COMPOSITIO MATHEMATICA

MASATO KUWATA

The field of definition of the Mordell-Weil group of an elliptic curve over a function field

Compositio Mathematica, tome 76, nº 3 (1990), p. 399-406

<http://www.numdam.org/item?id=CM_1990__76_3_399_0>

Compositio Mathematica **76**: 399–406, 1990.

The field of definition of the Mordell-Weil group of an elliptic curve over a function field

MASATO KUWATA
Department of Mathematics, Brown University, Providence, Rhode Island 02912, U.S.A.

Received 8 September 1989; accepted 20 March 1990

1. Introduction

Let $\pi: S \to C$ be an elliptic surface over a perfect field K. Let E be the fiber of S at the generic point of C. E is a curve of genus 1 defined over the function field $K(C)$ of C. In the following we assume E has a $K(C)$-rational point O, and regard E as an elliptic curve over $K(C)$. We also assume the j-invariant of E is non-constant. Let $\bar{K}$ be an algebraic closure of K. By the Mordell-Weil theorem, the group of $\bar{K}(C)$-rational points, $E(\bar{K}(C))$, is a finitely generated abelian group. Unfortunately, there is no algorithm currently known to compute this group. Though it is not guaranteed, a descent argument often works to determine the Mordell-Weil group over a number field (cf. [Sil]). In the case of a function field, however, this method does not work very well when the coefficient field is so large that the Mordell-Weil group of each fiber is no longer finitely generated.

Since $E(\bar{K}(C))$ is finitely generated, there exists a finite Galois extension L/K such that all the $\bar{K}(C)$-rational points are defined over $L(C)$. We call the smallest of these fields the *field of definition* of the Mordell-Weil group. Once we know this field K_0, it is often possible to compute $E(\bar{K}(C))$ by a descent argument. In this paper we obtain a slightly weaker result, but one which is just as useful for practical purposes. Our main result is that there is an explicitly computable integer $m > 0$ and an explicitly computable finite extension L/K such that $mE(\bar{K}(C)) = m(E(L(C))$. If $E(L(C))$ can be computed, it is easy to find $E(\bar{K}(C))$ itself. For example, the method in [K] may be very useful.

Our result has an important application to algebraic geometry. Let $S \to C$ be an elliptic surface defined over a number field K. The Néron-Severi group $NS(S, \mathbb{C})$ over the field of complex numbers $\mathbb{C}$ is spanned by

(i) The loci of generators of $E(\mathbb{C}(C))$ and the 0-section, and
(ii) a general fiber and the components of the singular fibers.

Suppose that all the components of the singular fibers are defined over K and that there exists a point of order 6 defined over $K(C)$. Choosing a base point in C, we embed C in its Jacobian $J(C)$; $j: C \hookrightarrow J(C)$. We denote by $J(C)[n]$ the subgroup of $J(C)$ consisting of all the n-torsion points. We define $K(J(C)[n])$ as the smallest extension of K such that all the points in $J(C)[n]$ are defined. With these assumptions and notations, one of our main results (Corollary 3.5) translates to:

THEOREM 1.1. *Let*

$$L = \begin{cases} K(J(C)[6]), & \text{if } genus(C) > 0, \\ K(\mu_3), & \text{if } genus(C) = 0, \end{cases}$$

and let m be the exponent of $E(\mathbb{C}(C))_{\text{tors}}$. *Then*

$$mNS(S, \mathbb{C}) = mNS(S, L).$$

In other words, any element in $mNS(S, \mathbb{C})$ *can be represented by an element that is defined over L.*

Our result tends to be simpler when $E(\bar{K}(C))$ has enough torsion points. In §2, we consider curves with full l-torsion for some prime number l. When the genus of the base curve C is 0 and l is greater than 2, L is simply a splitting field of the discriminant. When the genus of C is greater than 0, the geometry of C affects the result. In §3, we consider the case when E has only one l-torsion point. In this case, the result is not readily computable. However, if E has torsion for more than one prime, we can obtain a very simple estimate of the field of definition. In case E does not have torsion points at all, we choose a finite cover $C' \to C$ and a finite extension L/K such that $E(L(C'))$ has the necessary torsion points. We consider this case in §4.

