RAMIFIED PRIMES IN THE FIELD OF DEFINITION FOR THE MORDELL-WEIL GROUP OF AN ELLIPTIC SURFACE

MASATO KUWATA

(Communicated by William Adams)

ABSTRACT. Let $\pi: X \rightarrow C$ be an elliptic surface defined over a number field k . We consider the field K in which all the sections are defined. Assuming that the j -invariant is nonconstant, K is again a number field. We describe the primes of possible ramification of the extension K/k in terms of the configuration of the points of bad fibers in C . Aside from few possible exceptions, K/k is unramified outside of the primes of bad reduction of C and the primes p for which two or more points of bad fibers become identical modulo p .

INTRODUCTION

Let $\pi: X \rightarrow C$ be a smooth minimal elliptic surface defined over a number field k . Suppose that X has a k -rational section and that the j -invariant of X is nonconstant. Let E be the fiber of X at the generic point of C . E is an elliptic curve defined over the function field $k(C)$. Let $\bar{k}$ be an algebraic closure of k . By the generalization of the Mordell-Weil theorem by Néron, the group of $\bar{k}(C)$ -rational points, $E(\bar{k}(C))$, is a finitely generated abelian group. Thus there exists a finite Galois extension K/k in which all the $\bar{k}(C)$ -rational points are defined. We call the smallest of these fields the *field of definition* of the Mordell-Weil group.

In [K] we found an upper bound for the field of definition K . The construction was quite complicated because of the nature of this problem. In this paper we try to understand K better by looking at one of the most important properties of K as a number field, namely, the primes of ramification of K . Let Σ be the set of points in C where $\pi: X \rightarrow C$ has a bad fiber. Our main result is that we can describe the primes of ramification only by the geometry of C , configuration of the points in Σ , and the types of bad fibers. As is shown in [K], the torsion points play an important role. In §1 we will define a readily computable number m , which we will call the potential exponent of the Mordell-Weil group. In many cases this is equal to the exponent of the torsion subgroup of the Mordell-Weil group of E , and it is always divisible by the exponent. With this notation, we state our main theorem.

Received by the editors April 29, 1991.

1991 *Mathematics Subject Classification*. Primary 11G35, 14J27.

Key words and phrases. Elliptic surfaces.

Main Theorem. *The field of definition K ramifies only over a subset of the union of*

- (1) *the primes that divide 2, 3, or the potential exponent m ,*
- (2) *the primes of bad reduction of the base curve C , and*
- (3) *the primes $\mathfrak{p}$ for which two or more points in the singular locus Σ becomes identical modulo $\mathfrak{p}$.*

The proof of the main theorem consists of two parts. First we construct a branched covering $\tilde{C}$ of C so that $\tilde{\pi}: X \times_C \tilde{C} \rightarrow \tilde{C}$ has the necessary torsion. Two things have to be done here. First we have to study the field of definition of the covering $\tilde{C}$. This has been done by Beckmann [B]. Secondly, we have to know what the torsion subgroup of this new surface might be. Once these are done, we can use the result of [K] to study the field of definition of the Mordell-Weil group of $X \times_C \tilde{C}$.

Our result becomes simpler when the genus of the base curve is 0, in particular, when the surface is either a rational surface or a $K3$ surface. In his series of papers [Sh1, Sh2], Shioda studied the Mordell-Weil groups of rational elliptic surfaces. He presented some examples that have interesting fields of definition. In the last section, we study one of his examples from our point of view.

1. A BRANCHED COVERING OF C

In order to use the result in [K], we need to have enough torsion points in E . Adding a torsion point to E by extending the function field is equivalent to taking a branched covering of the base curve C and constructing a fiber product of X and this covering.

Lemma 1.1. *There exists a Galois covering $\tilde{C} \rightarrow C$ that satisfies the following:*

- (1) *The generic fiber of $\tilde{\pi}: X \times_C \tilde{C} \rightarrow \tilde{C}$ contains the full 2-torsion points and the full 3-torsion points.*
- (2) *The degree of the covering is $2^k 3^\ell$ for some integers k and ℓ .*
- (3) *The branch points are contained in Σ .*

Proof. Consider $\pi: X \rightarrow C$ over $\bar{k}$. Take a finite extension of $\bar{k}(C)$ so that $E(\bar{k}(C))$ has the prescribed torsion points. Corresponding to this extension, there exists a covering $\tilde{C} \rightarrow C$. Since we are adding the full torsion points to $E(\bar{k}(C))$, the extension of the function field is Galois. Thus, the covering is Galois.

