ACTA ARITHMETICA
LXXIII.1 (1995)

Galois descent and twists of an abelian variety

by

MASANARI KIDA (Yamagata)

Introduction. It is very interesting to describe the behavior of the Mordell–Weil group of an abelian variety in a field extension and many mathematicians study this problem (for instance, see Honda [2] and Ono [7]). Recently, A. Sato [9] obtained a general result for abelian varieties with certain complex multiplication (the corollaries in Section 2).

In this paper, we shall prove a theorem (Theorem in Section 2), from which Sato's results follow. Roughly speaking, our theorem describes the relation between the Galois descent and twists (see Section 1 for their definitions) and can be considered as a geometric counterpart of Sato's.

We will use the following notation throughout this paper.

For a number field k, the separable closure is denoted by k_{s} and we assume that all algebraic extensions of k lie in k_{s}.

Let A be an abelian variety defined over k. We set, for any finite extension K of k,

$$A_K = A \times_{\mathrm{Spec}(k)} \mathrm{Spec}(K), \qquad A(K) = \mathrm{Mor}_k(\mathrm{Spec}(K), A).$$

The latter forms a group called the *Mordell–Weil group* of A over K, which is a finitely generated abelian group. In particular, the *Mordell–Weil rank*

$$\mathrm{rank}(A;K) = \dim_{\mathbb{Q}} A(K) \otimes_{\mathbb{Z}} \mathbb{Q}$$

is finite. For each $m \in \mathbb{Z}$, we denote the multiplication-by-m map on A by $[m]_A$, where the subscript A is often dropped, if no confusion can arise. The symbol $A[m]$ stands for its kernel in $A(k_{\mathrm{s}})$ and we set

$$A[l^\infty] = \bigcup_{i=1}^{\infty} A[l^i], \qquad A\langle n\rangle = \bigoplus_{l:\,\mathrm{prime},\,(l,n)=1} A[l^\infty].$$

We define the *Tate module* by

$$\mathcal{T}_l(A) = \varprojlim_n A[l^n],$$

on which the absolute Galois group $\mathit{\Gamma}_k = \mathrm{Gal}(k_{\mathrm{s}}/k)$ of k acts. Here l is a prime number. If A_1 and A_2 are abelian varieties defined over k, the natural map

$$\mathrm{Hom}_k(A_1, A_2) \to \mathrm{Hom}_{\mathit{\Gamma}_k}(\mathcal{T}_l(A_1), \mathcal{T}_l(A_2))$$

is also denoted by $\mathcal{T}_l$. Finally, we use μ_m for the group of mth roots of unity in k_{s}.

1. In this section, we recall some facts on twists and the Galois descent (the Weil functor), which will play an important role in our theorem and its proof. We do not attempt at complete generality and concentrate on what we need later. See I-§3 of Satake's monograph [8] or 1.3 of Weil's lecture notes [11] for details.

1.1. *Twist.* Let A be an abelian variety defined over a number field k and K a finite Galois extension of k in k_{s} with Galois group $\mathit{\Gamma} = \mathrm{Gal}(K/k)$. For every element ξ in the first Galois cohomology set $H^1(\mathit{\Gamma}, \mathrm{Aut}_K(A))$, there exist an abelian variety A_ξ defined over k and an isomorphism $\theta : A_\xi \to A$ defined over K such that

$$\xi_\sigma = \theta^\sigma \circ \theta^{-1} \quad \text{for all } \sigma \in \mathit{\Gamma}.$$

Here the cocycle (ξ_σ) represents ξ. The abelian variety A_ξ is called the *twist* of A by ξ and is uniquely determined by ξ up to isomorphism over k.

1.2. *The variety $R_{K/k}(A)$.* Let K/k be a finite Galois extension as above. We put $\mathit{\Gamma}_k = \mathrm{Gal}(k_{\mathrm{s}}/k)$ and $\mathit{\Gamma}_K = \mathrm{Gal}(k_{\mathrm{s}}/K)$. Thus $\mathit{\Gamma}_K$ is a normal subgroup of $\mathit{\Gamma}_K$ of finite index $d = [K : k]$. Choose a coset decomposition $\mathit{\Gamma}_k = \bigcup_{i=1}^d \mathit{\Gamma}_K \sigma_i$ so that $\sigma_1 =$ identity. This time we consider an abelian variety A defined over K. Now let $\widetilde{A} = A^{\sigma_1} \times \ldots \times A^{\sigma_d}$. Every $\tau \in \mathit{\Gamma}_k$ permutes the cosets $\mathit{\Gamma}_K \sigma_i$ by right multiplication. We denote this permutation also by τ, therefore $i^\tau = j$ if and only if $\mathit{\Gamma}_K \sigma_i \tau = \mathit{\Gamma}_K \sigma_j$. For $\tau \in \mathit{\Gamma}_k$, define an isomorphism $\varphi_\tau : \widetilde{A} \to \widetilde{A}^\sigma = A^{\sigma_1 \tau} \times \ldots \times A^{\sigma_d \tau}$ by $\varphi_\tau(g_1, \ldots, g_d) = (g_{1^\tau}, \ldots, g_{d^\tau})$. In this setting, it is known that there exist an abelian variety $R_{K/k}(A)$ defined over k and an isomorphism $\psi : R_{K/k}(A) \to \widetilde{A}$ defined over K such that

