TWO-DESCENT FOR ELLIPTIC CURVES IN
CHARACTERISTIC TWO

BY
KENNETH KRAMER(1)

ABSTRACT. This paper is a study of two-descent to find an upper bound for
the rank of the Mordell-Weil group $A(F)$ of an elliptic curve $A$ defined over
a field $F$ of characteristic two. It includes local and global duality theorems
which are the analogs of known results for descent by an isogeny whose
degree is relatively prime to the characteristic of the field of definition.

Introduction. Let $A$ be an elliptic curve defined over a field $F$ of
characteristic two, and assume that $A$ is not supersingular. Multiplication by
two on $A$, which we denote by $2_A$, is the product of dual isogenies: the
Frobenius $\pi$ and a separable isogeny $\psi$. When $F$ is a global field, let $M(1)$ and
$M(2)$ denote the first and second Selmer groups obtained, respectively, from a
knowledge of the cokernels of $\psi$ and of $2_A$ at each completion of $F$. The point
of this paper is to prove the existence of an alternating bilinear form putting
$M(1)/M(2)$ in perfect self-duality.

Our approach is similar to that of Cassels [1] for three-descent in
characteristic zero. We begin by constructing exact sequences to study the
cokernels of $\pi$ and of $\psi$. Such exact sequences are known to occur from the
point of view of flat cohomology, though we describe the groups and maps
involved more concretely. We then show that when $F$ is a local field the
cokernels of $\pi$ and of $\psi$ are orthogonal complements under the Artin-Schreier
pairing. This agrees with a general duality theorem for $p$-isogenies in
characteristic $p$ obtained by Milne [3] using a suitable cohomological
interpretation.

After proving the global duality for $M(1)/M(2)$ we give examples of elliptic
curves defined over $k(t)$, where $k = Z/2Z$, for which
(i) $M(1)$ is arbitrarily large or
(ii) $M(2)$ is strictly smaller than $M(1)$ and can be computed by using our
bilinear form.

Much of this paper is based on the author's Ph.D. dissertation, done at
Harvard University under the direction of John Tate. I am grateful to

Received by the editors March 17, 1976.
(1) Partially supported by a grant from the Faculty Research Award Program of the City
University of New York.

© American Mathematical Society 1977

279
Professor Tate for the suggestions and encouragement which he provided at every step of the way.

1. Algebraic preliminaries. The results of this section are valid over any field $F$ of characteristic two. Our goal is to arrive at the exact commutative diagrams

$$
\begin{align*}
A(F) & \xrightarrow{2_A} A(F) \xrightarrow{\gamma_A} H \\
\pi & \downarrow 1 \downarrow j \\
B(F) & \xrightarrow{\psi} A(F) \xrightarrow{\alpha} F/\Phi(F)
\end{align*}
$$

(1)

$$
\begin{align*}
B(F) & \xrightarrow{2_B} B(F) \xrightarrow{\gamma_B = (\beta, \alpha_B)} F^*/F^{*2} \times F/\Phi(F) \\
\psi & \downarrow 1 \downarrow \text{proj} \\
A(F) & \xrightarrow{\pi} B(F) \xrightarrow{\beta} F^*/F^{*2}
\end{align*}
$$

(2)

with notation to be further explained below.

If the elliptic curve $A$ is given by a plane cubic model of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

then $A$ is not supersingular (i.e., there exists a point of order two defined over the algebraic closure of $F$) precisely when $a_1 \neq 0$. Translating variables and renaming coefficients, we assume from now on that we have a model of the form

$$A: y^2 + a_1xy = x^3 + a_2x^2 + a_6$$

with discriminant $\Delta = a_1^8a_6$, which we assume is not zero, and absolute invariant $j = a_1^6a_6^{-1}$.

By the usual tangent-chord methods for addition [7, p. 181], we see that $(0, \sqrt{a_6})$ is the unique point of order two on $A$ and that $2_A(s, t) = (x, y)$ with

$$
\begin{align*}
\lambda &= s/a_1 + t/s = t^2/a_1s^2 + a_2/a_1 + a_6/a_1s^2, \\
x &= x^2 + a_1\lambda + a_2 = s^2/a_1^2 + a_6/s^2, \\
y &= \lambda x + a_1a_6/s^2.
\end{align*}
$$

(4)

The Frobenius isogeny $\pi$ maps the curve $A$ with model (3) to the curve

$$B: y^2 + a_1^2xy = x^3 + a_2^2x^2 + a_6^2$$

by $\pi(x, y) = (x^2, y^2)$. Let $\psi: B \rightarrow A$ be the dual isogeny [7, p. 185] of
Frobenius, so that $\psi \circ \pi = 2_A$ and $\pi \circ \psi = 2_B$. If $Q = (S,T)$ is a point on $B$, the formulas for $(x,y) = \psi(Q)$ are therefore obtained by letting $S = s^2$ and $T = t^2$ in (4).

The sequences in the next proposition are known to be exact from a cohomological viewpoint. Exactness and the definitions of the homomorphisms involved can also be checked laboriously from our formulas for $\psi$ and $\pi$ and the rules for addition on $A$ [7, p. 181]. We illustrate this sort of calculation later on in Proposition 1.4.

**Proposition 1.1.** (a) Let $\Phi(f) = f^2 + f$. The map $\alpha: A(F) \to F/\Phi(F)$ given by

$$\alpha(x,y) = \text{coset}\{ (x + a_2)/a_1 \} = \text{coset}\{ a_6/a_1^2 x^2 \}$$

is a homomorphism and the following sequence is exact:

$$0 \to \{ 0_B, (0,a_6) \} \to B(F) \xrightarrow{\psi} A(F) \xrightarrow{\alpha} F/\Phi(F).$$

(b) Let $F^*$ denote the multiplicative group of $F$. The map $\beta: B(F) \to F^*/F^{*2}$ given by

$$\beta(x,y) = \begin{cases} \text{coset}\{ x \} & \text{if } x \neq 0, \\ \text{coset}\{ a_6 \} & \text{if } x = 0, \end{cases}$$

is a homomorphism and the following sequence is exact:

$$0 \to A(F) \xrightarrow{\pi} B(F) \xrightarrow{\beta} F^*/F^{*2}. $$

We now describe a group $H$ which we shall use to study the cokernel of multiplication by 2 on $A(F)$. Let $E$ be the $F$-algebra of elements of the form $f + gr$, where $f$ and $g$ are in $F$ and the relation $r^2 = a_6$ holds. We define a formal differentiation on $E$ by $D(f + gr) = g$ and we identify the kernel of $D$ with $F$. Note that then $E^2$ is contained in $F$. Let $H$ be defined by the exact sequence $E^* \xrightarrow{D} F^* \times a_6F^2 \to H \to 0$ where $\theta(\xi) = (\xi^2, \Phi(\xi r^{-1}D\xi^2))$. The following lemma, which can be checked directly, shows that the second coordinate of $\theta$ does in fact lie in $a_6F^2$.

**Lemma 1.2.** Suppose that $f$ is in $F^*$. Then $\Phi(f)$ is in $a_6F^2$ if and only if $f = (r\xi^{-1}D\xi^2)^2$ for some $\xi$ in $E^*$.

Using this lemma it is easy to see that another description of the relations in $H$ is

$$\theta(E^*) = \{ (a_6 fg^2, \Phi(f)) | f,g \in F^* \text{ and } \Phi(f) \in a_6F^2 \}. $$

We denote by $((a,b))$ the element in $H$ which is the coset of the element $(a,b)$ in $F^* \times a_6F^2$.

