J. Korean Math. Soc. **54** (2017), No. 4, pp. 1345–1356
https://doi.org/10.4134/JKMS.j160518
pISSN: 0304-9914 / eISSN: 2234-3008

SOME ARITHMETIC PROPERTIES ON NONSTANDARD NUMBER FIELDS

Junguk Lee

Abstract. For a given number field K, we show that the ranks of elliptic curves over K are uniformly finitely bounded if and only if the weak Mordell-Weil property holds in all (some) ultrapowers ${}^*K$ of K. We introduce the nonstandard weak Mordell-Weil property for ${}^*K$ considering each Mordell-Weil group as ${}^*\mathbb{Z}$-module, where ${}^*\mathbb{Z}$ is an ultrapower of $\mathbb{Z}$, and we show that the nonstandard weak Mordell-Weil property is equivalent to the weak Mordell-Weil property in ${}^*K$. In a saturated nonstandard number field, there is a nonstandard ring of integers ${}^*\mathbb{Z}$, which is definable. We can consider definable abelian groups as ${}^*\mathbb{Z}$-modules so that the nonstandard weak Mordell-Weil property is well-defined, and we conclude that the nonstandard weak Mordell-Weil property and the weak Mordell-Weil property are equivalent. We have valuations induced from prime numbers in nonstandard rational number fields, and using these valuations, we identify two nonstandard rational numbers.

1. Introduction

In this paper, we study some arithmetic properties of nonstandard rational number fields. At first, we are interested in the ranks of elliptic curves. The rank of an elliptic curve E on a given field K is important to measure the size of K-rational points $E(K)$. The set $E(K)$ of K-rational points forms an abelian group, called *the Mordell-Weil group* and $E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$ forms a $\mathbb{Q}$-vector space. The dimension of this vector space is called the rank of $E(K)$, denoted by $\operatorname{rank} E(K)$. The ranks of elliptic curves over global fields, (for example, number fields or the finite extensions of function fields over finite fields), are finite by the Mordell-Weil Theorem. One can ask how large the ranks of elliptic curves over a global field can be. In [9] and [11] it is shown that the rank of elliptic curve can be arbitrary large in $\mathbb{F}_p(t)$. But it is not known much about

Received August 2, 2016; Revised February 3, 2017.
2010 *Mathematics Subject Classification.* Primary 03H15; Secondary 11G05, 11U10.
Key words and phrases. ranks of elliptic curves, nonstandard weak Mordell-Weil property, infinite factorization in nonstandard rationals.
The author was supported by Samsung Science Technology Foundation under Project Number SSTF-BA1301-03. The author thanks Anand Pillay for his suggestions on a preliminary draft and thanks the referee for valuable comments and suggestions.

the boundedness of ranks of elliptic curves over number field. In [7] it was shown that the quadratic twists E_d of a elliptic curve E over $\mathbb{Q}$ have a bounded rank if and only if a series associated with E is convergent and in [1] the average rank of elliptic curves over $\mathbb{Q}$ has a finite value. Here, we show that the weak Mordell-Weil properties of $\aleph_1$-saturated nonstandard number fields imply that the ranks of elliptic curves over a given number field are uniformly finitely bounded. Next we focus on primes in the nonstandard rational number fields. A nonstandard rational number field ${}^*\mathbb{Q}$ has a nonstandard integer ring ${}^*\mathbb{Z}$ corresponding to $\mathbb{Z}$ in $\mathbb{Q}$. It satisfies some basic arithmetic properties of $\mathbb{Z}$: Its field of fractions is ${}^*\mathbb{Q}$, it is integrally closed in ${}^*\mathbb{Q}$, it satisfies the (nonstandard) Euclidean division. Unfortunately ${}^*\mathbb{Z}$ need not be a Dedekind domain and not Noetherian any more. But ${}^*\mathbb{Z}$ has the set of primes and each prime gives a valuation on ${}^*\mathbb{Q}$. Any two elements in ${}^*\mathbb{Q}$ are the same if and only if they have the same value for each valuation and the same sign. As a consequence, ${}^*\mathbb{Z}$ is the intersection of valuation rings with valuations induced from primes.

Let us briefly recall basic notations on the first order logic (from [2]). Logical symbols are consisted of parentheses $(,)$, connective symbols $\wedge, \vee, \rightarrow, \neg$, quantifier symbols $\forall, \exists$, equality symbol $=$, and variables $x, y, z, \ldots$. Let $\mathcal{L}_{ring} = \{+, -, \times; 0, 1\}$ be the ring language. The (first order) *formulas* in $\mathcal{L}_{ring}$ are well-formed sequences of logical symbols and symbols in $\mathcal{L}_{ring}$. A subformula of a given formula is a subsequence which is also a formula. For convenience, we may omit parentheses symbols, and we abbreviate $\overbrace{x + x + \cdots + x}^{n}$ and $\overbrace{y \times y \times \cdots \times y}^{m}$ to nx and y^m for integers $n, m \geq 1$. For example, '$x^2 + y^2 = 0$' is a formula but neither 'x^2' nor '$())x^2)$' is. A variable in a formula is *free* if it is not bounded by quantifiers. For example, consider a formula $\phi \equiv \exists y \left(\forall x(x^2 + y = z) \wedge (4x + 1 = y^2)\right)$, and $\phi_1 \equiv \forall x(x^2 + y = z)$ and $\phi_2 \equiv (4x + 1 = y^2)$ so that $\phi \equiv \exists y(\phi_1 \wedge \phi_2)$. In ϕ, x and z are free but y is not. Most of all, look at the variable x, which appears in the subformulas ϕ_1 and ϕ_2. It is bounded by the quantifier $\forall$ in the subformula ϕ_1 but is not in the subformula ϕ_2. To emphasize which variables are free in a given formula ψ, we write $\psi(x_1, \ldots, x_n)$ where $x_1, \ldots, x_n$ are free variables in ψ. A (first order) *sentence* is a formula having no free variables. A set of sentence is called *a theory*.

