KUMMER THEORY ON THE PRODUCT OF AN ELLIPTIC CURVE BY THE MULTIPLICATIVE GROUP

by D. BERTRAND

(Received 2 August, 1979)

This note extends classical results on certain Galois groups attached to one-dimensional algebraic groups. We prove that the fields arising from the division of a fixed set of rational points on the product of an elliptic curve by the multiplicative group are as "large" as possible.

1. Statement of the result. Let E be an elliptic curve defined over a number field K. We write End E for the ring of endomorphisms of E (for simplicity, we assume that all endomorphisms are defined over K). Given a prime number l, we consider:

the group μ_l of lth roots of unity, and the compositum $M_l = K(\mu_l)$ of K and the lth cyclotomic field;

the group E_l of lth torsion points on E, and the extension $K_l = K(E_l)$ they generate over K. As is well-known, K_l contains M_l.

The normal extension of K_l obtained by adjoining the coordinates of an lth division point of an element P of $E(K)$ (resp. an lth root of an element α of $K^\times$ will be denoted by $K_l((1/l)P)$ (resp. $K_l(\alpha^{1/l})$). Our aim is to determine the degree over K_l of the compositum of such fields.

THEOREM 1. *Let $P_1, \ldots, P_m$ be m elements of $E(K)$, linearly independent over* End E, *and let $\alpha_1, \ldots, \alpha_s$ be s multiplicatively independent elements of $K^\times$. There exists a number λ such that, for any prime l larger than λ, the Galois group of $K_l((1/l)P_1, \ldots, (1/l)P_m, \alpha_1^{1/l}, \ldots, \alpha_s^{1/l})$ over K_l is isomorphic to $E_l^m \times \mu_l^s$.*

The proof of this assertion will be given in section 3 below. The dependence of λ in the data of the theorem is discussed in section 2.

Theorem 1 generalizes a result of Ribet (see the appendix of [**3**]), which concerns the case $m = s = 1$. When $m = 0$, we recover the classical Kummer theory for $\mathrm{Gal}(M_l(\alpha_1^{1/l}, \ldots, \alpha_s^{1/l})/M_l)$, while the hypothesis $s = 0$ corresponds to the theory of Bashmakov ([**2**], Theorem C) on the Galois cohomology of elliptic curves (see [**5**], Theorem 2, for a partial result, due to Tate, and Ribet [**9**], for a generalization to CM abelian varieties). Both theories will in fact be used in the proof of Theorem 1.

Theorem 1 is readily seen to be equivalent to the following statement: let V be a *trivial* extension of E by the multiplicative group $\mathbf{G}_m$ (this means that, as an algebraic group over K, V is isomorphic to $E \times \mathbf{G}_m$), and let End V be the ring of endomorphisms of V (Note that, here, End V is isomorphic to End $E \times \mathbb{Z}$); let $Q_1, \ldots, Q_t$ be t elements of $V(K)$ linearly independent over End V, and, for each Q_i, let $(1/l)Q_i$ be any lth division point of Q_i; then, for $l > \lambda$, the Galois group of $K(V_l, (1/l)Q_1, \ldots, (1/l)Q_t)$ over $K(V_l)$ is isomorphic to V_l^t, where V_l denotes the group of lth torsion points on V. In connection

with the study of integrals of the third kind on E, I asked under which assumption the condition on the extension V can be removed. A complete solution of this problem has recently been given by Ribet (see [**10**]).

2. Preliminaries. *One of the motivations of the present study is the use of Kummer* theories in some problems of diophantine approximations (as, e.g., in [**1**], Chapters 1 and 7, [**5**], [**3**], [**4**], [**6**]). In this direction, it is important to obtain a bound for the constant λ appearing in Theorem 1. With this aim in mind, we now record the corollaries of Kummer theory and Bashmakov's result to be used in the course of the proof.

Throughout this paper, we assume that $P_1, \ldots, P_m, \alpha_1, \ldots, \alpha_s$ satisfy the hypotheses of Theorem 1. If $n \in [1, m]$ and $r \in [1, s]$ denote two integers, we set, for every prime number l:

$$G_l = \mathrm{Gal}(K_l/K),$$
$$M_{l,0,r} = M_l(\alpha_1^{1/l}, \ldots, \alpha_r^{1/l}),$$
$$K_{l,n,r} = K_l\left(\frac{1}{l}P_1, \ldots, \frac{1}{l}P_n, \alpha_1^{1/l}, \ldots, \alpha_r^{1/l}\right),$$

and we extend the last notation to $n = 0$ in the obvious way.

