Math. Res. Lett. **20** (2013), *no.* 5, 961–980

A UNIVERSAL FIRST-ORDER FORMULA DEFINING THE RING OF INTEGERS IN A NUMBER FIELD

Jennifer Park

Abstract. We show that the complement of the ring of integers in a number field K is Diophantine, for $f \in K[t, x_1, \ldots, x_n]$. We will use global class field theory and generalize the ideas originating from Koenigsmann's recent result giving a universal first-order formula for $\mathbb{Z}$ in $\mathbb{Q}$.

1. Introduction

Hilbert's tenth problem asked for an algorithm that decides whether an integer solution to a polynomial equation $f(x_1, \ldots, x_n) = 0$ exists, for any $f \in \mathbb{Z}[x_1, \ldots, x_n]$. Matiyasevich answered the question in the negative, building on earlier results by Davis, Putnam and Robinson, by showing the equivalence of Diophantine sets in $\mathbb{Z}$ and listable sets in $\mathbb{Z}$; a set $A \subseteq \mathbb{Z}$ is said to be *Diophantine* if there exists a polynomial $f \in \mathbb{Z}[t, x_1, \ldots, x_n]$ such that $A = \{t \in \mathbb{Z} \mid \exists x_1, \ldots, x_n, f(t, x_1, \ldots, x_n) = 0\}$, and A is *listable* if there is an algorithm that eventually prints all the elements and only the elements of A. With this equivalence, and the undecidability of the halting problem, one easily finds a listable set A whose membership cannot be determined by any algorithm. By Matiyasevich's theorem, A is also a Diophantine set, defined by some polynomial $f(t, x_1, \ldots, x_n)$. Then there is no algorithm for deciding which polynomials of the form $f(a, x_1, \ldots, x_n)$ with $a \in \mathbb{Z}$ has integer solutions.

Matiyasevich's work leads to the natural extensions of Hilbert's tenth problem to other settings where the notion of listable sets makes sense. More precisely stated, we ask:

Question 1.1. *Let R be a commutative and countable ring, with a fixed representation of elements of R by integers. Is there an algorithm that decides, given any polynomial $f \in R[x_1, \ldots, x_n]$, whether $f = 0$ has a solution in R?*

One possibility for R is the ring of integers $\mathcal{O}_K$ of a number field K. In the setting of $R = \mathcal{O}_K$, the above problem is open, although in many cases, it has been answered in the negative. Assuming the Shafarevich–Tate conjecture, it is in fact shown by Mazur and Rubin in [MR10] that Hilbert's tenth problem has a negative answer over the ring of integers of every number field.

We can also consider Hilbert's tenth problem over $\mathbb{Q}$, or, even more generally, over a number field K. This problem is of interest, because of its equivalence to one of the big open problems of arithmetic geometry asking for an algorithm for

Received by the editors August 5, 2012.

1991 *Mathematics Subject Classification.* Primary 11R37; Secondary 11R52, 11U05.

Key words and phrases. Hilbert's tenth problem, Diophantine set, quaternion algebra, class field theory, Artin reciprocity, Hilbert symbol.

deciding the existence of a rational point on a variety defined over K. This problem remains open. However, if a negative answer for $\mathcal{O}_K$ is known, then an existential definition of the ring of integers $\mathcal{O}_K$ in K would let us deduce a negative answer for Hilbert's tenth problem over K via the following reduction: an algorithm for K gives an algorithm for $\mathcal{O}_K$. Given an equation $f(x_1, \dots, x_n) = 0$ over $\mathcal{O}_K$, we can use the algorithm for K to decide whether it has a solution with $x_1, \dots, x_n \in K$. Since, by assumption, $\mathcal{O}_K$ is existentially definable in K, we can introduce extra equations that force $x_i \in \mathcal{O}_K$. Finally, since K is not algebraically closed, by using norm forms, a system of equations can be seen to be equivalent to a single equation over K. Hence, an existential definition of $\mathcal{O}_K$ in K would give a negative answer to Hilbert's tenth problem for all number fields K, where a negative answer is known for Hilbert's tenth problem over $\mathcal{O}_K$.

An existential definition for $\mathcal{O}_K$ in K is still out of reach, even in the case $K = \mathbb{Q}$, but we can define $\mathcal{O}_K$ inside K with a first-order formula. Robinson [Rob49] found a first-order definition of $\mathbb{Z}$ in $\mathbb{Q}$, given by an $\forall\exists\forall$-formula. Recently, Poonen [Poo09] gave an $\forall\exists$-definition of $\mathcal{O}_K$ in K, and Koenigsmann [Koe10] extended this result to give an $\forall$-definition of $\mathbb{Z}$ in $\mathbb{Q}$. In this paper, we generalize Koenigsmann's results to the setting of number fields to give an $\forall$-definition of $\mathcal{O}_K$ in K. We prove the following theorem:

Theorem 1.2. *There is a first-order universal formula defining $\mathcal{O}_K$ in K. That is, $K - \mathcal{O}_K$ is Diophantine in K.*

As in [Poo09, Koe10], the proof of the above theorem uses the sets of traces of norm-1 elements of quaternion algebras as building blocks in constructing various other Diophantine sets; these sets of traces are easily proven to be Diophantine, and they are also related to localizations of the ring of integers $\mathcal{O}_K$ at primes $\mathfrak{p}$, as in Proposition 2.3. These arguments are found in Section 2.

A key construction in [Koe10] in obtaining a universal first-order formula for $\mathbb{Z}$ in $\mathbb{Q}$ is to split up the odd prime numbers into four sets, depending on their values mod 8. Then he argues that for each congruence class of odd primes mod 8, there is a universal-existential definition of $\cap_p \mathbb{Z}_p$, where the intersection runs among the primes in the given congruence class. This construction does not at all generalize to the setting of $\mathcal{O}_K$ in K for several reasons. The main obstruction comes from the fact that in general, one cannot expect a prime ideal to be principal. Thus, it is no longer possible to split up the prime ideals based on simple modular arithmetic. Furthermore, even in the simplified cases of the class number of K being one, the number 8 does not have a natural interpretation; no straightforward generalizations of [Koe10] seem to exist.

Thus, in Section 3, we consider the Artin homomorphism of ideals to the Galois group of some carefully chosen (see Lemma 3.19) biquadratic extension of K and the modulus $\mathfrak{m}$, in order to clear up these issues; the preimage of each of the four elements of the Galois group of the biquadratic extension replaces the four congruence classes of prime numbers modulo 8 in [Koe10], hence obtaining a similar uniform definition of $(\mathcal{O}_K)_{\mathfrak{p}}$. Global class field theory, which explains the splitting of quaternion algebras over $K_{\mathfrak{p}}$, plays an essential role in proving that we also have a uniform definition here.

Finally, in Section 4, we make use of the construction appearing in Step 4 of [Koe10]: Lemma 14 of [Koe10] states that if the Jacobson radical of a semilocal ring

$R = \cap_{0\le i\le N} R_i$ is Diophantine (with R_i local rings), then the related ring $\widetilde{R} = \cup_{0\le i\le N} R_i$ is universally defined. We will need essentially identical arguments in our generalization of Koenigsmann's result to number fields.

The proofs that follow are further aided by a theorem, proved and communicated by Tate, which allows one to find an element $x \in K$ that has prescribed Hilbert symbols against finitely many elements of K. The special case where $K = \mathbb{Q}$ is well-known; for example, see [Ser73], Theorem 4, page 24, but the general case of K being a global field does not appear in the literature.

This proof contains Koenigsmann's proof as a special case, when $K = \mathbb{Q}$ and one chooses the biquadratic extension to be $K(\sqrt{-1}, \sqrt{2})$; global class field theory explains the somewhat mysterious appearance of these constants in [Koe10].

2. A universal-existential definition of $\mathcal{O}_K$ in K

Throughout, K is a fixed number field, $\mathcal{O}_K$ denotes its ring of integers. For a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, and its associated valuation v, $\mathcal{O}_v$ is the set of the elements of the completion K_v whose valuations are nonnegative. We denote $(\mathcal{O}_K)_\mathfrak{p}$ to be the localization of the ring of integers of K at the prime $\mathfrak{p}$. Then $(\mathcal{O}_K)_\mathfrak{p} \subset \mathcal{O}_v$.

Notation 2.1. *Let $\mathbb{P}$ be the set of all finite places of K, and let $\mathbb{P}\cup\infty$ be the set of all places of K, both finite and infinite. Prime ideals and their corresponding valuations are used interchangeably. Further, for $a, b \in K^\times$,*

- *$H_{a,b} := K\cdot 1 \oplus K\cdot\alpha \oplus K\cdot\beta \oplus K\cdot\alpha\beta$ is the quaternion algebra over K with multiplication defined by $\alpha^2 = a, \beta^2 = b$, and $\alpha\beta = -\beta\alpha$.*
- *$\Delta_{a,b} := \{v \in \mathbb{P}\cup\infty \mid H_{a,b}\otimes K_v$ does not split$\}$. We note that $\Delta_{a,b}$ is always finite.*
- *$S_{a,b} := \{2x_1 \in K \mid \exists x_2, x_3, x_4 \in K$ with $x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1\}$ is the set of traces of norm-1 elements of $H_{a,b}$.*
- *$T_{a,b} := S_{a,b} + S_{a,b}$.*

We note in particular that $S_{a,b}$ and $T_{a,b}$ are Diophantine.

For each place v of K, we can similarly define $S_{a,b}(K_v)$ and $T_{a,b}(K_v)$ by replacing K by K_v. For each infinite place σ we define

$$\mathcal{O}_\sigma := \begin{cases} \mathbb{R}, & \text{if } \sigma \text{ is a real place, and } \sigma(a) > 0 \text{ or } \sigma(b) > 0,\\ [-4,4], & \text{if } \sigma \text{ is a real place, and } \sigma(a), \sigma(b) < 0,\\ \mathbb{C}, & \text{if } \sigma \text{ is a complex place.}\end{cases}$$

Let v be a finite place of K, and let $\mathbb{F}_v$ be the residue field of v of size q, which is some power of a prime p. Then denote the reduction map by $\mathrm{red}_v\colon \mathcal{O}_v \to \mathbb{F}_v$. Further, define

$$U_v := \{s \in \mathbb{F}_v \mid x^2 - sx + 1 \text{ is irreducible over } \mathbb{F}_v\}.$$

Lemma 2.2.

