KYUNGPOOK Math. J. 49(2009), 419-424

# On the Mordell-Weil Groups of Jacobians of Hyperelliptic Curves over Certain Elementary Abelian 2-extensions

Hyunsuk Moon
*Department of Mathematics, College of Natural Sciences, Kyungpook National University, Daegu 702-701, Korea*
*e-mail* : hsmoon@knu.ac.kr

Abstract. Let $J$ be the Jacobian variety of a hyperelliptic curve over $\mathbb{Q}$. Let $M$ be the field generated by all square roots of rational integers over a finite number field $K$. Then we prove that the Mordell-Weil group $J(M)$ is the direct sum of a finite torsion group and a free $\mathbb{Z}$-module of infinite rank. In particular, $J(M)$ is not a divisible group. On the other hand, if $\widetilde{M}$ is an extension of $M$ which contains all the torsion points of $J$ over $\overline{\mathbb{Q}}$, then $J(\widetilde{M}^{\text{sol}})/J(\widetilde{M}^{\text{sol}})_{\text{tors}}$ is a divisible group of infinite rank, where $\widetilde{M}^{\text{sol}}$ is the maximal solvable extension of $\widetilde{M}$.

## 1. Introduction

Let $K$ be a number field. 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 $A(M)$ is the Mordell-Weil group of $A$ over $M$. In [1], Frey and Jarden 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 $K^{\text{ab}}$ of $K$. They proved that for elliptic curves $E$ defined over $\mathbb{Q}$, the Mordell-Weil group $E(\mathbb{Q}^{\text{ab}})$ has infinite rank. Imai [3] and Top [7] generalized independently this result to the Jacobian variety of a hyperelliptic curve defined over $\mathbb{Q}$. In fact, they showed the infiniteness of the Mordell-Weil rank for certain elementary abelian 2-extensions over $\mathbb{Q}$. Our aim in this paper is to give yet another proof of this result. Furthermore, our theorem gives slightly more precise information on the structure of the Mordell-Weil group than [3] and [7]. In addition to this result, we exhibit some cases where, over certain larger fields, the Mordell-Weil groups modulo torsion are infinite-dimensional $\mathbb{Q}$-vector spaces.

Our main theorem is the following:

**Theorem 1.** *Let $C$ be a hyperelliptic curve of genus at least 1 defined over $\mathbb{Q}$ and let $J$ be its Jacobian variety. Suppose that $C$ has a $\mathbb{Q}$-rational point. Let $K$ be a finite number field, and let $M = K(\sqrt{m} \mid m \in \mathbb{Z})$ be the field generated by all square roots of rational integers over $K$. Then the group $J(M)$ is the direct sum of a finite*

Received February 8, 2008; accepted April 17, 2008.
2000 Mathematics Subject Classification: 11G10, 11G05.
Key words and phrases: Mordell-Weil groups, hyperelliptic curves.
This research was suppoted by Kyungpook National University Research Fund, 2008.

*torsion group and a free $\mathbb{Z}$-module of infinite* (*countable*) *rank.*

In [1], [3], [7], the Mordell-Weil rank of $A$ over $M$ seems to mean $\dim_{\mathbb{Q}}(A(M)\otimes_{\mathbb{Z}}\mathbb{Q})$. However, for a $\mathbb{Z}$-module $X$, that $\dim_{\mathbb{Q}}(X\otimes_{\mathbb{Z}}\mathbb{Q})=\infty$ does not necessarily imply that $X$ modulo torsion is a free $\mathbb{Z}$-module of infinite rank (Example: $X=\mathbb{Q}^{\oplus\infty}$). Thus our statement above gives more precise information on the structure of $J(M)$ than those of [1], [3], [7].

This theorem will be proved in Section 2. Two key ingredients in our proof are the following results of Ribet and Siegel.

**Theorem 2**(Ribet, [5])**.** *Let $K(\zeta_\infty)$ be the field obtained by adjoining to $K$ all roots of unity. Then for any abelian variety $A$ over $K$, the group $A(K(\zeta_\infty))_{\mathrm{tors}}$ is finite.*

This is proved by showing that the $p$-primary part of $A(K(\zeta_\infty))_{\mathrm{tors}}$ vanishes for almost all $p$ and is finite for all $p$. In Theorem 1, since $M\subset K(\zeta_\infty)$, the theorem of Ribet guarantees the finiteness of torsion subgroup $J(M)_{\mathrm{tors}}$.

**Remark.** We can generalize Theorem 1 for hyperelliptic curves $C$ defined over an arbitrary finite number field $K$, if we could prove that $J(M)_{\mathrm{tors}}$ is finite for $M=K(\sqrt{m};\ m\in\mathcal{O}_K)$, where $\mathcal{O}_K$ is the ring of integers of $K$.