According to Kummer theory, $\mathrm{Gal}\,(M_{l,0,s}/M_l)$ is isomorphic to μ_l^s as soon as the classes of $\alpha_1, \ldots, \alpha_s$ in $K^\times/(K^\times)^l$ are multiplicatively independent. By "Cassels' remark" and the hypothesis on the α_i's (see, e.g. [**6**], p. 112), this condition holds for any prime l larger than

$$\lambda_1 = (C_K^{-1}A)^s;$$

in this formula A denotes the sum of the logarithmic Weil heights h_K of $\alpha_1, \ldots, \alpha_s$, and C_K is the minimum of $h_K(\alpha)$ as α runs through the non-torsion elements of $K^\times$. A result of Dobrowolski (see [**8**], §1) shows that C_K^{-1} is bounded from above by $C_0[(\log d)/\log\log(3d)]^3$, where d denotes the degree of K over $\mathbb{Q}$ and C_0 is an absolute constant.

We now turn to the elliptic division field $K_{l,m,0}$. Viewing the $\mathbb{F}_l$-vector space E_l as a G_l-module (under Galois action), we distinguish between the following cases:

(a) *E has no complex multiplication:* a fundamental result of Serre [**11**] then asserts the existence of a constant

$$\lambda_a = \lambda_a(E, K)$$

such that, for $l > \lambda_a$, G_l is isomorphic to $\mathrm{Aut}_{\mathbb{F}_l}(E_l)$. Unfortunately, effective upper bounds for λ_a are known only in special cases (see [**11**], Proposition 21 and 24).

(b) *End E is isomorphic to an order of the ring of integers $\mathcal{O}$ of a quadratic imaginary field F:* class field theory then implies that, for any prime l larger than some constant λ_b, G_l is isomorphic to $\mathrm{Aut}_{\mathcal{O}/l\mathcal{O}}E_l = (\mathcal{O}/l\mathcal{O})^\times$. Moreover, in view of (e.g.) the discussion in [**9**], §2, on the Frobenius endomorphisms π_v, and the fact that π_v generates $N_{K/F}v$ in $\mathcal{O}$, we

https://doi.org/10.1017/S001708950000450X Published online by Cambridge University Press

may choose

$$\lambda_b = \gamma_E^d,$$

where γ_E depends only on E, and is effectively computable.

For later purposes, we split case (b) as follows:

(b_1) *l remains prime in $\mathcal{O}$*; for $l > \lambda_b$, this implies that E_l is an irreducible G_l-module.

(b_2) *l splits in $\mathcal{O}$*, i.e. $\mathcal{O}/l\mathcal{O} \simeq (\mathbb{F}_l)^2$: for $l > \lambda_b$, E_l can then be decomposed as a direct sum of two irreducible G_l-modules $E_l^{(\chi_1)}$, $E_l^{(\chi_2)}$ upon which G_l acts via the canonical characters χ_1, χ_2 of $(\mathbb{F}_l^\times)^2$.

In each of the three cases, Bashmakov's theorem shows that $\mathrm{Gal}(K_{l,m,0}/K_l)$ is isomorphic to E_l^m as soon as the classes of $P_1, \ldots, P_m$ in $E(K)/lE(K)$ are linearly independent over $\mathrm{End}\, E/l\,\mathrm{End}\, E$. By Cassels' remark again, and the hypothesis on the P_i's (see, e.g., Masser's appendix to chapter 7 of [**1**]; [**4**], Proposition 4 and §3.1; or [**6**], chapter 5), this condition holds for any prime l larger than

$$\lambda_2 = \max(\lambda_a, (C_{E,K}^{-1} U)^{m/2}) \qquad \text{(in case (a))},$$
$$\lambda_2 = \max(\lambda_b, (C_{E,K}^{-1} U)^{m}) \qquad \text{(in case (b))};$$

in these formulae U denotes the sum of the logarithmic Néron–Tate heights $h_{E,K}$ of the points $P_1, \ldots, P_m$, and $C_{E,K}$ is the minimum of $h_{E,K}(P)$ as P runs through the non-torsion points of $E(K)$. In case (b), a result of Anderson (see [**8**], §1) shows that $C_{E,K}^{-1}$ is bounded from above by $C_E(d \log d)^3$, for some constant C_E effectively computable in terms of E. (This bound has recently been improved to $C_E d^2 (\log d)^3$ by Masser.)

A step-by-step inspection of the discussion of §3 implies:

THEOREM 2. *Theorem 1 holds with $\lambda = \max(\lambda_1, \lambda_2)$.*

In particular, Theorem 1 provides an effective result when E has complex multiplications.

3. Proof of Theorem 1. In cases (a) and (b_1) listed above, the following proof of Theorem 1 is a mere generalization of that of Ribet in [**3**]. Case (b_2), however, necessitates a new type of argument, based on the Weil pairing on E_l.