(a) *If $v \notin \Delta_{a,b}$, then $S_{a,b}(K_v) = K_v$.*

(b) *If $v \in \Delta_{a,b}\cap\mathbb{P}$, then $\mathrm{red}_v^{-1}(U_v) \subseteq S_{a,b}(K_v) \subseteq (\mathcal{O}_K)_v$.*

(c) *For an infinite place σ,*

$$S_{a,b}(K_\sigma) = \begin{cases} \mathbb{R}, & \textit{if } \sigma \textit{ is a real place, and } \sigma(a) > 0 \textit{ or } \sigma(b) > 0, \\ [-2,2], & \textit{if } \sigma \textit{ is a real place, and } \sigma(a), \sigma(b) < 0, \\ \mathbb{C}, & \textit{if } \sigma \textit{ corresponds to a complex embedding.} \end{cases}$$

(d) *For any v with $\#\mathbb{F}_v > 11$, we have $\mathbb{F}_v = U_v + U_v$.*

(e) *For each $a, b \in K^\times$ such that $\sigma(a) > 0$ or $\sigma(b) > 0$ for each real archimedean place σ,*

$$S_{a,b} = K \cap \bigcap_{v \in \Delta_{a,b}} S_{a,b}(K_v).$$

Proof.

(a) It is clear from the definition of $S_{a,b}$ that $S_{a,b}(K_v) \subseteq K_v$. Now, to prove the reverse inclusion, take any element $s \in K_v$. We will show that there is an element in the quaternion algebra $H_{a,b}$ over K_v whose reduced trace is s. Since $v \notin \Delta_{a,b}$, we have $H_{a,b} \otimes K_v \cong M_2(K_v)$, so every monic quadratic polynomial is a characteristic polynomial of some element of the matrix ring. In particular, $K_v \subseteq S_{a,b}(K_v)$, which shows the equality of part (a).

(b) See [Poo09], Lemma 2.1.

(c) In the first and third cases, one always has that the quaternion algebra $H_{a,b}$ splits, since if either a or b are perfect squares, then the quaternion algebra splits. These cases are handled by (a). The second case is a straightforward computation.

(d) See [Poo09], Lemma 2.3.

(e) This is a special case of the Hasse–Minkowski local–global principle.

□

Proposition 2.3. *For any $a, b \in K^\times$ such that $\sigma(a) > 0$ or $\sigma(b) > 0$ for each real archimedean place σ,*

$$T_{a,b} = \bigcap_{\mathfrak{p} \in \Delta_{a,b}} \mathcal{O}_\mathfrak{p}.$$

Proof. Let $T'_{a,b}$ be the right-hand side. By Lemma 2.2 (b) and (e), we have $S_{a,b} \subseteq T'_{a,b}$, so $T_{a,b} \subseteq T'_{a,b}$.

To prove the converse inclusion, we first compute U_v for $\#\mathbb{F}_v < 11$. Since U_v only depends on $\mathbb{F}_v$, we may write $U_v = U_{q_v}$, where $q_v = \#\mathbb{F}_v$. We get:

$$\begin{aligned} U_2 &= \{1\}, \\ U_3 &= \{0\}, \\ U_4 &= \{a, a+1\}, \text{ where } a^2 + a + 1 = 0, \\ U_5 &= \{1, 4\}, \\ U_7 &= \{0, 3, 4\}, \\ U_8 &= \{1, a, a^2, a^2 + a\}, \text{ where } a^3 + a + 1 = 0, \\ U_9 &= \{a, a+2, 2a, 2a+1\}, \text{ where } a^2 + 1 = 0, \\ U_{11} &= \{0, 1, 5, 6, 10\}. \end{aligned}$$

We have $\pm 2 \in S_{a,b}(K_v)$, since ± 2 is the reduced trace of ± 1. So for each finite place v, define $V_v \subseteq \mathcal{O}_v$ as follows:

$$V_v = \begin{cases} \operatorname{red}_v^{-1}(U_{q_v}) \cup \{\pm 2\} & \text{if } v|p, 2 \leq p \leq 11, \\ \operatorname{red}_v^{-1}(U_{q_v}) & \text{if } v|p, p > 11. \end{cases}$$

Then by the discussions in the previous paragraph, $V_v \subseteq S_{a,b}(K_v)$, and a case-by-case check on each $2 \leq q_v \leq 11$ shows that

$$(U_{q_v} \cup \{\pm 2\}) + U_{q_v} = \mathbb{F}_v,$$

so $V_v + V_v = \mathcal{O}_v$ for v with $2 \leq q_v \leq 11$. If v is such that $q_v > 11$, then by Lemma 2.2(d), $V_v + V_v = \mathcal{O}_v$.

So let $t \in T'_{a,b}$. Then for each $v \in \Delta_{a,b}$, we may choose $r_v \in \mathcal{O}_v$ such that $r_v, t - r_v \in V_v$. Since $\Delta_{a,b}$ is finite, we use strong approximation to find $r \in \mathcal{O}$ such that for all $v \in \Delta_{a,b}$, we have $r, t - r \in V_v$. Then by Lemma 2.2(e), we have $r, t - r \in S_{a,b}$, which proves the inclusion $T'_{a,b} \subseteq T_{a,b}$. □

3. Consequences arising from global class field theory

3.1. Background: Hilbert symbols and class field theory. In [Ser79], Corollary to Lemma XIV.3.2, an explicit formula for Hilbert symbols is given: for a number field K and a finite place $v = v_{\mathfrak{p}}$ not lying above 2,

$$(a, b)_v = \left((-1)^{v(a)v(b)} \operatorname{red}_v \left(\frac{a^{v(b)}}{b^{v(a)}} \right) \right)^{\frac{q-1}{2}}, \tag{3.1}$$

where $q = \#\mathbb{F}_v$. Then for a $\mathfrak{p}$-adic unit a,

$$(a, p)_v = -1 \Leftrightarrow v(p) \text{ is odd, and } \operatorname{red}_v(a) \text{ is not a square in the residue field } \mathbb{F}_v.$$

Also, we make the following observation:

$$\begin{aligned} \bar{a} \in \mathbb{F}_{v_{\mathfrak{p}}}^2 &\Leftrightarrow a \in K_v^2 \text{ (Hensel's lemma)} \\ &\Leftrightarrow \mathfrak{p}_v \text{ splits in } K(\sqrt{a})/K, \end{aligned}$$

where $\mathfrak{p}_v$ is the prime ideal associated to v.

Let us start by defining some notation arising from global class field theory. Let K be a global field, and let S be a finite set of primes of K. Then we define I^S to be the group of fractional ideals of K whose factorizations do not contain primes from S. Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus of K, where $\mathfrak{m}_0$ denotes the finite part, and $\mathfrak{m}_\infty$ denotes the infinite part.

Define

$$\begin{aligned} K_{\mathfrak{m},1} := \{a \in K^\times \mid v(a-1) \geq v(\mathfrak{m}) &\text{ for all finite } v \text{ dividing } \mathfrak{m}, \text{ and} \\ &\text{the image of } a \text{ in } K_v^\times \text{ is positive for all real } v \text{ dividing } \mathfrak{m}\}. \end{aligned}$$

Then, we have a well-defined map

$$\begin{aligned} i \colon K_{\mathfrak{m},1} &\to I^{S(\mathfrak{m})} \\ a &\mapsto (a), \end{aligned}$$

where $S(\mathfrak{m})$ denotes the set of finite primes appearing in the modulus $\mathfrak{m}$. We also define the *ray class group modulo* $\mathfrak{m}$ by

$$C_{\mathfrak{m}} = I^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1}).$$

Example 3.1. *If $K = \mathbb{Q}$, and $\mathfrak{m} = 2 \cdot \infty$, then the ray classes modulo $\mathfrak{m}$ give exactly the partition of $K_{\mathfrak{m},1} = \mathbb{Z}_{(2)}^{\times}$ appearing in* [Koe10], *page 7. Namely, these classes are $k + 8\mathbb{Z}_{(2)}$ for $k = 1, 3, 5, 7$.*

For a finite abelian extension L/K and a set S of primes of K containing all the primes ramifying in L, we also have the global Artin homomorphism

$$\begin{aligned} \psi_{L/K} \colon I^S &\to \mathrm{Gal}(L/K), \\ \mathfrak{p} &\mapsto (\mathfrak{p}, L/K), \end{aligned}$$

where $(\mathfrak{p}, L/K)$ denotes the Frobenius automorphism corresponding to the prime ideal $\mathfrak{p}$. This definition can be linearly extended to all of I^S.

Example 3.2. *For any number field K, let us consider the extension L/K, with $L = K(\sqrt{a})$ for $a \in K^{\times} \backslash K^{\times 2}$. Let S be the set of primes of K ramifying in this extension. We identify $\mathrm{Gal}(L/K)$ with $\{\pm 1\}$. Let $\mathfrak{m} = 2a \cdot \infty$. To explicitly write down the Artin homomorphism with respect to $\mathfrak{m}$, we want to compute the Frobenius elements of the prime ideals $\mathfrak{p}$ of K for $\mathfrak{p}$ coprime to $(2a)$. In this case, the Frobenius element $(\mathfrak{p}, L/K)$ is given by the power residue symbol $\left(\frac{a}{\mathfrak{p}}\right)$. For a more detailed discussion of the power residue symbol, see Exercise 1.5 of* [CF86].

Then the Artin homomorphism is given explicitly by

$$\begin{aligned} \psi_{L/K} \colon I^S &\to \mathrm{Gal}(L/K), \\ \mathfrak{p} &\mapsto \left(\frac{a}{\mathfrak{p}}\right), \end{aligned}$$

Furthermore, if we let I_K and I_L denote the groups of fractional ideals in L and K, respectively, the relative norm map on the prime ideals $\mathfrak{P}$ of L is defined as

$$\begin{aligned} \mathrm{Nm}_{L/K} \colon I_L &\to I_K, \\ \mathfrak{P} &\mapsto \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})} \end{aligned}$$

and extended linearly, where $\mathfrak{P}$ lies above $\mathfrak{p} \subseteq \mathcal{O}_K$.

In particular, the primes of K that split in L lie in $\mathrm{Nm}_{L/K}(I_L)$. Furthermore, we say that a homomorphism $\phi : I^S \to G$ admits a modulus if there exists a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$ such that $\phi(i(K_{\mathfrak{m},1})) = 1$.