**Notation.** If $\sigma$ is a homomorphism with domain $G$, let $\sigma G$ be its kernel.
Proposition 1.3. (a) We have the exact sequence

\[ 0 \to \pi_2 A(F) \stackrel{\psi}{\to} B(F) \stackrel{\beta}{\to} F^*/F^{*2} \to H \to F/\Phi(F) \to F/(\Phi(F) + a_6 F^2) \to 0 \]

where \( i(\text{coset}(a)) = ((a,0)) \) and \( j((a,b)) = \text{coset}(b) \).
(b) If \( a_6 \) is a square in \( F \) then \( H \simeq F^*/F^{*2} \times F/\Phi(F) \) by \( ((a,b)) \to (\text{coset}(a), \text{coset}(b^{1/2})) \).
(c) Suppose that \( m \in a_6 F^2 \) is a representative for \( j(h) \). Then \( h = ((l,m)) \) with \( l \in F^* \) determined up to multiplication by an element of \( \{1,a_6\} F^{*2} \).

Proof. Using the description of the relations in \( H \) given by (6), the exact sequence in part (a) is easy to check, and implies part (b) when \( a_6 \) is a square in \( F \). Part (c) results from the fact that if \( j(h) = \text{coset}(m) \), with \( m \) in \( a_6 F^2 \), then \( h + ((1,m)) \) is in \( \text{Ker} \ j = \text{Im} \ i \). Hence

\[ h = ((1,m)) + i(l) = ((l,m)). \]

\( l \) is determined as claimed because \( \text{Ker} \ i = \{1,a_6\} F^{*2} / F^{*2} \).

Proposition 1.4. Let \( P = (x,y) \) be a point on \( A \) and define

\[ \gamma_A(P) = \begin{cases} 
((x, a_6/a_1^2 x^2)) & \text{if } x \neq 0, \\
((a_1 a_6^{1/2}, a_2/a_1^2)) & \text{if } x = 0.
\end{cases} \]

Then the following diagram commutes

\[\begin{align*}
B(F) & \xrightarrow{\psi} A(F) \xrightarrow{1} A(F) \\
\beta \downarrow & \quad \gamma_A \downarrow \alpha \\
F^*/F^{*2} & \xrightarrow{i} H \xrightarrow{j} F/\Phi(F)
\end{align*}\]

and the following sequence is exact

\[ 0 \to \pi_2 A(F) \to A(F) \xrightarrow{\gamma_A} A(F) \xrightarrow{\gamma_A} \to H. \]

Proof. First we check that \( \gamma_A \) is a homomorphism. Suppose that \( P_1 + P_2 + P_3 = 0 \) on \( A \), so that the points \( P_1, P_2, P_3 \) also lie on a line \( L \) with equation, say, \( y = \lambda x + \nu \). Assume that \( x(P_1) = x_1 \neq 0 \). Solving the equations for \( L \) and \( A \) simultaneously, we find that \( x_1 x_2 x_3 = a_6 + \nu^2 \) and \( x_1 x_2 + x_1 x_3 + x_2 x_3 = a_6 \nu \). Now from the definition of \( \gamma_A \) we find that

\[ \gamma_A(P_1) + \gamma_A(P_2) + \gamma_A(P_3) = \left( (a_6 + \nu^2, a_6 \nu^2) / (a_6 + \nu^2)^2 \right). \]

This coset is trivial in \( H \), as desired, because its representative is \( \theta(\nu + r) \). We leave the exceptional cases to the reader.
The commutativity of diagram (7) can be checked by direct calculation. To prove exactness of (8) note that if \( \gamma_A(P) = 0 \), then by (7), \( \alpha(P) = 0 \) so \( P = \psi(Q) \) for some point \( Q \) in \( B(F) \) by Proposition 1.1(a). Then \( i \circ \beta(Q) = \gamma_A \circ \psi(Q) = \gamma_A(P) = 0 \). But

\[
\ker i = \beta(\psi B(F)) = \beta\{0_{B}, (0, a_6)\}.
\]

Correcting \( Q \) by \( (0, a_6) \) if necessary, we can assume that \( \beta(Q) = 1 \). Hence \( Q = \pi(R) \) for some \( R \) in \( A(F) \), and \( P = \psi \circ \pi(R) = 2R \). The rest is clear.

From Proposition 1.1(a) and Proposition 1.4 we get exactness of the rows of diagram (1). To obtain diagram (2) we observe that the constant term of the model (5) for the curve \( B \) is in \( F^2 \). Hence the analog of exact sequence (8) is

\[
B(F) \xrightarrow{2} B(F) \xrightarrow{\gamma_B} F^*/F^{*2} \times F/\Phi(F)
\]

with \( \gamma_B(x,y) \) represented by

\[
\gamma_B(x,y) = \begin{cases} 
(x, a_6/a_2^2x), & \text{if } x \neq 0, \\
(a_6, a_2/a_2^2), & \text{if } x = 0.
\end{cases}
\]

Let \( \alpha_B \) be the analog for the curve \( B \) of the map \( \alpha \) in Proposition 1.1(a). Then \( \gamma_B = (\beta, \alpha_B) \) and

\[
(9) \quad \alpha_B \circ \pi = \alpha.
\]

**Notation.** We write \( M_\alpha, M_\beta, M_{\gamma_A}, M_{\gamma_B} \) for the images of the homomorphisms \( \alpha, \beta, \gamma_A, \gamma_B \) respectively. If \( G \) is a finite group, we let \([G]\) be its order.

**Proposition 1.5.** If the abelian group \( A(F) \) has finite rank \( r \) then \( 2^{r+1} = [M_\alpha][M_\beta] \).

**Proof.** Since \( \psi \circ \pi = 2_\alpha \), we have the exact sequence

\[
0 \to 2A(F) \to \psi B(F) \to \text{Coker } \pi \to \text{Coker } 2_\alpha \to \text{Coker } \psi \to 0.
\]

The result follows from Proposition 1.1 and the Euler characteristic of this exact sequence, upon noting that \([\text{Coker } 2_\alpha] = 2/2A(F)\).

**Proposition 1.6.** Let \( P = (x, y) \) be a point in \( A(F) \), and let \( Q = (s, t) \) be in \( B(F) \). Let \( \Phi(\eta) = (x + a_2)/a_2^2 \). Then \( s \) and \( a_6 \) are norms from \( F[\eta] \).

**Proof.** We can assume that \( \eta \) is not in \( F \) and that \( s \) is not zero. The norm of an element of \( F[\eta] \) has the form

\[
N(a + b\eta) = a^2 + ab + b^2\Phi(\eta) \quad \text{with } a, b \in F.
\]

Using (3) and (5) one checks that

\[
sN[(a_1y + s) + (a_1^2x)\eta] = N[(t + a_2s + a_6) + (a_2^2s)\eta].
\]
Hence \( s \) is a norm, by multiplicativity of the map \( N \). Moreover \( a_6 \) is a norm by the equation (3).

2. Local duality. Throughout this section \( F \) is a local field of characteristic two, with finite residue field \( k \) and additive valuation \( v \). We denote by \([ , )\) the Artin-Schreier symbol [4, p. 221] which gives a perfect pairing:

\[
[F/\Phi(F) \times F^*/F^{*2} \to \mathbb{Z}/2\mathbb{Z}]
\]

We use a model for the curve \( A \) of the form (3) with \( v(a_i) > 0 \). Note that this model may not be minimal. The main result is

**Theorem 2.1.** The finite group \( M_a \subseteq F/\Phi(F) \) and the compact group \( M_\beta \subseteq F^*/F^{*2} \) are orthogonal complements under the Artin-Schreier pairing.

