Integral points for multi-norm tori

Dasheng Wei and Fei Xu

Abstract

We construct a finite subgroup of Brauer–Manin obstruction for detecting the existence of integral points on integral models of principle homogeneous spaces of multi-norm tori. Several explicit examples are provided.

Introduction

The integral points on homogeneous spaces of semi-simple and simply connected linear algebraic groups of noncompact type were studied by Borovoi and Rudnick in [2] and by Colliot-Thélène and the second named author in [3] by using the strong approximation theorem and the Brauer–Manin obstruction. Recently, Harari [7] showed that the Brauer–Manin obstruction accounts for the nonexistence of integral points. Colliot-Thélène noticed that a finite subgroup of the Brauer group is enough to account for the nonexistence of integral points by the compactness argument. However, this result is nonconstructive: one does not know which finite subgroup to use and cannot use it to determine the existence of integral points on the specific equations. In this paper, we give some explicit construction for such finite subgroups for multi-norm tori. The paper is also inspired by Colliot-Thélène’s suggestion of studying Gauss’ idea for determining integers represented by positive definite binary quadratic forms, which is beautifully explained by Cox in [4], from the point of view of Brauer–Manin obstruction. The advantage of using Brauer–Manin obstruction is to provide more perspective. For example, one can determine the solvability of the negative Pell equations by using the class field theory instead of the continued fractional method (the quadratic Diophantine approximation).

The paper is organized as follows. In Section 1, we construct the idele groups which are the so-called X-admissible groups for determining the integral points for some integral model X. In Section 2, we interpret the X-admissible subgroup in terms of finite Brauer–Manin obstruction and also explain that there is no finite Brauer–Manin obstruction to detect all separated integral models of finite type. In Section 3, we apply our construction to study the classical binary quadratic Diophantine equations. Such classical quadratic Diophantine equations have been studied for a long time by various methods. This construction is the natural extension of Gauss’ method for determining integers represented by a positive definite integral binary quadratic form and one can further determine all integers represented by a given binary inhomogeneous quadratic Diophantine equation. In Section 4, we provide several examples of 1-dimensional non-split tori where the splitting fields are imaginary quadratic fields. In Section 5, some examples of 1-dimensional non-split tori where the splitting fields are real quadratic fields are studied. In Section 6, we explain how to apply our construction to study the high-dimensional multi-norm tori by providing some more explicit examples.
Notation and terminology are standard if not explained. Let $F$ be a number field, $\mathfrak{o}_F$ be the ring of integers of $F$, $\Omega_F$ be the set of all primes in $F$ and $\infty_F$ be the set all infinite primes in $F$. For simplicity, we write $p < \infty_F$, for $p \in \Omega_F \setminus \infty_F$. Let $F_p$ be the completion of $F$ at $p$ and $\mathfrak{o}_{F_p}$ be the local completion of $\mathfrak{o}_F$ at $p$, for each $p \in \Omega_F$. Write $\mathfrak{o}_{F_p} = F_p$, for $p \in \infty_F$. For any positive integer, we use $(F_p^{x})^k$ (resp. $(F_p^{x})^{\emptyset}$) to denote the subgroup of $k$th powers in $F^x$ (resp. $F_p^{x}$). We also denote the adele (resp. the idele) of $F$ by $\mathbb{A}_F$ (resp. $\mathbb{I}_F$) and

$$F_{\infty} = \prod_{p \in \infty_F} F_p.$$ 

Let $E_1, \ldots, E_n$ be the finite extensions of $F$ and\n
$$\varphi : R_{E_1/F}(\mathbb{G}_m) \times \ldots \times R_{E_n/F}(\mathbb{G}_m) \longrightarrow \mathbb{G}_m$$

be the homomorphism of algebraic groups which represents\n
$$(E_1 \otimes_F A)^x \times \ldots \times (E_n \otimes_F A)^x \longrightarrow A^x; (x_1, \ldots, x_n) \mapsto \prod_{i=1}^n N_{E_i/F}(x_i),$$

for any $F$-algebra $A$. Define $G := \ker \varphi$ which is called a multi-norm torus over $F$. Let $\hat{G} = \text{Hom}_F(\mathbb{G}_m, \mathbb{G}_m)$ be the characters of $G$ where $\hat{F}$ is an algebraic closure of $F$ and $\mathbf{X}$ be a separated $\mathfrak{o}_F$-scheme of finite type whose generic fiber $X_F$ is a principal homogeneous space of $G$. The obvious necessary conditions for $\mathbf{X}(\mathfrak{o}_F) \neq \emptyset$ are\n
$$\prod_{p \in \Omega_F} \mathbf{X}(\mathfrak{o}_{F_p}) \neq \emptyset \text{ and } X_F(F) \neq \emptyset$$\n
(A)

which is assumed throughout this paper. It should be pointed out that the determination of $X_F(F) \neq \emptyset$ or not is well understood (see [1]).

The Brauer group $\text{Br}(X_F)$ of $X_F$ is defined as\n
$$\text{Br}(X_F) = H^2_{et}(X_F, \mathbf{G}_m) \text{ and } \text{Br}_1(X_F) = \ker[\text{Br}(X_F) \longrightarrow \text{Br}(\hat{X})],$$

where $\hat{X} = X_F \times_F \hat{F}$. Since the image of $\text{Br}(F)$ induced by the structure morphism lies in $\text{Br}_1(X_F)$, one defines\n
$$\text{Br}_a(X_F) = \ker[\text{Br}(F) \longrightarrow \text{Br}_1(X)].$$

For any subgroup $\mathfrak{s}$ of $\text{Br}_a(X_F)$, one can define the integral Brauer–Manin set with respect to $\mathfrak{s}$ as (see [3])\n
$$\left( \prod_{p \in \Omega_F} \mathbf{X}(\mathfrak{o}_{F_p}) \right)^{\mathfrak{s}} = \left\{ (x_p) \in \prod_{p \in \Omega_F} \mathbf{X}(\mathfrak{o}_{F_p}) : \sum_{p \in \Omega_F} \text{inv}_p(s(x_p)) = 0, \forall s \in \mathfrak{s} \right\}.$$

1. **Construction of $\mathbf{X}$-admissible groups**

Since $\mathbf{X}$ is separated over $\mathfrak{o}_F$, one can view $\mathbf{X}(\mathfrak{o}_{F_p})$ as an open subset of $X_F(F_p)$ by the natural map, for any $p < \infty_F$, and $G(F_p)$ acts on $X_F(F_p)$ continuously.

**Definition 1.1.** Let\n
$$\text{Stab}(\mathbf{X}(\mathfrak{o}_{F_p})) = \{ g \in G(F_p) : g\mathbf{X}(\mathfrak{o}_{F_p}) = \mathbf{X}(\mathfrak{o}_{F_p}) \},$$

for $p < \infty_F$ and\n
$$\text{Stab}(\mathbf{X}(\mathfrak{o}_{F_p})) = G(F_p) \text{ for } p \in \infty_F.$$
Define
\[ \text{Stab}_A(X) = G(\mathbb{A}_F) \cap \prod_{p \in \Omega_F} \text{Stab}(X(\mathfrak{o}_{F_p})). \]

One has the following basic property of \( \text{Stab}_A(X) \).

**Lemma 1.2.** \( \text{Stab}_A(X) \) is an open subgroup of \( G(\mathbb{A}_F) \).

**Proof.** Since the stabilizer of an open subset is open by the continuity, one obtains that \( \text{Stab}(X(\mathfrak{o}_{F_p})) \) is an open subgroup of \( G(F_{p}) \), for all \( p \in \Omega_F \).

Let \( S \) be a finite subset of \( \Omega_F \) containing \( \infty_F \) such that \( G \) has a model \( G \) over \( \mathfrak{o}_S \) and the morphism \( G \times_F X_F \to X_F \) can be extended to \( G \times_{\mathfrak{o}_S} X_S \to X_S \) where \( \mathfrak{o}_S \) is the \( S \)-integers of \( F \) and \( X_S = X \times_{\mathfrak{o}_F} \mathfrak{o}_S \). This implies that \( \text{Stab}(X(\mathfrak{o}_{F_p})) \supseteq G(\mathfrak{o}_{F_p}) \) for all \( p \notin S \).

Therefore one concludes that \( \text{Stab}_A(X) \) is an open subgroup of \( G(\mathbb{A}_F) \). \( \square \)

Since \( G \) is the subgroup of \( R_{E_1/F}(\mathbb{G}_m) \times \ldots \times R_{E_n/F}(\mathbb{G}_m) \) by the definition of \( G \), one has the injective map
\[
\lambda_{(E_1,\ldots,E_n)} : G(A) \to (E_1 \otimes_F A)^{\times} \times \ldots \times (E_n \otimes_F A)^{\times},
\]
for any \( F \)-algebra \( A \).

**Definition 1.3.** An open subgroup \( \Xi \) of \( \prod_{i=1}^n I_{E_i} \) is called \( X \)-admissible, if
\[
\lambda_{(E_1,\ldots,E_n)}[\text{Stab}_A(X)] \subseteq \Xi
\]
and the map induced by \( \lambda_{(E_1,\ldots,E_n)} \)
\[
\lambda_{(E_1,\ldots,E_n)} : G(\mathbb{A}_F)/G(F)\text{Stab}_A(X) \to \prod_{i=1}^n I_{E_i}/\left( \prod_{i=1}^n E_i^{\times} \right) \cdot \Xi
\]
is injective.

Since \( X_F \) is a trivial \( G \)-torsor over \( F \), one can fix an isomorphism \( X_F \cong G \) induced by a rational point \( P \). Combining with \( \lambda_{(E_1,\ldots,E_n)} \), one can define the injective map
\[
f_{(E_1,\ldots,E_n)} : X_F(A) \cong G(A) \xrightarrow{\lambda_{(E_1,\ldots,E_n)}} \prod_{i=1}^n (E_i \otimes_F A)^{\times},
\]
for any \( F \)-algebra \( A \).

Since \( X \) is separated over \( \mathfrak{o}_F \), one can regard \( \prod_{p \in \Omega_F} X(\mathfrak{o}_{F_p}) \) as the subset of \( X_F(\mathbb{A}_F) \) by the natural morphism. Then
\[
f_{(E_1,\ldots,E_n)} \left( \prod_{p \in \Omega_F} X(\mathfrak{o}_{F_p}) \right) \subseteq \prod_{i=1}^n I_{E_i}.
\]

The following proposition explains the reason for introducing the concept of \( X \)-admissible subgroups.
**Proposition 1.4.** Let $\Xi$ be an $X$-admissible subgroup of $\prod_{i=1}^{n} I_{E_i}$. Then

$$X(\mathfrak{p}_{F}) \neq \emptyset$$

if and only if $f_{(E_1,\ldots,E_n)} \left[ \prod_{p \in \Omega_F} X(\mathfrak{p}_p) \right] \cap \left( \prod_{i=1}^{n} E_i^\times \right) \cdot \Xi \neq \emptyset$.

**Proof.** Since $X$ is separated over $\mathfrak{p}_F$, one has $X(\mathfrak{p}_F) \subseteq X(\mathfrak{p}_F')$, for all $p \in \Omega_F$ and $X(\mathfrak{p}_F') \subseteq \prod_{p \in \Omega_F} X(\mathfrak{p}_F')$

by the diagonal map. If $X(\mathfrak{p}_F) \neq \emptyset$, then

$$f_{(E_1,\ldots,E_n)} \left[ \prod_{p \in \Omega_F} X(\mathfrak{p}_p) \right] \cap \left( \prod_{i=1}^{n} E_i^\times \right) \cdot \Xi \supseteq f_{(E_1,\ldots,E_n)}[X(\mathfrak{p}_F)] \cap \left( \prod_{i=1}^{n} E_i^\times \right) \neq \emptyset$$

and the necessity follows.

Conversely, assume that

$$y_A \in \prod_{p \in \Omega_F} X(\mathfrak{p}_p) \text{ such that } f_{(E_1,\ldots,E_n)}(y_A) \in \left( \prod_{i=1}^{n} E_i^\times \right) \cdot \Xi.$$ 

By Definition 1.3, there are $g \in G(F)$ and $\sigma_A \in \text{Stab}_h(X)$ such that $y_A = g \sigma_A(P)$ by injectivity of $f_{(E_1,\ldots,E_n)}$. This implies that

$$g(P) = \sigma_A^{-1}(y_A) \in \prod_{p \in \Omega_F} X(\mathfrak{p}_p).$$

Therefore, $g(P) \in X(\mathfrak{p}_F) \neq \emptyset$ and the proof is complete. $\square$

If $\Xi$ is an $X$-admissible subgroup of $\prod_{i=1}^{n} I_{E_i}$, there is an open subgroup $\Xi_i$ of $I_{E_i}$, for each $1 \leq i \leq n$, such that $\prod_{i=1}^{n} \Xi_i \subseteq \Xi$. By the class field theory, there is a finite abelian extension $K_{\Xi_i}/E_i$ such that the Artin map

$$\psi_{K_{\Xi_i}/E_i} : \mathbb{I}_{E_i}/E_i^\times \Xi_i \cong \text{Gal}(K_{\Xi_i}/E_i)$$

(1.5)

gives the isomorphism for $1 \leq i \leq n$. Projecting the image of $f_{(E_1,\ldots,E_n)}$ to $\mathbb{I}_{E_i}$, one can define

$$f_{E_i} : \prod_{p \in \Omega_F} X(\mathfrak{p}_p) \longrightarrow \prod_{j=1}^{n} \mathbb{I}_{E_j} \longrightarrow \mathbb{I}_{E_i},$$

for $1 \leq i \leq n$.