Theorem 3.3 (**Artin Reciprocity**). *Let L be a finite abelian extension of K, and let S be the set of primes of K ramifying in L. Then the Artin map $\psi : I^S \to \mathrm{Gal}(L/K)$ admits a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$, and it defines an isomorphism*

$$I_K^S/i(K_{\mathfrak{m},1}) \cdot \mathrm{Nm}(I_L^{S'}) \to \mathrm{Gal}(L/K),$$

where S' denotes the set of primes of L lying over a prime in $S(\mathfrak{m})$.

Thus, only the ray classes containing the primes of K that split in L have trivial image under this isomorphism.

Remark 3.4. For a quadratic extension $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$, $\mathfrak{m} = 4m \cdot \infty$ is an admissible modulus, so if $L = \mathbb{Q}(\sqrt{-1}, \sqrt{2})/\mathbb{Q}$, we can take $\mathfrak{m} = 8 \cdot \infty$. From Example 3.2, we see that the splitting behaviour of a prime in $\mathbb{Q}(\sqrt{-1}, \sqrt{2})/\mathbb{Q}$ depends on its ray class modulo $\mathfrak{m}$, characterized by $k + 8\mathbb{Z}_{(2)}$, for $k = 1, 3, 5, 7$.

3.2. Prescribing Hilbert symbols.

The main result of this section is Theorem 3.7, which was communicated by Tate [Tat11], generalizing [Ser73], Theorem 4, page 24 to the case of any global field and any norm residue symbol.

Let $n > 1$ be an integer, and let K be a global field containing the nth roots of unity, where $\operatorname{char} K \nmid n$. Let J be the idèle group of K, $I_v = K_v^\times / K_v^{\times n}$, and U_v denotes the image of units of $\mathcal{O}_v \subseteq K_v$ in I_v. Also, let $I = \prod'_v (I_v, U_v/U_v^n) = J/J^n$, where $\prod'_v$ denotes the restricted direct product. Let P be the image of $K^\times$ in I.

Proposition 3.5. *Let A be a finitely generated subgroup of P, and for each v, let A_v be its image in I_v. Then a character of $\prod_v A_v$ which is trivial on A can be extended to a character of I, which is trivial on P.*

Proof. We need to show that the natural restriction map between groups of continuous homomorphisms $\operatorname{Hom}(I/P, \mu_n) \to \operatorname{Hom}(\prod_v A_v/A, \mu_n)$ is surjective. This is equivalent to showing the injectivity of $\prod_v A_v/A \to I/P$. For this, it suffices to show that $P \cap \prod_v A_v = A$. The right-to-left inclusion is clear by construction. To show the left-to-right inclusion, let $\alpha \in K^\times$ be an element such that if we view it as an element of P, then $\alpha_v \in A_v$ for all v. Then $K(A^{1/n}, \alpha^{1/n})$ is an extension of $K(A^{1/n})$, which splits at every place. Hence, the two fields are equal, and by the Kummer theory, this means $\alpha \in A$, as required. □

Lemma 3.6. *For a global field K containing nth roots of unity with* $\operatorname{char} K \nmid n$, *the homomorphism*

$$I/P \to \operatorname{Hom}(K^\times/K^{\times n}, \mu_n),$$
$$(b_v)_v \mapsto (x \mapsto \prod_v (b_v, x)_v)$$

is an isomorphism.

Proof. Let C_K denote the idèle class group of K. Then $C_K = J/K^\times$, and $I/P = C_K/C_K^n$.

First assume that K is a number field. Using the class field theory, there is a surjective Artin homomorphism

$$\psi_K \colon C_K \to \operatorname{Gal}(K^{\mathrm{ab}}/K),$$

which gives an isomorphism

$$C_K/\ker(\psi_K) \cong \operatorname{Gal}(K^{\mathrm{ab}}/K).$$

Note that $\ker \psi_K$ can be described as the connected component of 1. Equivalently, this is the image in C_K of the product over the archimedean primes v of K_v^+, which is the connected component of 1 in K_v. This means $K_v^+ = \mathbb{C}^\times$ or $K_v^+ = \mathbb{R}_{>0}$, depending on whether v is a real or a complex place. Since C_K^n contains $\ker \psi_K$, taking the quotient of the Artin homomorphism by C_K^n gives the isomorphism

$$C_K/C_K^n \cong \operatorname{Gal}(K^{\mathrm{ab}}/K)/n \operatorname{Gal}(K^{\mathrm{ab}}/K) = \operatorname{Gal}(K^{\mathrm{ab}}/K)^{\exp\, n}.$$

Now suppose that K is a global function field. In this case, we have an Artin homomorphism $\psi_K \colon C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, which induces an isomorphism

$$\hat{\psi}_K : \hat{C}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

where $\hat{C}_K$ denotes the profinite completion of the group C_K. Using the argument from the above paragraph, we get the isomorphism

$$C_K/C_K^n \cong \hat{C}_K/\hat{C}_K^n \cong \mathrm{Gal}(K^{\mathrm{ab}}/K)^{\exp n}.$$

Then for any global field K, by the Kummer theory, there is a perfect pairing

$$K^\times/K^{\times n} \times \mathrm{Gal}(K^{\mathrm{ab}}/K)^{\exp\ n} \to \mu_n.$$

This gives the desired isomorphism

$$\mathrm{Gal}(K^{\mathrm{ab}}/K)^{\exp\ n} \cong \mathrm{Hom}(K^\times/K^{\times n}, \mu_n).$$

□

Proposition 3.5 implies a statement analogous to [Ser73], Theorem 4, page 24:

Theorem 3.7. *Let K be a global field. Let V be the set of places of K, and let Λ be a finite set of indices. Let $(a_i)_{i\in\Lambda}$ be a finite family of elements in $K^\times$ and let $(\varepsilon_{i,v})_{i\in\Lambda, v\in V}$ be a family of numbers equal to ±1. In order that there exists $x \in K^\times$ such that $(a_i, x)_v = \varepsilon_{i,v}$ for all $i \in \Lambda$ and $v \in V$, it is necessary and sufficient that the following conditions be satisfied:*

(1) *All but finitely many of the $\varepsilon_{i,v}$ are equal to 1.*
(2) *For all $i \in \Lambda$, we have $\prod_{v\in V} \varepsilon_{i,v} = 1$.*
(3) *For all $v \in V$, there exists $x_v \in K^\times$ such that $(a_i, x_v)_v = \varepsilon_{i,v}$ for all $i \in \Lambda$.*

Proof. Let A be the group generated by the images of the a_i in I, and let A_v be the image of A in I_v for each v. Let ε_v be a character on A_v defined by

$$\begin{aligned} \varepsilon_v \colon A_v &\to \mu_n, \\ a_i &\mapsto \varepsilon_{i,v}. \end{aligned}$$

By (3), ε_v is indeed a character. Then define

$$\begin{aligned} \chi \colon \prod_v A_v &\to \mu_n \\ (a_v)_v &\mapsto \prod_v \varepsilon_v(a_v) \end{aligned}$$

Since almost all $\varepsilon_{i,v}$ are 1 by (1), this gives a well-defined character on $\prod_v A_v$. By (2), χ is trivial on A.

Then by Proposition 3.5, χ can be extended to a character $\widetilde{\chi} : I \to \mu_n$ that is trivial on P. By Lemma 3.6, this corresponds naturally to an element x of $K^\times/K^{\times n}$, so that we can write $\widetilde{\chi}((b_v)_v) = \prod_v (b_v, x)_v$. This gives the conclusion of the theorem, since now we can uniformly write

$$\varepsilon_{i,v} = \varepsilon_v(a_i) = (a_i, x)_v$$

for this x. □

3.3. Uniform definition of the ring of integers as intersection of localization rings. Let a, b be totally positive elements of $K^\times$ whose images in $K^\times/K^{\times 2}$ are independent. Then we have in particular that $\mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K) = \{\pm 1\} \times \{\pm 1\}$, and further, $\sqrt{ab} \notin K$. We would like to see how primes split in the extensions $K(\sqrt{a})/K$ and $K(\sqrt{b})/K$ (and hence in $K(\sqrt{a}, \sqrt{b})/K$). This will give us some information about the Hilbert symbols $(a, p)_{\mathfrak{p}}$ and $(b, p)_{\mathfrak{p}}$. More precisely, let

$$\psi : C_{\mathfrak{m}} \to \mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K) = \{\pm 1\} \times \{\pm 1\}$$

be the Artin map. Then:

Lemma 3.8. *Take $a, b \in K^\times$ as above, and let $p \in K^\times$. Let $\mathfrak{m}$ be an admissible modulus, corresponding to the extension $K(\sqrt{a}, \sqrt{b})/K$. Furthermore, suppose that $\mathfrak{m}$ is divisible by all primes dividing $2ab$, and we also assume that $\mathfrak{m}$ contains all real places. For a prime $\mathfrak{p}$ in K such that $\mathfrak{p} \nmid \mathfrak{m}_0$, $\mathfrak{p} \in \Delta_{a,p} \cap \Delta_{b,p}$ if and only if $v_{\mathfrak{p}}(p)$ is odd and $\psi(\mathfrak{p}) = (-1, -1)$.*

Proof. For any prime ideal $\mathfrak{p}$ of K prime to the modulus $\mathfrak{m}$, a is a $\mathfrak{p}$-adic unit, so we use equation (3.1) to compute $(a, p)_{\mathfrak{p}}$. That is, $(a, p)_{\mathfrak{p}} = -1$ if and only if $v_{\mathfrak{p}}(p)$ is odd and a is not a square in the residue field modulo $\mathfrak{p}$. But we have observed that these conditions are equivalent to insisting that $\psi(\mathfrak{p}) = (-1, \pm 1)$. A similar argument applies to $(b, p)_{\mathfrak{p}}$, and we get our conclusion. □

Let us partition the primes of K by their images under ψ:

$$\mathbb{P}^{[i,j]} = \{\text{prime ideals } \mathfrak{p} \text{ of } K \mid \psi(\mathfrak{p}) = (i, j)\},$$

where $(i, j) \in \mathrm{Gal}(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q})$, with $i, j \in \{\pm 1\}$. We also let

$$\mathbb{P}(p) = \{\text{primes } \mathfrak{p} \in \mathbb{P} \mid v_{\mathfrak{p}}(p) \text{ is odd}\}$$

and

$$\mathbb{P}^{[i,j]}(p) = \{\text{primes } \mathfrak{p} \in \mathbb{P}^{[i,j]} \mid v_{\mathfrak{p}}(p) \text{ is odd}\}.$$