We consider a ring R as an $\mathcal{L}_{ring}$-structure. Interpret the binary function symbol $+$ as addition, the binary function symbol $\times$ as multiplication, the unary function symbol $-$ as the inverse of addition, the constant symbols 0, 1 as the usual zero and identity elements in R. For a formula $\phi(x_1, \ldots, x_n)$ and $\bar{a} \in R^n$, we write $R \models \phi(\bar{a})$ if $\phi(\bar{a})$ holds in R, and $\phi(R) := \{\bar{a} \in R^n | \, R \models \phi(\bar{a})\}$. For a positive integer $n \geq 1$, we say that a subset $X \subset R^n$ is *definable* if there is a formula ϕ such that $X = \phi(R)$. For a given sentence ϕ, we write $R \models \phi$ if ϕ is true in R. The theory of R is the set of sentences which hold in R, and denoted by $\mathrm{Th}(R)$. We say given two rings R_1 and R_2 are *elementary*

equivalent, denoted by $R_1 \equiv R_2$, if for any sentence ϕ,

$$R_1 \models \phi \Leftrightarrow R_2 \models \phi,$$

in other words, $\mathrm{Th}(R_1) = \mathrm{Th}(R_2)$. Given a theory T, a ring R is a model of T if $T \subset \mathrm{Th}(R)$.

Consider the theory $\mathrm{Th}(K)$ of K in $\mathcal{L}_{ring}$ for a number field K. We say a model of $\mathrm{Th}(K)$ is *standard* if it is isomorphic to K. Otherwise, it is called *nonstandard*. A model of $\mathrm{Th}(K)$ is nonstandard if and only if it contains a transcendental element. Robinson in [6] proved that the ring of integers $\mathbb{Z}$ is definable in any number fields in $\mathcal{L}_{ring}$ so that the theories of number fields are undecidable. Let $Z(x)$ and $Q(x)$ be formulas defining $\mathbb{Z}$ and $\mathbb{Q}$ in K respectively. Let ${}^*K$ be a nonstandard model of $\mathrm{Th}(K)$. We claim that $\mathbb{Z} \subsetneq Z({}^*K)$. Since K is a finite extension of $\mathbb{Q}$, there is an integral element $\alpha \in K$ such that $\mathbb{Q}(\alpha) = K$. It is expressed by the first order logic as the statement saying that there is an element α such that

• α is a zero of a monic polynomial with coefficients satisfying the formula Z.
• Any element is written uniquely as a linear combination of $\{1, \alpha^1, \ldots, \alpha^{d-1}\}$ with coefficients satisfying the formula Q, where $d = [K : \mathbb{Q}]$.

Suppose $\mathbb{Z} = Z({}^*K)$. Then we can find an integral element ${}^*\alpha \in {}^*K$ such that $\mathbb{Q}({}^*\alpha) = {}^*K$. Let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of ${}^*\alpha$. Since $f(X)$ is over $\mathbb{Z}$ and ${}^*K \models \exists x\,(f(x) = 0)$, $K \models \exists x\,(f(x) = 0)$. So, K contains a conjugate α of ${}^*\alpha$ and $K = \mathbb{Q}(\alpha)$. Therefore $K \cong {}^*K$ via the map sending α to ${}^*\alpha$. This contradicts with the choice of ${}^*K$ as a nonstandard model of $\mathrm{Th}(K)$. Moreover we conclude that between number fields, two notions of being elementary equivalent and being isomorphic coincide.

Theorem 1.1. *For any two number fields K_1 and K_2, we have that*

$$K_1 \equiv K_2 \Leftrightarrow K_1 \cong K_2.$$

Next we review elliptic curves over a field K of characteristic zero. An elliptic curve E over K is given by the following equation

$$y^2 = x^3 + Ax + B, 4A^3 + 27B^2 \neq 0$$

for $A, B \in K$. It is well-known that the set $E(K)$ of K-rational points of E

$$\{(x, y) \in K^2 |\ y^2 = x^3 + Ax + B\} \cup \{P_\infty\}$$

forms an abelian group called *the Mordell-Weil group*. If K is a global field for example a number field or a finite extension of function field over $\mathbb{F}_q$, then the Mordell-Weil Theorem says that $E(K)$ is finitely generated and its rank is finite. Now let K be a global field. By the Mordell-Weil Theorem, the cardinality of the weak nth Mordell-Weil group contains an information of the rank of $E(K)$. Let $n \geq 2$ and let

$$nE(K) := \{P \in E(K) \,|\, \exists Q \in E(K),\ P = \overbrace{Q +_E \cdots +_E Q}^{n}\}.$$

The *weak nth Mordell-Weil group* of E over K is the quotient of $E(K)$ by $nE(K)$, denoted by $E(K)/nE(K)$. Then $n^r \leq |E(K)/nE(K)| \leq n^r + n^2$ where r is the rank of E over K for all $n \geq 2$. From now on, if K is clear from the context, we omit 'over K'. We say a field L has *the weak Mordell-Weil property* if for any elliptic curve E over L, each weak nth Mordell-Weil group of E over L is finite.

2. Uniformly finite boundedness of the ranks of elliptic curves

We may consider elliptic curves as definable objects in K. Fix $A, B \in K$ such that $4A^3 + 27B^2 \neq 0$. Then $E(K)$ can be seen as a definable subset of K^3 by the following formula

$$E(A,B;x,y,z) \equiv (4A^3 + 27B^2 \neq 0) \wedge \big((y^2 = x^3 + Ax + B \wedge z = 1) \vee (x = 0 \wedge y = 1 \wedge z = 0)\big).$$