**Corollary 1.6.** With the notation as above, $X(\mathfrak{p}_F) \neq \emptyset$ if and only if there is

$$x_A \in \prod_{p \in \Omega_F} X(\mathfrak{p}_p)$$

such that $\psi_{K_{\Xi_i}/E_i}(f_{E_i}(x_A)) = 1$

in $\text{Gal}(K_{\Xi_i}/E_i)$, for all $1 \leq i \leq n$.

**Proof.** Since $\psi_{K_{\Xi_i}/E_i}(f_{E_i}(x_A)) = 1$, for $1 \leq i \leq n$, one has

$$f_{(E_1,\ldots,E_n)}(x_A) \in \left( \prod_{i=1}^{n} E_i^\times \right) \cdot \left( \prod_{i=1}^{n} \Xi_i \right) \subseteq \left( \prod_{i=1}^{n} E_i^\times \right) \cdot \Xi.$$ 

Then the result follows from the same argument as those in Proposition 1.4. $\square$
The main purpose of this section is to construct such $X$-admissible groups. First, we need to the following lemma.

**Lemma 1.7.** If $C_p$ is an open subgroup of $G(F_p)$ and $k$ is a positive integer, then

$$\lambda_{(E_1, \ldots, E_n)}(C_p) \cdot \{(a, \ldots, a) : a \in (F_p^\times)^k\}$$

is an open subgroup of $\prod_{i=1}^n E_{i,p}^\times$ for $p$-adic topology with $p < \infty_F$.

**Proof.** Since $C_p$ is an open subgroup of $G(F_p)$, there are positive integers $a_1, \ldots, a_n$ such that

$$\left(1 + p^{a_i} \mathcal{O}_{E_{i,p}}\right) \subseteq \lambda_{(E_1, \ldots, E_n)}(G(F_p)) \subseteq \lambda_{(E_1, \ldots, E_n)}(C_p).$$

By Hensel’s lemma, there is a sufficiently large positive integer $b_i > a_i$ such that

$$(1 + p^{b_i} \mathcal{O}_{E_{i,p}}) \subseteq (1 + p^{a_i} \mathcal{O}_{E_{i,p}})^{l_i},$$

where $l = \sum_{i=1}^n l_i$ and $l_i = [E_i : F]$, for all $1 \leq i \leq n$.

If $(x_i)_{i=1}^n \in \prod_{i=1}^n (1 + p^{b_i} \mathcal{O}_{E_{i,p}})$,

then

$$(x_i)_{i=1}^n = (y_i^{l_i})_{i=1}^n \text{ with } (y_i)_{i=1}^n \in \prod_{i=1}^n (1 + p^{a_i} \mathcal{O}_{E_{i,p}}).$$

Since

$$y_i^{l_i} = \left[\left(\prod_{i=1}^n N_{E_i/F}(y_i)\right)^{-k}\right] \cdot \left[\prod_{i=1}^n N_{E_i/F}(y_i)\right]^{-k};$$

and

$$\left[\left(\prod_{i=1}^n N_{E_i/F}(y_i)\right)^{-k}\right]_{i=1}^n \in \lambda_{(E_1, \ldots, E_n)}(C_p),$$

one concludes that

$$\prod_{i=1}^n (1 + p^{b_i} \mathcal{O}_{E_{i,p}}) \subseteq \lambda_{(E_1, \ldots, E_n)}(C_p) \cdot \{(a, \ldots, a) : a \in (F_p^\times)^k\}$$

and the proof is complete.

In order to prove the existence of $X$-admissible groups, we further need the following lemma.

**Lemma 1.8.** Let $k$ be a positive integer. Then there is a finite subset $T_0$ of $\Omega_F \setminus \infty_F$ such that

$$F^\times \cap \left[\prod_{p \in T} (F_p^\times)^{2kh_F} \times \prod_{p \notin T} \mathcal{O}_{F_p}^\times\right] \subseteq (F^\times)^k,$$

for any $T \supseteq T_0$, where $h_F$ is the class number of $F$. 
Proof. Since $\alpha_i(\mathfrak{o}_F^\times)^{2k}$ is finite by the Dirichlet unit theorem, there are only finitely many cosets $\alpha_i(\mathfrak{o}_F^\times)^{2k}$ of $\mathfrak{o}_F^\times$ such that $\alpha_i \notin (F_\infty^\times)^{2k}$, for some prime $p_i < \infty$. Fix one such prime $p_i$ for each $\alpha_i(\mathfrak{o}_F^\times)^{2k}$ and define $T_0$ to be the set consisting of all such $p_i$. It is possible that $T_0$ is empty.

Let

$$\alpha \in F^\times \cap \left[ \prod_{p \in T} (F_\infty^\times)^{2k} \times \prod_{p \notin T} \mathfrak{o}_F^\times \right],$$

for any finite set $T \supseteq T_0$. Since $p^{h_F}$ is a principal ideal, there is $\varpi_p \in F$ such that $p^{h_F} = \varpi_p \mathfrak{o}_F$, for each finite $p \in T$. There is $t_p \in \mathbb{Z}$, for each finite $p \in T$ such that

$$\beta = \alpha \left( \prod_{p \in T \setminus \infty_F} \varpi_p^{t_p} \right)^{2k} \in \mathfrak{o}_F^\times.$$

Then $\beta(\mathfrak{o}_F^\times)^{2k}$ is not one of the above-mentioned cosets $\alpha_i(\mathfrak{o}_F^\times)^{2k}$. This implies that

$$\alpha \in F^\times \cap \left[ \prod_{p \in \infty_F} F_p^\times \times \prod_{p \notin \infty_F} (F_\infty^\times)^{2k} \right].$$

Therefore,

$$F^\times \cap \left[ \prod_{p \in T} (F_\infty^\times)^{2k} \times \prod_{p \notin T} \mathfrak{o}_F^\times \right] \subseteq F^\times \cap \left[ \prod_{p \in \infty_F} F_p^\times \times \prod_{p \notin \infty_F} (F_\infty^\times)^{2k} \right].$$

Let

$$x \in F^\times \cap \left[ \prod_{p \in \infty_F} F_p^\times \times \prod_{p \notin \infty_F} (F_\infty^\times)^{2k} \right].$$

Applying (9.1.3) Theorem in [11] for $\mu_{2k}$, one obtains that $x^2 \in (F^\times)^{2k}$. There is $y \in F^\times$ such that $x = y^k$ or $x = -y^k$.

Suppose $x = -y^k$. Let $k = 2s_1 k_1$ with $2 \mid k_1$ and $\zeta_{2s_1}$ be a primitive $2s_1$th roots of unity. Then $\zeta_{2s_1} \in F_\infty^\times$, for all $p < \infty$. By the Chebotarev density theorem, one concludes that $\zeta_{2s_1} \in F$. Therefore, $-1 = (\zeta_{2s_1})^k \in (F^\times)^k$ and the proof is complete. \hfill $\Box$

The proof of Lemma 1.8 also provides the explicit method to determine the set $T_0$. For example, when $F = \mathbb{Q}$, one has $T_0 = \{2\}$ or $\{p\}$ with $p \equiv 3 \mod 4$. The following corollary has its own independent interest.

**Corollary 1.9.** For any open subgroup $\Xi$ of $\mathbb{I}_F$ and a positive integer $k$, there is an open subgroup $\Xi_k$ of $\mathbb{I}_F$ such that $(F^\times \cap \Xi_k) \subseteq (F^\times \cap \Xi)^k$.

**Proof.** Let $\Xi_p$ be an open subgroup of $F_p$ for each $p \in \Omega_F$ such that $\prod_{p \in \Omega_F} \Xi_p \subseteq \Xi$ and $\Xi_p = \mathfrak{o}_p^\times$ for almost all $p \in \Omega_F$. Let $S_0$ be a finite subset of $\Omega_F$ such that $\Xi_p = \mathfrak{o}_p^\times$ for all $p \notin S_0$. For each $p \in S_0$ and for a prime divisor $q$ of $k$, one defines $t_p(q)$ to be the maximal positive integer $t$ such that the primitive $q^t$-th roots of unity are in $F_p$. Let

$$t_p := \max\{t_p(q) : \text{prime divisor } q \text{ of } k\} \quad \text{and} \quad r := \prod_{p \in S_0} (t_p + 1).$$
Applying Lemma 1.8 for \( k^{r+1} \), one obtains a finite subset \( T_0 \) of \( \Omega_F \). Let \( S = S_0 \cup T_0 \) and defines

\[
\Xi_k = \prod_{p \in S} \Xi_p^{2h_F k^{r+1}} \times \prod_{p \not\in S} \Xi_p.
\]

For any \( x \in (F^\times \cap \Xi_k) \), there is \( y \in F^\times \) such that \( x = y^{k^{r+1}} \) by Lemma 1.8. Moreover, there is \( \xi_p \in \Xi_p \) such that

\[
x = y^{k^{r+1}} = \xi_p^{k^{r+1}},
\]

for all \( p \in S \).

If \( p \in S_0 \), one has that

\[
y^{k^r} = \xi_p^{k^r} \in \Xi_p
\]

by the maximality of \( t_p \).

If \( p \not\in S_0 \), one has

\[
y^{k^r} \in \sigma_p^\times \Xi_p = \Xi_p.
\]

Therefore, \( y^{k^r} \in (F^\times \cap \Xi) \) and the proof is complete.

Now we can show the existence of the admissible subgroups for \( X \).

**Theorem 1.10.** The \( X \)-admissible subgroups of \( \prod_{i=1}^n \mathbb{E}_i \) always exist.

**Proof.** Since \( X_F \) is a trivial torsor over \( F \) under \( G \), there is a finite subset \( S_0 \subset (\Omega_F \setminus \infty_F) \) such that:

1. The map \( \varphi \) can be extended to

\[
\Phi : R_{\sigma_{E_1,S_0}/\sigma_{F,S_0}}(\mathbb{G}_m) \times \cdots \times R_{\sigma_{E_n,S_0}/\sigma_{F,S_0}}(\mathbb{G}_m) \longrightarrow \mathbb{G}_m
\]

over \( \sigma_{F,S_0} \), where \( \sigma_{F,S_0} \) and \( \sigma_{E_1,S_0}, \ldots, \sigma_{E_n,S_0} \) are the \( S_0 \)-integers of \( F \) and \( E_1, \ldots, E_n \), respectively. Moreover, \( \ker(\Phi) = G \) is a model of \( G \) over \( \sigma_{F,S_0} \).

2. \( X_{S_0} \) is a trivial torsor over \( \sigma_{S_0} \) under \( G \), where \( X_{S_0} = X \times_{\sigma_F} \sigma_{F,S_0} \).

This implies that

\[
\lambda_{(E_1, \ldots, E_n)}[\text{Stab}(X(\sigma_{F,p}))] = \ker \left( \prod_{i=1}^n N_{E_i/F} : \prod_{i=1}^n \sigma_{E_i,p}^\times \longrightarrow \sigma_{F,p}^\times \right),
\]

for every \( p \not\in S_0 \).