As long as the image of (p) under the Artin map is nontrivial, the sets $\mathbb{P}^{[i,j]}(p)$ have a simple description using Hilbert symbols:

Lemma 3.9. *Suppose that $p \in K^\times$, and for the fixed modulus $\mathfrak{m}$ from above, suppose that the fractional ideal (p) has no common factors with $\mathfrak{m}$. Then we have the following identification of sets of primes, where the two sets differ at most by the primes dividing the modulus.*

$$\begin{aligned} \mathbb{P}^{[-1,-1]}(p) &\leftrightarrow \Delta_{a,p} \cap \Delta_{b,p}, \\ \mathbb{P}^{[-1,1]}(p) &\leftrightarrow \Delta_{a,p} \cap \Delta_{ab,p}, \\ \mathbb{P}^{[1,-1]}(p) &\leftrightarrow \Delta_{b,p} \cap \Delta_{ab,p}. \end{aligned}$$

Proof. $\mathbb{P}^{[-1,-1]}(p)$ is easy: by Lemma 3.8, it is $\Delta_{a,p} \cap \Delta_{b,p}$, excluding the primes not dividing the modulus. To prove the second (resp. third) equivalence, we express $\mathbb{P}^{[1,-1]}(p)$ (resp. $\mathbb{P}^{[-1,1]}(p)$) in a similar way, via the following identification of the Galois groups:

$$\mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K) \cong \mathrm{Gal}(K(\sqrt{ab}, \sqrt{b})/K)(\text{resp. } \mathrm{Gal}(K(\sqrt{a}, \sqrt{ab})/K)),$$
$$(\sigma_1, \sigma_2) \mapsto (\sigma_1\sigma_2, \sigma_2)(\text{resp. } (\sigma_1, \sigma_2) \mapsto (\sigma_1, \sigma_1\sigma_2)).$$

Composing the original Artin map ψ with this isomorphism, we can draw similar conclusions in these cases as in the case of $\mathbb{P}^{[-1,-1]}(p)$. □

As for $\mathbb{P}^{[1,1]}(p)$, we will start by defining an auxiliary set $\mathbb{P}(p,q)$ for $p,q \in K^\times$, given by $\mathbb{P}(p,q) := \Delta_{ap,q} \cap \Delta_{bp,q} \cap I^{S(\mathfrak{m})}$.

Definition 3.10. *For each $p,q \in K^\times$, let*

$$\begin{aligned} R_p^{[-1,-1]} &= \bigcap_{\mathfrak{p}\in\Delta_{a,p}\cap\Delta_{b,p}} (\mathcal{O}_K)_\mathfrak{p}, \\ R_p^{[1,-1]} &= \bigcap_{\mathfrak{p}\in\Delta_{ab,p}\cap\Delta_{b,p}} (\mathcal{O}_K)_\mathfrak{p}, \\ R_p^{[-1,1]} &= \bigcap_{\mathfrak{p}\in\Delta_{a,p}\cap\Delta_{ab,p}} (\mathcal{O}_K)_\mathfrak{p}, \\ R_{p,q}^{[1,1]} &= \bigcap_{\mathfrak{p}\in\Delta_{ap,q}\cap\Delta_{bp,q}} (\mathcal{O}_K)_\mathfrak{p}. \end{aligned}$$

The R's are existentially defined subrings of K containing $\mathcal{O}_K$ as long as no archimedean places are involved in the intersection, since for any $a,b,c,d \in K^\times$ such that $\sigma \notin \Delta_{a,b} \cap \Delta_{c,d}$ for each archimedean place σ,

$$T_{a,b} + T_{c,d} = \bigcap_{\mathfrak{p}\in\Delta_{a,b}\cap\Delta_{c,d}} (\mathcal{O}_K)_\mathfrak{p},$$

by Proposition 2.3.

We would now like to express $\mathcal{O}_K$ in terms of the R's, through the following lemmas:

Lemma 3.11. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ with $\mathfrak{p} \nmid \mathfrak{m}_0$, and suppose that $\psi(\mathfrak{p}) = (i,j)$ for $(i,j) \neq (1,1)$. Then $\mathfrak{p} \in \mathbb{P}^{[i,j]}(p)$ for some $p \in K^\times$. Hence, there exist $c,d \in K^\times$, such that $\mathfrak{p} \in \Delta_{c,p} \cap \Delta_{d,p}$.*

Proof. Choosing $p \in \mathfrak{p} - \mathfrak{p}^2$ will suffice, since we will then have $v_\mathfrak{p}(p) = 1$. □

Lemma 3.12. *For all prime ideals $\mathfrak{p}$ with $\mathfrak{p} \nmid \mathfrak{m}_0$ and satisfying $\psi(\mathfrak{p}) = (1,1)$, we have $\mathfrak{p} \in \Delta_{ap,q} \cap \Delta_{bp,q}$ for some $p,q \in K^\times$ such that q is totally positive.*

Proof. We can use the arguments exactly as in the proof of Lemma 3.11 to find p with $v_\mathfrak{p}(p)$ odd. Now, by the definition of $\mathbb{P}(p,q)$, we only need to find a totally positive q such that $v_\mathfrak{p}(q)$ is even (for example, 0), and q not a square in $\mathbb{F}_\mathfrak{p}$. This can be achieved by weak approximation. □

Corollary 3.13. *We have*

$$\mathcal{O}_K = \bigcap_{\mathfrak{p}|\mathfrak{m}_0} (\mathcal{O}_K)_\mathfrak{p} \cap \bigcap_{p,q\in(K^\times)^+} (R_p^{[1,1]} \cap R_p^{[1,-1]} \cap R_p^{[-1,1]} \cap R_{p,q}^{[1,1]}),$$

where $(K^\times)^+$ denotes the set of totally positive elements of K.

Proof. We use the fact that

$$\mathcal{O}_K = \bigcap_{\mathfrak{p}} (\mathcal{O}_K)_\mathfrak{p},$$

where $\mathfrak{p}$ ranges over all finite places of $\mathcal{O}_K$. Now we use Lemmas 3.11 and 3.12. Furthermore, the total positivity of p and q guarantees that no infinite places are included in the intersection. □

3.4. The Diophantine sets $J_{a,b}$ in K.

Here, we define the sets $J_{a,b}$ (see Definition 3.16), and show that these sets are Diophantine in K. In Section 3.6, we will relate $J_{a,b}$ with the Jacobson radicals of some of the rings $R_p^{[\sigma]}$ for $\sigma \in \operatorname{Gal} K(\sqrt{a}, \sqrt{b})/K$ with $\sigma \neq (1,1)$, and also with the Jacobson radicals of the rings $R_{p,q}^{[1,1]}$, thus concluding that the Jacobson radicals of some of these rings are Diophantine. This will be an important fact that allows us to eliminate the $\exists$-quantifier from [Poo09], and get an $\forall$-definition for $\mathcal{O}_K$ in K, as seen in Section S4.

Lemma 3.14.

$$K^{\times 2} \cdot T_{a,b}^{\times} = \bigcap_{\mathfrak{p} \in \Delta_{a,b}} v_{\mathfrak{p}}^{-1}(2\mathbb{Z}).$$

Proof. Let us first prove the inclusion of the left-hand side. Let $x \in K^2 \cdot T_{a,b}^{\times}$ and let $v \in \Delta_{a,b}$ be a nonarchimedean valuation. Writing $x = y^2 z$ for some $y \in K^{\times}$ and $z \in T_{a,b}^{\times}$, we have $v(x) = 2v(y) + v(z)$. Since $z \in T_{a,b}^{\times} = \bigcap_{\mathfrak{p} \in \Delta_{a,b}} \mathcal{O}_{\mathfrak{p}}^{\times}$, By Proposition 2.3, for $v \in \Delta_{a,b}$, we must have $v(z) = 0$, so $v(x)$ is even for all $x \in K^{\times 2} \cdot T_{a,b}^{\times}$ and all nonarchimedean $v \in \Delta_{a,b}$.

Conversely, suppose that we are given a nonzero element $q \in K$ whose valuation at each $v \in \Delta_{a,b}$ is even. Since $\Delta_{a,b}$ is finite, we can find $r \in K^{\times}$ whose valuation at each $v \in \Delta_{a,b}$ is $v(q)/2$ by weak approximation. Then q/r^2 has valuation 0 at each $v \in \Delta_{a,b}$, so $q/r^2 \in T_{a,b}^{\times}$ by Proposition 2.3. Therefore, $q \in K^{\times 2} \cdot T_{a,b}^{\times}$. □

Now, for $c \in K^{\times}$, we define

$$I_{a,b}^c := c \cdot K^2 \cdot T_{a,b}^{\times} \cap (1 - K^2 \cdot T_{a,b}^{\times}).$$

Then:

Lemma 3.15. *For $c \in K^{\times}$,*

$$I_{a,b}^c = \{y \in K \mid v(y) \text{ is odd and positive for all } v \in \Delta_{a,b} \cap \mathbb{P}(c), \text{ and } \\ v(y) \text{ and } v(1-y) \text{ are even for all } v \in \Delta_{a,b} \backslash \mathbb{P}(c)\}$$

Proof. By Lemma 3.14, $y \in I_{a,b}^c$ if and only if $v(y/c)$ and $v(1-y)$ are even for all $v \in \Delta_{a,b}$.

For $v \notin \mathbb{P}(c)$, $v(c)$ is even, so the condition becomes that $v(y)$ and $v(1-y)$ are even.