The field L tends to be very big, but this seems to be in the nature of this problem, especially when E can have a lot of twists. It is not hard to construct a surface with a large field of definition. In fact, Swinnerton-Dyer [S-D] constructed a surface whose field of definition K_0 satisfies $[K_0 : K] = 2^7 \cdot 3^4 \cdot 5$.

The idea of this work came from the paper by Swinnerton-Dyer [S-D], in which elliptic surfaces over $\mathbb{P}^1$ are the main concern. The author thanks Professors A. Bremner, M. Rosen, J. Silverman, and G. Stevens for their useful suggestions.

2. Elliptic curves with full l-torsion

In general, the torsion subgroup of the Mordell-Weil group can be determined easily (cf. [Sil] Ch. VIII). Suppose the torsion subgroup is determined and it is

$$E(\bar{K}(C))_{\text{tors}} \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \quad (m_2 \mid m_1).$$

Extending the field K if necessary, we assume all these torsion elements are defined over $K(C)$.

In this section, we assume $m_2 \neq 1$ or the characteristic of K. Let l be a prime divisor of m_2 different from the characteristic of K. In order to state the main theorem in this section, we have to make a few definitions. For a function $f \in \bar{K}(C)$, we denote by (f) the divisor on the curve C determined by f. The discriminant Δ of E is the divisor on C determined by a minimal model for E/C. Suppose the discriminant Δ is written $\Delta = \sum n_i P_i$. We define $K(\Delta)$ as the smallest finite extension of K such that all these P_i's are defined over $K(\Delta)$. By $K((1/l)\Delta)$ we mean the smallest finite extension of $K(\Delta)$ such that all the l-th roots of all the $j(P_i)$'s in the Jacobian $J(C)$ are defined over $K((1/l)\Delta)$.

With these notations, we can state our main theorem as follows:

THEOREM 2.1. *Let L be the field $K((1/l)\Delta)$ defined as above.*

(i) *If $l > 2$, then*

$$m_1 E(L(C)) = m_1 E(\bar{K}(C)).$$

(ii) *If $l = 2$, then there exist elements $d_1, \ldots, d_r$ in L such that the extension field $M = L(d_1^{1/2}, \ldots, d_r^{1/2})$ has the property:*

$$m_1 E(M(C)) = m_1 E(\bar{K}(C)).$$

For simplicity we use the notation $F = \bar{K}(C)$. The main idea of the proof is to consider the Galois action of $G_{\bar{K}/L}$ on $E(F)/lE(F)$. The following lemma will serve as a bridge between this group and $E(F)$ itself.

LEMMA 2.2. *Let A be a finitely generated free abelian group. Suppose that a finite group G acts on A and the induced action on A/lA is trivial.*

(i) *If $l > 2$, then G acts trivially on A.*
(ii) *If $l = 2$, then there exists a basis $\{\sigma_1, \ldots, \sigma_r\}$ for A such that each element $g \in G$ acts $g(\sigma_i) = \pm\sigma_i$ for all i.*

Proof. By choosing a basis of A, we embed G into $GL(r, \mathbb{Z})$, where r is the rank of A. Let σ be an element of order n in G. Let p be a prime dividing n and let $\sigma_1 = \sigma^{n/p}$. Since σ_1 acts trivially on A/lA, we can write $\sigma_1 = 1 + l^m\tau$ for some $m \geqslant 1$ and $\tau \in M_r(\mathbb{Z})$. We assume $\tau \not\equiv 0 \bmod l$. Then we have

$$0 = (1 + l^m\tau)^p - 1 = pl^m\tau + \binom{p}{2} l^{2m}\tau^2 + \cdots + l^{pm}\tau^p.$$

When l is greater than 2, it is easy to see that the power of l dividing the coefficient of τ is the smallest among all the terms. This implies that τ is congruent to zero modulo l, which contradicts the assumption. Thus, we have $\sigma_1 = \sigma^{n/p} = 1$, which contradicts the fact that the order of σ is n. Hence σ must be 1. In the case $l = 2$, we refer to Christie [C]. □