Let \( l = \sum_{i=1}^n l_i \) with \( l_i = [E_i : F] \), for all \( 1 \leq i \leq n \). For each \( p \in S_0 \) and prime divisor \( q \) of \( l \), one defines \( t_p(q) \) to be the maximal positive integer \( t \) such that the primitive \( q^t \) th roots of unity are in \( F_p \). Let

\[
t_p := \max\{t_p(q) : q \text{ divides } l\} \quad \text{and} \quad r := \prod_{p \in S_0} (t_p + 1).
\]

Let \( T_0 \) be a finite subset of \( \Omega_F \) outside \( \infty_F \) such that Lemma 1.8 holds for \( k = l^{r+1} \). Put \( S = S_0 \cup T_0 \) and

\[
\Xi = \left[ \prod_{p \in S} \lambda_{(E_1, \ldots, E_n)}[\text{Stab}(X(\sigma_{F,p}))] \cdot H_p \right] \times \left( \prod_{i=1}^n \prod_{p \not\in S} \sigma_{E_{i,p}}^\times \right),
\]

where

\[
H_p = \{(a, \ldots, a) : a \in (F_p^\times)^{2l^{r+1}} \}
\]
and \( h_F \) is the class number of \( F \). By Lemma 1.7, one has that \( \Xi \) is an open subgroup of \( \prod_{i=1}^{n} \mathbb{I}_{E_i} \) and

\[
\lambda_{(E_1,\ldots,E_n)}[\text{Stab}_k(X)] \subseteq \Xi.
\]

Suppose \( \sigma \in G(A_F) \) with \( \lambda_{(E_1,\ldots,E_n)}(\sigma) = a \iota \) where

\[
a = (a_i)_{i=1}^{n} \in \prod_{i=1}^{n} E_i^\times \quad \text{and} \quad i \in \Xi.
\]

Then

\[
\prod_{i=1}^{n} N_{E_i/F}(a_i) \in \left[ \prod_{\mathfrak{p} \in S} (F_{\mathfrak{p}}^\times)^{2n+1} h_F \times \prod_{\mathfrak{p} \notin S} \mathfrak{o}_{F_{\mathfrak{p}}}^\times \right].
\]

By Lemma 1.8, there is \( u \in F^\times \) such that \( \prod_{i=1}^{n} N_{E_i/F}(a_i) = u^{n+1} \). This implies that

\[
(a_1u^{-t'}, \ldots, a_nu^{-t'}) \in \lambda_{(E_1,\ldots,E_n)}(G(F)).
\]

Write \( i = (i_{\mathfrak{p}})_{\mathfrak{p} \in \Omega_F} \) and \( i_{\mathfrak{p}} = s_{\mathfrak{p}} \cdot (n_{\mathfrak{p}}, \ldots, n_{\mathfrak{p}}) \) with

\[
s_{\mathfrak{p}} \in \lambda_{(E_1,\ldots,E_n)}(\text{Stab}(X(\mathfrak{o}_{F_{\mathfrak{p}}}))) \quad \text{and} \quad n_{\mathfrak{p}} \in (F_{\mathfrak{p}}^\times)^{2n+1} h_F
\]

for \( \mathfrak{p} \in S \). Therefore, \( u^{n_{\mathfrak{p}}+1} = 1 \) for \( \mathfrak{p} \in S \).

If \( \mathfrak{p} \in S_0 \), one has that \( u^{n_{\mathfrak{p}}} = 1 \) by the maximality of \( t_{\mathfrak{p}} \).

If \( \mathfrak{p} \in S \setminus S_0 \), one has

\[
u^t (n_{\mathfrak{p}}, \ldots, n_{\mathfrak{p}}) \in \ker \left( \prod_{i=1}^{n} N_{E_i/F} : \prod_{i=1}^{n} \mathfrak{o}_{E_{\mathfrak{p}}}^\times \longrightarrow \mathfrak{o}_{F_{\mathfrak{p}}}^\times \right).
\]

Therefore one concludes that

\[
u^t i \in \lambda_{(E_1,\ldots,E_n)}[\text{Stab}_k(X)] \quad \text{and} \quad \sigma \in G(F) \text{ Stab}_k(X)
\]

and the proof is complete.

\[\square\]

2. \textit{Finite Brauer–Manin obstruction}

In this section, we interpret the \( X \)-admissible subgroup in terms of Brauer–Manin obstruction. We keep the same notation as before. By the definition of \( G \), one has the surjective map

\[
R_{E_1/F}(\mathbb{G}_m) \times \ldots \times R_{E_n/F}(\mathbb{G}_m) \longrightarrow \hat{G}
\]

which induces

\[
\phi : \prod_{i=1}^{n} H^2(F, R_{E_i/F}(\mathbb{G}_m)) = \prod_{i=1}^{n} H^2(E_i, \mathbb{Z}) \longrightarrow H^2(F, \hat{G}) \tag{2.1}
\]

by Shapiro’s lemma (see (1.6.3) Proposition in [11]).

Let \( \Xi \) be an \( X \)-admissible subgroup of \( \prod_{i=1}^{n} \mathbb{I}_{E_i} \). There is an open subgroup \( \Xi_i \) of \( \mathbb{I}_{E_i} \), for each \( 1 \leq i \leq n \) such that \( \prod_{i=1}^{n} \Xi_i \subseteq \Xi \). By the class field theory, there is a finite abelian extension \( K_{\Xi_i}/E_i \) satisfying (1.5), for \( 1 \leq i \leq n \).

By the short exact sequence

\[
0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0
\]

with the trivial action of \( \text{Gal}(K_{\Xi_i}/E_i) \), one obtains an isomorphism of finite groups

\[
\delta_i : \text{Hom}(\text{Gal}(K_{\Xi_i}/E_i), \mathbb{Q}/\mathbb{Z}) \cong H^2(\text{Gal}(K_{\Xi_i}/E_i), \mathbb{Z}). \tag{2.2}
\]
Let $b_i(\Xi_i)$ be the image of the inflation
\[ H^2(\Gal(K_{\Xi_i}/E_i), \mathbb{Z}) \longrightarrow H^2(E_i, \mathbb{Z}), \quad (2.3) \]
for $1 \leq i \leq n$. Since $X_F \cong G$ by the fixed rational point $P$, one has
\[ \rho : H^2(F, \hat{G}) \cong \Br_1(G) \cong \Br_1(X_F) \]
by [18, Theorem 1 of §4.3]. Let $b(\Xi)$ be the subgroup of $\Br_1(X_F)$ generated by the image of
\[ \{b_i(\Xi_i)\}_{i=1}^n \]
under the map $\rho \circ \phi$. It is clear that $b(\Xi)$ is finite.

**Proposition 2.4.** With the above notation,
\[ \mathbf{X}(\sigma_P) \neq \emptyset \text{ if and only if } \left[ \prod_{p \in \Omega_F} \mathbf{X}(\sigma_{F_p}) \right]^{b(\Xi)} \neq \emptyset. \]

**Proof.** One only needs to show the sufficiency. For any
\[ \chi \in \text{Hom}(\Gal(K_{\Xi_i}/E_i), \mathbb{Q}/\mathbb{Z}) \text{ and } (x_p)_{p \in \Omega_F} \in \left[ \prod_{p \in \Omega_F} \mathbf{X}(\sigma_{F_p}) \right]^{b(\Xi)}, \]
there is $\sigma_p \in G(\hat{A}_F)$ such that
\[ f_{(E_1, \ldots, E_n)}((x_p)_{p \in \Omega_F}) = \lambda_{(E_1, \ldots, E_n)}((\sigma_p)_{p \in \Omega_F}). \]
Since
\[ H^1(K_{\Xi_i}, \mathbb{Z}) \cong \text{Hom}_{\text{cont}}(\Gal(\hat{E}/K_{\Xi_i}), \mathbb{Z}) = 0, \]
the inflation map in (2.3) is injective. One can view $\delta_i(\chi) \in b_i(\Xi_i)$ and obtain
\[ 0 = \sum_{p \in \Omega_F} \inv_p(\rho \circ \phi(\delta_i(\chi))(x_p)) = \sum_{p \in \Omega_F} \inv_p(\phi(\delta_i(\chi))(\sigma_p)) \\
= \sum_{p \in \Omega_F} \inv_p(\delta_i(\chi) \cup (\lambda_{(E_1, \ldots, E_n)}(\sigma_p))) = \chi(\psi_{K_{\Xi_i}/E_i}(\lambda_{(E_1, \ldots, E_n)}((\sigma_p)_{p \in \Omega_F}))) \]
by the functoriality of the Brauer–Manin pairing (see [17, (5.3)]), the compatibility of Bauer–Manin pairing with the cup product (see [8, Section 6]) and (8.1.11) Proposition in [11]. This implies
\[ \psi_{K_{\Xi_i}/E_i}(f_{E_i}((x_p)_{p \in \Omega_F}) = 0, \]
for all $1 \leq i \leq n$. The result follows from Corollary 1.6. \qed

It should be pointed out that the finite subgroup $b(\Xi)$ of $\Br_1(X_F)$ depends on the integral
model $\mathbf{X}$. In general, there does not exist a universal finite subgroup $s$ of $\Br_1(X_F)$, which can be used to test the existence of the integral points for all integral model $\mathbf{X}$ of $X_F$.

**Example 2.5.** Let $F = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{-1})$ and
\[ G = X_\mathbb{Q} = \mathbb{R}_{E/F}(\mathbb{G}_m) = \text{Spec}(\mathbb{Q}[x, y]/(x^2 + y^2 - 1)). \]
For any finite subgroup $s$ of $\Br_1(X_\mathbb{Q})$, there exists a separated $\mathbb{Z}$-scheme $\mathbf{X}$ of finite type with the generic fiber $X_\mathbb{Q}$ such that
\[ \left( \prod_{p \leq \infty} \mathbf{X}(\mathbb{Z}_p) \right)^s \neq \emptyset \text{ but } \mathbf{X}(\mathbb{Z}) = \emptyset. \]
Proof. Since \((x + \sqrt{-1}y)(x - \sqrt{-1}y) = x^2 + y^2\), one has
\[
\overline{Q}[X_{\overline{Q}}]^x = \overline{Q}^x \times f_E^Z \quad \text{with} \quad f_E = x + y\sqrt{-1}.
\]
Define
\[
\Ind_{\text{Gal}(\overline{Q}/Q)}^{\text{Gal}(\overline{Q}/E)}(f_E^Z) \longrightarrow f_E^Z, \quad \xi \mapsto \sum_{\sigma \in \text{Gal}(E/Q)} \sigma \xi(\sigma^{-1}).
\]
One has the exact sequence of \(\text{Gal}(\overline{Q}/Q)\)-module
\[
1 \longrightarrow \mathbb{Z} \longrightarrow \Ind_{\text{Gal}(\overline{Q}/Q)}^{\text{Gal}(\overline{Q}/E)}(f_E^Z) \longrightarrow f_E^Z \longrightarrow 1.
\]
The Galois cohomology gives
\[
H^2(Q, \Ind_{\text{Gal}(\overline{Q}/Q)}^{\text{Gal}(\overline{Q}/E)}(f_E^Z)) \longrightarrow H^2(Q, f_E^Z) \longrightarrow H^3(Q, \mathbb{Z}).
\]
By [10, Corollary 4.17], one has \(H^3(Q, \mathbb{Z}) = 0\). By Shapiro’s lemma (see (1.6.4) Proposition [11]), the corestriction map
\[
\text{cor}_{E/Q} : H^2(E, f_E^Z) \longrightarrow H^2(Q, f_E^Z) \quad (2.6)
\]
is surjective. Since \(\text{Gal}(\overline{Q}/E)\) acts on \(f_E^Z\) trivially, one gets
\[
\delta : \text{Hom}(\text{Gal}(\overline{Q}/E), Q/\mathbb{Z}) \cong H^2(E, f_E^Z) \quad (2.7)
\]
by using the exact sequence with the trivial action
\[
0 \longrightarrow \mathbb{Z} \longrightarrow Q \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0.
\]
By [18, Theorem 1 of § 4.3], there is a finite subgroup
\[
S \subset \text{Hom}(\text{Gal}(\overline{Q}/E), Q/\mathbb{Z}) \quad \text{such that} \quad \text{cor}_{E/Q} \circ \delta(S) = s.
\]
By the class field theory, there are a finite abelian extension \(K_S/E\) such that
\[
S = \{ \chi \in \text{Hom}(\text{Gal}(\overline{Q}/E), Q/\mathbb{Z}) : \chi|_{\text{Gal}(\overline{Q}/K_S)} = 1 \}
\]
and an open subgroup \(U\) of \(I_E\) with
\[
\psi_S : I_E/E^x U \cong \text{Gal}(K_S/E)
\]
via the Artin map. Let \(l\) be an odd prime such that the invertible elements of the \(l\)-adic completion of \(\mathfrak{o}_E\) are contained in \(U\). Define \(X\) by the equations
\[
\begin{align*}
x^2 + y^2 &= 1, \\
x - l + l^2 z &= 0.
\end{align*}
\]
By Hensel’s lemma, there is \(y_0 \in \mathbb{Z}_l\) such that \((1 - l)^2 + 2y_0 + l^2y_0^2 = 0\). Choose the local solution \((s_p)_p \in \prod_{p \leq \infty} X(\mathbb{Z}_p)\) by
\[
s_p = (x_p, y_p, z_p) = \begin{cases} 
(1, 0, l^2(1 - l)) & \text{if} \ p \neq l, \\
(l(1 - l), 1 + l^2y_0, 1) & \text{if} \ p = l.
\end{cases}
\]
Since \(f_E(s_p)_p \in \prod_{p \mid \mathfrak{p}} E_p\) and more precisely
\[
f_E((x_p, y_p, z_p)) = \begin{cases} 
(x_p + y_p\sqrt{-1}, x_p - y_p\sqrt{-1}) & \text{if} \ p \text{ splits in} \ E/\mathbb{Q}, \\
x_p + y_p\sqrt{-1} & \text{otherwise}
\end{cases}
\]
for all primes \(p\) including \(\infty\), one has \(f_E((s_p)_p) \in U\). For any \(\beta \in \mathfrak{s}\), there is \(\chi \in S\) such that \(\beta = \text{cor}_{E/Q} \circ \delta(\chi)\). By [11, (8.1.4) Proposition and (7.1.4) Corollary], one has
\[
\sum_{p \leq \infty} \text{inv}_p(\beta(s_p)) = \sum_{p \in \Omega_E} \text{inv}_p(\delta(\chi)(s_p)).
\]
By [11, (8.1.11) Proposition], one concludes that
\[ \sum_{p \in \Omega_E} \text{inv}_p(\delta(\chi)(s_p)) = \chi(\psi_S(f_E((s_p)_p))) = 0. \]

This implies that
\[ (s_p)_{p \in \infty} \in \left( \prod_{p \in \infty} X(\mathbb{Z}_p) \right)^s. \]

However, it is clear that \( X(\mathbb{Z}) = \emptyset. \) \( \square \)

3. Binary quadratic Diophantine equations

In this section, we apply the results in the previous sections to \( \sigma_F \)-scheme \( X \) defined by the following irreducible polynomial:
\[ ax^2 + bxy + cy^2 + ex + fy + g = 0 \]  
(3.1)

\[ \text{with } a, b, c, e, f, g \in \sigma_F \text{ and } -d = b^2 - 4ac \in F^x. \]

Let \( V = Fv_1 + Fv_2 \) be a 2-dimensional quadratic space over \( F \) with a basis \( \{v_1, v_2\} \) and the associated symmetric bilinear map \( B : V \times V \to F \) satisfying
\[ B(v_1, v_1) = a, \quad B(v_2, v_2) = c \quad \text{and} \quad B(v_1, v_2) = \frac{1}{2} b. \]

Let the group \( G \) represent \( \text{SO}(V \otimes_F A) \), for any \( F \)-algebra \( A \). Then \( X_F \) is a \( G \)-torsor over \( F \) and \( G(F) = \text{SO}(V) \). Let \( \text{SO}_h(V) \) and \( GL_h(V) \) be the adelic groups of \( \text{SO}(V) \) and \( GL(V) \), respectively.