**Proof.** In the next two propositions, we show that the quotient of \( F^*/F^{*2} \) by \( M_\beta \) is a finite group with \([M_a] > [(F^*/F^{*2}): M_\beta]\). Let \( M_\beta^\perp \) denote the exact orthogonal complement of \( M_\beta \). Since the symbol \([a,b] \) is zero when \( b \) is a norm from \( F[x(a)] \), Proposition 1.6 implies that \( M_a \) is contained in \( M_\beta^\perp \) and the reverse inequality \([M_a] \leq [M_\beta^\perp] = [(F^*/F^{*2}): M_\beta] \) must also hold. Hence \( M_a = M_\beta^\perp \).

Before stating the next two propositions, we recall that \( A_n = \{(x,y) \in A(F)|v(x) < -2n\} \cup \{0\} \), for \( n > 1 \), is a subgroup of finite index in \( A(F) \). There is a formal group addition [7, p. 183] on the maximal ideal \( m \) of \( F \) such that \( A_n \cong m^n \) by \((x,y) \to z = xy^{-1}\). Let \( U_n = \{u \in F|v(u) = 0 \text{ and } v(u - 1) > n\} \).

**Proposition 2.2.** The quotient of \( F^*/F^{*2} \) by \( M_\beta \) is a finite group of order

\[
[(F^*/F^{*2}): M_\beta] = 2[k]^{v(a_1)}[A(F): A_1] + [(B(F): B_1].
\]

\( M_\beta \) contains \( U_{2v(a_1)F^{*2}}/F^{*2} \) with index

\[
[M_\beta: U_{2v(a_1)F^{*2}}/F^{*2}] = [B(F): B_1] + [A(F): A_1].
\]

**Proof.** The exactness of the following commutative diagram is clear, except possibly for the image of \( \beta \) in the top row.

\[
\begin{align*}
0 & \rightarrow A_1 \xrightarrow{\pi} B_1 \xrightarrow{\beta} U_{2v(a_1)F^{*2}}/F^{*2} \rightarrow 0 \\
0 & \rightarrow A(F) \xrightarrow{\pi} B(F) \xrightarrow{\beta} M_\beta \rightarrow 0
\end{align*}
\]

But the points \((x,y) \in B_1 \) correspond exactly to all \( z = xy^{-1} \) in \( m \). From the equation for \( B \), we get
\( x \left( \frac{x}{y} \right)^2 = \frac{y^2 + a_1^2xy + a_2^2x^2 + a_6^2}{y^2} = \left( 1 + a_2 \frac{x}{y} + a_6 \frac{1}{y} \right)^2 + a_1^2 \frac{x}{y}. \)

Now \( u = 1 + a_2x/y + a_6/y \) is a unit in \( F \) and

\[ \beta(x, y) \equiv x \equiv 1 + a_2^2u^{-2}z \quad \text{(modulo } F^*^2). \]

This proves the surjectivity of \( \beta \) in the top row.

All the vertical arrows in the diagram are injective. The proposition follows from the exact sequence of their cokernels upon noting that \([F^*/U_2(a)]F^*^2] = 2[k]^{v(a)}\).

**Proposition 2.3.** \([M_a] > [(F^*/F^*^2) : M_\beta]\).

**Proof.** Let \( i: B_1 \to B(F) \) be the natural injection and define \( \tilde{\psi} = \psi \circ i: B_1 \to A(F) \). It follows from the exact sequence

\[
0 \to \text{Ker } \tilde{\psi} \to \text{Ker } \psi \to \text{Coker } i \to \text{Coker } \tilde{\psi} \to \text{Coker } \psi \to 0
\]

that \([B(F): B_1, M_\alpha] = 2[A(F)/\tilde{\psi}(B_1)]. \) But if \( P = (S, T) \) is a point in \( B_1 \), then we see from the formula for the x-coordinate of \( \psi(P) \) obtained by letting \( S = s^2 \) in (4) that \( \tilde{\psi}(P) \) is in \( A_v(a_v + X). \)

Hence

\[
[A(F)/\tilde{\psi}(B_1)] > [A(F): A_v(a_v + X)] = [A(F): A_1][k]^{v(a)}
\]

and this implies the desired inequality on \([M_a]\).

**Remark.** In practice, one determines the index \([A(F): A_1]\) as follows. If \( A^{\text{min}} \) is a minimal model for \( A \) with discriminant \( \Delta^{\text{min}} \), then there is an isomorphism \( f: A^{\text{min}}(F) \to A(F) \) of the form \((x, y) \to (u^2x + r, u^3y + su^2x + t)\). Let \( n = v(u) \), so that \( 12n = v(\Delta) - v(\Delta^{\text{min}}) \). Then \( f \) clearly induces an isomorphism \( A^{\text{min}}(F)/A_n \cong A(F)/A_1 \). Let \( A_0 \) denote the subgroup of \( A^{\text{min}}(F) \) consisting of points whose reduction is nonsingular and let \( A_0 \) be the reduced curve. Then

\[
[A(F): A_1] = [A^{\text{min}}(F): A_0^{\text{min}}][A_0^{\text{min}}][k]^{n}
\]

and \([A^{\text{min}}(F): A_0^{\text{min}}]\) can be calculated by an algorithm of Tate [6]. A similar analysis applies to \([B(F): B_1]\). Moreover, \([A_0^{\text{min}}(k)] = [B_0^{\text{min}}(k)] \) because \( A \) and \( B \) are isogenous.

**Proposition 2.4.** If \( A \) has good reduction and the reduced curve \( \tilde{A} \) is not supersingular (i.e., if \( v(\Delta) = v(a) = 0 \) on a minimal model for \( A \)) then

\[ M_\alpha = (k + \Phi(F))/\Phi(F) \quad \text{and } M_\beta = UF^*^2/F^*^2. \]

**Proof.** Using the above remark and Proposition 2.2 we find that \([M_\beta: UF^*^2/F^*^2] = 1. \) The result for \( M_\alpha \) follows by duality.

**Proposition 2.5.** Suppose that \( A \) has multiplicative reduction.
(i) If $\nu(\Delta_A)$ is even and $\tilde{A}$ has irrational tangent lines at its node, then $M_\alpha = (k + \Phi(F))/\Phi(F)$ and $M_\beta = UF^{*2}/F^{*2}$.
(ii) Otherwise $M_\alpha = \{0\}$ and $M_\beta = F^*/F^{*2}$.

**Proof.** By Proposition 2.2 and the remark after it we find that

$$[M_\beta: UF^{*2}/F^{*2}] = \begin{cases} 1 & \text{case (i)}, \\ 2 & \text{case (ii)}. \end{cases}$$

When this index is 2, $M_\beta$ is of course $F^*/F^{*2}$. $M_\alpha$ is determined by duality.

**Proposition 2.6.** Suppose that the coefficients in the model (3) for $A$ are $\nu$-integral, and $\nu(a_1) = \nu(a_\delta) = 0$. If $((l, m))$ is in the image of $\gamma_A$ and $\nu(m) = 0$ then $l$ is in $UF^{*2}$.