We fix the integer m and a prime $l > \lambda$, and prove Theorem 1 by induction on $r = 0, \ldots, s$. If $r = 0$, we apply Bashmakov's theorem. Assume Theorem 1 is valid for $r = s-1$. In order to conclude, it suffices to show that $\alpha_s^{1/l}$ does not belong to $K_{l,m,s-1}$. We suppose this is false, and denote by n the smallest integer (possibly 0) such that $\alpha_s^{1/l}$ lies in $K_{l,n,s-1}$.

We start by assuming $n = 0$. This means that $A_l = \mathrm{Gal}(M_{l,0,s}/M_{l,0,s-1})$ is a quotient of $B_l = \mathrm{Gal}(K_{l,0,s}/M_{l,0,s-1})$. By the induction hypothesis, $\mathrm{Gal}(K_{l,0,s-1}/K_l)$ is isomorphic to μ_l^{s-1}, which Kummer theory identifies with $\mathrm{Gal}(M_{l,0,s-1}/M_l)$. Hence, $B_l \simeq \mathrm{Gal}(K_l/M_l)$. By Kummer theory again, A_l is isomorphic to μ_l. Thus, μ_l would be a quotient of $\mathrm{Gal}(K_l/M_l)$. In case (a), the latter group is isomorphic to $\mathrm{SL}_2(\mathbb{F}_l)$, which has no quotient of order l, while the desired contradiction follows in cases (b_1) and (b_2) from a comparison of degrees.

https://doi.org/10.1017/S001708950000450X Published online by Cambridge University Press

Consequently, n is positive, and we have the tower of fields

$$K \hookrightarrow K_l \hookrightarrow K_{l,n-1,s-1} \hookrightarrow K_{l,n-1,s} \hookrightarrow K_{l,n,s} = K_{l,n,s-1},$$

which the induction hypothesis (and a comparison of degrees) show to be strictly ascending. Consider the normal subgroups

$$X = \mathrm{Gal}(K_{l,n,s}/K_{l,n-1,s}), \qquad R_l = \mathrm{Gal}(K_{l,n,s}/K_{l,n-1,s-1}),$$
$$H_l = \mathrm{Gal}(K_{l,n,s}/K_l)$$

of $J_l = \mathrm{Gal}(K_{l,n,s}/K)$, and let $Y = \mathrm{Gal}(K_{l,n-1,s}/K_{l,n-1,s-1}) = R_l/X$. Conjugation in J_l yields an action of $G_l = J_l/H_l$ on R_l, under which X is stable. We can then view X (resp. Y) as a proper submodule (resp. quotient) of the G_l-module R_l.

It is now timely to recall the map $\psi = \psi_{P_n} : R_l \to E_l$ used in the proof of Bashmakov's theorem. It associates to an element σ of R_l the well-defined lth torsion point

$$\psi(\sigma) = \sigma\left(\frac{1}{l} P_n\right) - \frac{1}{l} P_n.$$

By the standard cocycle identities, we have, for any τ in G_l

$$\psi(\tau\sigma\tau^{-1}) = \tau\psi(\sigma).$$

In other words, ψ is a homomorphism of G_l-modules, and Bashmakov's theorem asserts that it is an isomorphism. Our assumption would thus imply that the G_l-module E_l has a proper submodule $\psi(X)$. In cases (a) and (b_1), this contradicts the irreducibility of E_l.

In order to deal with case (b_2), we introduce the map $\varphi = \varphi_{\alpha_s} : Y \to \mu_l$ given by

$$\eta \mapsto \varphi(\eta) = \eta(\alpha_s^{1/l})/\alpha_s^{1/l}.$$

Since $\alpha_s^{1/l}$ does not lie in $K_{l,n-1,s-1}$, φ is bijective. Let further τ be an element of G_l. Recalling the action of G_l on Y, we obtain

$$\varphi(\tau\eta\tau^{-1}) = \tau\varphi(\eta),$$

where the right-hand side represents the Galois action of G_l on μ_l. Hence, as G_l-modules, μ_l and Y are isomorphic, and μ_l can be viewed as a quotient of R_l. But, according to the Weil pairing, the action of G_l on μ_l is given by the determinant $\chi_1\chi_2$. Since the characters χ_1 and χ_2 are non-trivial, this contradicts, for $\lambda > \lambda_b$, the structure of G_l-module of R_l obtained by lifting back (via ψ) the decomposition $E_l = E_l^{(\chi_1)} \oplus E_l^{(\chi_2)}$.