An \( \sigma_F \)-lattice \( L \) in \( V \) is defined as a finitely generated \( \sigma_F \)-module satisfying \( FL = V \) and \( L_p \) is the local completion of \( L \) inside the local completion \( V_p \) of \( V \) at \( p \), for \( p < \infty_F \) and \( L_p = V_p \), for \( p \in \infty_F \).

**Lemma 3.2.** Let \( L \) be an \( \sigma_F \)-lattice in \( V \) and \( u_0 \in V \). For any \( (\sigma_p)_{p \in \Omega_F} \in GL_h(V) \), there is a unique \( \sigma_F \)-lattice \( L' \) in \( V \) and \( u'_0 \in V \) unique up to elements in \( L' \) such that
\[ L' + u'_0 = \sigma_p(L_p + u_0) \]
inside \( V_p \), for all \( p < \infty_F \).

**Proof.** By [13, 81:14], there is an \( \sigma_F \)-lattice \( L' \) of \( V \) such that \( L'_p = \sigma_p L_p \) for all \( p < \infty_F \). By the strong approximation theorem for \( \mathbb{G}_m \), there is \( u'_0 \in V \) such that
\[ \sigma_p u_0 - u'_0 \in L'_p, \]
for all \( p < \infty_F \). Therefore,
\[ L'_p + u'_0 = L'_p + \sigma_p u_0 = \sigma_p L_p + \sigma_p u_0 = \sigma_p(L_p + u_0), \]
for all \( p < \infty_F \) as required.

Suppose there is an \( \sigma_F \)-lattice \( M \) in \( V \) and \( x_0 \in V \) such that
\[ x_0 + M_p = u'_0 + L'_p, \]
for all \( p < \infty_F \). This implies that \( M_p = L'_p \) and \( x_0 - u'_0 \in L'_p \), for all \( p < \infty_F \). Therefore, \( M = L' \) and \( x_0 - u'_0 \in L' \) and the uniqueness follows. \( \square \)
By Lemma 3.2, one can define the action of $GL_A(V)$ on $L + u_0$ and set

$$SO_A(L + u_0) = \{ \sigma \in SO_A(V) : \sigma(L + u_0) = (L + u_0) \}.$$ 

By (A), $X_F(F) \neq \emptyset$ by the Hasse principle. To fix a rational point $P$ in $X_F(F)$ is equivalent to fix a non-zero vector $x_0 \in V$ such that

$$B(x_0, x_0) = B(u_0, u_0) - g.$$ 

In particular, we can choose

$$L = \sigma_F v_1 + \sigma_F v_2 \quad \text{and} \quad u_0 = d^{-1}(2ce - bf)v_1 + d^{-1}(2af - be)v_2 \in V.$$ 

If $\sigma \in SO(V)$ with $\sigma x_0 \in (L + u_0)$, there are $\alpha, \beta \in \sigma_F$ such that $\sigma x_0 = \alpha v_1 + \beta v_2 + u_0$. One can verify that $(\alpha, \beta)$ is a solution of the equation (3.1). This gives the map

$$\{ \sigma \in SO(V) : \sigma x_0 \in (L + u_0) \} \rightarrow X(\sigma_F).$$ 

In fact, this map is bijective by the Witt theorem [13, 42:16 and 42:17]. One can also extend this bijection to

$$X(\sigma_{F_p}) \cong \{ \sigma \in SO(V_F) : x_0 \in \sigma(L_p + u_0) \},$$ 

for all $p < \infty_F$. Since $u_0 \in L_p$ and $\sigma_{F_p} x_0$ splits $L_p$ for almost all $p$, one has

$$SO_A(L + u_0) \subseteq Stab_A(\mathbf{X})$$ 

with finite index. In practice, we replace $Stab_A(\mathbf{X})$ by $SO_A(L + u_0)$ which is much easier to be computed.

3.1. Split cases $-d = b^2 - 4ac \in (F^\times)^2$

Fix the isotropic basis of $V$

$$\{(b + \varpi)v_1 - 2av_2, (b - \varpi)v_1 - 2av_2\},$$

where $\varpi \in F^\times$ satisfying $\varpi^2 = b^2 - 4ac$. For any $F$-algebra $A$, there is a group isomorphism $SO(V \otimes_F A) \cong A^\times$ by sending $(\sigma \mapsto g)$ such that

$$\sigma((b + \varpi)v_1 - 2av_2) = g[(b + \varpi)v_1 - 2av_2].$$

The map gives $G \cong \mathbb{G}_m$. Such a case is not included in §1. However, this case is much simpler. Indeed one can factorize the Equation (3.1) into the following:

$$a \left[ x + \frac{b + \varpi}{2a} y + \frac{1}{2} \left( \frac{e}{a} + \frac{2f}{\varpi} \frac{eb}{a\varpi} \right) \right] \left[ x + \frac{b - \varpi}{2a} y + \frac{1}{2} \left( \frac{e}{a} + \frac{2f}{\varpi} - \frac{eb}{a\varpi} \right) \right] = (be^2 - c^2 - af^2)(b^2 - 4ac)^{-1} - g.$$ 

Define

$$f_F = 2ax + (b + \varpi)y + \left( e - \frac{2af}{\varpi} + \frac{eb}{\varpi} \right) \in F[X_F]^\times$$

which induces the injection

$$f_F : \prod_{p \in \Omega_F} X(\sigma_{F_p}) \rightarrow I_F.$$ 

With the above identification, one has

$$X(\sigma_F) \neq \emptyset \iff f_F \left[ \prod_{p \in \Omega_F} X(\sigma_{F_p}) \right] \cap [F^\times SO_A(L + u_0)] \neq \emptyset$$

by the same argument as those in Proposition 1.4. By the class field theory and [14, Theorem 8.1], there is a finite abelian extension $K_{L+u_0}/F$ such that the Artin map gives
the isomorphism
\[ \psi_{K_{L+u_0}/F} : \mathbb{I}_E/F^\times \text{SO}_k(L + u_0) \cong \text{Gal}(K_{L+u_0}/F). \]

The above criterion can be stated as \( X(\mathfrak{o}_F) \neq \emptyset \), if and only if there is
\[ x_A \in \prod_{p \in \Omega_F} X(\mathfrak{o}_F_p) \text{ such that } \psi_{K_{L+u_0}/F}(f_E(x_A)) = 1 \]
in \( \text{Gal}(K_{L+u_0}/F) \). This criterion does not need any knowledge of the fixed rational point \( P \) in \( X_F(F) \).

The class field theory only guarantees the existence of such abelian extension of \( K_{L+u_0}/F \). In order to obtain the explicit condition for \( X(\mathfrak{o}_F) \neq \emptyset \), one needs further explicit description of \( K_{L+u_0}/F \). There are no general theory for such explicit construction (Hilbert’s 12th problem) except the cyclotomic field theory over \( \mathbb{Q} \) and the complex multiplication theory of elliptic curves over imaginary quadratic fields (see [16]).

One can determine a finite set \( S \) which contains all ramification primes in \( K_{L+u_0}/F \). Such a set \( S \) can be chosen as all primes containing \( \infty_F \), all dyadic primes of \( F \), all finite primes such that \( x_0 \) or \( u_0 \) is not in \( L_F \), all finite primes such that \( B(x_0, x_0) \) or \( B(u_0, u_0) \) is not in \( \mathfrak{o}_F^\times \) and all primes such that \( L_F \) is not unimodular.

### 3.2. Non-split cases \( -d = b^2 - 4ac \notin (F^\times)^2 \)

Fix the orthogonal basis \( \{v_1, bv_1 - 2av_2\} \) of \( V \). For any \( F \)-algebra \( A \), there is a group isomorphism
\[ \text{SO}(V \otimes_F A) \cong \ker[(A \otimes_F E)^\times \overset{N_{E/F}}{\longrightarrow} A^\times]; \sigma \mapsto \alpha + \beta \sqrt{-d} \]
such that \( \sigma v_1 = \alpha v_1 + \beta (bv_1 - 2av_2) \), where \( E = F(\sqrt{-d}) \). This gives \( G \cong R_{E/F}(\mathbb{G}_m) \). By this identification, one can obtain an open subgroup \( \Xi \) of \( \mathbb{I}_E \) such that the map induced by inclusion
\[ \text{SO}_k(V)/\text{SO}(V) \text{SO}_k(L + u_0) \longrightarrow \mathbb{I}_E/E^\times \Xi \]
is injective by applying Theorem 1.10.

Let
\[ f_E = 2ax + (b + \sqrt{-d})y + \left( e - \frac{2af}{\sqrt{-d}} + \frac{eb}{\sqrt{-d}} \right) \in E[X_F \times_F E]^\times \]
which induces the injection
\[ f_E : \prod_{p \in \Omega_F} X(\mathfrak{o}_F_p) \longrightarrow \mathbb{I}_E. \]

By the same argument as those in Proposition 1.4, one has
\[ X(\mathfrak{o}_F) \neq \emptyset \Leftrightarrow f_E \left[ \prod_{p \in \Omega_F} X(\mathfrak{o}_F_p) \right] \cap (E^\times \Xi) \neq \emptyset. \]

Let \( K_\Xi/E \) be a finite abelian extension such that
\[ \psi_{K_\Xi/E} : \mathbb{I}_E/E^\times \Xi \cong \text{Gal}(K_\Xi/E) \]
by the Artin map. The above criterion can be stated as \( X(\mathfrak{o}_F) \neq \emptyset \) if and only if there is
\[ x_A \in \prod_{p \in \Omega_F} X(\mathfrak{o}_F_p) \text{ such that } \psi_{K_\Xi/E}(f_E(x_A)) = 1 \quad (3.3) \]
in \( \text{Gal}(K_\Xi/E) \).
Remark 3.4. The necessity of the above criterion does not need that \( \Xi \) is admissible. Therefore \( X(o_F) = \emptyset \), if there is an abelian extension \( K/E \) such that
\[
\psi_{K/E}(f_E(x_A)) \neq 1 \quad \text{for any } x_A \in \prod_{p \in \Omega_F} X(o_{F_p}),
\]
where \( \psi_{K/E} \) is the Artin map.

For determining a finite set \( S \) which contains all ramification primes in \( K_{\Xi}/F \), one needs to add \( T_0 \) in Lemma 1.8 as the part of \( S \) besides the above primes of \( F \) in split case.

4. Examples with imaginary quadratic splitting fields

In this section, we will provide some explicit examples with imaginary quadratic splitting fields over \( \mathbb{Q} \) to explain how to apply the result in §3 to obtain the explicit conditions for \( X(\mathbb{Z}) \neq \emptyset \). The explicit construction of the abelian extensions of the splitting fields with the required property is crucial. For the imaginary quadratic field case, such abelian extensions can be given by the complex multiplication of elliptic curves in principle (see [16, Theorem 5.5]). We will keep the same notation as that in §3.

The method described in §3 is also the natural extension of Gauss’ idea for determining the integral representation of the positive integers by a positive definite binary quadratic form. We explain this point by using one of the typical example \( x^2 + dy^2 \) with a positive integer \( d \), which is studied in detail in [4]. Let \( L = \mathbb{Z} + \mathbb{Z}\sqrt{-d} \) be an order in \( E = \mathbb{Q}(\sqrt{-d}) \).