If we take $m_1 E(F)$ as A in this lemma, the theorem follows immediately as soon as we prove that $G_{\bar{K}/L}$ acts trivially on $m_1E(F)/lm_1E(F)$. In order to prove the latter fact, we review the proof of the weak Mordell-Weil theorem. We start from the exact sequence of $G_{\bar{F}/F}$-module:

$$0 \to E[l] \to E \xrightarrow{[l]} E \to 0,$$

where $[l]$ stands for multiplication by l and $E[l]$ is the kernel of $[l]$. From this, we have the following long exact sequence:

$$\begin{aligned} 0 \longrightarrow\ & E[l](F) \longrightarrow E(F) \xrightarrow{[l]} E(F) \xrightarrow{\delta_E} \\ & H^1(G_{\bar{F}/F}, E[l]) \longrightarrow H^1(G_{\bar{F}/F}, E) \longrightarrow H^1(G_{\bar{F}/F}, E) \longrightarrow \cdots \end{aligned}$$

Since $E[l] \subset E(F)$ and thus $G_{\bar{F}/F}$ acts trivially on $E[l]$, we have

$$0 \to E(F)/lE(F) \xrightarrow{\delta_E} \mathrm{Hom}(G_{\bar{F}/F}, E[l]) \to H^1(G_{\bar{F}/F}, E).$$

Similarly we consider the exact sequence

$$1 \to \mu_l \to \bar{F}^* \xrightarrow{l} \bar{F}^* \to 1,$$

and we get

$$1 \to F^*/F^{*l} \xrightarrow{\delta_F} \mathrm{Hom}(G_{\bar{F}/F}, \mu_l) \to H^1(G_{\bar{F}/F}, \bar{F}^*).$$

The last term vanishes by Hilbert's theorem 90. So we have an isomorphism

$$\delta_F\colon F^*/F^{*l} \xrightarrow{\simeq} \mathrm{Hom}(G_{\bar{F}/F}, \mu_l).$$

With these notation we state the key lemma to prove the weak Mordell-Weil theorem.

PROPOSITION 2.3. *There is a bilinear pairing*

$$b\colon E(F)/lE(F) \times E[l] \to F^*/F^{*l}$$

satisfying for $P \in E(F)$, $T \in E[l]$, *and* $\sigma \in G_{\bar{F}/F}$

$$e_l(\delta_E(P)(\sigma), T) = \delta_F(b(P, T))(\sigma),$$

where e_l *is the Weil paring* (cf. [Sil] Ch. III).

(i) *This pairing is non-degenerate on the left.*
(ii) *Let* S *be the set of primes at which* E *has bad reduction. Then the image of the pairing lies in the subgroup of* F^*/F^{*l} *given by*

$$F(S, l) = \{b \in F^*/F^{*l} \mid \mathrm{ord}_v(b) \equiv 0 \pmod{l} \text{ for all } v \notin S\}.$$

(iii) *The pairing may be computed as follows: For each $T \in E[l]$, choose functions f_T and g_T on E defined over $L(C)$ satisfying the condition*

$$(f_T) = lT - lO, \quad f_T \circ [l] = g_T^l.$$

Then, provided $P \neq T$,

$$b(P, T) \equiv f_T(P) \pmod{F^{*l}}.$$

(iv) *The pairing b is compatible with the action of $G_{\bar{K}/L}$.*

Proof. Assertions (i) through (iii) are similar to [Sil] Ch., X Th. 1.1. As for (iv), for all $T \in E[l]$ and $\sigma \in G_{\bar{K}/L}$, we have

$$b(P^\sigma, T) = f_T(P^\sigma) = f_T(P)^\sigma = b(P, T)^\sigma$$

since T and f_T are defined over L. □

Choose generators $T_1, T_2 \in E[l]$, and we have a map

$$\begin{aligned} E(F)/lE(F) &\to \quad F(S, l) \times F(S, l) \\ P \quad &\mapsto (b(P, T_1), b(P, T_2)). \end{aligned}$$

This is an injection by (ii) and this injection is compatible with the action of $G_{\bar{K}/L}$ by (iv).