**Theorem 3**(Siegel, cf. [6])**.** *For an affine curve $C_0\subset\mathbb{A}^n$ of genus at least 1 over $K$, the group of integer points $C_0(\mathcal{O}_K)$ is finite.*

This is proved by using techniques for the theory of Diophantine approximation.

**Remark.** To prove Theorem 1 for curves $C$ of genus $\geq 2$, we may appeal to Faltings' theorem [2] (= Mordell's conjecture) instead of Siegel's theorem.

**Acknowledgment.** The author would like to thank Professor Akio Tamagawa for helpful comments. In particular, he pointed out that $M_0/K$ in Lemma 4 needs the assumption of Galois by providing a nice counterexample.

## 2. Proof of theorem 1

First, we prove a few algebraic lemmas. Let $X$ be a $\mathbb{Z}$-module. For a submodule $Y\subset X$, the saturation $Y^\sim$ of $Y$ in $X$ is defined by

$$Y^\sim=\{x\in X\mid ax\in Y \text{ for some nonzero integer } a\}.$$

We call $Y$ a saturated subgroup of $X$ if $Y=Y^\sim$. Note that $Y$ is a saturated subgroup if and only if the quotient group $X/Y$ is torsion-free.

**Lemma 4.** *Let $A$ be an abelian variety over $K$. Let $M_0$ be a Galois extension of $K$ such that $A(M_0)_{\mathrm{tors}}$ is finite. We denote the exponent of $A(M_0)_{\mathrm{tors}}$ by $N$. Let $L$ be a finite extension of $K$ contained in $M_0$. Then the saturation $A(L)^\sim$ of $A(L)$ in $A(M_0)$ is contained in*

$$\frac{1}{N}A(L):=\{P\in A(M_0)\mid NP\in A(L)\}.$$

*Proof.* Let $P$ be an element of $A(L)^{\sim}$ such that $nP \in A(L)$ for some nonzero integer $n$. Let $\sigma$ be an element of $\mathrm{Gal}(M_0/L)$. Then $P^{\sigma} - P$ is an $n$-torsion element of $A(M_0)$ since $n(P^{\sigma} - P) = (nP)^{\sigma} - nP = O$. Hence $n|N$, and also we have $NP \in A(L)$. □

**Lemma 5.** *Let $Y$ be a finitely generated abelian group. Let $Z$ be a saturated subgroup of $Y$. Then there exists a free subgroup $Z'$ of $Y$ such that*

$$Y = Z \oplus Z'.$$

*Proof.* Let $Z$ be a saturated subgroup of $Y$. Then it follows that the quotient group $Y/Z$ is a free $\mathbb{Z}$-module since it is a finitely generated torsion-free abelian group. If we take a basis $\{z_1' + Z, z_2' + Z, \cdots, z_r' + Z\}$ for $Y/Z$, and a basis $\{z_1, \cdots, z_l\}$ for $Z$, then $\{z_1, \cdots, z_l, z_1', \cdots, z_r'\}$ is a basis for Y. Hence we have $Y = Z \oplus Z'$ with $Z' := \langle z_1', \cdots, z_r' \rangle$. □

**Lemma 6.** *Let $X$ be a countably generated torsion-free abelian group. Let $(Y_i)_{i \geq 1}$ be an increasing sequence of finitely generated subgroups $Y_i$ of $X$ such that $X = \cup Y_i$. If there exists an integer $N \geq 1$ such that $Y_i^{\sim} \subset \dfrac{1}{N} Y_i$ for all $i$, then $X$ is a free $\mathbb{Z}$-module of countable rank.*

*Proof.* By the definition of saturation, we have $Y_1^{\sim} \subset Y_2^{\sim} \subset \cdots$, so $X = \cup_{i=1}^{\infty} Y_i^{\sim}$. Since $Y_i^{\sim} \subset \dfrac{1}{N} Y_i$, the saturation $Y_i^{\sim}$ is also a finitely generated subgroup of $X$ for all $i$. Using Lemma 5, we have $Y_i^{\sim} = Y_{i-1}^{\sim} \oplus (Y_{i-1}^{\sim})'$ for some free group $(Y_{i-1}^{\sim})'$. Hence any basis of $Y_{i-1}^{\sim}$ extends to a basis of $Y_i^{\sim}$. Therefore $X$ is a free $\mathbb{Z}$-module of countable rank. □

Lemmas 4 and 6 imply the following:

**Proposition 7.** *Let $A$ be an abelian variety over a finite number field $K$. Let $M_0$ be a Galois extension of $K$ such that $A(M_0)_{\mathrm{tors}}$ is finite. Then the group $A(M_0)/A(M_0)_{\mathrm{tors}}$ is a free $\mathbb{Z}$-module of at most countable rank.*