Proposition 4.1. Let \( X \) be the scheme over \( \mathbb{Z} \) defined by \( x^2 + dy^2 = n \) for a positive integer \( n \), and \( K_L \) be the ring class field corresponding to the order \( L \). Then \( X(\mathbb{Z}) \neq \emptyset \) if and only if there is
\[
(x_p, y_p)_{p \leq \infty} \in \prod_{p \leq \infty} X(\mathbb{Z}_p) \text{ such that } \psi_{K_L/E} \left( \tilde{f}_E \left( \prod_{p \leq \infty} (x_p, y_p) \right) \right) = 1,
\]
where \( \psi_{K_L/E} \) is the Artin map and
\[
\tilde{f}_E[(x_p, y_p)] = \begin{cases} (x_p + y_p\sqrt{-d}, x_p - y_p\sqrt{-d}) & \text{if } p \text{ splits in } E/\mathbb{Q}, \\ (x_p + y_p\sqrt{-d}) & \text{otherwise}. \end{cases}
\]

Proof. Let \( p \) be a prime and \( L_p \) be the \( p \)-adic completion of \( L \) inside \( E_p = E \otimes_{\mathbb{Q}} \mathbb{Q}_p \). Since the ring class field \( K_L \) of the order \( L \) corresponds to the open subgroup \( E^\times (\prod_{p \leq \infty} L_p^\times) \) of \( \mathbb{I}_E \) by the class field theory, one only needs to show that \( \prod_{p \leq \infty} L_p^\times \) is a \( L \)-admissible subgroup of \( \mathbb{I}_E \) with \( L^\times_{\infty} = \mathbb{C}^\times \) by (3.3).

Since \( xL_p = L_p \), for \( x \in E_p^\times \) if and only if \( x \in L_p^\times \), one has
\[
\text{SO}(L_p) = \{ \alpha \in L_p^\times : N_{E_p/\mathbb{Q}_p}(\alpha) = 1 \}.
\]
The natural group homomorphism
\[
\lambda_E : \text{SO}_A(V)/\text{SO}(V)\text{SO}_A(L) \to \mathbb{I}_E/ \left( E^\times \prod_{p \leq \infty} L_p^\times \right)
\]
is well defined.

Let \( \alpha \in E^\times \) and \( i \in \prod_{p \leq \infty} L_p^\times \) such that \( \alpha i \in \text{SO}_A(V) \). Then
\[
N_{E/\mathbb{Q}}(\alpha i) = N_{E/\mathbb{Q}}(\alpha)N_{E/\mathbb{Q}}(i) = 1.
\]
Since
\[ N_{E/Q}(\alpha) \in \mathbb{Q} \cap \prod_{p \leq \infty} \mathbb{Z}_p^\times = \{ \pm 1 \} \quad \text{and} \quad N_{E/Q}(\alpha) > 0, \]
one concludes \( N_{E/Q}(\alpha) = N_{E/Q}(i) = 1 \). This implies that
\[ \alpha \in \text{SO}(V) \quad \text{and} \quad i \in \text{SO}_L(L). \]
Therefore \( \lambda_E \) is injective and the proof is complete. \( \Box \)

One can recover the following classical result (see [4, Theorem 9.4]) which is obvious when \( L = \mathbb{Z} + \mathbb{Z}\sqrt{-d} \) is the ring of integers of \( E \) and \( K_L \) is the Hilbert class field of \( E \). In general, for example, if \( d \) is not square free, one needs to study the class groups of orders which are not Dedekind domains (see [4]).

**Corollary 4.2.** Let \( l \) be an odd prime not dividing \( d \). The equation \( x^2 + dy^2 = l \) is solvable over \( \mathbb{Z} \) if and only if \( l \) splits completely in \( K_L \).

**Proof.** Let \( X \) be the scheme over \( \mathbb{Z} \) defined by the equation. By a simple computation, \( \prod_{p \leq \infty} X(\mathbb{Z}_p) \neq \emptyset \) if and only if \( l \) splits completely in \( E \) and
\[
\begin{cases}
\left( \frac{l}{q} \right) = 1 & \text{for each odd prime } q \mid d, \\
l \equiv 1 \text{ or } d \text{ mod } 4 & \text{if } d \text{ is odd}, \\
l \equiv 1 \text{ or } d + 1 \text{ mod } 8 & \text{if } d \equiv 2 \text{ mod } 4, \\
l \equiv 1 \text{ mod } 4 & \text{if } d \equiv 4 \text{ mod } 8, \\
l \equiv 1 \text{ mod } 8 & \text{if } 8 \mid d.
\end{cases}
\]

First we show that the above local conditions can be obtained when \( l \) splits completely in \( K_L \). Indeed, for any odd prime \( q \mid d \), \( E(\sqrt{q^*})/E \) is unramified, for all primes except the primes above \( q \), where \( q^* = (-1/q)q \). To verify if \( \psi(x)(\sqrt{q^*}) = \sqrt{q^*} \), for all \( x \in \prod_{p \leq \infty} L_p^\times \), where \( \psi \) is the Artin map over \( E \). This is equivalent to check if the product of the Hilbert symbols \( \prod_{p \mid q} (q^*, x_p)_p = 1 \), where \( \mathfrak{p} \) runs over all primes of \( E \) and \( x = (x_p) \in \prod_{p \leq \infty} L_p^\times \). It is clear that \( (q^*, x_p)_p = 1 \), for \( \mathfrak{p} \nmid q \).

Since \( x = (x_p) \in \prod_{p \leq \infty} L_p^\times \), there are \( a_p, b_p \in \mathbb{Z}_p \) such that
\[
\begin{cases}
(x_p, x_{\mathfrak{p}}) = (a_p + b_p\sqrt{-d}, a_p - b_p\sqrt{-d}) & \text{if } p = \mathfrak{p}, \text{ \( \mathfrak{p} \) splits in } E/Q, \\
(x_p) = a_p + b_p\sqrt{-d} & \text{otherwise.}
\end{cases}
\]

Hence
\[
\prod_{\mathfrak{p} \mid q} (q^*, x_{\mathfrak{p}})_p = (q^*, a_q^2 - b_q^2 d)_q = 1
\]
by [11, (1.5.3) Proposition, (7.1.4) Corollary] and \( q \mid d \). Therefore, \( \sqrt{q^*} \in K_L \). This implies that \( l \) splits in \( \mathbb{Q}(\sqrt{q^*}) \) and \( (q^*/l) = (l/q) = 1 \). This means that \( l \) is a square in \( \mathbb{Z}_q \), for any odd prime \( q \mid d \). By the Hilbert reciprocity law, one has
\[
(-d, l)_2 = \prod_{\text{odd primes } q} (-d, l)_q = \prod_{q \mid d} (-d, l)_q = 1.
\]

One gets the local conditions for odd \( d \) and \( d \equiv 2 \mod 4 \) by \((-d, l)_2 = 1\).

If \( d \equiv 4 \mod 8 \), then \( \mathbb{Q}(\sqrt{-1}) \subset K_L \) by the same argument as above. So \( l \equiv 1 \mod 4 \).

If \( 8 \mid d \), then \( \mathbb{Q}(\sqrt{-1}, \sqrt{2}) \subset K_L \). So \( l \equiv 1 \mod 8 \).
Let \((x_p, y_p) \in X(\mathbb{Z}_p)\) for \(p \leq \infty\). Then \(\tilde{f}_E([x_p, y_p]) \in L_p^\times\) for \(p \neq l\). Since \(l\) splits in \(E/\mathbb{Q}\) by the local conditions and
\[
(x_l + y_l\sqrt{-d})(x_l - y_l\sqrt{-d}) = l,
\]
one can write \(\mathfrak{L}_1\) and \(\mathfrak{L}_2\) as two primes in \(E\) above \(l\) and assume \(\tilde{f}_E([x_l, y_l])\) is a prime element at \(E_{\mathfrak{L}_1}\) and a unit at \(E_{\mathfrak{L}_2}\). By the class field theory, one concludes that \(\mathfrak{L}_1\) splits in \(K_L/E\) if and only if
\[
\psi_{K_L/E} \left( \tilde{f}_E \left( \prod_{p \leq \infty} (x_p, y_p) \right) \right) = 1.
\]
If \(l\) splits completely in \(K_L/\mathbb{Q}\), then \(X(\mathbb{Z}) \neq \emptyset\) by Proposition 4.1.

Conversely, choose two integral solutions \((x_0, y_0)\) and \((x_0, -y_0)\) in \(X(\mathbb{Z})\). One obtains that both \(\mathfrak{L}_1\) and \(\mathfrak{L}_2\) split in \(K_L/E\) by the above argument. The proof is complete. \(\square\)

We give one more example to explain that the method provided in the previous sections is beyond Gauss’ method which only applies to the binary quadratic forms.

For any positive integer \(n\), one can write \(n = 2^s p_1^{e_1} \ldots p_g^{e_g}\) and define
\[
D(n) = \{ p_1, \ldots, p_g \},
\]
\[
D_1 = \left\{ p \in D(n) : \left( \frac{-1}{p} \right) = - \left( \frac{2}{p} \right) = 1 \right\},
\]
\[
D_2 = \left\{ p \in D(n) : \left( \frac{-1}{p} \right) = \left( \frac{2}{p} \right) = 1 \quad \text{and} \quad x^4 \equiv 2 \mod p \quad \text{is not solvable} \right\}.
\]

**Example 4.3.** Let \(n\) be a positive integer with the above notation. Then the equation
\[
x^2 + 64y^2 + 64y + 16 = n
\]
is solvable over \(\mathbb{Z}\) if and only if \(p_j \equiv 1 \mod 4\) for odd \(e_j\) with \(1 \leq j \leq g\) and one of the following conditions holds:

(1) \(s = 0\) and \(n \equiv 1 \mod 8\) and
\[
\left( D_1 \neq \emptyset \text{ or } \sum_{p_j \in D_2} e_j \equiv 1 \mod 2 \right) \text{ for } D_1 = \emptyset.
\]
(2) \(s = 2\) and \(2^{-2}n \equiv 5 \mod 8\).
(3) \(s = 4, 5\).

**Proof.** Let \(X\) be the scheme over \(\mathbb{Z}\) defined by the equation. By a simple computation, the necessary and sufficient conditions for \(\prod_{p \leq \infty} X(\mathbb{Z}_p) \neq \emptyset\) are \(p_j \equiv 1 \mod 4\) for odd \(e_j\) with \(1 \leq j \leq g\) and
\[
\begin{cases}
  s = 0 & \text{and} \quad n \equiv 1 \mod 8, \\
  s = 2 & \text{and} \quad 2^{-2}n \equiv 5 \mod 8, \\
  s = 4, 5.
\end{cases}
\]

Let \(E = \mathbb{Q}(\sqrt{-1})\) and \(L = \mathbb{Z} + 2\mathbb{Z}\sqrt{-1}\) be an order in \(E\) and \(u_0 = 4\sqrt{-1}\). For any prime \(p\), \(E_p = E \otimes_{\mathbb{Q}} \mathbb{Q}_p\) and \(L_p\) is the \(p\)-adic completion of \(L\) inside \(E_p\). Write \(E_{\infty} = L_{\infty} = \mathbb{C}\). Then
\[
\lambda_E[SO_h(L + u_0)] \subseteq \prod_{p \leq \infty} L_p^X
\]
and the induced map
\[ \lambda_E : \text{SO}_K(V)/\text{SO}(V)\text{SO}_K(L + u_0) \rightarrow \mathbb{I}_E/E^\times \left( \prod_{p \leq \infty} L_p^\times \right) \]
is injective by the same argument in Proposition 4.1. This implies that \( \prod_{p \leq \infty} L_p^\times \) is \((L + u_0)\)-admissible. The abelian extension \( K_L \) of \( E \) corresponding to \( E^\times \prod_{p \leq \infty} L_p^\times \) is the ring class field of \( L \). By [4, Proposition 9.5], \( K_L = E(\sqrt{2}) \). Then \( K_L/E \) is unramified at all places except 2 and 2 is totally ramified in \( K_L/Q \) and \( \text{Gal}(K_L/E) = \mu_4 \) where \( \mu_4 \) is the set of all 4th roots of unity.

Since \( p \in \mathbb{L}_2 \), for any odd prime \( p \), one concludes that
\[ 1 = \begin{cases} \psi_{K_L/E}(p) & \text{if } p \text{ is inert in } E/Q \text{ with } \mathfrak{P} | p, \\ \psi_{K_L/E}(p\mathfrak{P}) & \text{if } p = \mathfrak{P}\mathfrak{P} \text{ in } E/Q, \end{cases} \quad (4.4) \]
where \( p\mathfrak{P} \) (resp. \( p\overline{\mathfrak{P}} \)) is in \( \mathbb{I}_E \) such that its \( \mathfrak{P} \) (resp. \( \overline{\mathfrak{P}} \)) component is \( p \) and the other components are 1 and \( \psi_{K_L/E} \) is the Artin symbol.

Define
\[ \tilde{f}_E[(x_p, y_p)] = \begin{cases} (x_p + 4(2y_p + 1)\sqrt{-1}, x_p - 4(2y_p + 1)\sqrt{-1}) & \text{if } p \text{ splits in } E/Q, \\ (x_p + 4(2y_p + 1)\sqrt{-1}) & \text{otherwise}, \end{cases} \]
for any \((x_p, y_p) \in X(Z_p)\).

