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 $\mathbb{F}_q$. 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 $\mathbb{F}_q$. 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 $\mathbb{F}_q$-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 $k_1^*$ be the idele group of $k$ and identify $k^*$ with the principal ideles in $k_1^*$. Let $k_1^+$ be the ideles of module 1 and $U$ be the maximal compact subgroup of $k_1^+$. Let $D$ be a complete nonsingular curve defined over $\mathbb{F}_q$ with function field isomorphic to $k$. $D$ is unique up to $\mathbb{F}_q$ isomorphism. Let $J(D)(\mathbb{F}_q)$ denote the group of $\mathbb{F}_q$-rational points on $J(D)$, the Jacobian variety of $D$. $J(D)(\mathbb{F}_q)$ is a finite group. Let $h = \text{card}(J(D)(\mathbb{F}_q))$. $k_1^+/k^*$ is canonically isomorphic to $J(D)(\mathbb{F}_q)$.

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

Let $z \in k_1^*$ with module $(z) = q$. Let $u_1, \ldots, u_h$ be representatives of the cosets of $k^*U$ in $k_1^+$. Then $N_i = \{zu_i\} \times k^*U$ are distinct open subgroups of $k_1^*$ and each $k_1^*/N_i$ is canonically isomorphic to $k_1^+/k^*U$. 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 $\mathbb{F}_q$ and each $\text{Gal}(k_i/k)$ is canonically isomorphic to $J(D)(\mathbb{F}_q)$.

Furthermore, these $k_i$ are the only maximal unramified abelian extensions of $k$ with constant field $\mathbb{F}_q$, because any $x \in k_1^*$ with module $(x) = q$ lies in one of the cosets $zu^k, U$. Let $L$ be the constant field extension of $k$ of degree $h$. $L$ is the class field of the subgroup $\{z^h\} \times k_1^+$ so $Lk_i$ is the class field of $\{z^h\} \times k_1^+ \cap \{zu_i\} \times k^*U = \{(zu_i)^h\} \times k^*U$, $i = 1, \ldots, h$.

But $(zu_i)^h$ and $(zu_j)^h$ represent the same coset of $k_1^+$ in $k_1^*$, so $Lk_i = Lk_j$, $1 \leq i, j \leq h$.

Let $C_i$ be a complete nonsingular curve defined over $\mathbb{F}_q$ with function field...
isomorphic to $k_i$. The $C_i$ are unique up to $F_q$-isomorphism. Since $k_i$ is an unramified extension of $k$, there exist surjective étale morphisms $\gamma_i: C_i \to D$ defined over $F_q$. 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 $F_q$. Let $J(D)$ be the Jacobian variety of $D$ and $G = J(D)(F_q)$ be the group of $F_q$-rational points of $J(D)$. Let $h = \text{card } G$. Then there exist $h$ complete nonsingular curves $C_i$ defined over $F_q$ each of genus $h(g - 1) + 1$, and morphisms $\gamma_i: C_i \to D$ defined over $F_q$ such that $\gamma_i$ is an étale cover of degree $h$. The Galois group of the cover $\gamma_i$ is isomorphic to $G$.

Observe that for $i \neq j$ there does not exist any morphism $\delta: C_i \to C_j$ 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 $k$.

However, if $D$ has genus one, $C_i$ is $F_q$-isomorphic to $C_j$ for all $i, j, 1 \leq i, j \leq h$. 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 $k_i$, $1 \leq i < h$.

**Proof.** The places of $k_j$ which lie above $v$ are in one-to-one correspondence with the cosets of $k_v^*N_j$ in $k_v^*$ [3, Chapter XIII, Proposition 14], so $v$ splits completely in $k_j$ if and only if $[k_v^*: k_v^*N_j] = h$. On the other hand, $[k_v^*: N_j] = h$, so $v$ splits completely in $k_j$ if and only if $k_v^* \subset N_j = \{z_i\} \times k^*U$. Let $r_v$ be the valuation ring in $k_v$. $r_v^* \subset N_i$ for all $i, 1 \leq i < h$. Let $\pi_v$ 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 $\pi_vz^{-1} \in u_kk^*U$; 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 $F_{q_i}$ 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 $\sum e(w_i)f(w_i) = h, e(w_i) = 1$ 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 $\gamma_i^{-1}(P)$.
HILBERT CLASS FIELDS

Proof. $D$ is $\mathbb{F}_q$-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 $\rho: k \rightarrow k_v$ be an embedding of $k$ into the completion of $k$ at $v$. Let $k'$ be a field and $\alpha: k' \rightarrow k$ be an isomorphism. Denote by $\alpha v$ the place of $k'$ arising from the embedding $\rho \circ \alpha: k' \rightarrow k_v$. Denote by $v(i)$ the place of $k$ which corresponds to the class field $k_i$.

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

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

To prove the converse observe that there are $h$ distinct embeddings $\beta_i: k_j \rightarrow k$, $1 \leq i \leq h$, such that $\beta_i|_k = \alpha$.

