TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 232, 1977

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 π and a separable isogeny ψ. 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 ψ 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 π and of ψ. 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 π and of ψ 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 $k = \mathbf{Z}/2\mathbf{Z}$, 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.

AMS (MOS) subject classifications (1970). Primary 14G20, 14G25, 14H25.

(1)Partially supported by a grant from the Faculty Research Award Program of the City University of New York.

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

$$\text{(1)}\qquad \begin{tikzcd} A(F) \arrow[r, "2_A"] \arrow[d, "\pi"'] & A(F) \arrow[r, "\gamma_A"] \arrow[d, "1"'] & H \arrow[d, "j"] \\ B(F) \arrow[r, "\psi"'] & A(F) \arrow[r, "\alpha"'] & F/\Phi(F) \end{tikzcd}$$

$$\text{(2)}\qquad \begin{tikzcd} B(F) \arrow[r, "2_B"] \arrow[d, "\psi"'] & B(F) \arrow[r, "\gamma_B = (\beta, \alpha_B)"] \arrow[d, "1"'] & F^*/F^{*2} \times F/\Phi(F) \arrow[d, "\mathrm{proj}"] \\ A(F) \arrow[r, "\pi"'] & B(F) \arrow[r, "\beta"'] & F^*/F^{*2} \end{tikzcd}$$

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

$$\text{(3)}\qquad A: y^2 + a_1xy = x^3 + a_2x^2 + a_6$$

with discriminant $\Delta = a_1^6a_6$, 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

$$\text{(4)}\qquad \begin{aligned} \lambda &= s/a_1 + t/s = t^2/a_1s^2 + a_2/a_1 + a_6/a_1s^2, \\ x &= \lambda^2 + a_1\lambda + a_2 = s^2/a_1^2 + a_6/s^2, \\ y &= \lambda x + a_1a_6/s^2. \end{aligned}$$

The Frobenius isogeny π maps the curve A with model (3) to the curve

$$\text{(5)}\qquad B: y^2 + a_1^2xy = x^3 + a_2^2x^2 + a_6^2$$

by $\pi(x,y) = (x^2,y^2)$. Let ψ: $B \to A$ 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 ψ and π 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 α: $A(F) \to F/\Phi(F)$ given by*

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

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 β: $B(F) \to F^*/F^{*2}$ given by*

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

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 $E^* \xrightarrow{\theta} F^* \times a_6F^2 \to H \to 0$ where $\theta(\xi) = (\xi^2, \Phi(r\xi^{-1}D\xi)^2)$. The following lemma, which can be checked directly, shows that the second coordinate of θ 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 $f = (r\xi^{-1}D\xi)^2$ for some ξ in E^*.*

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

$$\theta(E^*) = \{(a_6^i fg^2, \Phi(f)) | f,g \in F^* \text{ and } \Phi(f) \in a_6F^2\}. \tag{6}$$

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 σ is a homomorphism with domain G, let ${}_\sigma G$ be its kernel.

PROPOSITION 1.3. (a) *We have the exact sequence*

$$0 \to {}_2A(F) \xrightarrow{\pi} {}_\psi B(F) \xrightarrow{\beta} F^*/F^{*2} \xrightarrow{i} H \xrightarrow{j} F/\Phi(F) \to F/\left(\Phi(F) + a_6F^2\right) \to 0$$

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* $m \in a_6F^2$ *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_6F^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*

$$\gamma_A(P) = \begin{cases} \left((x, a_6/a_1^2x^2)\right) & \text{if } x \neq 0, \\ \left((a_1a_6^{1/2}, a_2/a_1^2)\right) & \text{if } x = 0. \end{cases}$$

Then the following diagram commutes

(7)
$$\begin{tikzcd} B(F) \arrow[r, "\psi"] \arrow[d, "\beta"'] & A(F) \arrow[r, "1"] \arrow[d, "\gamma_A"] & A(F) \arrow[d, "\alpha"] \\ F^*/F^{*2} \arrow[r, "i"'] & H \arrow[r, "j"'] & F/\Phi(F) \end{tikzcd}$$

and the following sequence is exact

(8)
$$0 \to {}_2A(F) \to A(F) \xrightarrow{2} A(F) \xrightarrow{\gamma_A} H.$$

PROOF. First we check that γ_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 $x(P_i) = x_i \neq 0$. Solving the equations for L and A simultaneously, we find that $x_1x_2x_3 = a_6 + \nu^2$ and $x_1x_2 + x_1x_3 + x_2x_3 = a_1\nu$. Now from the definition of γ_A we find that