If \((p, 2n) = 1\), then
\[ \tilde{f}_E[(x_p, y_p)] \in L_p^\times \quad \text{and} \quad \psi_{K_L/E}(\tilde{f}_E[(x_p, y_p)]) = 1, \]
where \( \tilde{f}_E[(x_p, y_p)] \) is also regarded as an element in \( \mathbb{I}_E \) such that the components above \( p \) are given by the value of \( \tilde{f}_E[(x_p, y_p)] \) and 1 otherwise.

If \( p \) is inert in \( E/Q \) with \( p \in D(n) \), then \( \psi_{K_L/E}(\tilde{f}_E[(x_p, y_p)]) = 1 \) by (4.4).

If \( p \) splits in \( E/Q \) with \( p \in D(n) \), one has
\[ \begin{cases} \psi_{K_L/E}(p) = \psi_{K_L/E}(p\mathfrak{P}) = -1 & \text{for } p \in D_2, \\ \psi_{K_L/E}(p\mathfrak{P}) = \pm\sqrt{-1} & \text{for } p \in D_1, \end{cases} \]
by the definition of \( D_1, D_2 \) and (4.4). Since
\[ x_p + 4(2y_p + 1)\sqrt{-1} = (x_p - 4(2y_p + 1)\sqrt{-1}) = n, \]
one has
\[ \psi_{K_L/E}(\tilde{f}_E[(x_p, y_p)]) = \begin{cases} (-1)^{e} & \text{if } p \in D_2, \\ (-1)^a(\pm\sqrt{-1})^e & \text{if } p \in D_1, \\ 1 & \text{otherwise}, \end{cases} \quad (4.5) \]
where \( a = \text{ord}_{\mathfrak{P}}(x_p + 4(2y_p + 1)\sqrt{-1}) \) and \( e \) is the exponent of \( p \) inside \( n \). By the Hensel’s lemma, there are two local solutions \((x_p, y_p) \in X(Z_p)\) such that \( a = 0 \) and 1, respectively. Therefore, one can rewrite (4.5), for \( p \in D_1 \), as
\[ \psi_{K_L/E}(\tilde{f}_E[(x_p, y_p)]) = \begin{cases} \pm\sqrt{-1} & \text{e is odd,} \\ \pm1 & \text{e is even}, \end{cases} \quad (4.6) \]
where the sign can be chosen as one wishes.

Suppose \( s = 4 \) or 5. Since \( x^2 + (2y + 1)^2 = 2^{-4}n \) is solvable over \( Z \) by the above local conditions, one concludes that \( x^2 + 16(2y + 1)^2 = n \) is solvable over \( Z \).
Suppose $s = 2$. Then the local solution $(x_2, y_2) \in X(\mathbb{Z}_2)$ satisfies $x_2 \equiv 2 \mod 4$. Let $v$ be the unique place of $E$ over 2. Since 
\[(2, x_2 + 4(2y_2 + 1)\sqrt{-1})_v = (2, 2)_v \cdot (2, 2^{-1}x_2 + 2(2y_2 + 1)\sqrt{-1})_v = (2, 5)_2 = -1\]
by [11, (1.5.3) Proposition and (7.1.4) Corollary], this implies that 
\[
\psi_{K/L}(\tilde{f}_E((x_2, y_2))) = \pm \sqrt{-1}.
\]
Since $2^{-2}n \equiv 5 \mod 8$, the number of primes $p_j$ in $D_1$ with odd $e_j$ is odd. Therefore, there are an even number of local primes $p$ such that 
\[
\psi_{K/L}(\tilde{f}_E((x_p, y_p))) = \pm \sqrt{-1}
\]
by the above computation and (4.6). By choosing the sign properly, one concludes that there is
\[
(x_p, y_p)_{p \leq \infty} \in \prod_{p \leq \infty} X(\mathbb{Z}_p) \text{ such that } \psi_{K/L}(\tilde{f}_E\left[\prod_{p \leq \infty} (x_p, y_p)\right]) = 1.
\]
Therefore, $X(\mathbb{Z}) \neq \emptyset$ by (3.3).

Suppose $s = 0$. Then the local solution $(x_2, y_2) \in X(\mathbb{Z}_2)$ satisfies $x_2 \equiv 1 \mod 2$. Let $v$ be the unique place of $E$ over 2. Since 
\[
\tilde{f}_E((x_2, y_2)) = x_2 + 4(2y_2 + 1)\sqrt{-1} \equiv x_2 + 4\sqrt{-1} \equiv 1 + 4\sqrt{-1} \mod L_2^\chi,
\]
and $(1 + 4\sqrt{-1}) \in E^\times$ with $(1 + 4\sqrt{-1})(1 - 4\sqrt{-1}) = 17$, one concludes that $\psi_{K/L}(\tilde{f}_E((x_2, y_2)))$ is equal to the Frobenius of a prime above 17 in $\text{Gal}(K_L/E)$ which is $-1$.

If $D_1 \neq \emptyset$, one has that either all $e_j$ for $p_j \in D_1$ are even or the number of primes $p_j$ in $D_1$ with odd $e_j$ is even by using $n \equiv 1 \mod 8$. By (4.6) and choosing the sign properly, there is
\[
(x_p, y_p)_{p \leq \infty} \in \prod_{p \leq \infty} X(\mathbb{Z}_p) \text{ such that } \psi_{K/L}(\tilde{f}_E\left[\prod_{p \leq \infty} (x_p, y_p)\right]) = 1.
\]
Therefore, $X(\mathbb{Z}) \neq \emptyset$ by (3.3).

If $D_1 = \emptyset$, then
\[
\psi_{K/L}(\tilde{f}_E\left[\prod_{p \leq \infty} (x_p, y_p)\right]) = (-1)^{1 + \sum_{p_j \in D_2} e_j}
\]
by (4.5), for any $(x_p, y_p)_{p \leq \infty} \in \prod_{p \leq \infty} X(\mathbb{Z}_p)$. By (3.3), one concludes
\[
X(\mathbb{Z}) \neq \emptyset \iff \sum_{p_j \in D_2} e_j \equiv 1 \mod 2
\]
and the proof is complete. \hfill \box

5. **Examples with real quadratic splitting fields**

Gauss’ method cannot be applied to integral representations of indefinite binary quadratic forms in general either because the norms of the elements of real quadratic fields are not always positive and one cannot decide the sign effectively. The typical example is to determine exactly when the negative Pell equation $x^2 - dy^2 = -1$ is solvable over $\mathbb{Z}$ for a positive integer $d$.

In order to apply the method in §3, for example, to determine all integers represented by $x^2 - dy^2$, for a positive integer $d$ explicitly, one can take the order $L = \mathbb{Z} + \mathbb{Z} \sqrt{d}$ inside $E = \mathbb{Q}(\sqrt{d})$ and needs to determine the abelian extension of $E$ corresponding to an $L$-admissible subgroup of $\mathcal{I}_E$ explicitly. There is no general theory for obtaining such abelian extensions for real quadratic fields but ad hoc method. We will keep the same notation as that in §3.
With some extra conditions, one still has the analogous result to Proposition 4.1 for real quadratic fields.

**Proposition 5.1.** Let \( X \) be the scheme defined by \( x^2 - dy^2 = n \), for some integer \( n \) and \( K_L \) be the ring class field corresponding to the order \( L \). Suppose one of the following conditions holds:

1. the equation \( x^2 - dy^2 = -1 \) has an integer solution.
2. the equation \( x^2 - dy^2 = -1 \) has no local integral solutions at a prime.

Then \( X(\mathbb{Z}) \neq \emptyset \) if and only if there is

\[
(x_p, y_p) \in \prod_{p \leq \infty} X(\mathbb{Z}_p) \text{ such that } \psi_{K_L/E} \left( \prod_{p \leq \infty} (x_p, y_p) \right) = 1,
\]

where \( \psi_{K_L/E} \) is the Artin map and

\[
\tilde{f}_E[(x_p, y_p)] = \begin{cases} 
(x_p + y_p\sqrt{d}, x_p - y_p\sqrt{d}) & \text{if } p \text{ splits in } E/\mathbb{Q}, \\
(x_p + y_p\sqrt{d}) & \text{otherwise.}
\end{cases}
\]

**Proof.** The same argument as that in Proposition 4.1 with the crucial step to show that \( \lambda_E \) is injective is available except \( N_{E/\mathbb{Q}}(\alpha) > 0 \). Suppose \( N_{E/\mathbb{Q}}(\alpha) = -1 \). Then \( N_{E/\mathbb{Q}}(i) = -1 \). This contradicts Condition (2). If Condition (1) holds, there are \( x_0, y_0 \in \mathbb{Z} \) such that \( x_0^2 - dy_0^2 = -1 \). One can replace \( \alpha \) by \( \alpha(x_0 - y_0\sqrt{d}) \) and \( i \) by \( i(x_0 - y_0\sqrt{d})^{-1} \). The proof is complete. \( \square \)

When \( d \) is a prime, the condition (1) or (2) in Proposition 5.1 will be satisfied. For \( d = 2l \) with a prime \( l \), the condition (2) in Proposition 5.1 holds at prime 2, if \( l \equiv 3 \mod 4 \) and the condition (1) in Proposition 5.1 holds if \( l \equiv 5 \mod 8 \) by [5]. Such cases can also be treated by using the Gauss’ method.

However, the Gauss’ method only uses the ring class fields to detect which ideals are principal. Now we consider the case that one has to use the abelian extensions beyond the ring class fields. Let \( l \) be a prime with \( l \equiv 1 \mod 8 \). Fix an integral solution \( (x_0, y_0, z_0) \) of the equation \( x^2 - 2ly^2 = 2z^2 \) such that \( x_0 > 0 \) and \( (x_0, y_0, z_0) = 1 \) by the Hasse principle. Let \( \Theta = E(\sqrt{x_0 - y_0\sqrt{2l}}) \). Then \( \Theta \) is totally real and \( \Theta/E \) is unramified over all primes except the prime above 2 and 2 is totally ramified in \( \Theta/\mathbb{Q} \). This \( \Theta \) will play role for solving the equation \( x^2 - 2ly^2 = n \) over \( \mathbb{Z} \).

**Lemma 5.2.** Let \( l \) be a prime with \( l \equiv 1 \mod 8 \) satisfying \( 2l = r^2 + s^2 \) for two integers \( r \) and \( s \) with \( s \equiv \pm 3 \mod 8 \). If \( x \) and \( y \) in \( \mathbb{Q}_2 \) satisfy \( x_2^2 - 2ly_2^2 = -1 \), then the Hilbert symbol

\[
(x_2 + y_2\sqrt{2l}, x_0 - y_0\sqrt{2l})_v = -1,
\]

where \( \nu \) is the unique prime in \( E \) above 2 and \( (x_0, y_0) \) is given as above.

**Proof.** For any \( \xi \in E_v^\times \) with \( N_{L_v/Q_2}(\xi) = 1 \), there exists \( \beta \in E_v^\times \) such that \( \xi = \sigma(\beta)\beta^{-1} \) by Hilbert 90, where \( \sigma \) is the non-trivial element in \( \text{Gal}(E_v/Q_2) \). Then

\[
(\xi, x_0 - y_0\sqrt{2l})_v = (\sigma(\beta)\beta^{-1}, x_0 - y_0\sqrt{2l})_v = (N_{E_v/Q_2}(\beta), x_0 - y_0\sqrt{2l})_v = (N_{E_v/Q_2}(\beta), 2)_2
\]
by \cite[(1.5.3) Proposition and (7.1.4) Corollary]{corollaries}. Since \( l \equiv 1 \mod 8 \) and \( E_v = \Q_2(\sqrt{2l}) \), one has
\[
(\xi, x_0 - y_0 \sqrt{2l})_v = (N_{E_v/\Q_2}(\beta), 2)_2 = (N_{E_v/\Q_2}(\beta), 2l)_2 = 1.
\]
Therefore,
\[
(x_2 + y_2 \sqrt{2l}, x_0 - y_0 \sqrt{2l})_v = ((r - \sqrt{2l})s^{-1}, x_0 - y_0 \sqrt{2l})_v
= (r - \sqrt{2l}, x_0 - y_0 \sqrt{2l})(s, x_0 - y_0 \sqrt{2l})_v
= (r - \sqrt{2l}, x_0 - y_0 \sqrt{2l})(s, 2z_0^2)_2 = -(r - \sqrt{2l}, x_0 - y_0 \sqrt{2l})_v.
\]
By the Hilbert reciprocity law, one has
\[
(r - \sqrt{2l}, x_0 - y_0 \sqrt{2l})_v = \prod_{p \neq v} (r - \sqrt{2l}, x_0 - y_0 \sqrt{2l})_p.
\]
Since
\[
(r - \sqrt{2l})(r + \sqrt{2l}) = -s^2 \quad \text{and} \quad (x_0 - y_0 \sqrt{2l})(x_0 + y_0 \sqrt{2l}) = 2z_0^2
\]
with \((r, s) = 1 \) and \((x_0, y_0, z_0) = 1\), respectively, one has
\[
\text{ord}_p(r - \sqrt{2l}) = \text{ord}_p(x_0 - y_0 \sqrt{2l}) \equiv 0 \mod 2,
\]
for \( p \neq v \) and \( p < \infty_E \). Since \( x_0 - y_0 \sqrt{2l} > 0 \) over \( p \in \infty_E \), one obtains that
\[
(r - \sqrt{2l}, x_0 - y_0 \sqrt{2l})_p = 1,
\]
for all \( p \neq v \). One concludes that \((x_2 + y_2 \sqrt{2l}, x_0 - y_0 \sqrt{2l})_v = -1\). \(\square\)

The immediate corollary is the following result which was first proved in \cite{propositions} by using the continued fractional method and was reproved in \cite{reciprocities} by using the reciprocity law in a quite complicated way.