**Proof.** By assumption, there exists a point $P$ in $A(F)$ such that $\gamma_A(P) = ((l, m))$. Let $K = F[\Phi^{-1}(m)]$. Either $K = F$ or else, because $\nu(m) = 0$, $K$ is an unramified quadratic extension of $F$. Without ambiguity, we may denote the valuation of $K$ also by $\nu$. Now $\alpha(P) = j \circ \gamma_A(P) = \text{coset}(m)$ in $F/\Phi(F)$. Hence $\alpha(P)$ becomes trivial in $K/\Phi(K)$ and there is a point $Q$ in $B(K)$ such that $\psi(Q) = P$ by Proposition 1.1(a).

Let $E_K$ be the algebra $E \otimes K$ and let $H_K$ be the analog of the group $H$ but defined over $K$. In $H_K$ we have

$$((l, m)) = \gamma_A(P) = \gamma_A \circ \psi(Q) = i \circ \beta(Q) = ((x, 0))$$

where $\beta(Q) = \text{coset}(x)$ in $K^*/K^{*2}$ and $x$ has even valuation in $K$ by Proposition 2.4. Using the description (6) of the relations in $H_K$ we get $l = xa_\delta ab^2$, $m = a^2 + a$, with $a, b \in K^*$. But if $\nu(m) = 0$, then $\nu(a) = 0$ in the second equation, so $\nu(l)$ is even, as desired.

### 3. Global duality

We now assume that $F$ is a function field of transcendence degree one with finite constant field $k$ of characteristic 2. We denote the completion of $F$ at a prime $v$ by $F_v$ and the corresponding residue field by $k_v$. By the Mordell-Weil theorem, the rank $r$ of $A(F)$ is finite. Hence $2^{r+1} = [M_\alpha][M_\beta]$ by Proposition 1.5.

To obtain information about $M_\alpha$ and $M_\beta$ we study the corresponding local groups $M_\alpha^v = \alpha(A(F_v))$ and $M_\beta^v = \beta(B(F_v))$ at each prime $v$. We define the first Selmer group for $\alpha$ to be

$$M_\alpha^{(1)} = \{ a \in F/\Phi(F) | a \in M_\alpha^v \text{ for all } v \}.$$ We let

$$M_\alpha^{(1)} = \{ ((a, b)) \in H | ((a, b)) \in M_\alpha^v \text{ for all } v \},$$

and we define the second Selmer group for $\alpha$ to be $M_\alpha^{(2)} = j(M_\alpha^{(1)}) \subseteq F/\Phi(F)$. It is clear from diagram (1) that $M_\alpha \subseteq M_\alpha^{(2)} \subseteq M_\alpha^{(1)}$. 
Similarly, the first Selmer group for \( \beta \) is defined to be \( M^{(1)}_\beta = \{ a \in F^*/F^{*2} | a \in M^o_\beta \text{ for all } \nu \} \). We let

\[
M^{(1)}_{\gamma} = \{ (a,b) \in F^*/F^{*2} \times F/\Phi(F) | (a,b) \in M^o_{\gamma} \text{ for all } \nu \}
\]

and we define the second Selmer group for \( \beta \) to be

\[
M^{(2)}_\beta = \text{proj}(M^{(1)}_\gamma) \subseteq F^*/F^{*2}.
\]

By diagram (2) we have \( M^i_\beta \subseteq M^{(2)}_\beta \subseteq M^{(1)}_\beta \). In this section we prove

**Theorem 3.1.** There is an alternating bilinear form on \( M^{(1)}_\alpha \) (respectively, \( M^{(1)}_\beta \)) which puts \( M^i_\alpha / M^{(2)}_\alpha \) (respectively, \( M^i_\beta / M^{(2)}_\beta \)) in perfect self-duality.

**Definition of the Bilinear Form on \( M^{(1)}_\alpha \).** For each coset \( m \) in \( M^{(1)}_\alpha \) we choose elements \( l_\alpha \) in \( F^*_\alpha \) as follows:

**Step 1.** The lemma below shows that \( m \) can be represented by an element of \( a_\alpha F^2 \). Say \( m = \text{coset}\{a_\alpha F^2\} \).

**Step 2.** By definition of \( M^{(1)}_\alpha \) we can find points \( P_\alpha \) in \( A(F_\alpha) \) such that \( a(P_\alpha) = m \).

**Step 3.** By Proposition 1.3(c) we can find \( l_\alpha \) in \( F^*_\alpha \) such that \( \gamma_\alpha(P_\alpha) = \left((a_\alpha F^2)^{-1}\right) \).

**Lemma 3.2.** Every coset \( m \) in \( M^{(1)}_\alpha \) has a representative in \( a_\alpha F^2 \).

**Proof.** We may as well assume that \( m \neq 0 \) and \( a_\alpha \notin F^2 \), the other cases being trivial. Applying \( \beta \) to the point \( (0,a_\alpha) \) on \( B(F) \), we find that coset\{a_\alpha\} is in \( M^i_\beta \) for all \( \nu \). Since \( m \) is in \( M^o_\alpha \) for all \( \nu \), we have \( [m,a_\alpha]_\nu = 0 \) by Theorem 2.1. Hence \( a_\alpha \) is a norm everywhere locally from \( F_\alpha/\Phi^{-1}(m) \). It follows from the Hasse principle that \( a_\alpha \) is a norm globally from the quadratic extension \( F[\Phi^{-1}(m)] \). Let \( m_0 \) represent the coset \( m \). We may therefore write \( a_\alpha = e^2 + ef + f^2m_0 \) for some \( e,f \) in \( F \). But \( f \neq 0 \) since \( a_\alpha \notin F^2 \). Hence \( m = \text{coset}\{m_0\} = \text{coset}\{a_\alpha f^{-2}\} \) as desired.

**Proposition 3.3.** Associate to \( m \in M^{(1)}_\alpha \) the elements \( l_\alpha \in F^*_\alpha \) determined by Steps 1, 2, 3 above. Define

\[
U_\alpha: M^{(1)}_\alpha \times M^{(1)}_\alpha \to \mathbb{Z}/2\mathbb{Z}
\]

by \( U_\alpha(m',m) = \Sigma(m',l_\alpha)_\nu \). Then \( U_\alpha \) is a well-defined alternating bilinear form.

**Proof.** By Proposition 1.3(c), the element \( l_\alpha \) in Step 3 is determined up to multiplication by \( \{1,a_\alpha\}F^{*2} \). But this is harmless because \( \{1,a_\alpha\}F^{*2} \) is orthogonal to any \( m' \) in \( M^o_\alpha \).

Suppose in Step 2 we choose another point \( P_\alpha' \) such that \( \alpha(P_\alpha') = \alpha(P_\alpha) = m \). By Proposition 1.1(a) we may write \( P_\alpha' = P_\alpha + \psi(Q_\alpha) \) for some \( Q_\alpha \in B(F_\alpha) \). But
\[ \gamma_A(P_v') = \gamma_A(P_v) + \gamma_A \circ \psi(Q_v) \]
\[ = \left((l_v, a_6 f^2)\right) + \beta(Q_v) \]
\[ = \left((l_v, \beta(Q_v), a_6 f^2)\right). \]

Thus the choice of \( P_v' \) in Step 2 leads to the choice of \( l_v' = l_v \beta(Q_v) \) in Step 3. But \( \{m', l_v'\} = \{m', l_v\} \) by orthogonality of \( M_\alpha^v \) and \( M_\beta^v \). This proves independence of the choice in Step 2.