Moreover the group operation $+_E$ of the Mordell-Weil group $(E(K), +_E)$ is also definable, that is, the graph of $+_E : E(K) \times E(K) \to E(K)$ is a definable subset of $K^3 \times K^3 \times K^3$ given by the following formula: For $\bar{x} = (x_0, x_1, x_2)$, $\bar{y} = (y_0, y_1, y_2)$, and $\bar{z} = (z_0, z_1, z_2)$,

$$\begin{aligned}
+_E(\bar{x},\bar{y},\bar{z}) \equiv \Big(E(\bar{x}) \wedge E(\bar{y}) \wedge E(\bar{z})\Big) \wedge \Big(&\big(x_2 = 0 \to \bigwedge_{0\leq i\leq 2} y_i = z_i\big) \\
&\vee \big(y_2 = 0 \to \bigwedge_{0\leq j\leq 2} x_j = z_j\big) \\
&\vee \big(x_0 = y_0 \wedge x_1 \neq y_1 \to (z_0 = 0 \wedge z_1 = 1 \wedge z_2 = 0)\big) \\
&\vee \big(x_0 = y_0 \wedge x_1 = y_1 \to (z_0 = ((\frac{3x_0^2 + A}{2y_0})^2 - x_0 - x_1) \\
&\quad \wedge z_1 = -(\frac{3x_0^2 + A}{2y_0} z_0 - (x_1 - \frac{3x_0^2 + A}{2y_0} x_0)) \wedge z_2 = 1)\big) \\
&\vee \big(x_0 \neq y_0 \to (z_0 = (\frac{y_1 - x_1}{y_0 - x_0})^2 - x_0 - x_1)) \\
&\quad \wedge z_1 = (\frac{y_1 - x_1}{y_0 - x_0} z_0 - \frac{y_0 x_1 - y_1 x_0}{y_0 - x_0}) \wedge z_2 = 1)\big)\Big).
\end{aligned}$$

For $n \geq 2$, each $nE(K)$ is definable. Consider a formula

$$nE(\bar{x}) \equiv E(\bar{x}) \wedge \exists \bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n \left(\bigwedge_{1\leq i<n} (E(\bar{x}_i) \wedge +_E(\bar{x}_i, \bar{x}_1, \bar{x}_{i+1})) \wedge \bar{x}_n = \bar{x} \right),$$

where $\bar{x} = \bar{x}'$ is an abbreviation for $\bigwedge_i (x_i = x_i')$ for $\bar{x} = (x_0, \ldots, x_n)$ and $\bar{x}' = (x_0', \ldots, x_n')$, and this formula defines $nE(K)$.

We recall some basic properties of the notion of ultraproduct. Fix a countably infinite index set I and a nonprincipal ultrafilter $\mathcal{U}$ on I. Let $\{\mathcal{M}_i\}_{i\in I}$ be a set of $\mathcal{L}$-structures by the set I. Define an equivalence relation $\sim_{\mathcal{U}}$

on $\prod_{i\in I}\mathcal{M}_i$ as follows: For $(a_i),(b_i)\in\prod_{i\in I}\mathcal{M}_i$, $(a_i)\sim_{\mathcal{U}}(b_i)$ if and only if $\{i\in I|a_i=b_i\}\in\mathcal{U}$. The set $\prod_{i\in I}\mathcal{M}_i/\sim_{\mathcal{U}}$ (=: $\prod_{\mathcal{U}}\mathcal{M}_i$) of equivalence classes of $\sim_{\mathcal{U}}$ is called *the ultraproduct of $\mathcal{M}_i$'s with respect to the ultrafilter $\mathcal{U}$*. We denote by $[(a_i)]$ the equivalence class of $(a_i)\in\prod_{i\in I}\mathcal{M}_i$. A subset S of $\prod_{\mathcal{U}}\mathcal{M}_i$ is called *induced* if it is of the form of $\prod_{i\in I}S_i/\sim_{\mathcal{U}}$ for a set of subsets S_i of $\mathcal{M}_i$ indexed by I.

Remark 2.1. Let $\{\mathcal{M}_i\}_{i\in I}$ be a collection of infinite structures indexed by I.

(1) For a formula $\phi(x_1,\dots,x_n)$ and $a^1=[(a_i^1)],\dots,a^n=[(a_i^n)]\in\prod_{\mathcal{U}}\mathcal{M}_i$,

$$\prod_{\mathcal{U}}\mathcal{M}_i\models\phi(a^1,\dots,a^n)\ \Leftrightarrow\ \{i\in I|\ \mathcal{M}_i\models\phi(a_1^i,\dots,a_n^i)\}\in\mathcal{U}.$$

(2) The ultraproduct $\prod_{\mathcal{U}}\mathcal{M}_i$ is $\aleph_1$-saturated.

(3) An induced set $\prod_{\mathcal{U}}\mathcal{M}_i$ is finite or at least $\geq 2^{\aleph_0}$, and any definable set is induced.

For a fixed infinite structure $\mathcal{M}$, if $\mathcal{M}_i=\mathcal{M}$ for $i\in I$, we write ${}^*\mathcal{M}^{\mathcal{U}}$ for the ultrapower of $\mathcal{M}$ with respect to the ultrafilter $\mathcal{U}$. We write ${}^*\mathcal{M}$ if $\mathcal{U}$ is obvious. In this case, there is a canonical embedding $\iota:\mathcal{M}\to{}^*\mathcal{M}, m\mapsto[(m)]$ and this embedding is an elementary embedding, that is, for a formula $\phi(\bar{x})$ with $|\bar{x}|=n$ and $\bar{a}\in\mathcal{M}^n$, $\mathcal{M}\models\phi(\bar{a})$ if and only if ${}^*\mathcal{M}\models\phi(\iota(\bar{a}))$. So ${}^*\mathcal{M}$ is an $\aleph_1$-saturated elementary extension of $\mathcal{M}$.

Next we consider ultraproducts of abelian groups. Let $\{A_i\}_{i\in I}$ be a set of abelian groups indexed by I and consider the ultraproduct $\prod_{\mathcal{U}}A_i$. Then we can consider the ultraproduct $\prod_{\mathcal{U}}A_i$ as a ${}^*\mathbb{Z}$-module, where ${}^*\mathbb{Z}$ is the ultrapower $\prod_{\mathcal{U}}\mathbb{Z}$ of $\mathbb{Z}$ as follows: For $a=[(a_i)]\in\prod_{\mathcal{U}}A_i$ and $n=(n_i)\in\prod_{\mathcal{U}}\mathbb{Z}$, define $na:=[(n_ia_i)]$.

Remark 2.2. Let $\{A_i\}_{i\in I}$ be a set of abelian groups indexed by I.

(1) If each A_i is generated by n elements, then the ultraproduct $\prod_{\mathcal{U}}A_i$ is generated by n elements as ${}^*\mathbb{Z}$-module.

