TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 372, Number 8, 15 October 2019, Pages 5825–5850
https://doi.org/10.1090/tran/7810
Article electronically published on March 26, 2019

DIOPHANTINE DEFINABILITY OF NONNORMS OF CYCLIC EXTENSIONS OF GLOBAL FIELDS

TRAVIS MORRISON

ABSTRACT. We show that, for any square-free natural number n and any global field K with $(\mathrm{char}(K), n) = 1$ containing a primitive nth root of unity, the pairs $(x, y) \in K^\times \times K^\times$ such that x is not a relative norm of $K(\sqrt[n]{y})/K$ form a diophantine set over K. We use the Hasse norm theorem, Kummer theory, and class field theory to prove this result. We also prove that, for any $n \in \mathbb{N}$ and any global field K with $\mathrm{char}(K) \neq n$, $K^\times \setminus K^{\times n}$ is diophantine over K. For a number field K, this is a result of Colliot-Thélène and Van Geel, proved using results on the Brauer–Manin obstruction. Additionally, we prove a variation of our main theorem for global fields K without the nth roots of unity, where we parametrize varieties arising from norm forms of cyclic extensions of K without any rational points by a diophantine set.

1. Introduction

The diophantine subsets of a field K which is not algebraically closed are the subsets which are defined by a positive-existential formula.

Definition 1.1. Let R be a commutative domain. A set $A \subset R^n$ is diophantine over R if there exist an $m \in \mathbb{N}$ and a polynomial $f \in R[x_1, \ldots, x_m, y_1, \ldots, y_n]$ such that

$$A = \{(a_1, \ldots, a_n) : \exists r_1, \ldots, r_m \in R \text{ such that } f(r_1, \ldots, r_m, a_1, \ldots, a_n) = 0\}.$$

More geometrically, a subset $A \subseteq K^n$ is diophantine over K if there is an affine algebraic set X/K and a K-morphism $X \to \mathbb{A}^n_K$ such that A is the image of $X(K)$.

Diophantine sets feature prominently in decidability and definability in number theory. Hilbert's tenth problem, abbreviated as H10, asked whether there is an algorithm which takes as input an arbitrary polynomial equation with coefficients in $\mathbb{Z}$ and output YES if that equation has a solution over $\mathbb{Z}$, and NO otherwise. In [Mat70], Matiyasevich, building on the work of Davis, Putnam, and Robinson [DPR61], proves that such an algorithm cannot exist; i.e, H10 is undecidable. This is a consequence of the "DPRM" theorem: the diophantine subsets of $\mathbb{Z}$ are precisely the recursively enumerable subsets of $\mathbb{Z}$. We can then ask whether such an algorithm exists for other rings R by replacing $\mathbb{Z}$ with R. Over $\mathbb{Q}$, H10 is still open. If one could show that $\mathbb{Z}$ were diophantine over $\mathbb{Q}$, then a standard argument reduces H10 over $\mathbb{Z}$ to H10 over $\mathbb{Q}$, implying that H10 over $\mathbb{Q}$ would be undecidable

Received by the editors October 19, 2017, and, in revised form, November 1, 2018, and November 9, 2018.

2010 *Mathematics Subject Classification.* Primary 11D57; Secondary 11U99.

The author was partially supported by National Science Foundation grants DMS-1056703 and CNS-1617802, and in part by funding from the Natural Sciences and Engineering Research Council of Canada, the Canada First Research Excellence Fund, CryptoWorks21, Public Works and Government Services Canada, and the Royal Bank of Canada.

as well. The DPRM theorem resolved H10 by classifying the diophantine subsets of $\mathbb{Z}$, which suggests that understanding the sets which are diophantine over a global field K sheds some light on the difficulty of solving diophantine equations over K.

