. Let D be a complete nonsingular curve defined over $\mathbf{F}_q$ with function field isomorphic to k. D is unique up to $\mathbf{F}_q$ isomorphism. Let $J(D)(\mathbf{F}_q)$ denote the group of $\mathbf{F}_q$-rational points on $J(D)$, the Jacobian variety of D. $J(D)(\mathbf{F}_q)$ is a finite group. Let $h = \operatorname{card}(J(D)(\mathbf{F}_q))$. k_A^1/k^xU is canonically isomorphic to $J(D)(\mathbf{F}_q)$.

We now recall straightforward (and well-known) consequences of the existence theorem [1, Chapter VIII, in particular §3], [3, Chapter XIII, §9].

Let $z \in k_A^x$ with module $(z) = q$. Let $u_1, \ldots, u_h$ be representatives of the cosets of k^xU in k_A^1, $u_1 \in k^xU$. Then $N_i = \{zu_i\} \times k^xU$ are distinct open subgroups of k_A^x and each k_A^x/N_i is canonically isomorphic to k_A^1/k^xU. The class fields $k_1, k_2, \ldots, k_h$ of $N_1, N_2, \ldots, N_h$, respectively, are unramified abelian extensions of k each with constant field $\mathbf{F}_q$ and each $\operatorname{Gal}(k_i/k)$ is canonically isomorphic to $J(D)(\mathbf{F}_q)$.

Furthermore, these k_i are the only maximal unramified abelian extensions of k with constant field $\mathbf{F}_q$ because any $x \in k_A^x$ with module $(x) = q$ lies in one of the cosets zu_ik^xU of k^xU in k_A^x.

Let L be the constant field extension of k of degree h. L is the class field of the subgroup $\{z^h\} \times k_A^1$ so Lk_i is the class field of

$$\{z^h\} \times k_A^1 \cap \{zu_i\} \times k^xU = \left\{(zu_i)^h\right\} \times k^xU, \qquad i = 1, \ldots, h.$$

But $(zu_i)^h$ and $(zu_j)^h$ represent the same coset of k_A^1 in k_A^x, so $Lk_i = Lk_j$, $1 \leqslant i,j \leqslant h$.

Let C_i be a complete nonsingular curve defined over $\mathbf{F}_q$ with function field

Received by the editors March 8, 1976.

AMS (MOS) subject classifications (1970). Primary 12A65, 14G10, 14H30; Secondary 12A90, 14H40.

isomorphic to k_i. The C_i are unique up to $\mathbf{F}_q$-isomorphism. Since k_i is an unramified extension of k, there exist surjective étale morphisms γ_i: $C_i \to D$ defined over $\mathbf{F}_q$. Let g be the genus of D; then, $g(C_i)$, the genus of C_i, is given by $2g(C_i) - 2 = h(2g - 2)$ [3, Chapter VIII, Corollary to Proposition 14]. Summarizing the discussion in geometric terms we have

THEOREM 1. *Let D be a complete nonsingular curve of genus g defined over $\mathbf{F}_q$. Let $J(D)$ be the Jacobian variety of D and $G = J(D)(\mathbf{F}_q)$ be the group of $\mathbf{F}_q$-rational points of $J(D)$. Let $h =$ card G. Then there exist h complete nonsingular curves C_i defined over $\mathbf{F}_q$ each of genus $h(g - 1) + 1$, and morphisms γ_i: $C_i \to D$ defined over $\mathbf{F}_q$ such that γ_i is an étale cover of degree h. The Galois group of the cover γ_i is isomorphic to G.*

Observe that for $i \neq j$ there does not exist any morphism δ: $C_i \to C_j$ such that $\gamma_j \circ \delta = \gamma_i$; for the existence of such a morphism would imply the existence of a k-isomorphism of k_j onto a subfield of k_i, but this is impossible because k_j and k_i are distinct normal extensions of k in $\bar{k}$.

However, if D has genus one, C_i is $\mathbf{F}_q$-isomorphic to C_j for all i, j, $1 \leqslant i, j \leqslant h$. This is proven in §2.

2.

LEMMA 1. *Let v be a place of k of degree one. Then v splits completely in precisely one of the class fields k_i, $1 \leqslant i \leqslant h$.*

PROOF. The places of k_i which lie above v are in one-to-one correspondence with the cosets of $k_v^\times N_i$ in $k_A^\times$ [3, Chapter XIII, Proposition 14], so v splits completely in k_i if and only if $[k_A^\times\colon k_v^\times N_i] = h$. On the other hand, $[k_A^\times\colon N_i] = h$, so v splits completely in k_i if and only if $k_v^\times \subset N_i = \{zu_i\} \times k^\times U$. Let r_v be the valuation ring in k_v. $r_v^\times \subset N_i$ for all i, $1 \leqslant i \leqslant h$. Let π_v be a prime element in r_v. Since v is a place of degree one, module $(\pi_v^{-1}) = q$. So $\pi_v \in N_i$ if and only if $\pi_v z^{-1} \in u_i k^\times U$; there is a unique i for which this is the case.