(2) If the ultraproduct $\prod_{\mathcal{U}}A_i$ is finitely generated as ${}^*\mathbb{Z}$-module, then the cardinality of the quotient of $\prod_{\mathcal{U}}A_i$ by $k\prod_{\mathcal{U}}A_i$ is finite for all $k\geq 1$. More precisely, if $\prod_{\mathcal{U}}A_i$ is generated by n elements, then $|\prod_{\mathcal{U}}A_i/k\prod_{\mathcal{U}}A_i|\leq k^n$ for each $k\geq 1$.

Proof. (1) Suppose A_i is generated by $a_{i1},\dots,a_{in}$ for each $i\in I$. Then $\prod_{\mathcal{U}}A_i$ is generated by $a_1=[(a_{i1})],\dots,a_n=[(a_{in})]$ as ${}^*\mathbb{Z}$-module. Take $x=[(x_i)]\in$

$\prod_{\mathcal{U}} A_i$ arbitrary. For each $i \in I$, there are $c_{1i}, \ldots, c_{ni}$ in $\mathbb{Z}$ such that $x_i = c_{1i}a_{i1} + \cdots + c_{ni}a_{in}$ so that $x = c_1a_1 + \cdots + c_na_n$ for $c_1 = [(c_{1i})], \ldots, c_n = [(c_{ni})] \in {}^*\mathbb{Z}$. Thus $\prod_{\mathcal{U}} A_i$ is generated by n elements as ${}^*\mathbb{Z}$-module.

(2) Suppose $\prod_{\mathcal{U}} A_i$ is generated by $a_1, \ldots, a_n$ as ${}^*\mathbb{Z}$-module for some $n \geq 1$. Let $k \geq 1$. Define a map $f_k : {}^*\mathbb{Z}/k{}^*\mathbb{Z} \times \cdots \times {}^*\mathbb{Z}/k{}^*\mathbb{Z} \to \prod_{\mathcal{U}} A_i/k\prod_{\mathcal{U}} A_i$ by sending $(c_1, \ldots, c_n)$ to $c_1a_1 + \cdots + c_na_n$. Then this map is well-defined and it is onto. Since ${}^*\mathbb{Z}/k{}^*\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z}$, the domain of f_k is finite and its cardinality is k^n. Thus, the cardinality of $\prod_{\mathcal{U}} A_i/k\prod_{\mathcal{U}} A_i$ is less than or equal to k^n. □

Note that for an ultrapower ${}^*K$ of a field K and an elliptic curve E over ${}^*K$, the Mordell-Weil group $E({}^*K)$ is an ultraproduct of an elliptic curve over K and $E({}^*K)$ is an ultraproduct of abelian groups.

From now on, we fix a number field K. We see some relations between the ranks of elliptic curves over K and over ${}^*K$. Let E be an elliptic curve over K, then E is also over ${}^*K$ and $E(K) \subset E({}^*K)$. It can be directly shown that the rank of $E({}^*K)$ is larger than or equal to the rank of $E(K)$. But unfortunately the rank of elliptic curve is not an elementary invariant, that is, for an elliptic curve E over K, the rank of $E(K)$ need not be equal to the rank of $E({}^*K)$ unless $\operatorname{rank} E(K) = 0$.

Proposition 2.3. *If* $\operatorname{rank} E(K)$ *is not equal to* 0*, then* $\operatorname{rank} E({}^*K) > \operatorname{rank} E(K)$ *and* $\operatorname{rank} E({}^*K)$ *is always infinite. If* $\operatorname{rank} E(K) = 0$*, then* $E(K) = E({}^*K)$.

Proof. Let E be an elliptic curve over K. Suppose $\operatorname{rank} E(K) > 0$ so that $E(K)$ is infinite. Thus $E({}^*K)$ is infinite. Since $E({}^*K)$ is induced and infinite, the cardinality of $E({}^*K)$ is $2^{\aleph_0}$. Also there are countably many torsion points in $E({}^*K)$. Thus the vector space $E({}^*K) \otimes_{\mathbb{Z}} \mathbb{Q}$ is of cardinality of $2^{\aleph_0}$. So its dimension as $\mathbb{Q}$-vector space is $2^{\aleph_0}$ and $\operatorname{rank} E({}^*\mathbb{Z}) = 2^{\aleph_0}$.

Suppose $\operatorname{rank} E(K) = 0$ so that $E(K)$ is finite. Let $k = |E(K)|$. We can write down in the sentence ϕ saying there are only k-many points in E. Since K and ${}^*K$ are elementary equivalent, ${}^*K \models \phi$, that is, $k = |E({}^*K)|$. Always $E(K)$ is a subset of $E({}^*K)$ and therefore $E(K)$ and $E({}^*K)$ are same. □

From Proposition 2.3, the rank itself may not be an elementary invariant. By the way, each weak nth group may be a good elementary invariant. Consider an equivalence relation $\sim_{E,n}$ on E defined by the following formula

$$\exists \bar{z}\ \big(nE(\bar{z}) \wedge +_E(\bar{x}, \bar{z}, \bar{y})\big)$$

for each elliptic curve E and each $n \geq 2$.

Proposition 2.4. *Let* E *be an elliptic curve over* K*. For each* $n \geq 2$*,* $E(K)/nE(K) \cong E({}^*K)/nE({}^*K)$.

Proof. Let E be an elliptic curve over K with $|E(K)/nE(K)| = k_n < \infty$ for $n \geq 2$. Fix $n \geq 2$. There is a natural embedding ι_E from $E(K)$ to

$E(^*K)$ and it induces a map $\iota_{E,n}$ from $E(K)/nE(K)$ to $E(^*K)/nE(^*K)$. Since $E(K)\cap nE(^*K) = nE(K)$, this map is injective. It remains to show surjectivity. For $n \geq 2$ and $k \geq 1$, define a formula

$$\phi_{E,n,k}(\bar{x}_1, \ldots, \bar{x}_k) \equiv \bigwedge_{1\leq i\leq k} E(\bar{x}_i) \wedge \bigwedge_{1\leq i<j\leq k} \neg(\bar{x}_i \sim_{E,n} \bar{x}_j).$$

Next consider the following sentence

$$\phi'_{E,n} \equiv \exists \bar{x}_1 \ldots \bar{x}_{k_n} \left(\phi_{E,n,k_n}(\bar{x}_1, \ldots, \bar{x}_{k_n}) \wedge \forall \bar{x} \left(E(\bar{x}) \rightarrow \bigvee_{1\leq i\leq k_n} (\bar{x} \sim_{E,n} \bar{x}_i) \right) \right).$$

Since $|E(K)/nE(K)| = k_n < \infty$, $K \models \phi'_{E,n}$, and so $^*K \models \phi'_{E,n}$. Thus $|E(^*K)/nE(^*K)| = k_n$ also. Thus $\iota_{E,n}$ is surjective and it is bijective. Therefore $\iota_{E,n} : E(K)/nE(K) \cong E(^*K)/nE(^*K)$. □

We get the following equivalent conditions for the boundedness of ranks of elliptic curves over K.