The $\beta_i$ all have the same image $L$ in $k$. $L$ is an unramified abelian extension of $k$ with field of constants $\mathbb{F}_q$. 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 $\beta_i(k_j)$ such that $w = \beta_i u$. 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 $\gamma_i$ and $\gamma_j$ of Theorem 1 define injections $\gamma_i^*: k(D) \rightarrow k(C_i)$ and $\gamma_j^*: k(D) \rightarrow k(C_j)$. Choose $\mathbb{F}_q$-isomorphisms of $k(D)$ with $k$, of $k(C_i)$ with $k_i$, and of $k(C_j)$ with $k_j$; so that $\gamma_i^*$ (resp. $\gamma_j^*$) 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 $v(i)$, $1 \leq i \leq h$, of $k$ are thus identified with places of $k(D)$. Let $P_i$, $1 \leq i \leq h$, be the rational points of $D$ corresponding to the places $v(i)$, $1 \leq i \leq h$, 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 $\eta$ be an $\mathbb{F}_q$-automorphism of $D$. Then there exists an $\mathbb{F}_q$-isomorphism $\delta: C_i \rightarrow C_j$ such that $\gamma_j \circ \delta = \eta \circ \gamma_i$ if and only if $\eta(P_i) = P_j$.

Proof. Let $\eta^*: k(D) \rightarrow k(D)$ be the automorphism of $k(D)$ induced by $\eta$. $\eta(P_i) = P_j$ is equivalent to the condition $\nu(j) = \eta^* \nu(i)$. By Lemma 3 there is an $\mathbb{F}_q$-isomorphism $\beta: k(C_i) \rightarrow k(C_j)$ such that $\beta|_{k(D)} = \eta^*$. $\beta$ determines an $\mathbb{F}_q$-isomorphism $\delta: C_i \rightarrow C_j$ 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 $\mathbb{F}_q$-isomorphisms $\delta: C_i \rightarrow C_j$ for all $i, j$, $1 \leq i, j \leq h$.

Proof. Since $D$ has genus one, the group of $\mathbb{F}_q$-isomorphisms of $D$ acts transitively on the $\mathbb{F}_q$-rational points of $D$. The assertion now follows from the theorem.
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 $k^\times$. Let $\Omega_i$ be the group of characters of $k^\times_i$ trivial on $N_i$ and $\Omega_i'$ be the elements of $\Omega_i$ distinct from the trivial character. Then the Dedekind zeta function of $k_i$ is given by $\xi_k(s) = \xi_k(s) \cdot \prod_{\omega \in \Omega_i} L(s, \omega)$ [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 $s \in \mathbb{C}$, let $\omega_2^i : k^\times_i \rightarrow \mathbb{C}^\times$ be the quasicharacter defined by $\omega_2^i(z) = |z|^2$; $\omega_j^i : k^\times_i \rightarrow 1$.

**Lemma 4.** Let $\omega \in \Omega_1$, $\omega \neq 1$, and let $\omega(zu_i) = q^{-s_2(\omega)}$. There is a one-to-one correspondence between $\Omega_1$ and $\Omega_i$ given by $\omega \leftrightarrow \omega \omega_2(\omega)$.

**Proof.** $\omega$ has order $h$ so $q^{-s_2(\omega)}$ is an $h$th root of one and $s_2(\omega)$ is defined modulo elements of $(2\pi i / \log q)\mathbb{Z}$. $\omega$ and $\omega_2^i$ induce the trivial character on $k^\times U$, so $\omega_\omega_2^i \in \Omega_i$ if and only if $\omega \omega_2^i(zu_i) = 1$.

This is equivalent to $s \equiv s_2(\omega) \pmod{(2\pi i / \log q)\mathbb{Z}}$. The verification that the correspondence between $\Omega_1$ and $\Omega_i$ is one-to-one is left to the reader.

**Lemma 4 and the definition of the $L$-functions give**

**Proposition.**

$$L^*\left(s, \prod_{\omega_2^i} L(\omega_2^i, s) = \prod_{\omega_2^i} L(\omega, s + s_2(\omega)) \right).$$

$\xi_k^* = \xi_k^i$, for $1 \leq i, j \leq h$, if and only if $J(C_i)$ is $F_q$-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 $F_q$-isogenous to $J(C_2)$ and, hence, $C_1$ is not $F_q$-isomorphic to $C_2$.

**Proof.** Let $\omega \in \Omega_1$; then $\xi_k^i(\omega) = \xi_k^*\omega(\omega)$ if and only if $L(\omega_s, s) = L(\omega_s + s_2(\omega))$,

where $q^{-s_2(\omega)} = -1$ because $\omega_2^i(zu_i) \in \Omega_2^i$. So $s_2(\omega) \equiv \pi i / \log q \pmod{(2\pi i / \log q)\mathbb{Z}}$.

On the other hand $L(\omega, s)$ has period $2\pi i / \log q$, so $L(\omega, s) = L(\omega, s + s_2(\omega))$.

**References**