Obstructions to the existence of rational points on a variety can be used to produce diophantine definitions of sets. Poonen, in [Poo09b], uses results on the Brauer–Manin obstruction to show that the nonsquares of a global field K of characteristic not 2 are diophantine over K. With similar methods, in [VAV12], Várilly-Alvarado and Viray show that, assuming Schinzel's hypothesis, for any natural number n and number field K, the set of non-nth powers of K is diophantine over K. Colliot-Thélène and Van Geel unconditionally prove this result in [CTVG15]. This is further generalized in [Dit17], where Dittman shows that the irreducibility of polynomials over a global field is diophantine.

Because H10 is undecidable over $\mathbb{Z}$, a first-order definition of $\mathbb{Z}$ in $\mathbb{Q}$ shows that the full first-order theory of $\mathbb{Q}$ is undecidable. Robinson gave a first-order definition of $\mathbb{Z}$ in $\mathbb{Q}$, showing that it has a $\forall\exists\forall\exists$ definition in [Rob49], and Poonen improved on this in [Poo09a], showing that $\mathbb{Z}$ has a $\forall\exists$ definition in $\mathbb{Q}$. Koenigsmann proves that $\mathbb{Q}\setminus\mathbb{Z}$ is diophantine over $\mathbb{Q}$ and moreover that this implies that $\mathbb{Z}$ has a $\forall$ definition in $\mathbb{Q}$. Using similar methods, Koenigsmann gives a new proof that $\mathbb{Q}^\times \setminus \mathbb{Q}^{\times 2}$ is diophantine over $\mathbb{Q}$, and it also shows that the set

$$\{(x,y) \in K^\times \times K^\times : x \text{ is not a norm of } \mathbb{Q}(\sqrt{y})\}$$

is diophantine over $\mathbb{Q}$. Park shows that for a number field K, $\mathcal{O}_K$ has a first-order universal definition. In [Eis18], these results are generalized further: for a global field K with $\operatorname{char}(K) \neq 2$ and S being a finite, nonempty set of primes of K, the sets $K \setminus \mathcal{O}_S$, $K \setminus K^{\times 2}$, and

$$\{(x,y) \in K^\times \times K^\times : x \text{ is not a norm of } K(\sqrt{y})\}$$

are shown to be diophantine over K.

For a global field K such that $n \in K^\times$ and K contains a primitive root of unity ω, let $(a,b)_\omega$ denote the cyclic algebra corresponding to a, b, and ω (defined in Definition 2.6). In this paper, we prove the following theorem.

Theorem 1.2. *Let ℓ be an odd prime, and suppose that K is a global field with $\operatorname{char}(K) \neq \ell$. Further suppose that K contains a primitive ℓth root of unity ω. Then*

$$\{(x,y) \in K^\times \times K^\times : (x,y)_\omega \text{ is not split}\}$$

is diophantine over K.

This theorem is equivalent to the following.

Theorem 1.3. *Let ℓ be an odd prime, and suppose that K is a global field with $\operatorname{char}(K) \neq \ell$. Further suppose that K contains a primitive ℓth root of unity. Then*

$$\{(x,y) \in K^\times \times K^\times : x \text{ is not a norm of } K(\sqrt[\ell]{y})\}$$

is diophantine over K.

We prove Theorem 1.3 in Section 5. We use the Hasse norm theorem, which says that $x \in K$ is a relative norm of a cyclic extension L/K if and only if it is a relative local norm in every completion of L/K. For a fixed prime of K, whether x is a relative norm of $K_\mathfrak{p}(\sqrt[\ell]{y})$ is controlled by diophantine local conditions on x and y. This is not enough to prove Theorem 1.3: while finite unions of diophantine

sets are diophantine, infinite unions do not have to be diophantine. To reduce from infinitely many to finitely many conditions on x and y, we group the primes of K into finitely many ray classes for an abelian extension L/K, and we use Kummer theory and class field theory to relate the splitting of primes in these classes to the Hilbert symbol.