Definition 2.5. We say $^*K$ has *the nonstandard weak Mordell-Weil property* if each Mordell-Weil group of elliptic curve over $^*K$ is finitely generated as $^*\mathbb{Z}$-module.

Theorem 2.6. *The followings are equivalent*:

(1) *The ranks of elliptic curves over K are uniformly finitely bounded.*
(2) *For each $n \geq 2$, the cardinalities of weak nth Mordell-Weil groups over K are uniformly finitely bounded.*
(3) *For any (some) nonprincipal ultrafilter $\mathcal{U}$ on I, weak Mordell-Weil property holds for $^*K^{\mathcal{U}}$.*
(4) *For any (some) nonprincipal ultrafilter $\mathcal{U}$ on I, nonstandard Moredell-Weil property hold for $^*K^{\mathcal{U}}$.*

Proof. It is easy to check (1) ⇔ (2). It it enough to show (1) ⇒ (4), (4) ⇒ (3), and (3) ⇒ (2). Let $E(A, B; x, y, z)$ be a formula

$$(4A^3 + 27B^2 \neq 0) \wedge \left((z = 1 \wedge y^2 = x^3 + Ax + B) \vee (z = 0 \wedge x = 0 \wedge y = 1)\right),$$

which parametrizes all pairs of elliptic curves $E(A, B) : y^2 = x^3 + Ax + B$ and points in $E(A, B)$. Consider a two variable formula

$$\Phi_{n,m}(A, B) \equiv \exists \bar{x}_1, \ldots, \bar{x}_m \phi_{E(A,B),n,m}$$

for each $m \geq 1$ which parametrizes all nonsingular elliptic curves whose the weak nth Mordell-Weil group has the cardinality at least m.

(1) ⇒ (4) Suppose there is $C > 0$ such that $\operatorname{rank} E(K) < C$ for each elliptic curve E over K. There is $r > 0$ such that $E(K)$ is generated by at most r elements for all elliptic curves E over K because there are only finitely many possibilities for torsion points of elliptic curves over K. Then by Remark 2.2(1), each Mordell-Weil group of an elliptic curve over $^*K$ is finitely generated as $^*\mathbb{Z}$-module.

(4) $\Rightarrow$ (3) Suppose the nonstandard weak Mordell-Weil property holds for any (some) ${}^*K^{\mathcal{U}}$. By Remark 2.2 (2), each nth weak Mordell-Weil group of an elliptic curve over ${}^*K^{\mathcal{U}}$ is finite and so the weak Mordell-Weil property holds for ${}^*K^{\mathcal{U}}$.

(3) $\Rightarrow$ (2) Suppose (2) does not hold. Then there is $n \geq 2$ such that for each $m \geq 1$, there is $A_m, B_m \in \mathbb{Q}$ such that

$$\mathbb{Q} \models \Phi_{n,m}(A_m, B_m).$$

So for any (some) ${}^*K^{\mathcal{U}}$,

$${}^*K^{\mathcal{U}} \models \Phi_{n,m'}([(A_m)], [(B_m)])$$

for all $m' \geq 1$. So ${}^*K^{\mathcal{U}}$ does not have the weak Mordell-Weil property. □

We extend Remark 2.2 to arbitrary definable abelian groups in saturated nonstandard number fields in the ring language $\mathcal{L}_{ring} = \{+, -, \times; 0, 1\}$. Let ${}^*\mathbb{Q}$ be a saturated model of $\mathrm{Th}(\mathbb{Q})$ and ${}^*\mathbb{Z}$ be a nonstandard integer ring of ${}^*\mathbb{Q}$ corresponding to $\mathbb{Z}$ in $\mathbb{Q}$, which is definable in $\mathcal{L}_{ring}$. Let K be a number field and let ${}^*K$ be a saturated model of $\mathrm{Th}(K)$. First note that K is interpretable in $\mathbb{Q}$ in $\mathcal{L}_{ring}$. More precisely, fix $\alpha \in K$ which is integral over $\mathbb{Z}$ and $K = \mathbb{Q}(\alpha)$. Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ be the irreducible polynomial of α with $n = [K, \mathbb{Q}]$. We can associate a field structure on $\mathbb{Q}^{n-1}$. We define the plus $+_K$ and the multiplication $\times_K$ on $\mathbb{Q}^{n-1}$ as follows: for $(x_0, \ldots, x_{n-1}), (y_0, \ldots, y_{n-1}) \in \mathbb{Q}^{n-1}$,

$$(x_0, \ldots, x_{n-1}) +_K (y_0, \ldots, y_{n-1}) = (x_0 + y_0, \ldots, x_{n-1} + y_{n-1}),$$

and

$$(x_0, \ldots, x_{n-1} \times_K (y_0, \ldots, y_{n-1}) := (z_0, \ldots, z_{n-1}) \in \mathbb{Q}^{n-1}$$

such that $(\sum_{i=0}^{n-1} x_i\alpha^i) \cdot (\sum_{i=0}^{n-1} y_j\alpha^j) = \sum_{k=0}^{n-1} z_k\alpha^k \in K$. Note that $\times_K$ is definable with the parameter $\{a_0, \ldots, a_{n-1}\} (\subset \mathbb{Q})$ so that it is definable over $\emptyset$. The field $(\mathbb{Q}^n, +_K, \times_K)$ is isomorphic to K by the map

$$(x_0, \ldots, x_{n-1}) \in \mathbb{Q}^{n-1} \mapsto \sum_{i=0}^{n-1} x_i\alpha^i \in K.$$