For $v \in \mathbb{P}(c)$, $v(c)$ is odd, so the condition becomes that $v(y)$ is odd and $v(1-y)$ is even, which is equivalent to the condition that $v(y)$ is odd and positive, by the ultrametric inequality. □

Definition 3.16. *For $a, b \in K^{\times}$, let*

$$J_{a,b} := \bigcap_{\mathfrak{p} \in \Delta_{a,b} \cap (\mathbb{P}(a) \cup \mathbb{P}(b))} \mathfrak{p}\mathcal{O}_{\mathfrak{p}}.$$

Lemma 3.17. *We have*

$$\begin{aligned} J_{a,b} = \{0\} \cup \{x \in K^\times \mid \exists y_1, y_2 \in K \text{ such that } \\ y_1, x - y_1 \in a \cdot K^2 \cdot T_{a,b}^\times \cap (1 - K^2 \cdot T_{a,b}^\times), \\ y_2, x - y_2 \in b \cdot K^2 \cdot T_{a,b}^\times \cap (1 - K^2 \cdot T_{a,b}^\times)\}. \end{aligned}$$

Proof. Let $J'_{a,b}$ denote the right-hand side of the equality in the statement of the lemma.

We begin by showing that

$$I_{a,b}^c + I_{a,b}^c = \bigcap_{\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(c)} \mathfrak{p}\mathcal{O}_\mathfrak{p}. \tag{3.2}$$

We first show the inclusion of the left into the right. Take some $z = y_1 + y_2 \in I_{a,b}^c + I_{a,b}^c$, with $y_1, y_2 \in I_{a,b}^c$. Then, we want to show that $v(z) > 0$ for all $v \in \Delta_{a,b} \cap \mathbb{P}(c)$. By Lemma 3.15, $v(y_1), v(y_2) > 0$, so that $v(z) = v(y_1 + y_2) > 0$ as well.

For the reverse inclusion, take $z \in \cap_{\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(c)} \mathfrak{p}\mathcal{O}_\mathfrak{p}$. By weak approximation on the valuations $v \in \Delta_{a,b}$, we can find $y_1 \in K$ satisfying $y_1, z - y_1 \in I_{a,b}^c$. This proves the equality in the above claim.

Finally, we observe that $J'_{a,b} = (I_{a,b}^a + I_{a,b}^a) \cap (I_{a,b}^b + I_{a,b}^b)$. Using the above claim 3.2,

$$\begin{aligned} J'_{a,b} &= \bigcap_{\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(a)} \mathfrak{p}\mathcal{O}_\mathfrak{p} \cap \bigcap_{\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(b)} \mathfrak{p}\mathcal{O}_\mathfrak{p} \\ &= \bigcap_{\mathfrak{p} \in (\Delta_{a,b} \cap \mathbb{P}(a)) \cup (\Delta_{a,b} \cap \mathbb{P}(b))} \mathfrak{p}\mathcal{O}_\mathfrak{p} \\ &= \bigcap_{\mathfrak{p} \in \Delta_{a,b} \cap (\mathbb{P}(a) \cup \mathbb{P}(b))} \mathfrak{p}\mathcal{O}_\mathfrak{p} \\ &= J_{a,b} \end{aligned}$$

and the lemma is proven. □

Corollary 3.18. *$J_{a,b}$ is diophantine in K.*

Proof. Since $T_{a,b}$ is diophantine, so is $J_{a,b}$ by Lemma 3.17. □

3.5. More preliminaries.

Lemma 3.19. *We can choose $a, b \in K^\times$ so that the following conditions hold:*

(1) *The images of a and b in $K^\times / K^{\times 2}$ are independent.*
(2) *$a, b \in 1 + 8\mathcal{O}_K$.*
(3) *Given an ideal class of K and and element $\sigma \in \mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K)$, there exists a prime $\mathfrak{q}$ of K in the ideal class such that $\mathfrak{q} \in I^{S(\mathfrak{m})}$ and $\psi(\mathfrak{q}) = \sigma$.*
(4) *No prime ideal appears in the factorizations of both (a) and (b).*
(5) *a and b are totally positive.*

In particular, we deduce from the lemma that this choice of a and b implies that a and b are $\mathfrak{p}$-adic squares for all $\mathfrak{p}|2$, by Hensel's lemma. Furthermore, the splitting behaviour of primes in the extension $K(\sqrt{a}, \sqrt{b})/K$ is independent of its image under the Artin map.

Proof. Let H denote the Hilbert class field of K. Choose a prime ideal $\mathfrak{p}$ not dividing 2 in K. There is some totally positive $a \in K$, with $a \in 1 + 8\mathcal{O}_K$ and $v_\mathfrak{p}(a) = 1$. Then $K(\sqrt{a})/K$ is ramified at $\mathfrak{p}$, so $\sqrt{a} \notin H$.

Now, choose another prime ideal $\mathfrak{p}'$ different from $\mathfrak{p}$ and not dividing 2 in K. Again, we choose a totally positive $b \in K$, satisfying $b \in 1 + 8\mathcal{O}_K$ and $(a, b) = 1$. Then $\mathfrak{p}'$ ramifies in $K(\sqrt{b})$, so $\sqrt{b} \notin H$. Further, since they ramify in different places, $\sqrt{ab} \notin H$ as well.

Then the field $K(\sqrt{a}, \sqrt{b})$ is linearly disjoint from H over K, because of the ramification of $\mathfrak{p}$ and $\mathfrak{p}'$. Thus, by the Chebotarev density theorem, we can find a prime ideal $\mathfrak{q}$ of K whose Frobenius element in $\mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K)$ is σ and whose Frobenius element in $\mathrm{Gal}(H/K)$ is prescribed by the given ideal class. Because of the latter, $\mathfrak{q}$ belongs to the given ideal class as in (3). □

Corollary 3.20. *Choosing a and b as above,*

$$\mathbb{P}^{[(-1,-1)]}(p) = \Delta_{a,p} \cap \Delta_{b,p},$$
$$\mathbb{P}^{[(-1,1)]}(p) = \Delta_{a,p} \cap \Delta_{ab,p},$$
$$\mathbb{P}^{[(1,-1)]}(p) = \Delta_{b,p} \cap \Delta_{ab,p}.$$

Proof. From Lemma 3.9, we already know that $\mathbb{P}^{[(-1,-1)]}(p)$ and $\Delta_{a,p} \cap \Delta_{b,p}$ agree on the primes not dividing $\mathfrak{m}$. So we just need to check that they agree on the primes dividing $\mathfrak{m}$. Since a and b are totally positive, no archimedean primes appear on either side of the equality. So take a prime $\mathfrak{p}$ with $\mathfrak{p} \nmid \mathfrak{m}_0$. If $\mathfrak{p}|2$, then $\mathfrak{p} \notin \Delta_{a,p} \cap \Delta_{b,p}$ since $a, b \in 1 + 8\mathcal{O}_K$, so by Hensel's lemma, they are $\mathfrak{p}$-adic squares. So we suppose that $\mathfrak{p} \nmid 2$. Since p is a $\mathfrak{p}$-adic unit, if $(a, p)_\mathfrak{p} = -1$, then $v_\mathfrak{p}(a)$ must be odd. Similarly, if $(b, p)_\mathfrak{p} = -1$, then $v_\mathfrak{p}(b)$ must be odd. But we cannot have both $v_\mathfrak{p}(a)$ and $v_\mathfrak{p}(b)$ odd, since (a) and (b) are relatively prime. Hence, $\mathfrak{p} \notin \Delta_{a,p} \cap \Delta_{b,p}$, and the two sets agree exactly. The proofs of the other two statements are similar. □

Throughout the rest of the paper, we assume that a and b are fixed so that they satisfy Lemma 3.19.

3.6. An existential definition of the Jacobson radical.

In this section, we show that the Jacobson radicals of some of the rings R from Definition 3.10 are Diophantine. Using the auxiliary Diophantine sets Φ and Ψ, we will give a criterion for the p's and q's that make the Jacobson radicals of the rings R_p and $R_{p,q}$ Diophantine.

Definition 3.21. *For each $\sigma \in \mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K)$, let*

$$\Phi_\sigma = \{p \in K^\times \mid (p) \in I^{S(\mathfrak{m})}, \psi((p)) = \sigma, \text{ and } \mathbb{P}(p) \subseteq \mathbb{P}^{[1,1]} \cup \mathbb{P}^{[\sigma]}\}.$$

Lemma 3.22.

(a) *For each $\sigma \in \mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K)$, the set Φ_σ is diophantine in K.*

(b) *For any $p \in \Phi_\sigma$ and $\sigma \in \mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K)$ with $\sigma \neq (1,1)$, $\mathbb{P}^{[\sigma]}(p) \neq \emptyset$. Furthermore, the Jacobson radical of $R_p^{[\sigma]}$, denoted $J(R_p^{[\sigma]})$, is diophantine in K.*

(c) *For $\sigma \in \mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K)$ with $\sigma \neq (1,1)$, if $\mathfrak{p} \nmid \mathfrak{m}_0$ is a prime ideal of K satisfying $\psi(\mathfrak{p}) = \sigma$, then there exists $p \in \Phi_\sigma$ such that $\mathfrak{p} \in \mathbb{P}^{[\sigma]}(p)$.*

Proof.

(a) Let us first show that the property that the set $\{p \in K^\times \mid (p) \in I^{S(\mathfrak{m})}, \psi((p)) = \sigma\}$ is Diophantine. To do this, we start by recalling that the trivial ray class consists of ideals in $i(K_{\mathfrak{m},1})$, where $i : K_{\mathfrak{m},1} \to I^{S(\mathfrak{m})}$ is the (well-defined) inclusion given by $p \mapsto (p)$. And we recall that $K_{\mathfrak{m},1}$ is defined by a finite number of local conditions of the form

$$\operatorname{ord}_{\mathfrak{p}}(a-1) \geq m(\mathfrak{p}),$$

and the total positivity conditions. Since sets in K with constraints of above form are Diophantine by [PS05], Proposition 2.2, $K_{\mathfrak{m},1}$ is Diophantine.

The other ray classes consisting of principal ideals are a translate of the trivial ray class by some element $p \in K^\times$, with (p) being an element of this ray class. Hence, if we denote this ray class by R, the set $\{p \in K^\times \mid (p) \in R\}$ is also Diophantine. By the finiteness of the ray class number, Φ_σ is also Diophantine in K.