*Proof.* Clear. □

*Proof of theorem 1.* We may assume that $C$ is a smooth compactification of the affine plane curve $C_0 : y^2 = f(x)$, where $f(x)$ is a separable polynomial with integer coefficients. Let $P_0 = (\infty, \infty)$ be the point at infinity on $C$, which is rational over $\mathbb{Q}$. Let $j : C \to J$ be the embedding defined over $K$ such that $j(P_0) = O$, the identity point of $J$. Since $J(K(\zeta_{\infty}))_{\mathrm{tors}}$ is finite by Ribet, $J(M)_{\mathrm{tors}}$ is also finite. Then, by Proposition 7, 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:

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

Here, the left hand equality follows from $C_0(M) = C_0(\overline{K}) \cap J(M) = C_0(\overline{K}) \cap J(L) = C_0(L)$. By Siegel's theorem, $C_0(L)$ contains only finitely many integral points. This contradicts the fact that the set $C_0(M)$ contains the infinite set $\{(x, \sqrt{f(x)}) \mid x \in \mathbb{Z}\}$ of integral points. □

## 3. Divisibility

Let $A$ be a nonzero abelian variety defined over a number field $K$ and $\mathcal{M}$ be an extension of $K$. An element $P \in A(\mathcal{M})$ is said to be *divisible* if there is a solution $X \in A(\mathcal{M})$ to the equation $nX = P$ for every nonzero integer $n$. When every nonzero element of $A(\mathcal{M})$ is divisible, we say that $A(\mathcal{M})$ is a divisible group. For example, $\mathbb{Q}$ is a torsion-free divisible group and $\mathbb{Q}/\mathbb{Z}$ is a divisible torsion group. Then we see that Proposition 7 implies that the group $A(M_0)$ there (and hence $J(M)$ in Theorem 1) has no nonzero divisible elements. Note that a torsion-free divisible group is uniquely divisible and hence has a natural structure of $\mathbb{Q}$-vector space.

In this section, we consider for which extension $\mathcal{M}$ the Mordell-Weil group $A(\mathcal{M})$ contains a divisible subgroup (of countable rank). For example, if $\mathcal{M}$ is an algebraic closure of $\mathbb{Q}$, then for every nonzero integer $n$ and every point $P \in A(\overline{\mathbb{Q}})$, the equation $nX = P$ is solvable in $\overline{\mathbb{Q}}$. Hence we see that $A(\overline{\mathbb{Q}})$ is divisible. In fact, $A(\overline{\mathbb{Q}})/A(\overline{\mathbb{Q}})_{\mathrm{tors}}$ is an infinite dimensional $\mathbb{Q}$-vector space.

**Lemma 8.** *If $\mathcal{M}$ contains the field $K(A(\overline{\mathbb{Q}})_{\mathrm{tors}})$ obtained by adjoining the coordinates of all torsion points of $A$ over $\overline{\mathbb{Q}}$, then every element of $A(\mathcal{M})$ is divisible in $A(\mathcal{M}^{\mathrm{ab}})$, where $\mathcal{M}^{\mathrm{ab}}$ is the maximal abelian extension of $\mathcal{M}$.*

*Proof.* Let $P$ be an element of $A(\mathcal{M})$. We show that for every nonzero integer $n$, we have $\frac{1}{n}P \in A(\mathcal{M}^{\mathrm{ab}})$. Denote by $\mathcal{M}(\frac{1}{n}P)$ the field obtained by adjoining the coordinates of the points $X \in A(\overline{\mathbb{Q}})$ such that $nX = P$. Note that the extension $\mathcal{M}(\frac{1}{n}P)/\mathcal{M}$ is a Galois extension. Let $A(\overline{\mathbb{Q}})[n] \subset A(\overline{\mathbb{Q}})_{\mathrm{tors}}$ be the subgroup of elements of order dividing $n$. Choose a point $X \in A(\overline{\mathbb{Q}})$ such that $nX = P$. Then we have an injective homomorphism $\mathrm{Gal}(\mathcal{M}(\frac{1}{n}P)/\mathcal{M}) \hookrightarrow A(\overline{\mathbb{Q}})[n]$ by sending $\sigma \in \mathrm{Gal}(\mathcal{M}(\frac{1}{n}P)/\mathcal{M})$ to $X^\sigma - X \in A(\overline{\mathbb{Q}})[n]$. Since $A(\overline{\mathbb{Q}})[n] \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$, where

$g$ is the dimension of $A$, we know that $\mathcal{M}(\frac{1}{n}P)/\mathcal{M}$ is an abelian extension. Hence we have $\frac{1}{n}P \in A(\mathcal{M}^{\mathrm{ab}})$. □

Thus we have proved the following:

**Proposition 9.** *If $\mathcal{M} \supset K(A(\overline{\mathbb{Q}})_{\mathrm{tors}})$ and $A(\mathcal{M})/A(\mathcal{M})_{\mathrm{tors}}$ contains a subgroup isomorphic to $\mathbb{Z}^{\oplus r}$, then $A(\mathcal{M}^{\mathrm{ab}})/A(\mathcal{M}^{\mathrm{ab}})_{\mathrm{tors}}$ contains a subgroup isomorphic to $\mathbb{Q}^{\oplus r}$.*

Although any element of $A(\mathcal{M})$ is divisible in $A(\mathcal{M}^{\mathrm{ab}})$, we cannot say in general that $A(\mathcal{M}^{\mathrm{ab}})$ itself is divisible. This is because for an element $P \in A(\mathcal{M}^{\mathrm{ab}}) \setminus A(\mathcal{M}^{\mathrm{ab}})_{\mathrm{tors}}$, the coordinates of its $n$-division points $\frac{1}{n}P$ are a priori contained only in an abelian extension of $\mathcal{M}^{\mathrm{ab}}$. Therefore we obtain the following result:

**Theorem 10.** *Let $A$ be a nonzero abelian variety defined over $K$. Suppose that $\mathcal{M} \supset K(A(\overline{\mathbb{Q}})_{\mathrm{tors}})$. Let $\mathcal{M}^{\mathrm{sol}}$ be the maximal solvable extension of $\mathcal{M}$. Then $A(\mathcal{M}^{\mathrm{sol}})/A(\mathcal{M}^{\mathrm{sol}})_{\mathrm{tors}}$ is a torsion-free divisible group.*

*Proof.* Since $\mathcal{M}^{\mathrm{sol}} = ((\mathcal{M}^{\mathrm{ab}})^{\mathrm{ab}})^{\mathrm{ab}\cdots}$, by Lemma 8, every element of $A(\mathcal{M}^{\mathrm{sol}})/A(\mathcal{M}^{\mathrm{sol}})_{\mathrm{tors}}$ is divisible in $A(\mathcal{M}^{\mathrm{sol}})/A(\mathcal{M}^{\mathrm{sol}})_{\mathrm{tors}}$. This completes the proof. □

Now we apply the above to the situation of our main theorem.

**Theorem 11.** *Let $C$ be an hyperelliptic curve defined over $\mathbb{Q}$. Suppose that $C$ has a $\mathbb{Q}$-rational point. Let $J$ be the Jacobian variety of $C$. Let $M = K(\sqrt{m} \mid m \in \mathbb{Z})$ be as in Theorem 1, and put $\widetilde{M} := M(J(\overline{\mathbb{Q}})_{\mathrm{tors}})$. Then we have*

$$J(\widetilde{M}^{\mathrm{sol}})/J(\widetilde{M}^{\mathrm{sol}})_{\mathrm{tors}} \simeq \mathbb{Q}^{\oplus\infty}.$$

*Proof.* By Theorem 1, we know that $J(M)/J(M)_{\mathrm{tors}}$ is a free $\mathbb{Z}$-module of infinite rank. Since $J(\widetilde{M})_{\mathrm{tors}} \supset J(M)_{\mathrm{tors}}$, $J(\widetilde{M})/J(\widetilde{M})_{\mathrm{tors}}$ also contains a free $\mathbb{Z}$-module of infinite rank. Then Proposition 9 and Theorem 10 imply that $J(\widetilde{M}^{\mathrm{sol}})/J(\widetilde{M}^{\mathrm{sol}})_{\mathrm{tors}}$ is an infinite dimensional $\mathbb{Q}$-vector space. Thus we obtain the Theorem. □

**Remark.** It is expected that the field $\widetilde{M}^{\mathrm{sol}}$ is not too large (i.e., $\mathrm{Gal}(\overline{\mathbb{Q}}/\widetilde{M}^{\mathrm{sol}})$ is not too small). It is another interesting problem to study the structure of $\mathrm{Gal}(\overline{\mathbb{Q}}/\widetilde{M}^{\mathrm{sol}})$. Note that Ohtani [4] studied certain closed normal subgroups of free profinite groups of countably infinite rank. In particular, her results imply that, if $\mathcal{M}$ is a subfield of $\overline{\mathbb{Q}}$ such that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathcal{M})$ is free profinite of countably infinite rank, then $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathcal{M}^{\mathrm{sol}})$ is a so-called $\omega$-$\mathcal{N}$-free pro-$\mathcal{N}$ group, where $\mathcal{N}$ is the class of all finite groups which have no non-trivial solvable quotients.

# 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] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math., **73(3)**(1983), 349-366.
G. Faltings, *Erratum: "Finiteness theorems for abelian varieties over number fields"*, Invent. Math., **75(2)**(1984), 381.

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

[4] S. Ohtani, *On certain closed normal subgroups of free profinite groups of countably infinite rank*, Comm. Algebra, **32**(2004), 3257-3262.

[5] 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(3-4)**(1981), 285-319.

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

[7] 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.