**Corollary 5.3** (Epstein–Rédei). If \( l \) is a prime with \( l \equiv 1 \mod 8 \) satisfying \( 2l = r^2 + s^2 \) for two integers \( r \) and \( s \) with \( s \equiv \pm 3 \mod 8 \), then the equation \( x^2 - 2ly^2 = -1 \) is not solvable over \( \Z \).

**Proof.** Let \( X \) be the scheme defined by \( x^2 - 2ly^2 = -1 \). Then
\[
\psi_{E/E}(\tilde{f}_E((x_p, y_p)_{p \leq \infty})) = (x_2 + y_2 \sqrt{2l}, x_0 - y_0 \sqrt{2l})_v = -1,
\]
for any \( \prod_{p \leq \infty} (x_p, y_p) \in \prod_{p \leq \infty} X(\Z_p) \) by Lemma 5.2. The result follows from Remark 3.4. \(\square\)

It is natural to ask how to decide the solvability of the above equation if one replaces \(-1\) by an integer \( n \).

**Proposition 5.4.** Let \( l \) be a prime as in Lemma 5.2 and \( X \) be the scheme over \( \Z \) defined by \( x^2 - 2ly^2 = n \), for some integer \( n \). Then \( X(\Z) \neq \emptyset \) if and only if there is \((x_p, y_p)_{p \leq \infty} \in \prod_{p \leq \infty} X(\Z_p) \) such that
\[
\psi_{H/E}(\tilde{f}_E((x_p, y_p)_{p \leq \infty})) = 1 \quad \text{and} \quad \psi_{E/E}(\tilde{f}_E((x_p, y_p)_{p \leq \infty})) = 1,
\]
where \( H \) is the Hilbert class field of \( E \), \( \Theta \) is the quadratic extension of \( E \) defined as above, both \( \psi_{H/E} \) and \( \psi_{E/E} \) are Artin maps and
\[
\tilde{f}_E((x_p, y_p)) = \begin{cases} 
(x_p + y_p \sqrt{2l}, x_p - y_p \sqrt{2l}) & \text{if } p \text{ splits in } E/Q, \\
(x_p + y_p \sqrt{2l}) & \text{otherwise}.
\end{cases}
\]
Proof. Let \( L = \mathbb{Z} + \mathbb{Z} \sqrt{2l} \) be the maximal order of \( E \). For any prime \( p \), \( E_p = E \otimes_{\mathbb{Q}} \mathbb{Q}_p \) and \( L_p \) is the \( p \)-adic completion of \( L \) inside \( E_p \). Write \( E_{\infty} = L_{\infty} = \mathbb{R} \).

Let \( v \) be the unique prime of \( E \) above 2. By the computation in Lemma 5.2, one has \((\xi, x_0 - y_0 \sqrt{2l})_v = 1\), for any \( \xi \in E_v^\times \) with \( N_{E_v/\mathbb{Q}_2}(\xi) = 1 \). This implies that

\[
\lambda_E(\text{SO}(L_2)) \subseteq N_{\Theta_\infty/E_v}(\Theta_\infty^x),
\]

where \( \infty \) is the unique prime of \( \Theta \) above \( v \). Since \( \Theta/E \) is unramified over all primes except \( v \), one concludes that \( \lambda_E(\text{SO}_\lambda(L)) \subseteq N_{\Theta/E}(1_\Theta) \). Therefore the natural group homomorphism

\[
\lambda_E : \text{SO}_\lambda(V)/\text{SO}(V)\text{SO}_\lambda(L) \rightarrow \left[ \mathbb{I}_E/(E^x N_{\Theta/E}(1_\Theta)) \right] \times \left[ \mathbb{I}_E/ \left( E^x \prod_{p \leq \infty} I_p \right) \right]
\]

is well defined.

Let \( u \in \ker \lambda_E \). Then there are \( \alpha \in E^x \) and \( i \in \prod_{p \leq \infty} I_p \) with \( \lambda_E(u) = \alpha i \). Therefore,

\[
N_{E/\mathbb{Q}}(\alpha) = N_{E/\mathbb{Q}}(i)^{-1} \in \mathbb{Q}^x \cap \left( \prod_{p \leq \infty} \mathbb{Z}_p^x \right) = \{ \pm 1 \}.
\]

Suppose \( N_{E/\mathbb{Q}}(\alpha) \neq 1 \). Then \( N_{E/\mathbb{Q}}(\alpha) = N_{E/\mathbb{Q}}(i) = -1 \). Write \( i = (i_p)_p \in \mathbb{I}_E \). Since \( \Theta/E \) is unramified over all primes of \( E \) except \( v \), one has \( \psi_{\Theta/E}(i_p) \) is trivial, for all primes \( p \neq v \), where \( i_p \) is regarded as an idele whose \( p \)-component is \( i_p \) and 1 otherwise. Since \( N_{E/\mathbb{Q}}(i_v) = N_{E_v/\mathbb{Q}_2}(i_v) = -1 \), one gets

\[
\psi_{\Theta/E}(\alpha i) = \psi_{\Theta/E}(i) = \psi_{\Theta/E}(i_v) = -1
\]

by Lemma 5.2. This contradicts \( u \in \ker \lambda_E \).

Therefore, \( N_{E/\mathbb{Q}}(\alpha) = N_{E/\mathbb{Q}}(i) = 1 \). This implies that \( \alpha \in \text{SO}(V) \) and \( i \in \text{SO}_\lambda(L) \). One concludes that \( \lambda_E \) is injective. The result follows from Corollary 1.6.

Finally, we will use Proposition 5.4 to give an explicit example. For any integer \( n \), one can write \( n = (-1)^{e_0} 2^{e_1} 17^{e_2} p_1^{e_1} \ldots p_g^{e_5} \) and \( D(n) = \{p_1, \ldots, p_g\} \). Decompose \( D(n) \) into the disjoint union of the following subsets:

\[
D_1 = \{ p \in D(n) : \left( \frac{2}{p} \right) = \left( \frac{17}{p} \right) = -1 \} \quad \text{and} \quad D_2 = \{ p \in D(n) : \left( \frac{34}{p} \right) = -1 \},
\]

\[
D_3 = \{ p \in D(n) : \left( \frac{2}{p} \right) = \left( \frac{17}{p} \right) = 1 \quad \text{and} \quad x^4 - 12x^2 + 2 \equiv 0 \mod p \text{ is solvable} \},
\]

\[
D_4 = \{ p \in D(n) : \left( \frac{2}{p} \right) = \left( \frac{17}{p} \right) = 1 \quad \text{and} \quad x^4 - 12x^2 + 2 \equiv 0 \mod p \text{ is not solvable} \}.
\]

Let

\[
(n_1 = (-1)^{e_0} \prod_{p_i \in D(n) \setminus D_2} p_i^{e_i}.
\]

**Example 5.5.** Let \( n \) be an integer with the above notation. Then the equation

\[
x^2 - 34y^2 = n
\]

is solvable over \( \mathbb{Z} \) if and only if

1. \( n_1 \equiv 1 \mod 8 \), \( (n_1/17) = 1 \) and \( (34/p_i) = 1 \) for odd \( e_i \).
(2) \( D_1 \neq \emptyset \); or

\[
\sum_{p_i \in D_4} e_i \equiv \begin{cases} 
  s_2 \mod 2 & \text{if } n_1 \equiv 1, -9 \mod 16, \\
  s_2 + 1 \mod 2 & \text{if } n_1 \equiv -1, 9 \mod 16,
\end{cases}
\]

for \( D_1 = \emptyset \).

Proof. Let \( \mathbf{X} \) be the scheme over \( \mathbb{Z} \) defined by the equation. By [12] for odd primes \( p \) and [9] for \( p = 2 \), one has the condition (1) is equivalent to \( \prod_{p \leq \infty} \mathbf{X}(\mathbb{Z}_p) \neq \emptyset \).

Since \( 34 = 5^2 + 3^2 \), Proposition 5.4 can be applied. Moreover, the Hilbert class field \( H \) of \( E = \mathbb{Q}(\sqrt{34}) \) is \( \mathbb{Q}(\sqrt{2}, \sqrt{17}) \). Since the equation \( x^2 - 34y^2 = 2 \) has an integral solution for \( x = 6 \) and \( y = 1 \), one can choose \( \Theta = E(\sqrt{6 - \sqrt{34}}) \). For simplicity, we will denote both \( \text{Gal}(\Theta/E) \) and \( \text{Gal}(H/E) \) as \( \mu_2 = \{\pm 1\} \).

Define

\[
\tilde{f}_E([x_p, y_p]) = \begin{cases} 
  (x_p + y_p \sqrt{34}, x_p - y_p \sqrt{34}) & \text{if } p \text{ splits in } E/\mathbb{Q}, \\
  (x_p + y_p \sqrt{34}) & \text{otherwise},
\end{cases}
\]

for any \( (x_p, y_p) \in \mathbf{X}(\mathbb{Z}_p) \).

Then

\[
\psi_{H/E}(\tilde{f}_E([x_p, y_p])) = \begin{cases} 
  (-1)^{e_i} & \text{if } p \in D_1, \\
  1 & \text{otherwise}.
\end{cases}
\]

Since \( n_1 \equiv \pm 1 \mod 8 \) by the local condition (1), one always has \( \sum_{p_i \in D_1} e_i \equiv 0 \mod 2 \). This implies that

\[
\psi_{H/E}(\tilde{f}_E([x_p, y_p])) = 1 \quad \text{for any } (x_p, y_p)_{p \leq \infty} \in \prod_{p \leq \infty} \mathbf{X}(\mathbb{Z}_p).
\]

Next we compute \( \psi_{\Theta/E} \). It is clear that \( \psi_{\Theta/E}(\tilde{f}_E([x_p, y_p])) = 1 \) for \( p \nmid 34n \).

If \( p \in D_1 \), then \( p = \mathfrak{p} \mathfrak{P} \) over \( E \). Moreover, one of \( \mathfrak{p} \) and \( \mathfrak{P} \) splits in \( \Theta/E \) and the other is inert in \( \Theta/E \). Without loss of generality, we assume that \( \mathfrak{p} \) is inert in \( \Theta/E \). Then

\[
\psi_{\Theta/E}(\tilde{f}_E([x_p, y_p])) = (-1)^a \quad \text{with } a = \text{ord}_{\mathfrak{p}}(x_p + y_p \sqrt{34}).
\]

If \( p \in D_3 \), then \( p \) splits completely in \( \Theta/\mathbb{Q} \) and \( \psi_{\Theta/E}(\tilde{f}_E([x_p, y_p])) = 1 \).

If \( p \in D_4 \), then \( p = \mathfrak{p} \mathfrak{P} \) over \( E \) and both \( \mathfrak{p} \) and \( \mathfrak{P} \) are inert in \( \Theta/E \). One gets

\[
\psi_{\Theta/E}(\tilde{f}_E([x_p, y_p])) = (-1)^e,
\]

where \( e \) is the exponent of \( p \) inside \( n \).