Appendix (see [**10**]). Consider the product $V = E \times \boldsymbol{G}_m$ mentioned in §1. Ribet notes that the proof in §3 only uses the following properties of V_l: $H^1(\mathrm{Gal}(K(V_l)/K), V_l) = 0$; $\mathrm{End}_{\mathrm{Gal}(K(V_l)/K)} V_l = \mathrm{End}\, V/l\,\mathrm{End}\, V$; V_l is a semi-simple $\mathrm{Gal}(K(V_l)/K)$-module. This enables him, in particular, to prove Theorem 1 when E is replaced by an abelian variety A defined over any field $\mathcal{K}$ of characteristic 0. provided the above properties hold, together with the following "axiom" (see [**10**], §1, B_4, Prop. 1.1 and Remark 2.3).

(*) *Let $P_1, \ldots, P_m$ be m elements of $A(\mathcal{K})$, linearly independent over $\mathcal{O} = \mathrm{End}\, A$. For any*

https://doi.org/10.1017/S001708950000450X Published online by Cambridge University Press

sufficiently large prime number l, the classes of $P_1, \ldots, P_m$ in A/lA are linearly independent over $\mathcal{O}/l\mathcal{O}$.

We shall here show how the arguments of §2 imply, in an effective way, the validity of (*) for all simple abelian varieties A defined over $\mathcal{K}$. Without loss of generality, we may assume that $\mathcal{K}$ is a finitely generated regular extension of a number field K. Let ρ be the rank of $\mathcal{O}$ over $\mathbb{Z}$, and let (B, τ) be the $\mathcal{K}/K$-trace of A (see [7], chapter V). Considering the $\mathcal{O}$-module $\mathcal{O}P_1 + \ldots + \mathcal{O}P_m$, we may further assume that, for some integer $n \in [1, \ldots, m]$, the points $P_1, \ldots, P_{n-1}$ belong to $\tau(B)(K)$, while the classes of $P_n, \ldots, P_m$ in $A(\mathcal{K})/\tau(B)(K)$ are linearly independent over $\mathcal{O}$. Suppose that the conclusion of (*) does not hold. By the Dirichlet box principle (see [4], Proposition 4), there exist elements $\gamma_1, \ldots, \gamma_m$ of $\mathcal{O}$, not all zero, of size $< l^{1-(1/\rho m))}$, such that

$$\gamma_1 P_1 + \ldots + \gamma_m P_m = lQ,$$

where Q belongs to $A(\mathcal{K})$. If the class of Q modulo $\tau(B)(K)$ is not zero, the quadraticity of the "geometric" height $h_{A,\mathcal{K}}$ associated to a symmetric divisor on $A(\mathcal{K})$ provides a contradiction as soon as

$$l \geq \left[C(A, \mathcal{K}) \sum_{i=n}^{m} h_{A,\mathcal{K}}(P_i) \right]^{\rho m/2}.$$

If Q belongs to $\tau(B)(K)$, then $\gamma_n, \ldots, \gamma_m$ vanish, and the quadraticity of the "arithmetic" height $h_{B,K}$ associated to a symmetric divisor on $\tau(B)(K)$ provides a contradiction as soon as

$$l \geq \left[C'(B, K) \sum_{i=1}^{n-1} h_{B,K}(P_i) \right]^{\rho m/2}.$$

(In these formulae, C and C' denote positive numbers depending only on A and $\mathcal{K}$.)

The author wishes to thank J. Coates, K. Ribet and the referee for several helpful remarks.

REFERENCES

1. A. Baker and D. Masser, *Transcendence theory: advances and applications* (Academic Press, 1977).

2. M. Bashmakov, The cohomology of abelian varieties over a number field, *Russian Math. Surveys* **27** (1972), 25–70.

3. D. Bertrand, Sous-groupes à un paramètre p-adique de variétés de groupe, *Invent. Math.* **40** (1977), 171–193.

4. D. Bertrand, Approximations diophantiennes p-adiques sur les courbes elliptiques admettant une multiplication complexe, *Compositio Math.* **37** (1978), 21–50.

5. J. Coates, An application of the division theory of elliptic curves to diophantine approximation, *Invent. Math.* **11,** (1970), 167–182.

6. S. Lang, *Elliptic curves: diophantine analysis* (Springer, 1978).

7. S. Lang, *Diophantine geometry* (Wiley-Interscience, 1962).

8. D. Masser, Some results in transcendence theory, Journées arithmétiques de Luminy, 1978, *Asterisque* **61.**

9. K. Ribet, Dividing rational points on abelian varieties of CM-type, *Compositio Math.* **33** (1976), 69–74.

10. K. Ribet, Kummer theory on extensions of abelian varieties by tori, *Duke Math. J.* **46** (1979), 745–761.

11. J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

Centre de Mathématiques de
L'Ecole Polytechnique
91128 Palaiseau Cedex
France

https://doi.org/10.1017/S001708950000450X Published online by Cambridge University Press