Suppose in Step 1 we choose a different representative in \( a_6 F^2 \) for the coset \( m \). Say \( a_6 f^2 \equiv a_6 g^2 \) (modulo \( \Phi(F) \)). By Lemma 1.2 we may write \( a_6 f^2 + a_6 g^2 = \Phi(r \xi^{-1} D \xi^2) \) with \( \xi \) in \( E^* \). Using \( a_6 f^2 \) in Step 1 and doing Steps 2 and 3 we arrive at \( \gamma_A(P_v) = ((l_v, a_6 f^2)) \). If we change this representative for \( \gamma_A(P_v) \) by \( \theta(\xi) \) we get \( \gamma_A(P_v) = ((l_v \xi^2, a_6 g^2)) \). Thus the choice of \( a_6 g^2 \) in Step 1 leads to the choice of \( l_v' = l_v \xi^2 \) in Step 3. Now
\[ \sum_v \left[m', l_v \xi^2\right] = \sum_v \left[m', l_v\right] + \sum_v \left[m', \xi^2\right] \]
and the last summation is zero by reciprocity as \( m' \) and \( \xi^2 \) are global elements of \( F \). This proves independence of the choice in Step 1.

We now show that all but finitely many terms in the summation defining \( U_\alpha \) are zero. Let \( S \) be the finite set of primes \( v \) for which any of the following holds:

- (i) \( v(a_i) < 0 \) for some coefficient \( a_i \) in the model (3),
- (ii) \( v(\Delta) \neq 0 \),
- (iii) \( v(a_6 f^2) \neq 0 \) for \( a_6 f^2 \) chosen in Step 1.

For primes \( v \notin S \), the element \( l_v \) of Step 3 is in \( U_v F_v^2 \) by Proposition 2.6 and the element \( m' \) is in \( (k_v + \Phi(F_v))/\Phi(F_v) \) by Proposition 2.4. Thus
\[ \sum_v \left[m', l_v\right] = 0 \quad \text{for } v \in S. \]

Finally, we show that \( U_\alpha \) is alternating; that is, \( U_\alpha(m, m) = 0 \). We may assume that \( m = \coset\{a_6 f^2\} \) is not zero. Translating by an element of \( 2A(F_v) \) if necessary, we may assume that, in Step 2, \( P_v = (x_v y_v) \) with \( x_v \neq 0 \). Write \( \gamma_A(P_v) = ((l_v, a_6 f^2)) \) in Step 3. Using the definition of \( \gamma_A \) in Proposition 1.4 we have
\[ \left((l_v, a_6 f^2)\right) = \gamma_A(P_v) = \left((x_v a_6/a_1^2 x_v^2)\right). \]

It follows from the description (6) of the relations in \( H \) that there exists an element \( g_v \) in \( F_v^2 \) such that
\[ l_v \equiv x_v g_v \pmod{1, a_6 F_v^2} \]
and \( a_6 f^2 = a_6 / a_1^2 x_v^2 + g_v^2 + g_v \). The latter equation implies that
\[ g_v (a_1 x_v f)^{-1} = g_v^2 + g_v \left[ 1 + \frac{1}{a_1 x_v f} \right] + \left[ 1 + \frac{1}{a_1 x_v f} \right]^2 a_6 f^2. \]
which gives \( g_v(a_1 x_v f)^{-1} \) explicitly as a norm from the quadratic extension \( F_v[\Phi^{-1}(a_\delta f^2)] = F_v[\Phi^{-1}(m)] \). Hence \( [m, g_v(a_1 x_v f)^{-1}]_v = 0 \). Now

\[
U_\alpha(m, m) = \sum_v [m, l_v]_v = \sum_v [m, x_v g_v]_v = \sum_v [m, a_1 f]_v = 0
\]

by reciprocity.

**Proposition 3.4.** Let \( m \) be an element of \( M^{(1)}_\beta \). For each prime \( v \), choose \( P_v \) in \( B(F_v) \) such that \( \beta(P_v) = m \). Let \( l_v = \alpha_\beta(P_v) \) and define

\[
U_\beta : M^{(1)}_\beta \times M^{(1)}_\beta \to \mathbb{Z}/2\mathbb{Z}
\]

by \( U_\beta(m, m') = \sum [l_v, m']_v \). Then \( U_\beta \) is a well-defined alternating bilinear form.

**Proof.** The argument showing independence of the choice of \( P_v \) is analogous to the argument in the previous proof showing independence of the choice in Step 2. We omit it.

Let \( S \) be the finite set of primes for which the curve \( B \) has bad reduction or supersingular reduction. If \( v \not\in S \) then by Proposition 2.4 the image of \( \alpha_\beta \) is \( (k_v + \Phi(F_v))/\Phi(F_v) \) and \( M^{(1)}_\beta \) is \( U_v F_v^{*2} \). Hence \( [l_v, m']_v = 0 \) for all \( v \not\in S \).

To show that \( U_\beta(m, m) = 0 \), choose points \( P_v = (x_v, y_v) \) such that \( \beta(P_v) = m \) and (translating by an element of \( 2B(F_v) \) if necessary) \( x_v \neq 0 \). Now

\[
m = \beta(P_v) = \text{coset}(x_v) \text{ in } F_v^{*}/F_v^{*2} \text{ and } l_v = \alpha_\beta(P_v) = \text{coset}((x_v + a_2^2)/a_4) \text{ in } F_v/\Phi(F_v).
\]

Hence

\[
U_\beta(m, m) = \sum_v [l_v, m]_v = \sum_v [x_v/a_4, m]_v + \sum_v [a_2^2/a_4, m]_v.
\]

The last sum is zero by reciprocity and the next to last sum is zero by the fact that \( m \equiv x_v/a_4 (\text{mod } F_v^{*2}) \).

**Lemma 3.5.** (a) Let \( m \in a_\delta F_2^2 \) represent an element of \( M^{(1)}_\alpha \). Let \( S \) be a finite set of primes containing those \( v \) for which \( v(m) \neq 0 \) or \( v(a_i) \neq 0 \) for some coefficient \( a_i \) in the model (3). Then \( m \) represents an element of \( M^{(2)}_\alpha \) if and only if there exists \( l \in F^* \) such that

\[
(l, m) \in M^{(2)}_\alpha \text{ for } v \in S \text{ and } l \in U_v F_v^{*2} \text{ for } v \not\in S.
\]

(b) Let \( m \) represent an element of \( M^{(1)}_\beta \). Let \( S \) be a finite set of primes containing those for which \( A \) has bad reduction or supersingular reduction. Then \( m \) represents an element of \( M^{(2)}_\beta \) if and only if there exists \( l \in F \) such that

\[
(m, l) \in M^{(2)}_\beta \text{ for } v \in S \text{ and } l \in k_v + \Phi(F_v) \text{ for } v \not\in S.
\]

**Proof.** Suppose that \( m \) represents a class in \( M^{(2)}_\alpha \). Then there is an element \( h \in H \) and points \( P_v \) in \( A(F_v) \) for each prime \( v \) such that \( h = \gamma_A(P_v) \) and \( j(h) = \text{coset}(m) \). By Proposition 1.3(c) we may write \( h = ((l, m)) \) with \( l \) in \( F^* \) determined up to multiplication by \( (1, a_\delta) F_v^{*2} \). Then the element \( l \) is in \( U_v F_v^{*2} \) for \( v \not\in S \) by Proposition 2.6, and the conditions (11) hold.
Conversely, assuming that conditions (11) hold, we must show that \(((l,m)) \in M_2^\circ\) also for the primes \(v\) not in \(S\) in order to prove that \(m\) represents an element of \(M_2\). Since \(\coset{m}\) is an element of \(M_2^\circ\), we can find points \(Q_v\) in \(A(F_v)\) such that \(\alpha(Q_v) = \coset{m}\). Then \(\gamma_A(Q_v) = ((l_v,m))\) for some choice of \(l_v\) by Proposition 1.3(c). It follows from Proposition 2.6 and the conditions (11) that \(l_v^{-1} \in U_v F_v^{\mathbb{Z}_2}\) for \(v \not\in S\). By Proposition 2.4, we may find \(R_v \in B(F_v)\) such that \(\beta(R_v) = \coset{1/l_v}\) for \(v \not\in S\). Letting \(P_v = Q_v + \psi(R_v)\), we get \(((l,m)) = \gamma_A(P_v)\) for \(v \not\in S\) as desired.