$$(*) \qquad \varphi_\tau = \psi^\tau \circ \psi^{-1} \quad \text{for all } \tau \in \mathit{\Gamma}_k.$$

We call the abelian variety $R_{K/k}(A)$ the *Galois descent* of A by the Galois extension K/k, which is unique up to isomorphism over k. Note that $\dim R_{K/k}(A) = [K : k] \cdot \dim A$. For the future use, we denote by π_i the projection of $\widetilde{A}$ onto its ith factor and define $\pi = \pi_1 \circ \psi$. They satisfy the following relations:

$$\pi_i^\tau \circ \varphi_\tau = \pi_{i^\tau} \quad \text{for all } \tau \in \mathit{\Gamma}_k; \qquad \pi_i \circ \psi = \pi^{\sigma_i}.$$

2. Let A be an abelian variety defined over a number field k and K a Galois extension of k of finite degree d in $k_{\rm s}$. As before, we set $\Gamma_k = \mathrm{Gal}(k_{\rm s}/k)$, $\Gamma_K = \mathrm{Gal}(k_{\rm s}/K)$ and choose a coset decomposition $\Gamma_k = \bigcup_{i=1}^{d} \Gamma_K \sigma_i$ such that $\sigma_1 =$ identity. In the following, we sometimes identify the set $\{\sigma_1, \ldots, \sigma_d\}$ with the Galois group $\Gamma = \mathrm{Gal}(K/k)$ via an isomorphism $\Gamma \cong \Gamma_k/\Gamma_K$.

We now impose the following two conditions on the abelian variety A and the extension K/k:

(C1) There exists a homomorphism $\iota : \mathbb{Z}[\mu_m] \to \mathrm{End}_k(A)$;
(C2) The extension K/k is abelian of exponent dividing m,

where m is an integer greater than one.

Remark. These are essentially the same conditions as Sato used in his paper [9]. See Remarks 2.1 and 2.2 in that paper for comments on these conditions.

Let χ be any element of the character group $\widehat{\Gamma}$ of Γ. By the condition (C2), we may think that the values of χ lie in $\mu_m \subset k_{\rm s}$. By (C1), the composite map $\iota \circ \chi$ gives an element of $\mathrm{Hom}(\Gamma, \mathrm{Aut}_k(A)) \subset H^1(\Gamma, \mathrm{Aut}_K(A))$. Therefore, by the result quoted in the previous section, there exist an abelian variety A_χ (= the twist by χ) and an isomorphism $\theta_\chi : A_\chi \to A$ defined over K such that

$$(\iota \circ \chi)(\sigma_i) = \theta_\chi^{\sigma_i} \circ \theta_\chi^{-1} \quad \text{for all } \sigma_i \in \Gamma.$$

On the other hand, for the variety A_K, there exist the Galois descent $R_{K/k}(A_K)$ and an isomorphism $\psi : R_{K/k}(A_K) \to \widetilde{A}_K$ satisfying the condition $(*)$.

Our theorem is as follows.

Theorem. *Let A be an abelian variety defined over a number field k and K a finite Galois extension of k in $k_{\rm s}$ with Galois group Γ. Suppose that A and K/k are subject to the conditions* (C1) *and* (C2) *stated above. Then the abelian variety $R_{K/k}(A_K)$ is isogenous over k to the product $\prod_{\chi \in \widehat{\Gamma}} A_\chi$ of the twists of A, where the product is taken over all elements in the character group $\widehat{\Gamma}$. Furthermore, the degree of the isogeny divides a power of the degree $d = [K:k]$ of the field extension.*

We give a proof of the theorem in the next section. Here we show that Sato's results follow from it.

Since we can identify $R_{K/k}(A_K)(k)$ with $A(K)$ via the map π, the following two corollaries are immediate consequences of the theorem.

Corollary 1 (A. Sato [9], Theorem 2.3 and Corollary 2.4). *The isogeny* *in the theorem induces a group isomorphism*

$$A(K) \underset{\mathbb{Z}}{\otimes} \mathbb{Q} \cong \bigoplus_{\chi\in\widehat{\Gamma}} (A_\chi(k) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}).$$

In particular, this implies $\operatorname{rank}(A;K) = \sum_{\chi\in\widehat{\Gamma}} \operatorname{rank}(A_\chi;k)$.