Proof of Theorem 2.1. By Lemma 2.2 we only have to show that $G_{\bar{K}/L}$ acts trivially on $E(F)/lE(F)$. Furthermore, by Proposition 2.3, we only have to show that $G_{\bar{K}/L}$ acts trivially on $F(S, l)$.

Suppose $b \in F^*$ satisfies $\mathrm{ord}_v(b) \equiv 0 \pmod{l}$ for all $v \notin S$. Then the divisor determined by b is

$$(\mathrm{b}) = \sum \alpha_i P_i + \sum l\beta_j Q_j, \qquad P_i \in S,\ Q_j \notin S.$$

Since $\sum \alpha_i j(P_i) + \sum l\beta_j j(Q_j) = 0$ in $J(C)$, we can choose suitable l-th roots of $j(P_i)$'s and we have

$$\sum \alpha_i \left(\frac{1}{l} j(P_i)\right) + \sum \beta_j j(Q_j) = 0.$$

By Abel's theorem there exists a function h whose divisor corresponds to $\sum \alpha_i((1/l)j(P_i)) + \sum \beta_j j(Q_j)$. Hence the support of the divisor of the function b/h^l is contained in the union of $\{P_i\}$ and the support of $(1/l)j(P_i)$ for all i. By the definition of L, these are defined over L. Hence $b^\sigma \equiv b \pmod{F^{*l}}$ for all $\sigma \in G_{\bar{K}/L}$. □

3. Elliptic curves with one l-torsion point

In this section, we consider the case $m_2 = 1$ and $m_1 > 1$. Let T be a torsion point of order l, a prime. Then we have an elliptic curve $E'/K(C)$ and an isogeny $\phi: E \to E'$ such that the kernel of ϕ is the group generated by T.

First we note a couple of properties of E'.

PROPOSITION 3.1. (i) *There is an l-torsion point T' in E' defined over $K(\mu_l)(C)$. The kernel of the dual isogeny $\hat{\phi}$ is the group generated by T'.*

(ii) *Let v be a place in $K(C)$. Then either both E and E' have good reduction at v, or neither does.*

Proof. The assertion (i) is the consequence of the following generalization of the Weil pairing with respect to ϕ (See [Sil] Ch. III §8 and Ex. 3.15).

LEMMA 3.2. (Generalization of the Weil pairing). *Let $\phi: E \to E'$ be an isogeny of degree l. Then there exists a pairing*

$$e_\phi: \ker \phi \times \ker \hat{\phi} \to \mu_l$$

which is bilinear, non-degenerate, and Galois invariant.

As for (ii), see [Sil] Ch. VIII. □

Now we state the main result of this section. As in §2, we assume

$$E(\bar{K}(C))_{\text{tors}} = E(K(C))_{\text{tors}} \cong \mathbb{Z}/m_1 \oplus \mathbb{Z}/m_2, \quad (m_2 \mid m_1).$$

THEOREM 3.3. *Suppose that $E(K(C))$ contains a point of order l prime to the characteristic of K and that K contains all the l-th roots of unity. Let L be the field $K((1/l)\Delta)$. Then there exists a field M such that $[M:L] = l^k$ for some k and*

$$m_1(E(M(C)) = m_1 E(\bar{K}(C)).$$

Proof. We need a generalization of Proposition 2.3.

PROPOSITION 3.4. *There is a bilinear pairing*

$$b: E'(F)/\phi(E(F)) \times E'[\hat{\phi}] \to F^*/F^{*l}.$$

satisfying for $P \in E(F)$, $T \in E'[\hat{\phi}]$, and $\sigma \in G_{\bar{F}/F}$

$$e_\phi(\delta_E(P)(\sigma), T) = \delta_F(b(P, T))(\sigma),$$

where e_ϕ is the Weil pairing.