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

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

$$\operatorname{Ker} i = \beta({}_{\psi}B(F)) = \beta\{0_B, (0, a_6)\}.$$

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

$$\gamma_B(x, y) \equiv \begin{cases} (x, a_6/a_1^2x), & x \neq 0, \\ (a_6, a_2/a_1^2), & x = 0. \end{cases}$$

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

(9) $$\alpha_B \circ \pi = \alpha.$$

Notation. We write M_α, M_β, M_{γ_A}, M_{γ_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 $\psi \circ \pi = 2_A$, we have the exact sequence

$$0 \to {}_2A(F) \to {}_{\psi}B(F) \to \operatorname{Coker} \pi \to \operatorname{Coker} 2_A \to \operatorname{Coker} \psi \to 0.$$

The result follows from Proposition 1.1 and the Euler characteristic of this exact sequence, upon noting that $[\operatorname{Coker} 2_A] = 2^r[{}_2A(F)]$.

PROPOSITION 1.6. *Let $P = (x, y)$ be a point in $A(F)$, and let $Q = (s,t)$ be in $B(F)$. Let $\Phi(\eta) = (x + a_2)/a_1^2$. Then s and a_6 are norms from $F[\eta]$.*

PROOF. We can assume that η 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

$$sN\big[(a_1y + s) + (a_1^2x)\eta\big] = N\big[(t + a_2s + a_6) + (a_1^2s)\eta\big].$$

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:

$$[\ ,\ ): F/\Phi(F) \times F^*/F^{*2} \to \mathbf{Z}/2\mathbf{Z}.$$

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

THEOREM 2.1. *The finite group $M_\alpha \subseteq F/\Phi(F)$ 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_β is a finite group with $[M_\alpha] \geqslant [(F^*/F^{*2}): M_\beta]$. Let $M_\beta^\perp$ denote the exact orthogonal complement of M_β. Since the symbol $[a,b)$ is zero when b is a norm from $F[\Phi^{-1}(a)]$, Proposition 1.6 implies that M_α is contained in $M_\beta^\perp$ and the reverse inequality $[M_\alpha] \leqslant [M_\beta^\perp] = [(F^*/F^{*2}): M_\beta]$ must also hold. Hence $M_\alpha = M_\beta^\perp$.

Before stating the next two propositions, we recall that $A_n = \{(x,y) \in A(F) | v(x) \leqslant -2n\} \cup \{0_A\}$, for $n \geqslant 1$, 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 $A_n \xrightarrow{\sim} m^n$ by $(x,y) \to z = xy^{-1}$. Let $U_n = \{u \in F | v(u) = 0 \text{ and } v(u-1) \geqslant n\}$.

PROPOSITION 2.2. *The quotient of F^*/F^{*2} by M_β is a finite group of order*

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

M_β contains $U_{2v(a_1)}F^{*2}/F^{*2}$ with index

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

PROOF. The exactness of the following commutative diagram is clear, except possibly for the image of β in the top row.

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r, "\pi"] \arrow[d] & B_1 \arrow[r, "\beta"] \arrow[d] & U_{2v(a_1)}F^{*2}/F^{*2} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A(F) \arrow[r, "\pi"] & B(F) \arrow[r, "\beta"] & M_\beta \arrow[r] & 0
\end{tikzcd}$$

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

$$\beta(x,y) \equiv x \equiv 1 + a_1^2u^{-2}z \quad (\text{modulo } F^{*2}).$$

This proves the surjectivity of β 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 $[F^*/U_{2v(a_1)}F^{*2}] = 2[k]^{v(a_1)}$.

PROPOSITION 2.3. $[M_\alpha] \geqslant [(F^*/F^{*2}): M_\beta]$.

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

$$0 \to \operatorname{Ker}\hat{\psi} \to \operatorname{Ker}\psi \to \operatorname{Coker} i \to \operatorname{Coker}\hat{\psi} \to \operatorname{Coker}\psi \to 0$$

that $[B(F)\colon B_1][M_\alpha] = 2[A(F)/\hat{\psi}(B_1)]$. 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 $\hat{\psi}(P)$ is in $A_{v(a_1)+1}$.

