ON THE STRUCTURE OF THE MORDELL-WEIL GROUPS OF THE JACOBIANS OF CURVES DEFINED BY $y^n = f(x)$

Hyunsuk Moon

ABSTRACT. Let A be an abelian variety defined over a number field K. It is proved that for the composite field K_n of all Galois extensions over K of degree dividing n, the torsion subgroup of the Mordell-Weil group $A(K_n)$ is finite. This is a variant of Ribet's result ([7]) on the finiteness of torsion subgroup of $A(K(\zeta_\infty))$. It is also proved that for the Jacobians of superelliptic curves $y^n = f(x)$ defined over K the Mordell-Weil group over the field generated by all nth roots of elements of K is the direct sum of a finite torsion group and a free $\mathbb{Z}$-module of infinite rank.

Let K be a number field of finite degree. Let A be a nonzero abelian variety defined over K. For an extension M over K, we denote the group of M-rational points by $A(M)$ and its torsion subgroup by $A(M)_{\text{tors}}$. We call $A(M)$ the Mordell-Weil group of A over M. It is well-known that $A(M)$ is a finitely generated abelian group for a finite algebraic extension M of K; then the Mordell-Weil rank means the number of generators of the torsion-free part of $A(M)$.

Frey and Jarden ([1]) have asked whether the Mordell-Weil group of every nonzero abelian variety A defined over K has infinite Mordell-Weil rank over the maximal abelian extension K^{ab} of K. Here, the Mordell-Weil rank of A over an arbitrary M means $\dim_{\mathbb{Q}}(A(M) \otimes_{\mathbb{Z}} \mathbb{Q})$. They proved that for elliptic curves E defined over $\mathbb{Q}$, the Mordell-Weil group $E(\mathbb{Q}^{\text{ab}})$ has infinite rank. In [3], [12], [4], this is generalized to the Jacobians of hyperelliptic curves defined over $\mathbb{Q}$. In fact, they showed the infiniteness of the Mordell-Weil rank for certain elementary abelian 2-extensions over $\mathbb{Q}$ and, in [4], we studied more precise structures of the Mordell-Weil groups in addition to the rank. Murabayashi [6] generalized it to the Jacobians of superelliptic curves $y^p = f(x)$, where p is an arbitrary prime number, by showing the infiniteness of the rank for certain elementary abelian p-extensions over $\mathbb{Q}(\zeta_p)$. Rosen and Wong [9] proved the infiniteness of the rank for the Jacobian of any curve that can be realized over K as a cyclic geometrically irreducible cover of $\mathbb{P}^1$. This implies in particular the conjecture of Frey and Jarden is affirmative for

any geometrically irreducible, principally polarized abelian surface defined over K. Recently, Sairaiji and Yamauchi [10] proved the conjecture of Frey and Jarden for the Jacobians of non-singular projective curves defined over K under the assumption that the curves have infinitely many K^{ab}-rational points. Im and Larsen [2] proved the infiniteness of the Mordell-Weil rank for abelian varieties over any fields which have topologically cyclic absolute Galois groups and are not algebraic over finite fields. Our aim in this paper is to give another proof of Rosen-Wong's result in the case of the Jacobians of superelliptic curves together with slightly more precise information on the structure of the Mordell-Weil group.

Throughout this paper, n is an integer ≥ 2. Our main theorem is the following:

Theorem 1. *Let C be a smooth projective curve of genus ≥ 1 which is the smooth compactification of an affine plane curve defined by the equation $y^n = f(x)$ with coefficients in K, and let J be its Jacobian variety. Suppose that C has a K-rational point. Let $M = K(\sqrt[n]{m} \mid m \in \mathcal{O}_K)$, where $\mathcal{O}_K$ is the ring of integers of K. Then the Mordell-Weil group $J(M)$ is the direct sum of a finite torsion group and a free $\mathbb{Z}$-module of infinite rank.*

Remark. By definition, M contains a primitive nth root ζ_n of unity. In general, M is not abelian over K but is abelian over $K(\zeta_n)$.

The key ingredient in the proof is the following variant of Ribet's result ([7]) which may be of some interest in its own right.

Proposition 2. *Let K be a number field and let K_n be the composite field of all Galois extensions over K of degree dividing n. Then for any abelian variety A over K, the torsion group $A(K_n)_{\mathrm{tors}}$ is finite.*

Proof. It is sufficient to show that there exist integers p_0 and N_0 such that for any prime number p and integer $m \geq 1$,
(i) if $p \geq p_0$, then $A(K_n)$ does not contain a point of order p, and
(ii) if $p < p_0$ and $p^m \geq N_0$, then $A(K_n)$ does not contain a point of order p^m.

Consider the following Galois representation

$$\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(A[p^m]) \simeq \mathrm{GL}_{2g}(\mathbb{Z}/p^m\mathbb{Z}),$$

where g is the dimension of A. Then by Serre (cf. [11], p. 6), there exists an integer $c = c(A) \geq 1$, independent of p and m, such that the image of ρ contains Z^c, where Z is the center of $\mathrm{GL}_{2g}(\mathbb{Z}/p^m\mathbb{Z})$ and Z^c is the group of cth power elements of Z. If we let $C := \mathrm{Im}(\rho) \cap Z$, then $C \supset Z^c$ and hence

$$(\text{exponent of } C) \geq \begin{cases} \max\{\frac{p-1}{(c,p-1)}, \frac{p^{m-1}}{(c,p^{m-1})}\} & \text{if } p \neq 2, \\ \frac{2^{m-2}}{(c,2^{m-2})} & \text{if } p = 2. \end{cases}$$

Take integers p_0 and N_0 which satisfy

$$\frac{p_0 - 1}{c} > n \ \text{ and } \ \frac{N_0}{cp_0} > n.$$

Then we have

$$(\text{exponent of } C) \ > \ n$$

if p and m are the same as in (i), (ii).