(i) *This pairing is non-degenerate on the left.*

(ii) *Let S be the set of primes at which E' has bad reduction. Then the image of the pairing lies in the subgroup of F^*/F^{*l} given by*

$$F(S, l) = \{b \in F^*/F^{*l} \mid \operatorname{ord}_v(b) \equiv 0 \pmod{l} \text{ for all } v \notin S\}.$$

(iii) *The pairing may be computed as follows: For each $T \in E'[\hat{\phi}]$, choose function f_T and g_T on E' defined over $L(C)$ satisfying the condition*

$$(f_T) = lT - lO, \quad f_T \circ \hat{\phi} = g_T^l.$$

Then, provided $P \neq T$,

$$b(P, T) \equiv f_T(P) \pmod{F^{*l}}.$$

(iv) *The pairing b is compatible with the action of* $G_{\bar{K}/L}$.

By the same argument as in Theorem 2.1 we can show that $G_{\bar{K}/L}$ acts trivially on $E'(F)/\phi(E(F))$. In the meantime, since we have $K((1/l)\Delta_E) = K((1/l)\Delta_{E'})$ from Proposition 3.1, we get the same result on $E(F)/\hat{\phi}(E'(F))$ by exchanging the rôle of ϕ and $\hat{\phi}$. Now consider the exact sequence:

$$E'(F)/\phi(E(F)) \xrightarrow{\hat{\phi}} E(F)/lE(F) \to E(F)/\hat{\phi}(E'(F)).$$

Since all these three groups are l-torsion groups, it is easy to see if $\sigma \in G_{\bar{K}/L}$ acts on $E(F)/lE(F)$, the order of σ must be either 1 or l. Hence the assertion of the theorem follows. □

Let $K(\Delta, J(C)[l])$ be the smallest extension of $K(\Delta)$ such that all the l-torsion points in $J(C)$ are defined. When E has torsion points for two different primes, we have very simple estimate of the field of definition.

COROLLARY 3.5. *Let* l_1 *and* l_2 *be two distinct primes dividing* m_1, *neither of them is equal to the characteristic of K. Let L be the field* $K(\Delta, J(C)[l_1 l_2])$. *Then*

$$m_1 E(L(C)) = m_1 E(\bar{K}(C)).$$

Proof. Let M_1 and M_2 be the fields in Theorem 3.3 for l_1 and l_2 respectively. The assertion follows if we show $L = M_1(J(C)[l_2]) \cap M_2(J(C)[l_1])$. However, this is clear from the facts $[M_1(J(C)[l_2]):L] = l_1^r$ and $[M_2(J(C)[l_1]):L] = l_2^s$ for some r and s. □

REMARK. (1) We can make better estimate if we can compute the intersection of M_1 and M_2.

(2) If the genus of C is 0, then L equals $K(\Delta)$.

4. Elliptic curves with no torsion points

In this section we assume that $E(\bar{K}(C))_{\text{tors}} = 0$. For simplicity, we assume that the characteristic of K is neither 2 nor 3. From the previous section, our estimate of the field of definition is simplest when $E(\bar{K}(C))$ contains 2 and 3-torsion at the same time. Let F be a finite extension of $K(C)$ such that $E(F)_{\text{tors}} \supset \mathbb{Z}/6$. There exist a finite extension L/K and a curve C' defined over L such that F is a function field of the curve C'. Let m_1 be the smallest integer to kill $E(F)_{\text{tors}}$ and let M be the field $L(\Delta, J(C)[6])$. Note that here we are considering the divisors on the curve C'.

THEOREM 4.1. *With above notations, we have*

$$m_1 E(M(C)) = m_1 E(\bar{K}(C)).$$

Proof. The assertion follows from the fact that $E(M(C))$ is a subgroup of $E(M(C'))$ and $G_{\bar{K}/M}$ acts trivially on $E(M(C'))$. □

REMARK. In [S-D], Swinnerton-Dyer extends the field to have full 2-torsion points. In that case, you have to determine d_i's in Theorem 2.1. They are determined by considering the twists of the elliptic curve E. Usually it is hard to tell which method is more efficient and practical.

References

[C] M. R. Christie, Positive definite rational functions of two variables which are not the sum of three squares, *Journal of Number Theory*, 8 (1976), 224–232.

[K] Masato Kuwata, *The Canonical Height and Elliptic Surfaces*, (to appear from *Journal of Number Theory*).

[Sil] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[S-D] H. P. F. Swinnerton-Dyer, The field of definition of the Néron-Severi group, *Studies in Pure Mathematics*, 719–731.