Hence

$$[A(F)/\hat{\psi}(B_1)] \geqslant [A(F)\colon A_{v(a_1)+1}] = [A(F)\colon A_1][k]^{v(a_1)}$$

and this implies the desired inequality on $[M_\alpha]$.

REMARK. In practice, one determines the index $[A(F)\colon A_1]$ as follows. If $A^{\min}$ is a minimal model for A with discriminant $\Delta^{\min}$, then there is an isomorphism f: $A^{\min}(F) \to A(F)$ of the form $(x,y) \to (u^2x + r, u^3y + su^2x + t)$. Let $n = v(u)$, so that $12n = v(\Delta) - v(\Delta^{\min})$. Then f clearly induces an isomorphism $A^{\min}(F)/A^{\min}_{n+1} \xrightarrow{\sim} A(F)/A_1$. Let A_0 denote the subgroup of $A^{\min}(F)$ consisting of points whose reduction is nonsingular and let $\bar{A}_0$ be the reduced curve. Then

$$[A(F)\colon A_1] = [A^{\min}(F)\colon A_0^{\min}][\bar{A}_0(k)][k]^n$$

and $[A^{\min}(F)\colon A_0^{\min}]$ can be calculated by an algorithm of Tate [6]. A similar analysis applies to $[B(F)\colon B_1]$. Moreover, $[\bar{A}_0^{\min}(k)] = [\bar{B}_0^{\min}(k)]$ because A and B are isogenous.

PROPOSITION 2.4. *If A has good reduction and the reduced curve $\bar{A}$ is not supersingular* (*i.e., if* $v(\Delta) = v(a_1) = 0$ *on a minimal model for* A) *then*

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

PROOF. Using the above remark and Proposition 2.2 we find that $[M_\beta\colon UF^{*2}/F^{*2}] = 1$. The result for M_α follows by duality.

PROPOSITION 2.5. *Suppose that A has multiplicative reduction.*

(i) *If* $v(\Delta_A)$ *is even and* $\bar{A}$ *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

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

When this index is 2, M_β is of course F^*/F^{*2}. M_α is determined by duality.

PROPOSITION 2.6. *Suppose that the coefficients in the model* (3) *for* A *are* v*-integral, and* $v(a_1) = v(a_6) = 0$. *If* $((l,m))$ *is in the image of* γ_A *and* $v(m) = 0$ *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 $v(m) = 0$, K is an unramified quadratic extension of F. Without ambiguity, we may denote the valuation of K also by v. 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 $l = xa_6^i ab^2$, $m = a^2 + a$, with $a,b \in K^*$. But if $v(m) = 0$, then $v(a) = 0$ in the second equation, so $v(l)$ 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_α and M_β 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 α to be

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

We let

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

and we define the *second Selmer group* for α to be $M_\alpha^{(2)} = j(M_{\gamma_A}^1) \subseteq F/\Phi(F)$. It is clear from diagram (1) that $M_\alpha \subseteq M_\alpha^{(2)} \subseteq M_\alpha^{(1)}$.

Similarly, the *first Selmer group* for β is defined to be $M_\beta^{(1)} = \{a \in F^*/F^{*2} | a \in M_\beta^v \text{ for all } v\}$. We let

$$M_{\gamma_B}^1 = \left\{(a,b) \in F^*/F^{*2} \times F/\Phi(F) | (a,b) \in M_{\gamma_B}^v \text{ for all } v\right\}$$

and we define the *second Selmer group* for β to be

$$M_\beta^{(2)} = \mathrm{proj}\left(M_{\gamma_B}^1\right) \subseteq F^*/F^{*2}.$$

By diagram (2) we have $M_\beta \subseteq M_\beta^{(2)} \subseteq M_\beta^{(1)}$. In this section we prove

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

DEFINITION OF THE BILINEAR FORM ON $M_\alpha^{(1)}$. For each coset m in $M_\alpha^{(1)}$ we choose elements l_v in F_v^* as follows:

Step 1. The lemma below shows that m can be represented by an element of a_6F^2. Say $m = \mathrm{coset}\{a_6 f^2\}$.