Let $({}^*A, +_{{}^*A}, 1_{{}^*A})$ be a definable abelian group in ${}^*K$. It is clear that ${}^*A$ is a $\mathbb{Z}$-module as

$$n \cdot a := \begin{cases} \overbrace{a +_{{}^*A} \cdots +_{{}^*A} a}^{|n|} & \text{if } n > 0 \\ 1_{{}^*A} & \text{if } n = 0 \\ \underbrace{(-a) +_{{}^*A} \cdots +_{{}^*A} (-a)}_{|n|} & \text{if } n < 0 \end{cases}$$

for $a \in {}^*A$ and $n \in \mathbb{Z}$. Our main aim in the rest of this section is to show that we can see ${}^*A$ as a ${}^*\mathbb{Z}$-module extending the $\mathbb{Z}$-module structure, that is, there

is a map $\cdot^* : {}^*\mathbb{Z} \times {}^*A \to {}^*A$ to make ${}^*A$ as ${}^*\mathbb{Z}$-module and $n \cdot^* a = n \cdot a$ for $a \in {}^*A$ and $n \in \mathbb{Z}$.

Let V be the standard model of the ZFC axioms in the language $\mathcal{L}_{set} = \{\in\}$. From now on, we mean 'formula' and 'definable' in $\mathcal{L}_{set}$, not in $\mathcal{L}_{ring}$. The ring and field structures of $\mathbb{Z}$ and $\mathbb{Q}$ are definable and let $\phi_{\mathbb{Z}}(x)$ and $\phi_{\mathbb{Q}}(x)$ be formulas defining $\mathbb{Z}$ and $\mathbb{Q}$ respectively. Also there is a formula $\phi_K(x)$ defining a field isomorphic to K. We identify K and $\phi_K(V)$. Consider a definable group $(G, +_G, 1_G)$ in K, which includes the case of definable groups in $\mathcal{L}_{ring}$ since the field structure of K is interpretable in $\mathcal{L}_{set}$, and let $\theta(\bar{x}, \bar{y})$ be a formula and $\bar{a} \in K^{|\bar{y}|}$ such that the formula $\theta(\bar{x}, \bar{a})$ defines the set G and says the function $+_G$ on G is a group operation with the identity 1_G. Let $\delta(\bar{y})$ be a formula saying that for $\bar{b} \in K^{|\bar{y}|}$, $\delta(\bar{b})$ holds if and only if $\theta(\bar{x}, \bar{b})$ defines a group $(G_{\bar{b}}, +_{G_{\bar{b}}}, 1_{G_{\bar{b}}})$. Consider a formula

$$\mathcal{F}_\theta(x_1, \ldots, x_n, y_1, \ldots, y_m) \equiv \bigwedge_i \phi_K(x_i) \wedge \bigwedge_j \phi_j(y_j) \wedge \delta(\bar{y}) \wedge \theta(\bar{x}, \bar{y})$$

parametrizing all pairs of groups definable in K by the formula θ and elements in such groups. Consider a function $f : \mathbb{Z} \times \mathcal{F}_\theta(V) \to \mathcal{F}_\theta(V)$ such that

- $f(0, \bar{g}, \bar{b}) = (1_{G_{\bar{b}}}, \bar{b})$ for $\bar{b} \in K^{|\bar{y}|}$ and $\bar{g} \in G_{\bar{b}}$; and
- $f(n+1, \bar{g}, \bar{b}) = (\bar{g} +_{G_{\bar{b}}} \pi(f(n, \bar{g}, \bar{b})), \bar{b})$ for $n \in \mathbb{Z}$ and $(\bar{g}, \bar{b}) \in \mathcal{F}_\theta(V)$, where π is the projection map from $\mathcal{F}_\theta(V)$ to $\bigcup_{\bar{b} \in \mathcal{C}_\theta(K)} G_{\bar{b}}$.

Then by recursion theorem, this function f is definable. Moreover if $G_{\bar{b}}$ is commutative for $\bar{b} \in K^{|\bar{y}|}$, then the $\mathbb{Z}$-module structure on $G_{\bar{b}}$ is given by $f(\cdot, \cdot, \bar{b})$. Thus we have the following.

Proposition 2.7. *Let K be a number field. Let $\theta(\bar{x}, \bar{y})$ be a formula such that for some $\bar{a} \in K^{|\bar{y}|}$, $\theta(K, \bar{a})$ defines a group G. Then for each $\bar{b} \in K^{|\bar{y}|}$ with $\theta(\bar{x}, \bar{b})$ defining a group $G_{\bar{b}}$, there is a uniformly definable function $f_{\bar{b}} : \mathbb{Z} \times G_{\bar{b}} \to G_{\bar{b}}$ such that*

- *$f_{\bar{b}}(0, g) = 1_{G_{\bar{b}}}$ for any $g \in G_{\bar{b}}$; and*
- *$f_{\bar{b}}(n+1, g) = f_{\bar{b}}(n, g) + g$ for any $g \in G_{\bar{b}}$ and $n \in \mathbb{Z}$.*

Now let κ be an inaccessible cardinal and let ${}^*V$ be a saturated extension of V of cardinality κ. Let ${}^*\mathbb{Z} = \phi_{\mathbb{Z}}({}^*V)$, ${}^*\mathbb{Q} = \phi_{\mathbb{Q}}({}^*V)$, and ${}^*K = \phi_K({}^*V)$, which are saturated models of cardinality κ of $\mathrm{Th}(\mathbb{Z})$, $\mathrm{Th}(\mathbb{Q})$, and $\mathrm{Th}(K)$ respectively. Let $({}^*G, +_{{}^*G}, 1_{{}^*G})$ be a definable abelian group in ${}^*K$ by the formula $\theta(\bar{x}, {}^*\bar{a})$ for some ${}^*\bar{a} \in {}^*K^{|\bar{y}|}$. It has a ${}^*\mathbb{Z}$-module structure extending the $\mathbb{Z}$-module structure given by the definable function $f_{{}^*\bar{a}}(\cdot, \cdot) : {}^*\mathbb{Z} \times {}^*G \to {}^*G$. Since any saturated model is unique up to isomorphism, we get the following result:

Theorem 2.8. *Any abelian group definable in ${}^*K$ has a ${}^*\mathbb{Z}$-module structure extending the $\mathbb{Z}$-module structure. Especially any elliptic curves over ${}^*K$ has a ${}^*\mathbb{Z}$-module structure.*

As a corollary, we extend Theorem 2.6 to arbitrary saturated models of $\mathrm{Th}(K)$.