Some examples of explicit rank calculations by using this corollary are given in [9] and [3].

COROLLARY 2 (A. Sato [9], Corollary 2.6). *The isogeny induces an isomorphism*

$$A(K)\langle d\rangle \cong \bigoplus_{\chi\in\widehat{\Gamma}} A_\chi(k)\langle d\rangle.$$

As is well known, the *L-function* $L(A,K;s)$ of an abelian variety A (defined over a subfield k of K) over K is defined by

$$L(A,K;s) = \prod_v \det(1-(N_v)^{-s}\cdot F_v|\mathcal{T}_l(A_K))^{-1},$$

where the product runs over almost all finite places of K, and N_v and F_v denote the number of elements of the residue class field and the Frobenius endomorphism modulo v, respectively.

We have another corollary of the theorem.

COROLLARY 3 (A. Sato [9], Theorem 5.1). *Let A and K/k be as in the theorem. Then*

$$L(A,K;s) \sim \prod_{\chi\in\widehat{\Gamma}} L(A_\chi,k;s).$$

Here the symbol $\sim$ denotes coincidence up to a finite number of Euler factors.

To show this, we need the following lemmata.

LEMMA 1. *Let A_1, A_2 be abelian varieties defined over k. Then*

$$L(A_1\times A_2,k;s) \sim L(A_1,k;s)\times L(A_2,k;s).$$

Proof. It is readily seen that $\mathcal{T}_l(A_1\times A_2) \cong \mathcal{T}_l(A_1)\oplus\mathcal{T}_l(A_2)$ as Γ_k-modules. From this, the result follows. ∎

LEMMA 2. *Let A and K/k be as in the theorem. Then, as Γ_k-modules,*

$$\mathcal{T}_l(R_{K/k}(A_K)) = M_k^K\mathcal{T}_l(A_K),$$

where $M_k^K\mathcal{T}_l(A_K)$ denotes the Γ_k-module induced by the Γ_K-module $\mathcal{T}_l(A_K)$ (cf. [10]). *Consequently,*

$$L(R_{K/k}(A_K),k;s) \sim L(A,K;s).$$

Proof. Since $R_{K/k}(A_K) \cong \bigoplus_{i=1}^d A_K^{\sigma_i}$, it is readily seen that

$$\mathcal{T}_l(R_{K/k}(A_K)) = \bigoplus_{i=1}^{d} \mathcal{T}_l(A_K^{\sigma_i})$$

as Γ_K-modules.

On the other hand, it follows from the construction of $R_{K/k}(A_K)$ that $\mathcal{T}_l(\varphi_\tau)$ $(\tau \in \Gamma_k)$ gives a representation of Γ_k on $\bigoplus \mathcal{T}_l(A_K^{\sigma_i})$ that is induced by that of Γ_K on $\mathcal{T}_l(A_K)$. This shows the first half of the assertion.

Now we shall show the second half. It is, of course, enough to show that the corresponding local factors are equal. Take a finite place w of k which is unramified in K/k and at which the abelian variety A has a good reduction. Let $v_1, \ldots, v_g$ be the places of K lying above w. We set $f = d/g$ and $q = N_w$. Thus $N_{v_i} = q^f$ and also $F_{v_i} = F_w^f$ on $\mathcal{T}_l(A_K)$. Hence what remains to be shown is that

$$\det(1 - q^{-s} \cdot F_w | M_k^K \mathcal{T}_l(A_K)) = \det(1 - (q^{-s} \cdot F_w)^f | \mathcal{T}_l(A_K))^g.$$

The rest of the proof is essentially the same as that for the equality of the Artin L-function with an induced character (cf., e.g., Chapter V, Theorem 4.2(iv) in [6]). ■

Now we can prove Corollary 3.

Proof of Corollary 3. Since an L-function is isogeny-invariant, we have, by our theorem,

$$L(R_{K/k}(A_K), k, s) = L\Big(\prod_{\chi} A_\chi, k, s\Big).$$

Combining this with Lemmata 1 and 2, we get the desired relation. ■

Remark. By Faltings' isogeny theorem ([1], Corollary 2 to Theorems 3 and 4), the following equivalence holds (modulo the assertion on the degree in the theorem):

$$\text{Theorem} \Leftrightarrow \text{Corollary 3} + \text{Lemma 1} + \text{Lemma 2}.$$

In other words, our theorem follows from Sato's Theorem 5.1 plus our lemmata.

By the same theorem due to Faltings, the L-functions are equal in Corollary 3. The same is true in Lemmata 1 and 2.