The proof for part (b) is analogous.

Some preliminary work is now necessary to show that \(M_2\) is the precise orthogonal complement of \(M_1\) under the \(U\)-pairing. Let \(S\) be a nonempty finite set of primes containing representatives for generators of the divisor class group of \(F\) as well as those primes \(v\) for which \(v(a_i) \neq 0\) for some coefficient \(a_i\) in the model (3). We need the following notation:

\[
L_a = \{l \in F/\Phi(F)|l \in (k_v + \Phi(F_v))/\Phi(F_v)\} \text{ for } v \not\in S,
\]
\[
L_\beta = \{l \in F^*/F^{\mathbb{Z}_2}|l \in U_v F_v^{\mathbb{Z}_2}/F_v^{\mathbb{Z}_2}\} \text{ for } v \not\in S,
\]
\[
Z_a = \bigcup_{v \in S} F_v/\Phi(F_v), Z_\beta = \bigcup_{v \in S} F_v/F_v^{\mathbb{Z}_2},
\]
\[
X_a = \bigcup_{v \in S} M_a, Z_\beta = \bigcup_{v \in S} M_\beta,
\]
\[
Y_a = \{\langle l, l, \ldots \rangle \in Z_a|l \in L_a\}, Y_\beta = \{\langle l, l, \ldots \rangle \in Z_\beta|l \in L_\beta\}.
\]

**Lemma 3.6.** (a) The diagonal map \(L_a \to Z_a\) is an injection with image \(Y_a\).
(b) The diagonal map \(L_\beta \to Z_\beta\) is an injection with image \(Y_\beta\).

**Proof.** (a) If \(l\) is in the kernel of the diagonal map, then \(F[\Phi^{-1}(l)]\) is an unramified extension of \(F\) which is split completely over \(S\). By class field theory, \(F[\Phi^{-1}(l)] = F\) so that the diagonal map is injective.

(b) Injectivity follows from the fact that if an element of a global field \(F\) of characteristic \(p\) is a \(p\)th power at one completion, then it is a \(p\)th power globally. One can see this by noting that \(L = \{f \in F|f \in F_p\}\) is a subfield of \(F\) which contains \(F_p\). But \([F:F_p] = p\); hence, \(F_p = L\).

**Lemma 3.7.** In the perfect pairing of \(Z_a \times Z_\beta \to \mathbb{Z}/2\mathbb{Z}\) given by the sum of local Artin-Schreier symbols, \(Y_a\) and \(Y_\beta\) are orthogonal complements. \([Y_\beta]\) is finite and equals \([Z_a/Y_a]\).

**Proof.** Let \(J\) denote the idele group of \(F\). We have the subgroups

\[
J_S = \prod_{v \in S} F_v^* \times \prod_{v \in S} U_v \quad \text{and} \quad J^S = \prod_{v \in S} \{1\} \times \prod_{v \in S} U_v.
\]

Let \(F\) denote the image of \(F^*\) on the diagonal of \(J\). Then the following sequence is exact:

\[
0 \to J^S J^2 F/F \to J_S J^2 F/F \to Z_\beta/Y_\beta \to 0.
\]

But \(S\) contains representatives for generators of the divisor class group of \(F\),
so $J_2 F = J$ and (12) implies that there is an isomorphism
(13) \[ J/J^2 J^2 F \simeq Z_B / Y_B. \]

Now consider the pairing of Kummer theory and class field theory:

(14) \[ F/\Phi(F) \times J/J^2 F \to \mathbb{Z}/2\mathbb{Z} \text{ by } (f,\langle a_v \rangle) \to \sum_{\nu} [f,a_{a_\nu}], \]

The group $L_{\alpha} \subseteq F/\Phi(F)$ corresponds to the maximal extension of $F$ of type $(2,2,\ldots)$ unramified outside $S$. Hence the orthogonal complement of $L_{\alpha}$ in the pairing (14) is $J^2 J^2 F/J^2 F$. If we identify $L_{\alpha}$ with $Y_{\alpha}$ via Lemma 3.6(a) and $J/J^2 J^2 F$ with $Z_{\beta}/Y_{\beta}$ via (13) we obtain a perfect pairing $Y_{\alpha} \times Z_{\beta}/Y_{\beta} \to \mathbb{Z}/2\mathbb{Z}$ given by the sum of local Artin-Schreier symbols, i.e., compatible with the pairing of $Z_{\alpha} \times Z_{\beta} \to \mathbb{Z}/2\mathbb{Z}$ in the statement of the lemma. Hence $Y_{\alpha}$ and $Y_{\beta}$ are complementary under that pairing.

Note that if $l$ is in $L_{\beta}$, then $l$ can be represented modulo squares by an element of the finitely generated group $U_S = \{ f \in F^* | v(f) = 0 \text{ for } v \in S \}$. Hence $Y_{\beta} \approx L_{\beta}$ is a finite group, and $[Y_{\beta}] = [Z_{\alpha}/Y_{\alpha}]$ by duality.

**Proposition 3.8.** Let $W_{\alpha}$ be the group of characters $w_m: Z_{\alpha} \to \mathbb{Z}/2\mathbb{Z}$ of the form $w_m((a_\nu)) = \sum_{\nu} [a_\nu, m]_v$ with $m \in M_{\alpha}^{(1)}$. Let $\Omega_{\beta}$ be the group of characters $\omega_m: Z_{\beta} \to \mathbb{Z}/2\mathbb{Z}$ of the form $\omega_m((b_\nu)) = \sum_{\nu} [m, b_\nu]_v$ with $m \in M_{\beta}^{(1)}$. Then

\[ \bigcap_{w_m \in W_{\alpha}} \ker w_m = X_{\alpha} + Y_{\alpha} \quad \text{and} \quad \bigcap_{\omega_m \in \Omega_{\beta}} \ker \omega_m = X_{\beta} Y_{\beta}. \]

**Proof.** $X_{\alpha}$ is in the kernel of each $w_m \in W_{\alpha}$ by Theorem 2.1. $Y_{\alpha}$ is annihilated by each $w_m \in W_{\alpha}$ because, if $\langle l,l,\ldots \rangle \in Y_{\alpha}$, then

\[ w_m((l,l,\ldots)) = \sum_{v \in S} [l,m]_v = \sum_{v \not\in S} [l,m]_v + \sum_{v \in S} [l,m]_v. \]

The sum over $v \not\in S$ is zero by local duality and Proposition 2.4. The sum over all $v$ is zero by reciprocity. Similar reasoning applies to $X_{\beta}$, $Y_{\beta}$ and $\Omega_{\beta}$, so that

\[ X_{\alpha} + Y_{\alpha} \subseteq \bigcap \ker w_m \quad \text{and} \quad X_{\beta} Y_{\beta} \subseteq \bigcap \ker \omega_m. \]

We now use a counting argument. $W_{\alpha}$ is a subgroup of characters on the finite group $Z_{\alpha}/(X_{\alpha} + Y_{\alpha})$. Hence