Theorem 2.9. *The followings are equivalent*:

(1) *The ranks of elliptic curves over K are uniformly finitely bounded.*
(2) *For each $n \geq 2$, the cardinalities of weak nth Mordell-Weil groups over K are uniformly finitely bounded.*
(3) *Weak Mordell-Weil property holds for ${}^*K$.*
(4) *Nonstandard Moredell-Weil property hold for ${}^*K$.*

3. Factorization in ${}^*\mathbb{Z}$

We fix a nonstandard rational number field ${}^*\mathbb{Q}$. We know that $\mathbb{Z}$ is definable in $\mathbb{Q}$ (see [5] and [6]) by a formula $Z(x)$. So ${}^*\mathbb{Q}$ also has a nonstandard integer ring ${}^*\mathbb{Z} := Z({}^*\mathbb{Q})$ corresponding to $\mathbb{Z}$ in $\mathbb{Q}$ as a definable subset in ${}^*\mathbb{Q}$. By Lagrange theorem, the set of natural numbers $\mathbb{N}$ is definable in $\mathbb{Q}$ by the formula

$$N(x) \equiv \exists y_1, y_2, y_3, y_4 (\bigwedge_{1 \leq i \leq 4} Z(y_i) \wedge x = y_1^2 + y_2^2 + y_3^2 + y_4^2),$$

and let ${}^*\mathbb{N} := N({}^*\mathbb{Q})$ corresponding to $\mathbb{N}$ of $\mathbb{Q}$. The nonstandard integer ${}^*\mathbb{Z}$ inherits some basic arithmetic properties of $\mathbb{Z}$:

- The quotient field of ${}^*\mathbb{Z}$ is ${}^*\mathbb{Q}$.
- ${}^*\mathbb{Z}$ is integrally closed in ${}^*\mathbb{Q}$.
- ${}^*\mathbb{Z}^\times = \{\pm 1\}$.
- Any finitely generated ideal is a principal ideal.
- There is a linear order $<$ on ${}^*\mathbb{Z}$ to make ${}^*\mathbb{Z}$ as an ordering ring so that $({}^*\mathbb{Q}, <)$ is an ordered field.

The nonstandard Euclidean division holds in ${}^*\mathbb{Z}$ as follows:

- For any $a, b \in {}^*\mathbb{Z}$, there are unique $q, r \in {}^*\mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < |a|$,

where $|a| = a$ if $0 \leq a$, or $= -a$ otherwise. By the way, ${}^*\mathbb{Z}$ need not be a PID, a Dedekind domain, and a Noetherian ring.

Example 3.1. Let ${}^*\mathbb{Q}$ be $\aleph_1$-saturated. Let $I = \bigcap_{i \in \omega} 2^i {}^*\mathbb{Z}$. Then I is not a finite product of prime ideals and it is not finitely generated.

The following theorem holds in $\mathbb{Q}$:

Theorem 3.2. *Let ν_p denote the valuation on $\mathbb{Q}$ induced from a prime number p. For $a_0, a_1 \in \mathbb{Q} \setminus \{0\}$,*

$a_0 = a_1$ if and only if $\nu_p(a_0) = \nu_p(a_1)$ for each prime number p and $0 < a_0 a_1$.

So we have

$$\mathbb{Z} = \bigcap_{p \in \mathcal{P}(\mathbb{N})} \mathbb{Z}_p,$$

where $\mathbb{Z}_p$ is the ν_p-valuation ring of $\mathbb{Q}$.

Our goal in this section is to show that Theorem 3.2 holds in ${}^*\mathbb{Q}$ even though ${}^*\mathbb{Z}$ need not be a UFD. More precisely, we will show that the statement in Theorem 3.2 can be expressed by the first order logic.

We define a binary relation by a formula

$$x|y \equiv Z(x) \wedge Z(y) \wedge \exists z(Z(z) \wedge z \neq 0 \wedge y = zx)$$

saying that x and y are integers and x divides y. Next we consider a formula defining primes as follows:

$$P(x) \equiv N(x) \wedge (x \neq 1) \wedge \forall y\big((y|x) \to ((y = \pm 1) \vee (y = \pm x))\big).$$

So, $P(\mathbb{Q})$ gives the set $\mathcal{P}(\mathbb{N})$ of primes in $\mathbb{N}$ and $P({}^*\mathbb{Q})$ is the set $\mathcal{P}({}^*\mathbb{N})$ of primes in ${}^*\mathbb{Z}$ corresponding $\mathcal{P}(\mathbb{N})$. For each prime, we define the set of powers of a given prime. Consider a formula

$$pw(x;y) \equiv N(x) \wedge N(y) \wedge \Big(y = 1 \vee \forall z\big((N(z) \wedge z \neq \pm 1 \wedge z|y) \to x|z\big)\Big).$$

For each $p \in \mathcal{P}({}^*\mathbb{N})$, let $p^{{}^*\mathbb{N}} := pw(p; {}^*\mathbb{N})$ be the set of 1 and elements in ${}^*\mathbb{N}$ divisible only by p. Next consider a function $\nu_p : {}^*\mathbb{Z} \setminus \{0\} \to p^{{}^*\mathbb{N}}$ sending each x to y such that $y|x$ but $\neg(py|x)$, which is definable by a formula

$$d_p(x,y) \equiv (Z(x) \wedge x \neq 0) \wedge pw(p;y) \wedge y|x \wedge \neg(py|x)$$