REMARK. The hypothesis of Lemma 1 is not always satisfied. There exist global fields which do not have places of degree one.

LEMMA 2. *If k has genus one and k_i is the class field determined by N_i, then there is a unique place v of k of degree one that splits completely in k_i.*

PROOF. k_i has genus one, hence has a place w of degree one. w has residue field $\mathbf{F}_q$ and lies over a place v of k of degree one. w has h distinct conjugates $w = w_1, \ldots, w_h$ over v because $\Sigma e(w_i)f(w_i) = h$, $e(w_i) = 1$ for $i = 1, \ldots, h$, and $f(w) = 1$.

THEOREM 2. *Let notations be as in Theorem 1 and assume that D is a curve of genus one. Then there is a canonical one-to-one correspondence between the rational points of D and the curves C_i. A rational point P of D corresponds to the curve C_i if and only if there are h points of C_i in the fiber $\gamma_i^{-1}(P)$.*

PROOF. D is $\mathbf{F}_q$-isomorphic to $J(D)$, so D has h rational points. The theorem now follows from Lemmas 1 and 2.

Throughout the rest of this section we assume that k has genus one.

Let v be a place of k and ρ: $k \to k_v$ be an embedding of k into the completion of k at v. Let k' be a field and α: $k' \to k$ be an isomorphism. Denote by αv the place of k' arising from the embedding $\rho \circ \alpha$: $k' \to k_v$. Denote by $v(i)$ the place of k which corresponds to the class field k_i.

LEMMA 3. *Let β: $k_j \to k_i$ be an $\mathbf{F}_q$-isomorphism such that $\beta(k) \subset k$ and let $\alpha = \beta|_k$. Then $v(j) = \alpha v(i)$. Conversely, if α: $k \to k$ is an $\mathbf{F}_q$-isomorphism such that $v(j) = \alpha v(i)$, then there is an $\mathbf{F}_q$-isomorphism β: $k_j \to k_i$ such that $\beta|_k = \alpha$.*

PROOF. Let w be a place of k_i of degree one. βw is a place of k_j of degree one. By Lemma 2, w lies over $v(i)$ and βw lies over $v(j)$ so $v(j) = \alpha v(i)$.

To prove the converse observe that there are h distinct embeddings β_i: $k_j \to \bar{k}$, $1 \leqslant i \leqslant h$, such that $\beta_i|_k = \alpha$.

The β_i all have the same image L in $\bar{k}$. L is an unramified abelian extension of k with field of constants $\mathbf{F}_q$. It suffices to show that $L = k_i$. Let w be a place of k_j of degree one and u be the place of $\beta_1(k_j)$ such that $w = \beta_1 u$. By Lemma 2, w lies over $v(j)$ and u lies over $v(i)$ because $v(j) = \alpha v(i)$. So u is a place of k_i and $L = k_i$.

Let $k(D)$, $k(C_i)$ and $k(C_j)$ be the function fields of D, C_i and C_j, respectively. The morphisms γ_i and γ_j of Theorem 1 define injections γ_i^*: $k(D) \to k(C_i)$ and γ_j^*: $k(D) \to k(C_j)$. Choose $\mathbf{F}_q$-isomorphisms of $k(D)$ with k, of $k(C_i)$ with k_i, and of $k(C_j)$ with k_j; so that γ_i^* (resp. γ^*) is compatible with the inclusion $k \subset k_i$ (resp. $k \subset k_j$). Identify $k(D)$ with k, $k(C_i)$ with k_i, and $k(C_j)$ with k_j by means of these isomorphisms. The places $v(i)$, $1 \leqslant i \leqslant h$, of k are thus identified with places of $k(D)$. Let P_i, $1 \leqslant i \leqslant h$, be the rational points of D corresponding to the places $v(i)$, $1 \leqslant i \leqslant h$, of $k(D)$, respectively.

THEOREM 3. *Let the notations be as in Theorem 1 and assume that D is a curve of genus one. Let η be an $\mathbf{F}_q$-automorphism of D. Then there exists an $\mathbf{F}_q$-isomorphism δ: $C_i \to C_j$ such that $\gamma_j \circ \delta = \eta \circ \gamma_i$ if and only if $\eta(P_i) = P_j$.*

PROOF. Let η^*: $k(D) \to k(D)$ be the automorphism of $k(D)$ induced by η. $\eta(P_i) = P_j$ is equivalent to the condition $v(j) = \eta^* v(i)$. By Lemma 3 there is an $\mathbf{F}_q$-isomorphism β: $k(C_j) \to k(C_i)$ such that $\beta|_{k(D)} = \eta^*$. β determines an $\mathbf{F}_q$-isomorphism δ: $C_i \to C_j$ such that $\gamma_j \circ \delta = \eta \circ \gamma_i$. The proof of the converse follows similarly from the first assertion of Lemma 3.