(15) \[ [W_{\alpha}] \leq [Z_{\alpha}/(X_{\alpha} + Y_{\alpha})] = [Z_{\alpha}/Y_{\alpha}][X_{\alpha} \cap Y_{\alpha}][X_{\alpha}]^{-1}. \]

Similarly

(16) \[ [\Omega_{\beta}] \leq [Z_{\beta}/X_{\beta} Y_{\beta}] = [Z_{\beta}/X_{\beta}][X_{\beta} \cap Y_{\beta}][Y_{\beta}]^{-1}. \]

$[Z_{\beta}/X_{\beta}] = [X_{\alpha}]$ by Theorem 2.1 and $[Z_{\alpha}/Y_{\alpha}] = [Y_{\beta}]$ by Lemma 3.7. It is clear that the diagonal maps of Lemma 3.6 give isomorphisms $M_{\alpha}^{(1)} \cong X_{\alpha} \cap$
Y\alpha and $M^{(1)}_{\alpha} \simeq X_\beta \cap Y_\beta$. (In particular, this implies that the first Selmer groups are finite.) Multiplying (15) and (16) we get

$$[W_\alpha][\Omega_\beta] \leq [M^{(1)}_\alpha][M^{(1)}_\beta].$$

But $[M^{(1)}_\alpha] = [\Omega_\beta]$ because the map $M^{(1)}_\alpha \rightarrow \Omega_\beta$ by $m \rightarrow \omega_m$ is an isomorphism by the arguments in Lemma 3.6(a). Similarly $[M^{(1)}_\beta] = [W_\alpha]$. Hence we must have equality in (17) and therefore in (15) and (16). This implies the desired result.

We will now show that if $U_\alpha(m',m) = 0$ for all $m'$ in $M^{(1)}_\alpha$ then $m$ is in $M^{(2)}_\alpha$. Making the choices in Steps 1, 2, 3 we get $\gamma_\alpha(P_v) = ((l_v,m))$. Hence

$$U_\alpha(m',m) = \sum_{\nu \in S} [m',l_\nu]_\nu = 0 \quad \text{for all } m' \in M^{(1)}_\alpha.$$ 

Let $S$ be a finite nonempty set of primes including representatives for generators of the divisor class group of $F$ as well as those primes $\nu$ for which $\nu(a_\nu) \neq 0$ in the model (3) or $\nu(a_\nu f^2) \neq 0$ for $a_\nu f^2$ chosen in Step 1. Form the vector $\langle l_\nu \rangle \in Z_\beta$ from the $l_\nu$'s chosen in Step 3. For any $m' \in M^{(1)}_\alpha$ we have

$$\omega_m(\langle l_\nu \rangle) = \sum_{\nu \in S} [m',l_\nu]_\nu = \sum_{\nu \in S} [m',l_\nu]_\nu + \sum_{\nu \in S} [m',l_\nu]_\nu.$$

The sum over $\nu \not\in S$ is zero by (10) and the sum over all $\nu$ is zero by (18). By Proposition 3.8, $\langle l_\nu \rangle$ is in $X_\beta Y_\beta$. For each $\nu$ in $S$, we can therefore write $l_\nu = \beta(Q_\nu)l$, with $Q_\nu$ in $B(F_\nu)$ and $l$ in $L_\beta$. Then

$$\gamma_\alpha(P_v + \psi(Q_\nu)) = ((l_v,m)) + i \circ \beta(Q_\nu) = ((l,m))$$

for $\nu$ in $S$. Hence $l$ meets the conditions (11) and $m$ is in $M^{(2)}_\alpha$ by Lemma 3.5.

Conversely, if $m \in a_\nu F^2$ represents a class in $M^{(2)}_\alpha$ then by definition we can choose a global element $l$ in $F^*$ and points $P_v$ in $A(F_\nu)$ such that $\gamma_\alpha(P_v) = ((l,m))$ for all $\nu$. Hence $U_\alpha(m',m) = \sum_{\nu}[m',l_\nu]_\nu = 0$ by reciprocity.

This proves the self-duality of $M^{(1)}_\alpha/M^{(2)}_\alpha$ stated in Theorem 3.1. The proof of self-duality for $M^{(1)}_\beta/M^{(2)}_\beta$ is analogous so we omit it.

4. Examples. Throughout this section $F = k(t)$ with $k = \mathbb{Z}/2\mathbb{Z}$.

Example I. Let $A$ be the curve $y^2 + t^2xy = x^3 + t$ with discriminant $\Delta = t^{12\alpha+1}$. Then $[M^{(1)}_\alpha] = 2^\alpha$.

Proof. The bad primes are $t$ and $s = t^{-1}$. The algorithm [6] shows that $A$ has multiplicative reduction at $s$. By Proposition 2.5, $M^{(2)}_\alpha = \{0\}$ and $M^{(1)}_\beta = F_2^*/F_2^{2*}. From the point $(0,a_\delta)$ on the model (5) for $B$ we see that coset$(t)$ occurs globally in $M_\beta$. By Proposition 2.4 and the definition of $M^{(1)}_\beta$, the elements of $M^{(1)}_\beta$ can be represented by units outside $s$ and $t$. Hence we have $M_\beta = M^{(1)}_\beta = \{1,t\}F^*/F^{2*}$. Since coset$(t)$ is in particular an element of $M^{(1)}_\beta$, the elements of $M^{(1)}_\beta$ must
be orthogonal to \( t \) in the pairing of Theorem 2.1. Thus they can be represented by polynomials in \( t^{-1} \). Such polynomials are automatically in \( \Phi(F_v) \) and in \( k_v + \Phi(F_v) \) for \( v \neq s,t \). Hence these polynomials survive everywhere locally to give elements of \( M_a^{(1)} \). Conversely, any representative \( m \) for an element of \( M_a^{(1)} \) can be corrected by one of the polynomials, say \( m_i \), of the form described above to get \( m + m_i \) in \( \Phi(F_v) \) for \( v = s,t \) and in \( k_v + \Phi(F_v) \) for \( v \neq s,t \). It follows by class field theory that \( m + m_i \) is in \( \Phi(F) \). Hence \( [M_a^{(1)}] = [M_a^0] \). But \( [M_a^0] = [(F_v^*/F_v^{*2})] : M_{\beta}^0 = 2^n \) by Propositions 2.2 and 2.3 and the remark after them.

**Example II.** Taking \( n = 2 \) in the previous example, we obtain a curve \( A \) for which a second descent using the pairing \( U_a \) is needed to determine \( M_a \).

**PROOF.** As above, we have \( [M_a^0] = 4 \). One checks that locally in \( A(F_t) \) there exist points \( P \) with \( x \)-coordinates \( x(P) \) given below.

<table>
<thead>
<tr>
<th>( x(P) )</th>
<th>representative for ( \alpha(p) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( (1 + t + t^8)^{-1} )</td>
<td>( t^{-7} + t^{-5} )</td>
</tr>
<tr>
<td>( t^{-2}(1 + t^5 + t^7 + t^{10})^{-1} )</td>
<td>( t^{-3} )</td>
</tr>
</tbody>
</table>

As explained in Example I we find that \( M_a^{(1)} \) is generated by the cosets of \( t^{-7} + t^{-5} \) and of \( t^{-3} \). By (10) we get

\[
U_a(t^{-7} + t^{-5}, t^{-3}) = \left[ t^{-7} + t^{-5}, l_t \right]_s + \left[ t^{-7} + t^{-5}, l_t \right]_s,
\]

the other Artin-Schreier symbols in the definition of \( U_a \) being zero. But \( t^{-7} + t^{-5} \) is in \( \Phi(F_s) \), so pairs trivially with any \( l_s \). Hence it remains to determine \( l_t \) by the procedures of \( \S 3 \) and compute \( \left[ t^{-7} + t^{-5}, l_t \right]_s \).