Now, we need to show that the second condition $\mathbb{P}(p) \subseteq \mathbb{P}^{[1,1]} \cup \mathbb{P}^{[\sigma]}$ is Diophantine. For all $\sigma \in \operatorname{Gal}(K(\sqrt{a}, \sqrt{b})/K)$ with $\sigma \neq (1,1)$, by Corollary 3.20,

$$\mathbb{P}^{[\sigma]}(p) = \emptyset \Leftrightarrow p \in (K^\times)^2 \cdot (R_p^{[\sigma]})^\times.$$

Hence, the condition $\mathbb{P}^{[\sigma]}(p) = \emptyset$ is Diophantine. Since $\mathbb{P}(p) \subseteq \mathbb{P}^{[1,1]} \cup \mathbb{P}^{[-1,-1]}$ is equivalent to $\mathbb{P}^{[-1,1]}(p) = \mathbb{P}^{[1,-1]}(p) = \emptyset$, the condition $\mathbb{P}(p) \subseteq \mathbb{P}^{[1,1]} \cup \mathbb{P}^{[-1,-1]}$ is Diophantine. Similar statements hold for other $\sigma \in \operatorname{Gal}(K(\sqrt{a}, \sqrt{b})/K)$.

Since Φ_σ is given as the intersection of the two conditions, it is also Diophantine.

(b) For $\sigma = (-1,-1), (1,-1), (-1,1)$, the hypothesis $p \in \Phi_\sigma$ implies that $\mathbb{P}^{[\sigma]}(p) \neq \emptyset$, since if $p = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$, then

$$\sigma = \psi((p)) = \prod_{\mathfrak{p}} \psi(\mathfrak{p})^{e_{\mathfrak{p}}}$$

and $\psi(\mathfrak{p}) = (1,1)$ or $\psi(\mathfrak{p}) = \sigma$. Then we have, for example, $J(R_p^{[-1,-1]}) = J_{a,p} + J_{b,p}$ from Definition 3.16 and Corollary 3.20. Then by Corollary 3.18, $J(R_p^{[\sigma]})$ is Diophantine. From this, the assertion follows from the definition of $R_p^{[\sigma]}$.

(c) Suppose that $\mathfrak{p} \nmid \mathfrak{m}_0$ is a prime ideal of K satisfying $\psi(\mathfrak{p}) = \sigma$. By Lemma 3.19, we can choose a prime ideal $\mathfrak{q}$ whose ideal class can be represented by $\mathfrak{p}^{-1}$, and satisfies $\psi(\mathfrak{q}) = (1,1)$. Then $\mathfrak{p}\mathfrak{q} = (p)$ for some $p \in K^\times$, and $\mathfrak{p} \in \mathbb{P}(p)$. Furthermore, $\psi(p) = \psi(\mathfrak{p})\psi(\mathfrak{q}) = \sigma$. So $\mathfrak{p} \in \mathbb{P}^{[\sigma]}(p)$, as desired. □

It remains to obtain analogous statements to Lemma 3.22 in the case of $\sigma = (1,1)$.

Lemma 3.23. *Let $\mathfrak{m}$ be a fixed modulus for a number field K, and let $\mathfrak{p}_0$ be a prime ideal such that $\mathfrak{p}_0 \nmid \mathfrak{m}_0$. Then there exist infinitely many principal ideals (q), with its generator $q \in K^\times$ satisfying*

(A) $\psi((q)) = (-1,-1)$;
(B) $\left(\frac{q}{\mathfrak{p}_0}\right) = -1$;
(C) (q) *is a prime ideal.*

Proof. We begin by first showing that there exists an $x' \in K^\times$ satisfying $\psi((x')) = (-1,-1)$ and $\left(\frac{x'}{\mathfrak{p}_0}\right) = -1$. Let

$$K_{\mathfrak{m}'} := K^{S(\mathfrak{m}')} = \{\alpha \in K^\times \mid \operatorname{ord}_\mathfrak{p}(\alpha) = 0 \text{ for all } \mathfrak{p}|\mathfrak{m}'\}.$$

For any modulus $\mathfrak{m}'$ of K, there is a canonical isomorphism

$$K_{\mathfrak{m}'}/K_{\mathfrak{m}',1} \simeq \prod_{\substack{\mathfrak{p}|\mathfrak{m}' \\ \mathfrak{p} \text{ real}}} \{\pm\} \times (\mathcal{O}_K/\mathfrak{m}'_0)^\times,$$

Since $\mathfrak{m}$ is a modulus for K, so is $\mathfrak{m}\mathfrak{p}_0$. Then in particular, we have the canonical isomorphisms

$$K_\mathfrak{m}/K_{\mathfrak{m},1} \simeq \prod_{\substack{\mathfrak{p}|\mathfrak{m} \\ \mathfrak{p} \text{ real}}} \{\pm\} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times \text{ and} \tag{3.3}$$

$$K_{\mathfrak{m}\mathfrak{p}_0}/K_{\mathfrak{m}\mathfrak{p}_0,1} \simeq \prod_{\substack{\mathfrak{p}|\mathfrak{m}\mathfrak{p}_0 \\ \mathfrak{p} \text{ real}}} \{\pm\} \times (\mathcal{O}_K/\mathfrak{m}_0\mathfrak{p}_0)^\times \tag{3.4}$$

$$\simeq K_\mathfrak{m}/K_{\mathfrak{m},1} \times (\mathcal{O}_K/\mathfrak{p}_0)^\times, \tag{3.5}$$

where the last isomorphism follows by the Chinese remainder theorem, since $\mathfrak{p}_0 \nmid \mathfrak{m}$. Since $K_\mathfrak{m}/K_{\mathfrak{m},1}$ surjects onto the group of ray classes of principal ideals modulo $\mathfrak{m}$, each element of $K_\mathfrak{m}/K_{\mathfrak{m},1}$ determines a ray class of principal ideals modulo $\mathfrak{m}$. Similarly, each element of $K_{\mathfrak{m}\mathfrak{p}_0}/K_{\mathfrak{m}\mathfrak{p}_0,1}$ determines a ray class of principal ideals modulo $\mathfrak{m}\mathfrak{p}_0$.

By Lemma 3.19 (3), there exists a principal ideal (x_1) such that $\psi((x_1)) = (-1,-1)$. Then choose a ray class $x'' \in K_{\mathfrak{m}\mathfrak{p}_0}/K_{\mathfrak{m}\mathfrak{p}_0,1}$ mapping under 3.5 to the class of x_1 in $K_\mathfrak{m}/K_{\mathfrak{m},1}$ and to a nonsquare in $(\mathcal{O}_K/\mathfrak{p}_0)^\times$. Then this mod-$\mathfrak{m}\mathfrak{p}_0$ ray class consists of principal ideals (x') satisfying $\psi((x')) = (-1,-1)$ and $\left(\frac{x'}{\mathfrak{p}_0}\right) = -1$. By the Chebotarev density theorem, there are infinitely many prime ideals in the same ray class. For any such ideal $\mathfrak{q}$, since $\mathfrak{q}$ maps to an element of $K_\mathfrak{m}/K_{\mathfrak{m},1}$, it is principal, say $\mathfrak{q} = (q)$. This q satisfies (A), (B), and (C). □

Definition 3.24. *For $\sigma \in \mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K)$, define*

$$\widetilde{\Phi_\sigma} := K^{\times 2} \cdot \Phi_\sigma$$

$$\Psi := \left\{ (p,q) \in \widetilde{\Phi_{(1,1)}} \times \widetilde{\Phi_{(-1,-1)}} \;\middle|\; \prod_{\mathfrak{p}|\mathfrak{m}} (ap,q)_\mathfrak{p} = -1 \text{ and } p \in a \cdot K^{\times 2} \cdot (1 + J(R_q^{[-1,-1]})) \right\}.$$

Lemma 3.25.

(a) *Ψ is Diophantine in K.*

(b) *For $(p,q) \in \Psi$, we have $\Delta_{ap,q} \cap \Delta_{bp,q} \cap I^{S(\mathfrak{m})} \neq \emptyset$, and consequently, $J(R_{p,q}^{[1,1]})$ is Diophantine in K.*

(c) *For each prime ideal $\mathfrak{p}_0$ satisfying $\mathfrak{p}_0 \nmid \mathfrak{m}$ and $\psi(\mathfrak{p}_0) = (1,1)$, there exists $(p,q) \in \Psi$, such that $\Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}_0\}$.*

Proof.

(a) By Lemma 3.22(a), Φ_σ is Diophantine, so $\widetilde{\Phi_\sigma}$ is Diophantine. The fact that Ψ is Diophantine follows from the previous sentence, Lemma 3.22(b) and the fact that the condition $\prod_{\mathfrak{p}|\mathfrak{m}} (ap,q)_\mathfrak{p} = -1$ consists of finitely many local conditions and hence it cuts out a Diophantine set from $K^\times \times K^\times$, by [PS05], Proposition 2.2.

(b) Suppose that $(p,q) \in \Psi$. By Hilbert reciprocity, there is at least one prime ideal $\mathfrak{p} \nmid \mathfrak{m}$ such that $(ap,q)_\mathfrak{p} = -1$. Then either $v_\mathfrak{p}(ap)$ or $v_\mathfrak{p}(q)$ is odd by equation (3.1). But $v_\mathfrak{p}(a) = 0$ and $p \in \widetilde{\Phi_{(1,1)}}$ and $q \in \widetilde{\Phi_{(-1,-1)}}$, so $\mathfrak{p} \in \mathbb{P}(p) \cup \mathbb{P}(q) \subseteq \mathbb{P}^{[1,1]} \cup \mathbb{P}^{[-1,-1]}$.

We claim that $\mathfrak{p} \in \mathbb{P}^{[1,1]}$. Suppose otherwise, that is, $\mathfrak{p} \in \mathbb{P}^{[-1,-1]}$. Then in particular, $\mathfrak{p} \notin \mathbb{P}(p)$, so $v_\mathfrak{p}(ap)$ is even. So $v_\mathfrak{p}(q)$ must be odd. Therefore, $\mathfrak{p} \in \mathbb{P}^{[-1,-1]}(q)$, which means that $R_q^{[-1,-1]} \subset \mathcal{O}_\mathfrak{p}$. Then we have by Definition 3.16 that $J(R_q^{[-1,-1]}) \subset \mathfrak{p}\mathcal{O}_\mathfrak{p}$, which implies by Hensel's lemma that $1 + J(R_q^{[(-1,-1)]}) \subset \mathcal{O}_\mathfrak{p}^{\times 2}$. From $p \in a \cdot K^{\times 2} \cdot (1 + J(R_q^{[-1,-1]})$, we deduce that $ap \in K_\mathfrak{p}^{\times 2}$, which implies that $(ap,q)_\mathfrak{p} = 1$, a contradiction. Hence, $\mathfrak{p} \in \mathbb{P}^{[1,1]}$, as claimed.