with the parameter p. This map extends on ${}^*\mathbb{Q}\setminus\{0\}$. Let $pw'(x;y) \equiv pw(x;y) \vee \exists z(pw(x;z) \wedge zy = 1)$. Let $p^{{}^*\mathbb{Z}} := pw'(p; {}^*\mathbb{Q}) = p^{{}^*\mathbb{N}} \cup \{1/x | x \in p^{{}^*\mathbb{N}}\}$. Note that we give an order $<_p$ on $p^{{}^*\mathbb{Z}}$ as follows: $a <_p b$ if $b/a \in p^{{}^*\mathbb{N}}$ and $(p^{{}^*\mathbb{Z}}, \times, <_p)$ forms an ordered group. Extend ν_p to the map from ${}^*\mathbb{Q}\setminus\{0\}$ into $p^{{}^*\mathbb{Z}}$ by sending a/b with $a, b \in {}^*\mathbb{Z}$ into $\nu_p(a)/\nu_p(b)$, which is a surjective group homomorphism from $({}^*\mathbb{Q} \setminus \{0\}, \times)$ to $(p^{{}^*\mathbb{Z}}, \times)$. For any $a, b \in {}^*\mathbb{Q} \setminus \{0\}$, if $a + b \neq 0$, then $\nu_p(a+b) \geq \min\{\nu_p(a), \nu_p(b)\}$. Thus $\nu_p : {}^*\mathbb{Q} \setminus \{0\} \to p^{{}^*\mathbb{Z}}$ is a valuation, which is definable by a formula

$$d'_p(x,y) \equiv \exists x_1 x_2 y_1 y_2 \, (x_2 x = x_1 \wedge y_2 y = y_1 \wedge d_p(x_1, y_1) \wedge d_p(x_2, y_2)).$$

We already note that ${}^*\mathbb{Q}$ has the order $<$ which gives the absolute value $|a| = a$ if $0 \leq a$ and $= -a$ otherwise. Consider an order $<$ on ${}^*\mathbb{Z}$ as $a < b$ if $b - a \in {}^*\mathbb{N}$ and extend $<$ on ${}^*\mathbb{Q}$ by defining $a_1/b_1 < a_2/b_2$ with $a_1, a_2 \in {}^*\mathbb{Z}$ and $b_1, b_2 \in {}^*\mathbb{N}$ if $a_2 b_1 - a_1 b_2 \in {}^*\mathbb{N}$. This ordering is definable by a formula

$$\begin{aligned} x < y \equiv \exists x_1 x_2 y_1 y_2 \big(&Z(x_1) \wedge Z(y_1) \wedge N(x_2) \wedge N(y_2) \\ &\wedge (xx_2 = x_1) \wedge (yy_2 = y_1) \wedge N(y_1 x_2 - x_1 y_2)\big). \end{aligned}$$

Using these valuations and the absolute value, we get the following theorem:

Theorem 3.3. *For $a_0, a_1 \in {}^*\mathbb{Q} \setminus \{0\}$,*

$a_0 = a_1$ if and only if $\nu_p(a_0) = \nu_p(a_1)$ for all $p \in \mathcal{P}({}^*\mathbb{N})$ and $|a_0 a_1| = a_0 a_1$.

We have an injective group homomorphism from ${}^*\mathbb{Q} \setminus \{0\}$ to $\prod_{p \in \mathcal{P}({}^*\mathbb{Z})} p^{{}^*\mathbb{Z}} \times \{\pm 1\}$ by sending a to $((\nu_p(a))_p, a/|a|))$.

Proof. By Theorem 3.2, the following sentence

$$\phi \equiv \forall xy\Big(\big((xy \neq 0) \wedge \forall z\,(P(z) \to \forall w\,(d'_z(x,w) \leftrightarrow d'_z(y,w))) \wedge (x > 0 \leftrightarrow y > 0)\big) \to (x = y)\Big)$$

holds in $\mathbb{Q}$, and so does in ${}^*\mathbb{Q}$ because $\mathbb{Q} \equiv {}^*\mathbb{Q}$. □

As corollary, we have that ${}^*\mathbb{Z}$ is the intersection of all ν_p-valuation rings for $p \in \mathcal{P}({}^*\mathbb{N})$.

Corollary 3.4. *Let ${}^*\mathbb{Z}_p$ be the ν_p-valuation ring of ${}^*\mathbb{Q}$ for $p \in \mathcal{P}({}^*\mathbb{N})$. Then,*

$$ {}^*\mathbb{Z} = \bigcap_{p \in \mathcal{P}({}^*\mathbb{N})} {}^*\mathbb{Z}_p.$$

Remark 3.5. From Corollary 3.4, one can expect that for any two ideals I_1 and I_2 in ${}^*\mathbb{Z}$, if $I_1{}^*\mathbb{Z}_p = I_2{}^*\mathbb{Z}_p$ for all $p \in \mathcal{P}({}^*\mathbb{N})$, then $I_1 = I_2$. Unfortunately, this fails. If we take a nonprincipal ultrapower ${}^*\mathbb{Z}$ of $\mathbb{Z}$, there is a maximal ideal $\mathfrak{m}$ of ${}^*\mathbb{Z}$ which is not contained in $p{}^*\mathbb{Z}$ for any $p \in \mathcal{P}({}^*\mathbb{N})$. This maximal ideal satisfies $\mathfrak{m}{}^*\mathbb{Z}_p = {}^*\mathbb{Z}_p$ for all $p \in \mathcal{P}({}^*\mathbb{N})$ but $\mathfrak{m} \neq {}^*\mathbb{Z}$.

References

[1] M. Bhargava and A. Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. **181**, (2015), no. 1, 191–242.

[2] H. B. Enderton, *A Mathematical Introduction to Logic*, 2nd edition, Academic Press, 2001.

[3] M. D. Fried and M. Jarden, *Field Arithmetic*, 3rd edition, Springer,Berlin, 2008.

[4] D. Marker, *Model Theory: An Introduction*, Springer, New York, 2002.

[5] J. Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114.

[6] ———, *The undecidability of algebraic rings and fields*, Proc. Amer. Math. Soc. **10** (1959), 950–957.

[7] K. Rubin and A. Silverberg, *Ranks of elliptic curves in families of quadratic twists*, Experiment. Math. **9** (2000), no. 4, 583–590.

[8] ———, *Ranks of elliptic curves*, Bull. Amer. Math. Soc. **39** (2002), no. 4, 455–471.

[9] I. R. Shafarevich and J. Tate, *The rank of elliptic curves*, AMS Transl. **8** (1967), 917–920.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition, Springer, New York, 2009.

[11] D. Ulmer, *Elliptic curves with large rank over function fields*, Ann. of Math. **155** (2002), no. 1, 295–315.

Junguk Lee
Department of Mathematics
Yonsei University
Seoul 03722, Korea
E-mail address: ljw@yonsei.ac.kr