If \( p \in D_2 \), the exponent \( e \) of \( p \) inside \( n \) satisfies \( e \equiv 0 \mod 2 \) by the condition (1) and \( p \) is inert in \( E/\mathbb{Q} \). Moreover, the prime \( \mathfrak{P} \) above \( p \) in \( E \) splits in \( \Theta/E \) if and only if \( 6 - \sqrt{34} \) is a square in \( E_\mathfrak{P} \). By the Hensel’s lemma, this is equivalent to \( (6 - \sqrt{34}, p)_\mathfrak{P} = (2, p)_p = 1 \). Since \( \text{ord}_{\mathfrak{P}}(x_p + y_p \sqrt{34}) = \frac{1}{2} \text{ord}_n(n) \), one has

\[
\psi_{\Theta/E}(\tilde{f}_E([x_p, y_p])) = \left( \frac{2}{p} \right)^{(1/2)e}.
\]

We summarize

\[
\psi_{\Theta/E}(\tilde{f}_E([x_p, y_p])) = \begin{cases} 
  1 & \text{if } (p, 34n) = 1 \text{ or } p \in D_3, \\
  (-1)^{e_2} & \text{if } p = 17, \\
  (-1)^a & \text{if } p \in D_1, \\
  \left( \frac{2}{p} \right)^{(1/2)e} & \text{if } p \in D_2, \\
  (-1)^e & \text{if } p \in D_4,
\end{cases}
\]

for any \( (x_p, y_p) \in \mathbf{X}(\mathbb{Z}_p) \).
When $D_1 \neq \emptyset$, there are two local solutions $(x_p, y_p) \in X(\mathbb{Z}_p)$ such that $a = 0$ and 1, respectively, for any $p \in D_1$ by the Hensel’s Lemma. This implies that there is $(x_p, y_p)_{p \leq \infty} \in \prod_{p \leq \infty} X(\mathbb{Z}_p)$ such that

$$\psi_{\emptyset/E}(\tilde{f}_E[(x_p, y_p)_{p \leq \infty}]) = 1.$$ 

When $D_1 = \emptyset$, one needs further to compute $\psi_{\emptyset/E}(\tilde{f}_E[(x_2, y_2)])$. Since there is $\delta \in \mathbb{Z}_2^\times$ with

$$\delta \equiv \begin{cases} 
\pm 1 \mod 8 & \text{if } n_1 \equiv \pm 1 \mod 16, \\
\pm 3 \mod 8 & \text{if } n_1 \equiv \pm 9 \mod 16
\end{cases}$$

such that

$$\delta^2 = \begin{cases} 
17^{s_2}n_1 & \text{if } n_1 \equiv 1, 9 \mod 16, \\
-17^{s_2}n_1 & \text{if } n_1 \equiv -1, -9 \mod 16
\end{cases}$$

by the Hensel’s lemma, one has

$$N_{E_v/\mathbb{Q}_2} \left( \beta^{s_1} \delta \prod_{p_i \in D_2} p_i^{(1/2)e_i} \right) = \begin{cases} 
n & \text{if } n_1 \equiv 1, 9 \mod 16, \\
-n & \text{if } n_1 \equiv -1, -9 \mod 16,
\end{cases}$$

where $v$ is the unique prime of $E$ above 2 and $\beta = 6 - \sqrt{34}$. For any $(x_2, y_2) \in X(\mathbb{Z}_2)$, one has

$$\psi_{\emptyset/E}(\tilde{f}_E[(x_2, y_2)]) = \begin{cases} 
(\beta^{s_1} \delta \prod_{p_i \in D_2} p_i^{(1/2)e_i}, \beta)_v & \text{if } n_1 \equiv 1, 9 \mod 16, \\
-(\beta^{s_1} \delta \prod_{p_i \in D_2} p_i^{(1/2)e_i}, \beta)_v & \text{if } n_1 \equiv -1, -9 \mod 16
\end{cases}$$

by the computation in Lemma 5.2. Since

$$\left( \beta^{s_1} \prod_{p_i \in D_2} p_i^{(1/2)e_i}, \beta \right)_v = (\beta, \beta)_v \left( \delta \prod_{p_i \in D_2} p_i^{(1/2)e_i}, \beta \right)_v \left( \delta \prod_{p_i \in D_2} p_i^{(1/2)e_i}, 2 \right)_2 = (2, -1)^{s_1}_2 \left( \delta \prod_{p_i \in D_2} p_i^{(1/2)e_i}, 2 \right)_2$$

$$= (\delta, 2)_2 \prod_{p_i \in D_2} \left( \frac{2}{p_i} \right)^{(1/2)e_i} = \begin{cases} 
\prod_{p_i \in D_2} \left( \frac{2}{p_i} \right)^{(1/2)e_i} & \text{if } n_1 \equiv \pm 1 \mod 16, \\
-\prod_{p_i \in D_2} \left( \frac{2}{p_i} \right)^{(1/2)e_i} & \text{if } n_1 \equiv \pm 9 \mod 16,
\end{cases}$$

one concludes that

$$\psi_{\emptyset/E}(\tilde{f}_E[(x_2, y_2)]) = \begin{cases} 
\prod_{p_i \in D_2} \left( \frac{2}{p_i} \right)^{(1/2)e_i} & \text{if } n_1 \equiv 1, -9 \mod 16, \\
-\prod_{p_i \in D_2} \left( \frac{2}{p_i} \right)^{(1/2)e_i} & \text{if } n_1 \equiv -1, 9 \mod 16,
\end{cases}$$

for any $(x_2, y_2) \in X(\mathbb{Z}_2)$. By Proposition 5.4, $X(\mathbb{Z}) \neq \emptyset$ if and only if

$$\prod_{p_i \in D_4} (-1)^{e_i} \prod_{p_i \in D_2} \left( \frac{2}{p_i} \right)^{(1/2)e_i} = \begin{cases} 
(-1)^{s_2} \prod_{p_i \in D_2} \left( \frac{2}{p_i} \right)^{(1/2)e_i} & \text{if } n_1 \equiv 1, -9 \mod 16, \\
(-1)^{s_2+1} \prod_{p_i \in D_2} \left( \frac{2}{p_i} \right)^{(1/2)e_i} & \text{if } n_1 \equiv -1, 9 \mod 16.
\end{cases}$$

The proof is complete. \qed
6. Examples for higher-dimensional tori

In this section, we further explain how effective the method in § 1 is for high dimension tori by providing the explicit examples. Fix an integral solution \((x_0, y_0, z_0)\) of the equation \(x^2 - 2ly^2 = 2z^2\) for \(l \equiv 1 \mod 8\) such that \(x_0 > 0\) and \((x_0, y_0, z_0) = 1\). Let

\[
L = \mathbb{Q}(\sqrt{2l}) \quad \text{and} \quad \Theta = L(\sqrt{x_0 - y_0\sqrt{2l}}).
\]

Then \(\Theta\) is totally real and \(\Theta/L\) is unramified over all primes except the prime above 2 and 2 is totally ramified in \(\Theta/\mathbb{Q}\).

**Proposition 6.1.** Let \(l\) be a prime with \(l \equiv 1 \mod 8\) satisfying \(2l = r^2 + s^2\) for two integers \(r\) and \(s\) with \(s \equiv \pm 3 \mod 8\) and \(\Theta\) and \(L\) be as above. Suppose \(E\) is a field containing \(L\) and \(X\) is the scheme over \(\mathbb{Z}\) defined by the equation

\[
f(x_1, \ldots, x_k) = N_{E/\mathbb{Q}}(x_1e_1 + \ldots + x_ke_k) = n,
\]

where \(\{e_1, \ldots, e_k\}\) is a basis of \(\mathfrak{o}_E\) over \(\mathbb{Z}\) and \(n\) is an integer. Then \(X(\mathbb{Z}) \neq \emptyset\) if and only if \(X(\mathbb{Q}) \neq \emptyset\) and there is

\[
(x_{1p}, \ldots, x_{kp})_{p \leq \infty} \in \prod_{p \leq \infty} X(\mathbb{Z}_p)
\]

such that both

\[
\psi_{H/E}[(x_{1p}e_1 + \ldots + x_{kp}e_k)_{p \leq \infty}] \quad \text{and} \quad \psi_{\Theta/L}[(N_{E/L}(x_{1p}e_1 + \ldots + x_{kp}e_k))_{p \leq \infty}]
\]

are trivial, where \(H\) is the Hilbert class field of \(E\) and both \(\psi_{H/E}\) and \(\psi_{\Theta/L}\) are the Artin maps.

**Proof.** Since \(G = R^1_{E/\mathbb{Q}}(\mathbb{G}_m)\), one has

\[
\text{Stab}_h(X) = \left\{(x_p) \in \prod_{p \leq \infty} \mathfrak{o}_{E_p}^\times : N_{E/\mathbb{Q}}((x_p)) = 1 \in \mathfrak{l}_\mathbb{Q}\right\}.
\]

By the computation in Lemma 5.2, one has \((\xi, x_0 - y_0\sqrt{2l})_v = 1\), for any \(\xi \in L_v^\times\) with \(N_{L_v/\mathbb{Q}_v}(\xi) = 1\) where \(v\) is the unique prime of \(L\) above 2. This implies that

\[
N_{E/L}((\text{Stab}(X)(\mathbb{Z})) \subseteq N_{\Theta_L/L_v}(\Theta_L^\times),
\]

where \(\mathfrak{m}\) is the unique prime of \(\Theta\) above \(v\). Since \(\Theta/L\) is unramified over all primes except \(v\), one concludes that

\[
N_{E/L}((\text{Stab}_h(X)) \subseteq N_{\Theta/L}(\mathfrak{l}_\Theta),
\]

where \(\mathfrak{l}_\Theta\) is the idele group of \(\Theta\). Then the group homomorphism

\[
f_E : G(\mathbb{A}_\mathbb{Q})/G(\mathbb{Q})\text{Stab}_h(X) \longrightarrow \left[\mathbb{I}_L/(L^\times N_{\Theta/L}(\mathfrak{l}_\Theta))\right] \times \left[\mathbb{I}_E / \left(E^\times \prod_{p \leq \infty} \mathfrak{o}_{E_p}^\times\right)\right],
\]

\[
(x_p)_{p \leq \infty} \mapsto (N_{E/L}(x_p), (x_p))_{p \leq \infty}
\]

is well defined. By Lemma 5.2 and the same argument in Proposition 5.4, one obtains that \(f_E\) is injective and the result follows.

For any integer \(n\), one can write

\[
n = (-1)^s_0 2^{e_1} 17^{e_2} p_1^{e_1} \ldots p_g^{e_s} \quad \text{and} \quad D(n) = \{p_1, \ldots, p_g\}.
\]
Decompose $D(n)$ into the disjoint union of the following subsets:

$$D_1 = \left\{ p \in D(n) : \left( \frac{2}{p} \right) = \left( \frac{17}{p} \right) = -1 \right\} \quad \text{and} \quad D_2 = \left\{ p \in D(n) : \left( \frac{34}{p} \right) = -1 \right\},$$

$$D_3 = \left\{ p \in D(n) : \left( \frac{2}{p} \right) = \left( \frac{17}{p} \right) = 1 \quad \text{and} \quad x^4 - 12x^2 + 2 \equiv 0 \mod p \text{ is solvable} \right\},$$

$$D_4 = \left\{ p \in D(n) : \left( \frac{2}{p} \right) = \left( \frac{17}{p} \right) = 1 \quad \text{and} \quad x^4 - 12x^2 + 2 \equiv 0 \mod p \text{ is not solvable} \right\}.$$

Let

$$n_1 = (-1)^{s_0} \prod_{p \in D(n) \setminus D_2} p_i^{e_i}.$$

One can have one more explicit example.

**Example 6.2.** Let $n$ be an integer with the above notation and $E = \mathbb{Q}(\sqrt{5}, \sqrt{34})$. Then $n \in N_{E/\mathbb{Q}}(\sigma_E)$ if and only if

1. $s_1 \equiv s_2 \equiv 0 \mod 2$, $n_1 \equiv \pm 1 \mod 8$, $(n_1/17) = 1$ and $(34/p_i) = (5/p_i) = 1$ for odd $e_i$;
2. $D_1 \neq \emptyset$; or

$$\sum_{p_i \in D_4} e_i \equiv\begin{cases} 0 \mod 2 & \text{if } n_1 \equiv 1, -9 \mod 16, \\ 1 \mod 2 & \text{if } n_1 \equiv -1, 9 \mod 16, \end{cases}$$

for $D_1 = \emptyset$.

**Proof.** We apply Proposition 6.1 by taking $E = \mathbb{Q}(\sqrt{5}, \sqrt{34})$, $L = \mathbb{Q}(\sqrt{34})$ and $\Theta = L(\sqrt{6 - \sqrt{34}})$. The Hilbert class field of $E$ is $E(\sqrt{2})$.

The local condition $n \in N_{E/\mathbb{Q}}(\sigma_E)$ for all primes $p \leq \infty$ is equivalent to the condition (1). Since $\text{Gal}(E/\mathbb{Q}) = \text{Gal}(E_\Theta/\mathbb{Q}_2)$, one concludes that $n \in N_{E/\mathbb{Q}}(E^\times)$ by [14, Theorem 6.11].

If $(x_p)_{p \leq \infty}$ is the local solution with $x_p \in \sigma_E$, and $N_{E/\mathbb{Q}}(x_p) = n$, for all $p \leq \infty$, one can verify that $\psi_{\Theta}/L((N_{E/L}(x_p))_{p \leq \infty}) = 1$. The computation of $\psi_{\Theta}/L((N_{E/L}(x_p))_{p \leq \infty})$ is the same as that in Example 5.5.

**Acknowledgements.** We would like to thank Jean-Louis Colliot-Thélène for introducing us to study the Brauer–Manin obstruction and a lot of helpful discussion. He also pointed out a flaw in the original version of the paper. We would also like to thank David Harari for sending us his paper [7]. Both authors would also like to thank the referee for the suggestion of improving the paper.

**References**


Dasheng Wei  
Academy of Mathematics and System Science  
CAS  
Beijing 100190  
P.R. China  
dshwei@amss.ac.cn

Fei Xu  
School of Mathematics  
Capital Normal University  
Beijing 100048  
P.R. China  
xufei@math.ac.cn