On the other hand, if $v_\mathfrak{p}(q)$ is even, then $(a,q)_\mathfrak{p} = (b,q)_\mathfrak{p} = 1$. If $v_\mathfrak{p}(q)$ is odd, then by Lemma 3.8, $(a,q)_\mathfrak{p} = (b,q)_\mathfrak{p} = -1$. In either case, $(a,q)_\mathfrak{p} = (b,q)_\mathfrak{p}$, so $(bp,q)_\mathfrak{p} = (ap,q)_\mathfrak{p} = -1$, so $\mathfrak{p} \in \Delta_{ap,q} \cap \Delta_{bp,q}$. Since we had $\mathfrak{p} \nmid \mathfrak{m}$, in fact $\mathfrak{p} \in \Delta_{ap,q} \cap \Delta_{bp,q} \cap I^{S(\mathfrak{m})}$. Hence, $\Delta_{ap,q} \cap \Delta_{bp,q} \cap I^{S(\mathfrak{m})} \neq \emptyset$. Then $J(R_{p,q}^{[1,1]}) = J_{ap,q} + J_{bp,q}$, so $J(R_{p,q}^{[1,1]})$ is Diophantine by Corollary 3.18.

(c) Fix a prime $\mathfrak{p}_0 \nmid \mathfrak{m}$ satisfying $\psi(\mathfrak{p}_0) = (1,1)$. We would like to find $(p,q) \in \Psi$ such that $\mathfrak{p}_0 \in \Delta_{ap,q} \cap \Delta_{bp,q}$.

For each $\mathfrak{p}|\mathfrak{m}_0$, let $E_\mathfrak{p}$ be a finite subset of $K^\times$ whose image in $K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times 2}$ is a basis. By Chinese remainder theorem, we choose each $e \in \bigcup_{\mathfrak{p}|\mathfrak{m}_0} E_\mathfrak{p}$ so that $e \equiv 1 \pmod{\mathfrak{p}_0}$. Since $\bigcup_{\mathfrak{p}|\mathfrak{m}_0} E_\mathfrak{p}$ is finite, there are only finitely many prime ideals that are generated by elements in it.

By Lemma 3.23, there are infinitely many ideals (q) with $q \in K^\times$ satisfying:

(A) $\psi((q)) = (-1, -1)$;

(B) $\left(\frac{q}{\mathfrak{p}_0}\right) = -1$;

(C) (q) is a prime ideal.

Choose an ideal (q) that is not generated by elements in $\bigcup_{\mathfrak{p}|\mathfrak{m}_0} E_\mathfrak{p}$. We note that this choice of q implies that

$$\Delta_{a,q} \cap \Delta_{b,q} = \{(q)\}. \tag{3.6}$$

By (A), $q \in \Phi_{(-1,-1)} \subseteq \widetilde{\Phi_{(-1,-1)}}$. Also, we choose e_0 so that $\left(\frac{e_0}{(q)}\right) = -1$ and $\left(\frac{e_0}{\mathfrak{p}_0}\right) = 1$. From $\left(\frac{e_0}{(q)}\right) = -1$, the image of $\{q, e_0\} \subseteq K^\times$ is a basis for $K_{(q)}/K_{(q)}^{\times 2}$. Furthermore, $v_{(q)}(e_0) = 0$, and $v_{\mathfrak{p}_0}(e_0)$ is even.

We claim that there exists $p \in K^\times$ satisfying the following constraints.

1. $(e, p)_\mathfrak{p} = 1$ for all $\mathfrak{p}|\mathfrak{m}_0$ and $e \in E_\mathfrak{p}$.
2. $(e_0, p)_{(q)} = 1$ and $(q, p)_{(q)} = -1$.
3. $(a, p)_\mathfrak{p} = 1$ and $(b, p)_\mathfrak{p} = 1$ for each $\mathfrak{p} \nmid \mathfrak{m}$.
4. $(q, p)_{\mathfrak{p}_0} = -1$.
5. $\prod_{\mathfrak{p}|\mathfrak{m}} (ap, q)_\mathfrak{p} = -1$.
6. For all archimedean places $\mathfrak{q}$, $(p, q)_\mathfrak{q} = 1$.

We will use Theorem 3.7 to choose such a p according to the prescription of the Hilbert symbol given by the following table. The columns are indexed by the places v, the rows are indexed by the a_i to be used in Theorem 3.7, and the entries in the table are the $\varepsilon_{i,v}$.

	$\mathfrak{p}_0$	(q)	All other places
any $e \in E_\mathfrak{p}$ for $\mathfrak{p}\vert\mathfrak{m}_0$	1	1	1
e_0	1	1	1
q	-1	-1	1
a	1	1	1
b	1	1	1

Almost all entries in the above table are 1. Also, the product of the entries in each row is 1. For the existence of a local element satisfying the prescription in the (q)-column, we claim that a is one such element: $(a, e)_{(q)} = 1$ for all $e \in \bigcup_{\mathfrak{p}|\mathfrak{m}_0} E_\mathfrak{p} \cup \{a, b, e_0\}$, since a and e are q-adic units. From Lemma 3.8, $(a, q)_{(q)} = -1$. For the existence of a local element satisfying the prescription in the $\mathfrak{p}_0$-column, we claim that any $x \in \mathfrak{p}_0 - \mathfrak{p}_0^2$ works. By equation (3.1), $(x, q)_{\mathfrak{p}_0} = -1$, since q is not a square modulo $\mathfrak{p}_0$ by construction. Furthermore, $(x, e)_{\mathfrak{p}_0} = 1$ for $e \in E_\mathfrak{p}$ with $\mathfrak{p}|\mathfrak{m}_0$ by equation (3.1) and the choice of e such that $e \equiv 1 \pmod{\mathfrak{p}_0}$. Also, $(x, a)_{\mathfrak{p}_0} = (x, b)_{\mathfrak{p}_0} = 1$ since $\psi(\mathfrak{p}_0) = (1, 1)$, by Lemma 3.8. Finally, by equation (3.1), $(x, e_0)_{\mathfrak{p}_0} = \left(\frac{e_0}{\mathfrak{p}_0}\right) = 1$, so x satisfies the prescription on the $\mathfrak{p}_0$-column.

Thus, the conditions of Theorem 3.7 hold, so there exists p satisfying the above prescription of Hilbert symbols. We now show that this p satisfies the five constraints given earlier in the proof. Constraints (1), (2), (3) and (4) are evident from the definition of p: constraint (1) from the first row; constraint (2) from the second and third rows; constraint (3) from the last entries of fourth and fifth rows; and constraint (4) comes from the prescription in the $(q, \mathfrak{p}_0)$-entry. Constraint (5) is automatic, since

$$\begin{aligned}\prod_{\mathfrak{p}|\mathfrak{m}}(ap, q)_{\mathfrak{p}} &= \prod_{\mathfrak{p}|\mathfrak{m}}(a, q)_{\mathfrak{p}} \text{ (since } (p, q)_{\mathfrak{p}} = 1 \text{ for all } \mathfrak{p}|\mathfrak{m}) \\ &= \prod_{\mathfrak{p}\nmid\mathfrak{m}}(a, q)_{\mathfrak{p}} \text{ (Hilbert Reciprocity)} \\ &= (a, q)_{(q)} = -1.\end{aligned}$$

Finally, constraint (6) is clear from the prescription of the third row.

Since $(e_0, a)_{(q)} = 1$ and $(q, a)_{(q)} = -1$, the first half of (2) implies that $(e_0, ap)_{(q)} = 1$ and $(q, ap)_{(q)} = 1$, so $v_{(q)}(ap)$ is even. Choose $y \in K^\times$ such that $v_{(q)}(y) = v_{(q)}(ap)/2$, and let $z = ap/y^2$. Then $v_{(q)}(z) = 0$, and $(q, z)_{(q)} = (e_0, z)_{(q)} = 1$. Since the Hilbert symbol is a nondegenerate pairing, z is a (q)-adic square. Thus, $ap = zy^2$ is also a (q)-adic square.

Now we will show that $(p, q) \in \Psi$. By the nondegeneracy of the Hilbert symbol as a bilinear pairing on $K_v^\times/K_v^{\times 2} \times K_v^\times/K_v^{\times 2} \to \{\pm 1\}$, the first constraint implies that $v_{\mathfrak{p}}(p)$ is even for each $\mathfrak{p}|\mathfrak{m}_0$. Now, using weak approximation, find some $r \in K^\times$ satisfying $v_{\mathfrak{p}}(r) = v_{\mathfrak{p}}(p)/2$ for each $\mathfrak{p}|\mathfrak{m}_0$. We may divide p by r^2, without changing any of the Hilbert symbols involving p, so as to assume that $(p) \in I^{S(\mathfrak{m})}$. We claim that constraint (3) implies that $\psi((p)) = (1, 1)$. Write $(p) = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$. For each prime $\mathfrak{p} \nmid \mathfrak{m}$, we have $(a, p)_{\mathfrak{p}} = (b, p)_{\mathfrak{p}} = 1$. then either $v_{\mathfrak{p}}(p)$ is even, or a and b are squares mod $\mathfrak{p}$. If $e_{\mathfrak{p}}$ is odd, then $\psi(\mathfrak{p}) = (1, 1)$ since a and b are squares mod $\mathfrak{p}$. If $e_{\mathfrak{p}}$ is even, then $\psi(\mathfrak{p})^{e_{\mathfrak{p}}} = (1, 1)$. Hence, $\psi((p)) = \prod_{\mathfrak{p}} \psi(\mathfrak{p})^{e_{\mathfrak{p}}} = (1, 1)$. The two conditions in (2) implies that ap is a (q)-adic square. Then $p \in a \cdot K^{\times 2} \cdot (1 + J(R_q^{[(-1,-1)]}))$, by the following reason: from 3.6, $\Delta_{a,q} \cap \Delta_{b,q} = \{(q)\}$. Since a and b were chosen to be $\mathfrak{p}$-adic squares for $\mathfrak{p}|2$, $J(R_q^{[(-1,-1)]}) = q(\mathcal{O}_K)_{(q)}$. Then $K^{\times 2}(1 + J(R_q^{[(-1,-1)]})) = K_{(q)}^{\times 2} \cap K^\times$. Since $ap \in K_{(q)}^{\times 2} \cap K^\times$, the equality from the previous sentence gives that $p \in a \cdot K^{\times 2} \cdot (1 + J(R_q^{[(-1,-1)]}))$. Thus, constraints (1), (2), (3), (5) give that $(p, q) \in \Psi$.