3. In this section, we give a proof of our theorem, which is a geometric variant of Sato's (cf. [9], Lemma 1.2).

Let A and K/k be as in the statement of the theorem. We use the notation in the previous sections except that for short $\widetilde{\chi}_\sigma$ will be used instead of $(\iota \circ \chi)(\sigma)$. Recall that $\widetilde{\chi}_\sigma$ is defined over k.

For each $\chi \in \widehat{\Gamma}$, define the map $f_\chi : R_{K/k}(A_K) \to A_\chi$ by

$$f_\chi = \theta_\chi^{-1} \circ \Big(\sum_{i=1}^{d} \widetilde{\chi}_{\sigma_i} \circ \pi^{\sigma_i} \Big),$$

and set

$$f = \prod_{\chi \in \widehat{\Gamma}} f_\chi : R_{K/k}(A_K) \to \prod_{\chi \in \widehat{\Gamma}} A_\chi.$$

Then f is a morphism defined over k between abelian varieties of the same dimension. In fact, for any element $\tau \in \Gamma_k$, we have

$$\begin{aligned} f_\chi^\tau &= (\theta_\chi^{-1})^\tau \circ \Big(\sum_{i=1}^{d} \widetilde{\chi}_{\sigma_i} \circ \pi^{\sigma_i \tau} \Big) \\ &= (\theta_\chi^{-1})^\tau \circ \widetilde{\chi}_{\tau^{-1}} \circ \Big(\sum_{i=1}^{d} \widetilde{\chi}_{\sigma_i} \circ \pi^{\sigma_i} \Big) \\ &= \theta_\chi^{-1} \circ \Big(\sum_{i=1}^{d} \widetilde{\chi}_{\sigma_i} \circ \pi^{\sigma_i} \Big) = f_\chi. \end{aligned}$$

Define

$$\widehat{f} = \pi^{-1} \circ \sum_{\chi \in \widehat{\Gamma}} \theta_\chi : \prod_{\chi \in \widehat{\Gamma}} A_\chi \to R_{K/k}(A_K).$$

Then it follows that

$$\begin{aligned} \widehat{f} \circ f &= \pi^{-1} \circ \sum_{\chi \in \widehat{\Gamma}} \theta_\chi \circ \theta_\chi^{-1} \circ \Big(\sum_{i=1}^{d} \widetilde{\chi}_{\sigma_i} \circ \pi^{\sigma_i} \Big) \\ &= \pi^{-1} \circ \sum_{\chi \in \widehat{\Gamma}} \Big(\sum_{i=1}^{d} \widetilde{\chi}_{\sigma_i} \circ \pi^{\sigma_i} \Big) \\ &= \pi^{-1} \circ \iota(\#\Gamma) \circ \pi = \pi^{-1} \circ [d]_A \circ \pi = [d]_{R_{K/k}(A)}. \end{aligned}$$

The last equality follows from the functorial property of $R_{K/k}$ and the fact $R_{K/k}([d]_A) = [d]_{R_{K/k}(A)}$. This completes the proof. ■

Acknowledgements. I would like to express my gratitude to Professors Takashi Ono and Kevin Keating for helpful conversations during the preparation of this paper.

After finishing this paper, Professor Momose kindly informed me of Milne's paper [4] and pointed out that a similar result was proved there.

References

[1] G. Faltings, *Finiteness theorems for abelian varieties over number fields*, in: Arithmetic Geometry, G. Cornell and J. H. Silverman (eds.), Springer, 1986, 9–27.
[2] T. Honda, *Isogenies, rational points and section points of group varieties*, Japan. J. Math. 30 (1960), 84–101.
[3] M. Kida, *On the rank of an elliptic curve in elementary* 2*-extensions*, Proc. Japan Acad. 69 (1993), 422–425.
[4] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. 17 (1972), 177–190.
[5] —, *Abelian varieties*, in: Arithmetic Geometry, G. Cornell and J. H. Silverman (eds.), Springer, 1986, 103–150.
[6] J. Neukirch, *Class Field Theory*, Springer, 1986.
[7] T. Ono, *On the relative Mordell–Weil rank of elliptic quartic curves*, J. Math. Soc. Japan 32 (1980), 665–670.
[8] I. Satake, *Classification Theory of Semi-simple Algebraic Groups*, Marcel Dekker, New York, 1971.
[9] A. Sato, *The behavior of Mordell–Weil groups under field extensions*, preprint.
[10] J.-P. Serre, *Représentations linéaires des groupes finis*, deuxième éd., Hermann, Paris, 1971.
[11] A. Weil, *Adeles and Algebraic Groups*, Birkhäuser, 1982.

DEPARTMENT OF MATHEMATICAL SCIENCES
YAMAGATA UNIVERSITY
YAMAGATA, 990 JAPAN

Received on 5.12.1994
and in revised form on 7.2.1995 (2708)