Let

$$Y^2 = X^3 + AX + B, \quad A, B \in \bar{k}(C),$$

be the minimal Weierstrass equation of $E(\bar{k}(C))$. In order to add the full 2-torsion points, it is sufficient to take the splitting field of $X^3 + AX + B = 0$. Thus, the degree is no greater than 3. As for 3-torsion points, we first take the splitting field of $3X^4 + 6AX^2 + 12BX - A^2 = 0$ to add the x coordinates of the 3-torsion points. The y coordinates are obtained by taking square roots of $X^3 + AX + B$. Thus the degree of extension is of the form $2^k 3^\ell$ for some k and ℓ . This proves the second assertion.

When we add an m -torsion point to an elliptic curve, the field ramifies only at the primes that divide m and the primes of bad reduction (cf. [Mil1, Propo-

sition 20.7]). In our situation this fact tells us that the branch points of the covering are contained in the set of points of bad fibers Σ . $\square$

When we add full 2- and 3-torsion points, it is conceivable that we might get more torsion points. These unwanted torsion points may cause a problem later, so we must know how much more torsion we might get.

Lemma 1.2. *If the curve $E(\bar{k}(\tilde{C}))$ has a p -torsion point for $p \geq 5$, then $X \rightarrow C$ has at least one bad fiber of type I_{np} or I_{np}^* for some integer n .*

Proof. It is well known that the specialization of a torsion section to each fiber is injective (cf. [Mir]). Thus, if there is a p -torsion section for $p \geq 5$, then all the bad fibers are of type I_N . Also it is known that only the zero section passes through the identity components of all the bad fibers. This implies that there exists at least one fiber of type I_{np} for some n . We constructed $\tilde{C}$ by taking double or triple coverings consecutively from C and the branch points are contained in Σ . Computing how each type of bad fibers is transformed by taking double or triple covering, we conclude that the original surface must have at least one bad fiber of type I_{np} or I_{np}^* . $\square$

Definition 1.3. Let $\mathcal{N}$ be the set of integers defined by the following property: If $X \rightarrow C$ has a bad fiber of type I_N or I_N^* , then $N \in \mathcal{N}$. Let m be the product of all the primes that divide at least one member of $\mathcal{N}$. We call m the potential exponent.

Looking at the proof of the previous lemma, we know that the exponent of $E(k(C))$ divides m .

We now study the arithmetic properties of the covering $\tilde{C}$. A recent result by Beckmann [B] is exactly what we need.

Lemma 1.4 (Beckmann). *Let K_0 be the field of definition of the covering $\tilde{C} \rightarrow C$. K_0 ramifies only at the primes of bad reduction of the covering. The primes of bad reduction are contained in a subset of the union of*

- (1) *the primes that divide 2 or 3,*
- (2) *the primes of bad reduction of the base curve C , and*
- (3) *the primes $\mathfrak{p}$ for which two or more points in the singular locus Σ becomes identical modulo $\mathfrak{p}$.*

Proof. Since the degree of the covering is $2^k 3^l$, the first statement is the result in §3 of [B] and the second is in §§4 and 5. Note that in [B] the result is stated for the field of moduli of the Galois covering, but the field of definition of the covering without the Galois action is contained in it. $\square$

Corollary 1.5. *The Jacobian $J(\tilde{C})$ of the curve $\tilde{C}$ has bad reduction only at the subset of the primes described above.*

Proof. This follows from a well-known fact that if the curve C has good reduction at $\mathfrak{p}$ then its Jacobian has good reduction at $\mathfrak{p}$ (cf. [Mil2, Theorem 8.1]).

2. PROOF OF THE MAIN THEOREM

We now prove our main theorem.

Lemma 2.1. *Let K_1 be the smallest extension of K_0 in which all the 6-torsion points of the Jacobian of $\tilde{C}$ are defined. Then any point in the generic fiber of $\tilde{\pi}: X \times_C \tilde{C} \rightarrow \tilde{C}$ is defined over K_1 after it is multiplied by $6m$.*

Proof. Since multiplying $6m$ kills all the possible torsion in $E(\bar{k}(C))$, the assertion of the lemma follows from Theorem 1.1 of [K]. $\square$

Lemma 2.2. *Let P be a point in $E(\bar{k}(C))$. Suppose that nP is defined over L and P itself is defined over its extension L_0 . Then L_0/L ramifies possibly over the primes that divide n and the primes of bad reduction of C .*