From (4), $(ap, q)_{\mathfrak{p}_0} = (bp, q)_{\mathfrak{p}_0} = -1$. Furthermore, $(ap, q)_{(q)} = 1$ from the second half of (2), since $(a, q)_{(q)} = -1$. For any other place $\mathfrak{q} \nmid \mathfrak{m}$, $(ap, q)_{\mathfrak{q}} = 1$ by the prescription of the Hilbert symbols along the q-row. Thus, $\Delta_{ap,q} \cap \Delta_{bp,q} \cap I^{S(\mathfrak{m})} = \{\mathfrak{p}_0\}$.

Now, if we could show that $\Delta_{ap,q} \cap \Delta_{bp,q}$ contains no primes dividing $\mathfrak{m}$, we would be done. Since a and b were chosen to be totally positive, $(a, q)_{\mathfrak{q}} = (b, q)_{\mathfrak{q}} = 1$ for any archimedean place $\mathfrak{q}$. Further, from the prescription of Hilbert symbols, $(p, q)_{\mathfrak{q}} = 1$ for any archimedean place $\mathfrak{q}$. Thus, no archimedean primes appear in $\Delta_{ap,q} \cap \Delta_{bp,q}$. Now suppose $\mathfrak{q}|2$. Then $(a, q)_{\mathfrak{q}} = 1$ since a is a 2-adic square, and $(p, q)_{\mathfrak{q}} = 1$ from the construction of p. This means $(ap, q)_{\mathfrak{q}} = 1$, so $\mathfrak{q} \notin \Delta_{ap,q} \cap \Delta_{bp,q}$. So suppose that $\mathfrak{q}|\mathfrak{m}$ and $\mathfrak{q} \nmid 2$. Then by constraint (1), $(p, q)_{\mathfrak{q}} = 1$. But then since (a) and (b) are coprime, at most one of $(a, q)_{\mathfrak{q}}$ and $(b, q)_{\mathfrak{q}}$ can be -1 by equation (3.1) since $v_{\mathfrak{q}}(q)$ is even. Hence, we again have $\mathfrak{q} \notin \Delta_{ap,q} \cap \Delta_{bp,q}$. This implies that $\Delta_{ap,q} \cap \Delta_{bp,q} \cap I^{S(\mathfrak{m})} = \Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}_0\}$. □

4. Proof of the main theorem

For a semilocal subring $R = \bigcap_{\mathfrak{p}\in\Delta} \mathcal{O}_\mathfrak{p}$ of K, where Δ is some finite set of finite places of K, we define

$$\widetilde{R} = \{x \in K \mid \nexists y \in J(R) \text{ with } xy = 1\}.$$

Lemma 4.1. *Keeping the notation from above,*

(a) *If $J(R)$ is diophantine in K, then $\widetilde{R}$ is defined by a universal formula in K.*
(b) *$\widetilde{R} = \bigcup_{\mathfrak{p}\in\Delta} \mathcal{O}_\mathfrak{p}$, provided that $\Delta \neq \emptyset$ (that is, $R \neq K$).*

Proof. See [Koe10], Lemma 14. □

Theorem 4.2. *For any number field K,*

$$\mathcal{O}_K = \bigcap_{\mathfrak{p}\mid\mathfrak{m}_0} \widetilde{(\mathcal{O}_K)_\mathfrak{p}} \cap \left(\bigcap_{\sigma\neq(1,1)} \bigcap_{p\in\Phi_\sigma} \widetilde{R_p^\sigma} \right) \cap \bigcap_{(p,q)\in\Psi} \widetilde{R_{p,q}^{[1,1]}},$$

where Φ_σ and Ψ are the diophantine sets defined in the previous section.

Proof. By Lemmas 3.22(b) and 3.25(b), all the sets $\mathbb{P}^{[\sigma]}(p)$ and $\Delta_{ap,q} \cap \Delta_{bp,q}$ are nonempty for $p \in \Phi_\sigma$ and $(p,q) \in \Psi$. So by Corollary 3.20, Lemma 4.1(b) and Definition 3.10, the right-hand side is equal to

$$\bigcap_{\mathfrak{p}\mid\mathfrak{m}_0} (\mathcal{O}_K)_\mathfrak{p} \cap \left(\bigcap_{\sigma\neq(1,1)} \bigcap_{p\in\Phi_\sigma} \bigcup_{\mathfrak{p}\in\mathbb{P}^{[\sigma]}(p)} (\mathcal{O}_K)_\mathfrak{p} \right) \cap \bigcap_{(p,q)\in\Psi} \bigcup_{\mathfrak{p}\in\Delta_{ap,q}\cap\Delta_{bp,q}} (\mathcal{O}_K)_\mathfrak{p}.$$

Assume first that $\mathfrak{p}_0$ is a prime ideal satisfying $\psi(\mathfrak{p}_0) = \sigma$, where $\sigma \neq (1,1)$. We claim that we can find $p, p' \in \Phi_\sigma$ such that

$$(\mathcal{O}_K)_{\mathfrak{p}_0} = \bigcup_{\mathfrak{p}\in\mathbb{P}^\sigma(p)} (\mathcal{O}_K)_\mathfrak{p} \cap \bigcup_{\mathfrak{p}\in\mathbb{P}^\sigma(p')} (\mathcal{O}_K)_\mathfrak{p}.$$

First suppose that $\sigma = (-1,-1)$. By Lemma 3.22(c), choose a $p \in \Phi_\sigma$ such that $\mathfrak{p}_0 \in \mathbb{P}^\sigma(p)$, and let $\mathfrak{p}_1$, $dots, \mathfrak{p}_n$ be the rest of the primes in $\Delta_{a,p}\cap\Delta_{b,p}$. By Lemma 3.19, choose a prime ideal $\mathfrak{q}$ in the ideal class of $\mathfrak{p}_0^{-1}$, with $\psi(\mathfrak{q}) = (1,1)$. Since there are infinitely many choices for $\mathfrak{q}$, we may further assume that $\mathfrak{q}$ is not equal to $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Let $(p') = \mathfrak{p}_0\mathfrak{q}$. Then $p' \in \Phi_\sigma$ by construction, and

$$(\Delta_{a,p} \cap \Delta_{b,p}) \cap (\Delta_{a,p'} \cap \Delta_{b,p'}) = \mathbb{P}^{[-1,-1]}(p) \cap \mathbb{P}^{[-1,-1]}(p') = \{\mathfrak{p}_0\},$$

where the first equality follows by Corollary 3.20. So the integrality at $\mathfrak{p}_0$ is imposed. The arguments for $\sigma = (-1,1)$ and $\sigma = (1,-1)$ are similar to the above argument.

Now, if $\mathfrak{p}_0$ is a prime satisfying $\psi(\mathfrak{p}_0) = (1,1)$, then Lemma 3.25 lets us choose $(p,q) \in \Psi$ such that $\{\mathfrak{p}_0\} = \Delta_{ap,q} \cap \Delta_{bp,q}$, so that

$$\bigcup_{\mathfrak{p}\in\Delta_{ap,q}\cap\Delta_{bp,q}} (\mathcal{O}_K)_\mathfrak{p} = (\mathcal{O}_K)_{\mathfrak{p}_0}.$$

Then the integrality at $\mathfrak{p}_0$ is imposed, and the theorem is proven. □

Corollary 4.3. *For any number field K, $\mathcal{O}_K$ is defined by a first-order universal formula.*

Proof. By Lemmas 3.22(b) and 3.25(b), $J(R_p^\sigma)$ and $J(R_{p,q}^{[1,1]})$ are diophantine, for

$$\sigma \in \mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K)$$

with $\sigma \neq (1, 1)$. Then by Lemma 4.1(a), the right-hand side is defined by a universal formula. By Lemmas 3.22(a) and 3.25(a), Φ_σ and Ψ are diophantine. Hence, the right-hand side appearing in the statement of Theorem 4.2 is defined by a first-order universal formula. □

Acknowledgments

I would like to thank my advisor, Bjorn Poonen, for suggesting this problem, for many helpful conversations, and for the comments on improving the exposition. I also thank John Tate for providing an outline of the proof of Theorem 3.7, and for giving his permission to include it in this paper. I am also grateful to Gregory Minton and Bianca Viray for helpful discussions. Finally, I thank the anonymous referee for carefully reviewing this manuscript, and for the helpful comments to make the exposition clearer.

References

[CF86] J.W.S. Cassels and A. Fröhlich (eds), *Algebraic Number Theory*, Proceedings of the instructional Conference held at the University of Sussex, Brighton, September 1–17, 1965, Reprint of the 1967 original, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1986, xviii+366.

[Koe10] J. Koenigsmann, *Defining* $\mathbb{Z}$ *in* $\mathbb{Q}$, 2010, `arXiv:1011.3424v1`.

[MR10] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem* Invent. Math. **181**(3) (2010), 541–575, doi 10.1007/s00222-010-0252-0.

[PS05] B. Poonen and A. Shlapentokh *Diophantine definability of infinite discrete nonarchimedean sets and Diophantine models over large subrings of number fields*, J. Reine Angew. Math. **588** (2005), 27–47, doi 10.1515/crll.2005.2005.588.27.

[Poo09] B. Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131**(3) (2009), 675–682, doi 10.1353/ajm.0.0057.

[Rob49] J. Robinson, *Definability and decision problems in arithmetic*, J. Symbol. Logic **14** (1949), 98–114.

[Ser73] J.-P. Serre, *A course in arithmetic*, Translated from the French, Graduate Texts in Mathematics, No. 7, Springer-Verlag, New York, 1973, viii+115.

[Ser79] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, **67**, Translated from the French by Marvin Jay Greenberg, Springer-Verlag, New York, 1979, viii+241.

[Tat11] J. Tate, *Personal communication* (2011).

Department of Mathematics, Massachusetts Institute of Technology, 77
Massachusetts Avenue, Cambridge, MA 02139, USA
E-mail address: `jmypark@math.mit.edu`
`URL: http://math.mit.edu/~jmypark`