Step 2. By definition of $M_\alpha^{(1)}$ we can find points P_v in $A(F_v)$ such that $\alpha(P_v) = m$.

Step 3. By Proposition 1.3(c) we can find l_v in F_v^* such that $\gamma_A(P_v) = ((l_v, a_6 f^2))$.

LEMMA 3.2. *Every coset m in $M_\alpha^{(1)}$ has a representative in a_6F^2.*

PROOF. We may as well assume that $m \neq 0$ and $a_6 \not\in F^2$, the other cases being trivial. Applying β to the point $(0,a_6)$ on $B(F)$, we find that coset$\{a_6\}$ is in M_β^v for all v. Since m is in M_α^v for all v, we have $[m,a_6)_v = 0$ by Theorem 2.1. Hence a_6 is a norm everywhere locally from $F_v[\Phi^{-1}(m)]$. It follows from the Hasse principle that a_6 is a norm globally from the quadratic extension $F[\Phi^{-1}(m)]$. Let m_0 represent the coset m. We may therefore write $a_6 = e^2 + ef + f^2 m_0$ for some e,f in F. But $f \neq 0$ since $a_6 \not\in F^2$. Hence $m = \mathrm{coset}\{m_0\} = \mathrm{coset}\{a_6 f^{-2}\}$ as desired.

PROPOSITION 3.3. *Associate to $m \in M_\alpha^{(1)}$ the elements $l_v \in F_v^*$ determined by Steps* 1, 2, 3 *above. Define*

$$U_\alpha \colon M_\alpha^{(1)} \times M_\alpha^{(1)} \to \mathbf{Z}/2\mathbf{Z}$$

by $U_\alpha(m',m) = \Sigma[m',l_v)_v$. Then U_α is a well-defined alternating bilinear form.

PROOF. By Proposition 1.3(c), the element l_v in Step 3 is determined up to multiplication by $\{1,a_6\}F_v^{*2}$. But this is harmless because $\{1,a_6\}F_v^{*2}$ is orthogonal to any m' in M_α^v.

Suppose in Step 2 we choose another point P_v' such that $\alpha(P_v') = \alpha(P_v) = m$. By Proposition 1.1(a) we may write $P_v' = P_v + \psi(Q_v)$ for some $Q_v \in B(F_v)$. But

$$\begin{aligned}\gamma_A(P'_v) &= \gamma_A(P_v) + \gamma_A \circ \psi(Q_v)\\ &= \big((l_v, a_6 f^2)\big) + i \circ \beta(Q_v)\\ &= \big((l_v \beta(Q_v), a_6 f^2)\big).\end{aligned}$$

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 $[m', l'_v)_v = [m', l_v)_v$ by orthogonality of M^v_α and M^v_β. This proves independence of the choice in Step 2.

Suppose in Step 1 we choose a different representative in a_6F^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 ξ 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

$$\sum_v \left[m', l_v\xi^2\right)_v = \sum_v \left[m', l_v\right)_v + \sum_v \left[m', \xi^2\right)_v$$

and the last summation is zero by reciprocity as m' and ξ^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_α 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

$$\left[m', l_v\right)_v = 0 \quad \text{for } v \notin S. \tag{10}$$

Finally, we show that U_α is alternating; that is, $U_\alpha(m,m) = 0$. We may assume that $m = \text{coset}\{a_6 f^2\}$ 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 γ_A in Proposition 1.4 we have

$$\big((l_v, a_6 f^2)\big) = \gamma_A(P_v) = \big((x_v, a_6/a_1^2 x_v^2)\big).$$

It follows from the description (6) of the relations in H that there exists an element g_v in F_v^* such that

$$l_v \equiv x_v g_v \quad \left(\text{modulo } \{1, a_6\} F_v^{*2}\right)$$

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 $g_v(a_1x_vf)^{-1}$ explicitly as a norm from the quadratic extension $F_v[\Phi^{-1}(a_6f^2)] = F_v[\Phi^{-1}(m)]$. Hence $[m,g_v(a_1x_vf)^{-1})_v = 0$. Now

$$U_\alpha(m,m) = \sum_v [m,l_v)_v = \sum_v [m,x_vg_v)_v = \sum_v [m,a_1f)_v = 0$$

by reciprocity.