Proof. Once again, this follows from [Mil1, Proposition 20.7]. $\square$

Proof of Main Theorem. The extension K_1/K_0 ramifies possibly over the primes that divide $6m$ or the primes of bad reduction of $J(\tilde{C})$. By Corollary 1.5, the primes of bad reduction of $J(\tilde{C})$ are contained in the subset of the primes described in the theorem. Thus K_1/K_0 ramifies only over the primes described in the theorem. Finally, combining Lemmas 1.4 and 2.2, we conclude that the primes of possible ramification of the field of definition K is still in the list of primes described in the theorem. $\square$

3. SHIODA'S EXAMPLE

Let E be the elliptic curve $E: y^2 = x^3 + x + t^5$ defined over $\mathbf{Q}(t)$. In [Sh1] Shioda considered the above elliptic curve as an example of his theory for the rational elliptic surfaces (cf. [Sh2]). He obtained the following

Theorem 3.1 (Shioda). *There is a natural isomorphism*

$$E(\bar{\mathbf{Q}}(t)) \simeq \mathbf{Z}[\zeta_{20}](1/G)^{1/20}$$

that is compatible with the action of the Galois group $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Here $\zeta_{20} = e^{2\pi i/20}$ and G is an element of $\mathbf{Q}(\zeta_{20})$ given by

$$G = \frac{-11261 + 6745\sqrt{5}}{8} + \frac{-2550 + 1365\sqrt{5}}{2} \sqrt{\frac{5 + \sqrt{5}}{2}}.$$

When the base curve C is a rational curve, our main result is reduced to the following.

Corollary of Main Theorem. *Let E be an elliptic curve*

$$E: y^2 = x^3 + A(t)x + B(t), \quad A(t), B(t) \in \mathbf{Q}(t),$$

defined over $\mathbf{Q}(t)$. Let δ be the discriminant of the polynomial $\Delta(t) = 4A(t)^3 + 27B(t)^2$. Then the field of definition for the Mordell-Weil group $E(\bar{\mathbf{Q}}(t))$ is unramified outside of the primes that divides $6m\delta$.

Note that it is not hard to compute the potential exponent m in this case using the algorithm of computing the types of bad fibers (cf., for example, [Sil]).

In Shioda's example we have $\Delta(t) = 4 + 27t^{10}$ and thus $\delta = -2^{28}3^{27}5^{10}$. E has 10 bad fibers of type I_1 and one bad fiber of type II at $t = \infty$. Hence the potential exponent m for this curve is 1. Thus the field of definition K is unramified outside of the primes that divide 2, 3, or 5. Considering this result, we can predict some properties of G . For example, the norm $N_{\mathbf{Q}(\zeta_{20})/\mathbf{Q}}(G)$ must be the product of the powers of 2, 3, and 5 together with some 20th powers. In fact, calculation shows that it equals 2^{-8} . Further calculation shows that G is of the form $\frac{1}{4} \cdot (\text{unit in } \mathbf{Q}(\zeta_{20}))^5$.

ACKNOWLEDGMENT

The author would like to thank Joe Silverman for useful conversation. Also he would like to acknowledge the Symbolics Corporation for its powerful Macsyma on the 3670 computer.

REFERENCES

- [B] Sybilla Beckmann, *Ramified primes in the field of moduli of branched coverings of curves*, J. Algebra **125** (1989), 236–255.
- [K] Masato Kuwata, *The field of definition of the Mordell-Weil group of an elliptic curve over a function field*, Compositio Math. **76** (1990), 399–406.
- [Mil1] J. S. Milne, *Abelian varieties*, Arithmetic Geometry (G. Cornell and J. H. Silverman, eds.), Springer-Verlag, New York, 1986, pp. 103–105.
- [Mil2] ———, *Jacobian varieties*, Arithmetic Geometry (G. Cornell and J. H. Silverman, eds.), Springer-Verlag, New York, 1986, pp. 167–212.
- [Mir] Rick Miranda, *The basic theory of elliptic surfaces*, Dottorato di Ricerca in Matematica, Dipartimento di Matematica dell'Università di Pisa, ETS Editrice Pisa, 1989.
- [Sil] Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.
- [Sh1] Tetsuji Shioda, *The Galois representation of type E_8 arising from certain Mordell-Weil groups*, Proc. Japan Acad. Ser. A Math. Sci. **65** (1989), 195–197.
- [Sh2] ———, *Mordell-Weil lattices and Galois representation*. I, Proc. Japan Acad. Ser. A Math. Sci. **65** (1989), 268–271; II, *ibid*, 296–299; III, *ibid*, 300–303.

DEPARTMENT OF MATHEMATICS, MCGILL UNIVERSITY, 805 SHERBROOKE STREET WEST,
MONTREAL, QUEBEC H3A 2K6, CANADA

E-mail address: kuwata@gauss.math.mcgill.ca