COROLLARY. *Let the notations be as in Theorem 1 and assume that D has genus one. Then there exist $\mathbf{F}_q$-isomorphisms δ: $C_i \to C_j$ for all i,j, $1 \leqslant i,j \leqslant h$.*

PROOF. Since D has genus one, the group of $\mathbf{F}_q$-isomorphisms of D acts transitively on the $\mathbf{F}_q$-rational points of D. The assertion now follows from the theorem.

3. Returning to the discussion in §1, recall that the fields $k_i \subset \bar{k}$ were defined as the class fields of subgroups N_i of $k_A^\times$. Let Ω_i be the group of characters of $k_A^\times$ trivial on N_i and Ω_i' be the elements of Ω_i distinct from the trivial character. Then the Dedekind zeta function of k_i is given by $\zeta_{k_i}(s) = \zeta_k(s) \cdot \prod_{\omega \in \Omega_i'} L(s,\omega)$ [3, Chapter XIII, §10].

In case k has genus one, the $L(s,\omega)$ are all identically one [3, Chapter VII, §7], but if the genus of k is greater than one, these L-functions are nontrivial. Throughout this section we assume that the genus of k is at least two.

For $s \in \mathbf{C}$, let ω_s: $k_A^\times \to \mathbf{C}^\times$ be the quasicharacter defined by $\omega_s(z) = |z|^s$; ω_s: $k_A^1 \to 1$.

LEMMA 4. *Let $\omega \in \Omega_1$, $\omega \neq 1$, and let $\omega(zu_i) = q^{-s_i(\omega)}$. There is a one-to-one correspondence between Ω_1 and Ω_i given by $\omega \leftrightarrow \omega\omega_{s_i(\omega)}$.*

PROOF. ω has order h so $q^{-s_i(\omega)}$ is an hth root of one and $s_i(\omega)$ is defined modulo elements of $(2\pi i/\log q)\mathbf{Z}$. ω and ω_s induce the trivial character on $k^\times U$, so $\omega\omega_s \in \Omega_i$ if and only if $\omega\omega_s(zu_i) = 1$.

This is equivalent to $s \equiv s_i(\omega)\ (\mathrm{mod}(2\pi i/\log q)\mathbf{Z})$. The verification that the correspondence between Ω_1 and Ω_i is one-to-one is left to the reader.

Lemma 4 and the definition of the L-functions give

PROPOSITION.

$$\zeta_{k_i}(s) = \zeta_k(s) \prod_{\omega \in \Omega_1'} L(\omega\omega_{s_i(\omega)}, s) = \zeta_k(s) \prod_{\omega \in \Omega_1'} L(\omega, s + s_i(\omega)).$$

$\zeta_{k_i} = \zeta_{k_j}$, for $1 \leqslant i,j \leqslant h$, if and only if $J(C_i)$ is $\mathbf{F}_q$-isogenous to $J(C_j)$ [2, Theorem 1].

COROLLARY. *Let the notations be as in Theorem 1 and assume that D has genus at least two and that $h = 2$. Then $J(C_1)$ is not $\mathbf{F}_q$-isogenous to $J(C_2)$ and, hence, C_1 is not $\mathbf{F}_q$-isomorphic to C_2.*

PROOF. Let $\omega \in \Omega_1'$; then $\zeta_{k_1}(s) = \zeta_{k_2}(s)$ if and only if

$$L(\omega,s) = L(\omega, s + s_2(\omega)),$$

where $q^{-s_2(\omega)} = -1$ because $\omega\omega_{s_2(\omega)} \in \Omega_2'$. So

$$s_2(\omega) \equiv \pi i/\log q(\mathrm{mod}(2\pi i/\log q)\mathbf{Z}).$$

On the other hand $L(\omega,s)$ has period $2\pi i/\log q$, so

$$L(\omega,s) \neq L(\omega, s + s_2(\omega)).$$

REFERENCES

1. E. Artin and J. Tate, *Class field theory*, Benjamin, New York, 1968. MR **36** #6383.

2. J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR **34** #5829.

3. A. Weil, *Basic number theory*, Grundlehren math. Wiss. Band 144, Springer-Verlag, New York, 1967. MR **38** #3244.

DEPARTAMENTO DE MATEMÁTICA, PONTIFICIA UNIVERSIDADE CATÓLICA DO RIO DE JANEIRO, RUA MARQUÊS DE SÃO VICENTE 209/263, RIO DE JANEIRO, BRAZIL