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

$$U_\beta\colon M_\beta^{(1)}\times M_\beta^{(1)}\to \mathbf{Z}/2\mathbf{Z}$$

by $U_\beta(m,m') = \Sigma[l_v,m')_v$. Then U_β 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 $v \notin S$ then by Proposition 2.4 the image of α_B is $(k_v + \Phi(F_v))/\Phi(F_v)$ and M_β^v is $U_vF_v^{*2}$. Hence $[l_v,m')_v = 0$ for all $v \notin S$.

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 $m = \beta(P_v) = \text{coset}\{x_v\}$ in F_v^*/F_v^{*2} and $l_v = \alpha_B(P_v) = \text{coset}\{(x_v + a_2^2)/a_1^4\}$ in $F_v/\Phi(F_v)$. Hence

$$U_\beta(m,m) = \sum_v [l_v,m)_v = \sum_v \left[x_v/a_1^4,m\right)_v + \sum_v \left[a_2^2/a_1^4,m\right)_v.$$

The last sum is zero by reciprocity and the next to last sum is zero by the fact that $m \equiv x_v/a_1^4 \pmod{F_v^{*2}}$.

LEMMA 3.5. (a) *Let $m \in a_6F^2$ represent an element of $M_\alpha^{(1)}$. 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 $M_\alpha^{(2)}$ if and only if there exists l in F^* such that*

(11) $$((l,m)) \in M_{\gamma_A}^v \quad \text{for } v \in S \text{ and } l \in U_vF_v^{*2} \quad \text{for } v \notin S.$$

(b) *Let m represent an element of $M_\beta^{(1)}$. 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 $M_\beta^{(2)}$ if and only if there exists l in F such that*

$$(m,l) \in M_{\gamma_B}^v \quad \text{for } v \in S \text{ and } l \in k_v + \Phi(F_v) \quad \text{for } v \notin S.$$

PROOF. Suppose that m represents a class in $M_\alpha^{(2)}$. 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 $\{1,a_6\}F^{*2}$. Then the element l is in $U_vF_v^{*2}$ for $v \notin S$ by Proposition 2.6, and the conditions (11) hold.

Conversely, assuming that conditions (11) hold, we must show that $((l,m)) \in M^v_{\gamma_A}$ also for the primes v not in S in order to prove that m represents an element of $M^{(2)}_\alpha$. Since coset$\{m\}$ is an element of $M^{(1)}_\alpha$, we can find points Q_v in $A(F_v)$ such that $\alpha(Q_v) = \text{coset}\{m\}$. 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 $l_v^{-1}l \in U_vF_v^{*2}$ for $v \notin S$. By Proposition 2.4, we may find $R_v \in B(F_v)$ such that $\beta(R_v) = \text{coset}\{l_v^{-1}l\}$ for $v \notin S$. Letting $P_v = Q_v + \psi(R_v)$ we get $((l,m)) = \gamma_A(P_v)$ for $v \notin S$ 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:

$L_\alpha = \{l \in F/\Phi(F) | l \in (k_v + \Phi(F_v))/\Phi(F_v) \text{ for } v \notin S\}$,
$L_\beta = \{l \in F^*/F^{*2} | l \in U_vF_v^{*2}/F_v^{*2} \text{ for } v \notin S\}$,
$Z_\alpha = \amalg_{v\in S}F_v/\Phi(F_v)$, $Z_\beta = \amalg_{v\in S}F_v^*/F_v^{*2}$,
$X_\alpha = \amalg_{v\in S}M_\alpha^v$, $X_\beta = \amalg_{v\in S}M_\beta^v$,
$Y_\alpha = \{\langle l,l,\dots\rangle \in Z_\alpha | l \in L_\alpha\}$, $Y_\beta = \{\langle l,l,\dots\rangle \in Z_\beta | l \in L_\beta\}$.