Let p and m be the same as in (i), (ii) and let P be an element of $A(\overline{K})$ of order p^m ($m = 1$ in case (i)). We denote the field generated by the coordinates of P over K by $K(P)$ and its Galois closure over K by $K(P)^{\mathrm{Gal}}$. We also denote by $K(A[p^m])$ the field obtained by adjoining all coordinates of p^m-torsion points of A. Now, we show that $K(P)^{\mathrm{Gal}}$ is not contained in K_n. Let $G := \mathrm{Im}(\rho) = \mathrm{Gal}(K(A[p^m]/K))$, $H_P := \mathrm{Gal}(K(A[p^m])/K(P)^{\mathrm{Gal}}) \subset G$, $G_P := \mathrm{Gal}(K(P)^{\mathrm{Gal}}/K) = G/H_P$. Since the group H_P acts on P trivially and the action of a scalar matrix ($\neq 1$) is not trivial, we have $H_P \cap C = 1$, and hence C embeds into G_P by the canonical projection $G \twoheadrightarrow G_P$. Therefore the exponent of G_P is greater than n. On the other hand, the exponent of $\mathrm{Gal}(K_n/K)$ is n. We conclude that there cannot exist a surjection $\mathrm{Gal}(K_n/K) \twoheadrightarrow G_P$, and hence $P \notin A(K_n)_{\mathrm{tors}}$. $\square$

Remarks. (1) The above proposition remains true if we replace the definition of K_n by the composite field $K_{(n)}$ of all extensions over K of degree $\leq n$, because we have $K_{(n)} \subset K_N$ with $N = n!$.
(2) A proof of the Proposition which uses a different method is given in [5].

In [4], we showed that the Mordell-Weil group with finite torsion group has free $\mathbb{Z}$-module structure modulo torsion:

Proposition 3. *Let A be an abelian variety over a number field K. Let M be a Galois extension of K such that $A(M)_{\mathrm{tors}}$ is finite. Then the group $A(M)/A(M)_{\mathrm{tors}}$ is a free $\mathbb{Z}$-module of at most countable rank.*

Proof of Theorem 1. We may assume that C is a smooth compactification of the affine plane curve $C_0 : y^n = f(x)$, where $f(x)$ is a polynomial with coefficients in $\mathcal{O}_K$. Let P_0 be a K-rational point of C. Let $j : C \to J$ be the embedding defined over K such that $j(P_0) = O$, where O is the identity point of J. By Propositions 2 and 3, it only remains to show that $J(M)$ is not finitely generated. If $J(M)$ is finitely generated, then it is equal to $J(L)$ for some finite extension L/K. Indeed, such L is constructed by adjoining to K all coordinates of a finite set of generators of $J(M)$. Then we have the

following commutative diagram:

$$
\begin{array}{ccc}
C_0(M) & \hookrightarrow & J(M) \\[2mm]
\| & & \| \\[2mm]
C_0(L) & \hookrightarrow & J(L)
\end{array}
$$

Here, the left hand equality follows because $C_0(M) = C_0(\overline{K}) \cap J(M) = C_0(\overline{K}) \cap J(L) = C_0(L)$. By Siegel's theorem ([8], Chap. 8, Thm. 2.4), $C_0(L)$ contain only finitely many integral points. This contradicts the fact that the set $C_0(M)$ contains the infinite set $\{(x, \sqrt[n]{f(x)}) \mid x \in \mathcal{O}_K\}$ of integral points. □

References

[1] G. Frey and M. Jarden, *Approximation theory and the rank of abelian varieties over large algebraic fields*, Proc. London Math. Soc. **28** (1974), 112–128.

[2] B. Im and M. Larsen, *Abelian varieties over cyclic fields*, Amer. J. Math. **130** (2008), 1195–1210.

[3] H. Imai, *On the rational points of some Jacobian varieties over large algebraic number fields*, Kodai Math. J. **3** (1980), 56–58.

[4] H. Moon, *On the Mordell-Weil groups of Jacobians of hyperelliptic curves over certain elementary abelian 2-extensions*, Kyungpook Math. J. **49** (2009), 419–424.

[5] ———, *On the structure of Mordell-Weil groups over infinite number fields*, Surikaisekikenkyusho Kokyuroku **1639** (2009), 56–60.

[6] N. Murabayashi, *Mordell-Weil rank of the Jacobians of curves defined by $y^p = f(x)$*, Acta Arith. **64** (1993), 297–302.

[7] K. Ribet, *Torsion points of abelian varieties in cyclotomic extensions*, appendix to N. Katz and S. Lang, *Finiteness theorems in geometric classfield theory*, Enseign. Math. (2) **27**(1981), no. 3-4, 285–319.

[8] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, 1983.

[9] M. Rosen and S. Wong, *The rank of abelian varieties over infinite Galois extensions*, J. Number Theory **92** (2002), 182–196.

[10] F. Sairaiji and T. Yamauchi, *The ranks of Jacobian varieties over the maximal abelian extensions of algebraic number fields: Toward Frey-Jarden's conjecture*, preprint.

[11] J-P. Wintenberger, *Démonstration d'une conjecture de Lang dans des cas particuliers*, J. reine angew. Math. **553** (2002), 1–16

[12] J. Top, *A remark on the rank of Jacobians of hyperelliptic curves over $\mathbb{Q}$ over certain elementary Abelian 2-extension*, Tohoku Math. J. **40** (1988), 613–616.

Hyunsuk Moon: Department of Mathematics, College of Natural Sciences Kyungpook National University, Daegu 702-701, KOREA

e-mail address: hsmoon@knu.ac.kr