**Step 1.** The element \( t^{-3} \) is already in \( a_6 F^2 \).

**Step 2.** Let \( P_t \) be the point above with \( \alpha(P_t) = \coset(t^{-3}) \).

**Step 3.** From the definition of \( \gamma_a \) in Proposition 1.4 we have

\[
\gamma_a(P_t) = \left( (t^{-2}(1 + t^5 + t^7 + t^{10})^{-1}, t^{-3} + t^7 + t^{11} + t^{17}) \right).
\]

Changing the above representative by the relations in (6) so that the second coordinate is \( t^{-3} \) we get \( \gamma_a(P_t) = ((l_t, t^{-3})) \) with

\[
l_t \equiv 1 + t^4 + t^5 + t^9 + \ldots \quad (\text{modulo } \{1,a_6\} F_t^{*2}).
\]

It follows that \( U_a(t^{-7} + t^{-5}, t^{-3}) = [t^{-7}, t^{-5}, l_t] \) in \( \Phi(F) \). Hence \( M_a = M_a^{(2)} = \{0\} \). Furthermore, by Proposition 1.5, the rank of \( A(F) \) is zero.

**Example III.** Let \( p_1, \ldots, p_n \) be distinct primes in \( k[t] \). Let \( A \) be the curve \( y^2 + p_1 \cdots p_n x y = x^3 + (p_1 \cdots p_n)^5 \) with discriminant \( \Delta = (p_1 \cdots p_n)^{11} \). Then \( M_{\beta}^{(1)} \) has order \( 2^n \) and is generated by the cosets of \( p_1, \ldots, p_n \).

**PROOF.** The bad primes are \( p_1, \ldots, p_n \) and \( s = t^{-1} \). By Proposition 2.2 and the remark after it we find that \( [(F_v^*/F_v^{*2})] : M_{\beta}^{(v)} = 1 \) for \( v = p_1, \ldots, p_n \).
Hence for $v = p_1, \ldots, p_n$ we have

$$M'^\circ = \{0\} \quad \text{and} \quad M'^\circ = F* / F*^2.$$  

By the algorithm [6], $A$ has multiplicative reduction at $s$. Hence (19) also applies for $v = s$ by Proposition 2.5. Since the elements of $M'^{(1)}$ can be represented by units outside $S$ according to Proposition 2.4, it is clear that $M'^{(1)}$ is generated by the cosets of $p_1, \ldots, p_n$ in $F* / F*^2$. Furthermore, $M'^{(1)} = \{0\}$ by Lemma 3.6(a), together with Proposition 2.4 and (19).

**Example IV.** Let $A$ be the curve

$$y^2 + xy = x^3 + t(l + t^2 + t^5)(l + t^4 + t^7),$$

with discriminant $\Delta = t(l + t^2 + t^5)(l + t^4 + t^7)$. Then a second descent using the bilinear form $U_B$ is needed to determine $M_B$.

**Proof.** At the primes $v = t, l + t^2 + t^5, l + t^4 + t^7$ the curve $A$ has multiplicative reduction by [6], so that for these $v, M'^{\circ} = \{0\}$ and $M'^{B} = F* / F*^2$ by Proposition 2.5. Running through the algorithm [6] at the prime $s = t^{-1}$ and using Proposition 2.2 and the remark after it, we find that

$$[M'^{B} : (U_s)_2 F_s^* / F_s^*] = 8.$$  

We must now hunt for the remaining elements of $M'^{B}$. The coset of $s^{18}a_6 = s^5(l + s^3 + s^5)(l + s^3 + s^7)$ lies in $M'^{B}$ globally as the image of the point of order 2 on $B$. Correcting this representative by an element of $(U_s)_6$, we find that $s$ is in $M'^{B}$. It can be checked that there is a point $P_s$ in $B(F_s)$ with x-coordinate

$$x(P_s) = s^4(1 + s^3 + s^5)(1 + s^8).$$

Hence $\beta(P_s) = \text{coset}\{1 + s^3 + s^5\}$ is in $M'^{B}$, and from $s^{18}a_6$ we also get $\text{coset}\{1 + s^3 + s^5\}$ in $M'^{B}$. The elements $s, 1 + s^3 + s^5, 1 + s^3 + s^7$ together with $(U_s)_6 F_s^* 2$ generate $\{1, s\}(U_s)_2 F_s^* 2$. Hence by (20)

$$M'^{B} = \{1, s\}(U_s)_2 F_s^* 2 / F_s^* 2.$$  

By duality $M'^{B} = ((0, s^{-1}) + \Phi(F)) / \Phi(F)$. One checks that $s^{-1} = t$ is in $\Phi(F)$ for the other bad primes. Hence coset $\{t\}$ is the only nontrivial element to survive everywhere locally in $M'^{B}$ and

$$M'^{(1)} = ((0, t) + \Phi(F)) / \Phi(F).$$

Furthermore, $M'^{(1)}$ is generated by the cosets of the bad primes $t, 1 + t^2 + t^5, 1 + t^4 + t^7$ in $F* / F*^2$.

To compute $U_B(t(1 + t^4 + t^7), t)$ we observe that the only nontrivial Artin-Schreier symbols can occur at the primes which divide $\Delta$, and at $s = t^{-1}$. Hence

$$U_B(t(1 + t^4 + t^7), t) = [\alpha_B(P_s), t]_s + \sum_{v|\Delta} [\alpha_B(P_v), t]_v.$$
Now the curve $B$ has multiplicative reduction with rational tangents at the three primes which divide $\Delta$. Hence $\alpha_B(B(F_v)) = \{0\}$ at these primes by the analog of Proposition 2.5 applied to the curve $B$ instead of the curve $A$. It follows that $U_B(t(1 + t^4 + t^7), t) = [\alpha_B(P_s), t]$ with $P_s$ chosen as in (21). Now $\alpha_B(P_s) = \coset{j-5 + 1}$ and $[s^{-5} + 1, s] = 1$.

Using the fact that $U_B$ is alternating and that $U_B(a_6, \text{anything}) = 0$ because $a_6$ occurs globally in $M_\beta$ we obtain the following table of values:

<table>
<thead>
<tr>
<th>$t$</th>
<th>$1 + t^2 + t^5$</th>
<th>$1 + t^4 + t^7$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$1 + t^2 + t^5$</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$1 + t^4 + t^7$</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Hence the only nontrivial coset of $M_\beta^{(2)}$ is represented by

$$a_6 = t(1 + t^2 + t^5)(1 + t^4 + t^7)$$

and we have $M_\beta = M_\beta^{(2)} = \{1, a_6\} F^{*2}/F^{*2}$.

As far as the rank of $A(F)$ is concerned, we note that the inequality $[M_\alpha] < [M_\alpha^{(1)}] = 2$ leads to the bound $r < 1$ by Proposition 1.5. Since it is conjectured that the actual rank differs from this bound by an even number, we suspect that $r = 1$. It would be interesting to find a point of infinite order on $A(F)$.

REFERENCES


DEPARTMENT OF MATHEMATICS, QUEENS COLLEGE (CUNY), FLUSHING, NEW YORK 11367