LEMMA 3.6. (a) *The diagonal map $L_\alpha \to Z_\alpha$ is an injection with image Y_α.*
(b) *The diagonal map $L_\beta \to Z_\beta$ is an injection with image Y_β.*

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 pth power at one completion, then it is a pth power globally. One can see this by noting that $L = \{f \in F | f \in F_v^p\}$ 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 $Z_\alpha \times Z_\beta \to \mathbf{Z}/2\mathbf{Z}$ given by the sum of local Artin-Schreier symbols, Y_α and Y_β are orthogonal complements. $[Y_\beta]$ is finite and equals $[Z_\alpha/Y_\alpha]$.*

PROOF. Let J denote the idele group of F. We have the subgroups

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

Let $\mathbf{F}$ denote the image of F^* on the diagonal of J. Then the following sequence is exact:

$$(12) \qquad 0 \to J^SJ^2\mathbf{F}/\mathbf{F} \to J_SJ^2\mathbf{F}/\mathbf{F} \to Z_\beta/Y_\beta \to 0.$$

But S contains representatives for generators of the divisor class group of F, so $J_S\mathbf{F} = J$ and (12) implies that there is an isomorphism

(13) $$J/J^SJ^2\mathbf{F} \xrightarrow{\sim} Z_\beta/Y_\beta.$$

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

(14) $$F/\Phi(F) \times J/J^2\mathbf{F} \to \mathbf{Z}/2\mathbf{Z} \quad \text{by } (f,\langle a_v\rangle) \to \sum_v [f,a_v)_v.$$

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

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

PROPOSITION 3.8. *Let W_α be the group of characters w_m: $Z_\alpha \to \mathbf{Z}/2\mathbf{Z}$ of the form $w_m(\langle a_v\rangle) = \Sigma_{v\in S}[a_v,m)_v$ with $m \in M_\beta^{(1)}$. Let Ω_β be the group of characters ω_m: $Z_\beta \to \mathbf{Z}/2\mathbf{Z}$ of the form $\omega_m(\langle b_v\rangle) = \Sigma_{v\in S}[m,b_v)_v$ with $m \in M_\alpha^{(1)}$. Then*

$$\bigcap_{w_m \in W_\alpha} \operatorname{Ker} w_m = X_\alpha + Y_\alpha \quad \textit{and} \quad \bigcap_{\omega_m \in \Omega_\beta} \operatorname{Ker} \omega_m = X_\beta Y_\beta.$$

PROOF. X_α is in the kernel of each $w_m \in W_\alpha$ by Theorem 2.1. Y_α is annihilated by each $w_m \in W_\alpha$ because, if $\langle l,l,\dots\rangle \in Y_\alpha$, then

$$w_m(\langle l,l,\dots\rangle) = \sum_{v\in S} [l,m)_v = \sum_{v\notin S} [l,m)_v + \sum_{\text{all } v} [l,m)_v.$$

The sum over $v \notin S$ is zero by local duality and Proposition 2.4. The sum over all v is zero by reciprocity. Similar reasoning applies to X_β, Y_β and Ω_β, so that

$$X_\alpha + Y_\alpha \subseteq \bigcap \operatorname{Ker} w_m \quad \text{and} \quad X_\beta Y_\beta \subseteq \bigcap \operatorname{Ker} \omega_m.$$

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

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

Similarly

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

$[Z_\beta/X_\beta] = [X_\alpha]$ 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 $M_\alpha^{(1)} \xrightarrow{\sim} X_\alpha \cap$

Y_α and $M_\beta^{(1)} \simeq X_\beta \cap Y_\beta$. (In particular, this implies that the first Selmer groups are finite.) Multiplying (15) and (16) we get

$$[W_\alpha][\Omega_\beta] \leqslant [M_\alpha^{(1)}][M_\beta^{(1)}]. \tag{17}$$

But $[M_\alpha^{(1)}] = [\Omega_\beta]$ because the map $M_\alpha^{(1)} \to \Omega_\beta$ by $m \to \omega_m$ is an isomorphism by the arguments in Lemma 3.6(a). Similarly $[M_\beta^{(1)}] = [W_\alpha]$. 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 $M_\alpha^{(1)}$ then m is in $M_\alpha^{(2)}$. Making the choices in Steps 1,2,3 we get $\gamma_A(P_v) = ((l_v,m))$. Hence

$$U_\alpha(m',m) = \sum_{\text{all } v} [m',l_v)_v = 0 \quad \text{for all } m' \in M_\alpha^{(1)}. \tag{18}$$

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 v for which $v(a_i) \neq 0$ in the model (3) or $v(a_6 f^2) \neq 0$ for $a_6 f^2$ chosen in Step 1. Form the vector $\langle l_v \rangle \in Z_\beta$ from the l_v's chosen in Step 3. For any $\omega_{m'} \in \Omega_\beta$ we have

$$\omega_{m'}(\langle l_v \rangle) = \sum_{v \in S} [m',l_v)_v = \sum_{v \notin S} [m',l_v)_v + \sum_{\text{all } v} [m',l_v)_v.$$

The sum over $v \notin S$ is zero by (10) and the sum over all v is zero by (18). By Proposition 3.8, $\langle l_v \rangle$ is in $X_\beta Y_\beta$. For each v in S, we can therefore write $l_v = \beta(Q_v)l$, with Q_v in $B(F_v)$ and l in L_β. Then

$$\gamma_A(P_v + \psi(Q_v)) = ((l_v,m)) + i \circ \beta(Q_v) = ((l,m))$$

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

Conversely, if $m \in a_6 F^2$ represents a class in $M_\alpha^{(2)}$ then by definition we can choose a global element l in F^* and points P_v in $A(F_v)$ such that $\gamma_A(P_v) = ((l, m))$ for all v. Hence $U_\alpha(m', m) = \Sigma_v [m', l)_v = 0$ by reciprocity.

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

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

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

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, $M_\alpha^s = \{0\}$ and $M_\beta^s = F_s^*/F_s^{*2}$. From the point $(0,a_6)$ on the model (5) for B we see that coset$\{t\}$ occurs globally in M_β. By Proposition 2.4 and the definition of $M_\beta^{(1)}$, the elements of $M_\beta^{(1)}$ can be represented by units outside s and t. Hence we have $M_\beta = M_\beta^{(1)} = \{1,t\}F^{*2}/F^{*2}$.

Since coset$\{t\}$ is in particular an element of M_β^t, the elements of M_α^t 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 $\Phi(F_s)$ and in $k_v + \Phi(F_v)$ for $v \neq s,t$. Hence these polynomials survive everywhere locally to give elements of $M_\alpha^{(1)}$. Conversely, any representative m for an element of $M_\alpha^{(1)}$ can be corrected by one of the polynomials, say m_t, of the form described above to get $m + m_t$ 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 $m + m_t$ is in $\Phi(F)$. Hence $[M_\alpha^{(1)}] = [M_\alpha^t]$. But $[M_\alpha^t] = [(F_t^*/F_t^{*2})\colon M_\beta^t] = 2^n$ 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_α is needed to determine M_α.

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

$x(P)$	representative for $\alpha(p)$
$(1 + t + t^8)^{-1}$	$t^{-7} + t^{-5}$
$t^{-2}(1 + t^5 + t^7 + t^{10})^{-1}$	t^{-3}

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

$$U_\alpha(t^{-7} + t^{-5}, t^{-3}) = \left[t^{-7} + t^{-5}, l_t\right)_t + \left[t^{-7} + t^{-5}, l_s\right)_s,$$

the other Artin-Schreier symbols in the definition of U_α 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 §3 and compute $[t^{-7} + t^{-5}, l_t)_t$.

Step 1. The element t^{-3} is already in a_6F^2.

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

Step 3. From the definition of γ_A in Proposition 1.4 we have

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

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

$$l_t \equiv 1 + t^4 + t^5 + t^9 + \dots \qquad \left(\text{modulo } \{1, a_6\} F_t^{*2}\right).$$

It follows that $U_\alpha(t^{-7} + t^{-5}, t^{-3}) = [t^{-7}, t^{-5}, l_t)_t = 1$. Hence $M_\alpha = M_\alpha^{(2)} = \{0\}$. Furthermore, by Proposition 1.5, the rank of $A(F)$ is zero.

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

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

Hence for $v = p_1, \ldots, p_n$ we have

$$M_\alpha^v = \{0\} \quad \text{and} \quad M_\beta^v = F_v^*/F_v^{*2}. \tag{19}$$

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 $M_\beta^{(1)}$ can be represented by units outside S according to Proposition 2.4, it is clear that $M_\beta^{(1)}$ is generated by the cosets of $p_1, \ldots, p_n$ in F^*/F^{*2}. Furthermore, $M_\alpha^{(1)} = \{0\}$ by Lemma 3.6(a), together with Proposition 2.4 and (19).

EXAMPLE IV. Let A be the curve

$$y^2 + xy = x^3 + t(1 + t^2 + t^5)(1 + t^4 + t^7)$$

with discriminant $\Delta = t(1 + t^2 + t^5)(1 + t^4 + t^7)$. Then a second descent using the bilinear form U_β is needed to determine M_β.

PROOF. At the primes $v = t,\ 1 + t^2 + t^5, 1 + t^4 + t^7$ the curve A has multiplicative reduction by [6], so that for these v, $M_\alpha^v = \{0\}$ and $M_\beta^v = F_v^*/F_v^{*2}$ 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

$$\left[M_\beta^s\colon (U_s)_6 F_s^{*2}/F_s^{*2}\right] = 8. \tag{20}$$

We must now hunt for the remaining elements of M_β^s. The coset of $s^{18}a_6 = s^5(1 + s^3 + s^5)(1 + s^3 + s^7)$ lies in M_β 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_β^s. It can be checked that there is a point P_s in $B(F_s)$ with x-coordinate

$$x(P_s) = s^4(1 + s^3 + s^7)(1 + s^8). \tag{21}$$

Hence $\beta(P_s) = \text{coset}\{1 + s^3 + s^7\}$ is in M_β^s and from $s^{18}a_6$ we also get $\text{coset}\{1 + s^3 + s^5\}$ in M_β^s. 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)

$$M_\beta^s = \{1,s\}(U_s)_2 F_s^{*2}/F_s^{*2}.$$

By duality $M_\alpha^s = (\{0,s^{-1}\} + \Phi(F_s))/\Phi(F_s)$. One checks that $s^{-1} = t$ is in $\Phi(F_v)$ for the other bad primes. Hence $\text{coset}\{t\}$ is the only nontrivial element to survive everywhere locally in M_α^v and

$$M_\alpha^{(1)} = (\{0,t\} + \Phi(F))/\Phi(F).$$

Furthermore, $M_\beta^{(1)}$ 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 $U_\beta(t(1 + t^4 + t^7),t)$ we observe that the only nontrivial Artin-Schreier symbols can occur at the primes which divide Δ, and at $s = t^{-1}$. Hence

$$U_\beta\big(t(1 + t^4 + t^7),t\big) = \big[\alpha_B(P_s),t\big)_s + \sum_{v\mid\Delta} \big[\alpha_B(P_v),t\big)_v.$$

Now the curve B has multiplicative reduction with rational tangents at the three primes which divide Δ. 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 $U_\beta(t(1 + t^4 + t^7),t) = [\alpha_B(P_s),t)_s$ with P_s chosen as in (21). Now $\alpha_B(P_s) = \text{coset}\{s^{-5} + 1\}$ and $[s^{-5} + 1,s)_s = 1$.

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

	t	$1 + t^2 + t^5$	$1 + t^4 + t^7$
t	0	1	1
$1 + t^2 + t^5$	1	0	1
$1 + t^4 + t^7$	1	1	0

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 $[M_\alpha] \leqslant [M_\alpha^{(1)}] = 2$ leads to the bound $r \leqslant 1$ 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

1. J. W. S. Cassels, *Arithmetic on curves of genus* 1. I: *On a conjective of Selmer*, J. Reine Angew. Math. **202** (1959), 52–99. MR **22** #24; **22** p. 2545.

2. ______, *Arithmetic on curves of genus* 1. IV: *Proof of the Hauptvermütung*, J. Reine Angew. Math. **211** (1962), 95–112. MR **29** #1214.

3. J. S. Milne, *Weil-Châtelet groups over local fields*, Ann. Sci. École Norm. Sup. **4** (1970), 273–284. MR **43** #1996.

4. J.-P. Serre, *Corps Locaux*, Publ. Inst. Math. Univ. Nancago VIII, Hermann, Paris, 1968. MR **50** #7096.

5. J. T. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki: Vol. 1965/66, Exposé 306, Benjamin, New York, 1966. MR **34** #5605.

6. ______, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular Functions of One Variable (IV), Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin and New York, 1975, pp. 33–52.

7. ______, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.

Department of Mathematics, Queens College (CUNY), Flushing, New York 11367