Next, we show that, for each union of ray classes C, the set

$$\{(x,y) \in K^\times \times K^\times : \exists \mathfrak{p} \in C \text{ such that } x \text{ is not a norm of } K_\mathfrak{p}(\sqrt[\ell]{y})\}$$

is diophantine over K. Taking the union over these subsets of $K^\times \times K^\times$ gives our diophantine definition of

$$\{(x,y) \in K^\times \times K^\times : x \text{ is not a norm of } K(\sqrt[\ell]{y})\}.$$

Our approach to this is as follows. We encode the local conditions using certain semilocal subrings of K, along with their Jacobson radicals. These semilocal rings are defined by the norm and trace forms of cyclic algebras and are diophantine by a result of [Dit17]. This is an extension of ideas in [Eis05, Poo09a, Koe16, Par13, Eis18], where quaternion algebras are used to produce diophantine definitions of semilocal rings. We also show that their Jacobson radicals are diophantine. Then we parametrize these families by sets which are diophantine over K, and which ensure that the primes of any semilocal ring in a family are all in the same union of ray classes.

As a corollary to Theorem 1.3, we obtain the following.

Corollary 1.4. *Suppose that $n > 1$ is a square-free integer, K is a global field containing a primitive nth root of unity, and assume that $(\mathrm{char}(K), n) = 1$ if $\mathrm{char}(K) > 0$. Then*

$$\{(x,y) \in K^\times \times K^\times : x \textit{ is not a norm of } K(\sqrt[n]{y})\}$$

is diophantine over K.

As an additional corollary to Theorem 1.3, we prove the following.

Corollary 1.5. *Suppose that $n > 1$ is a square-free integer. Let K be a global field such that $(\mathrm{char}(K), n) = 1$ if $\mathrm{char}(K) > 0$. Then $K^\times \setminus K^{\times n}$ is diophantine over K.*

Thus we recover the result of [CTVG15] in the case in which K is a number field, and we extend it to the case in which K is a global function field with $(\mathrm{char}(K), n) = 1$. We replace the use of the Brauer–Manin obstruction with class field theory to prove Corollary 1.5.

Finally, we reinterpret Corollary 1.4 in order to remove the assumption that K contains a primitive root of unity in our results on nonnorms. Suppose that K is a global field, that $n > 1$ is a square-free number, and that $(\mathrm{char}(K), n) = 1$ if $\mathrm{char}(K) > 0$. Let $d := \binom{2n-1}{n}$ be the dimension of the space of homogeneous polynomials of degree n in n variables over K. For a cyclic extension L/K of degree n, the norm form is such a polynomial. Given a vector $\vec{a} = (a_1, \ldots, a_d) \in K^d$, denote by $f_{\vec{a}}$ the homogeneous polynomial of degree n in the n variables $t_1, \ldots, t_n$ whose ith coefficient, using the lexicographical ordering, is a_i. In Section 7, we prove the following.

Theorem 1.6. *Suppose that $n > 1$ is square-free and that K is a global field such that if $\mathrm{char}(K) > 0$, then $(\mathrm{char}(K), n) = 1$. The set*

$$D(n,K) := \{(x,\vec{a}) \in K^\times \times K^d \colon f_{\vec{a}} \text{ is the norm form of a degree } n \text{ cyclic extension of } K \text{ and } f_{\vec{a}}(t_1,\dots,t_n) = x \text{ has no solutions in } K^n\}$$

is diophantine over K.

2. Class field theory, the Hilbert symbol, and cyclic algebras

For a number field K, a *finite prime* $\mathfrak{p}$ of K is a maximal ideal in $\mathcal{O}_K$, the ring of integers of K, and an *infinite prime* of K is an equivalence class of Archimedean absolute values. If K is a global function field, a finite prime $\mathfrak{p}$ is the maximal ideal of a local ring in K. If $\mathfrak{p}$ is a finite prime of a global field K, let $v_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}$ be the associated normalized valuation. For a global field K and a finite prime $\mathfrak{p}$, a local ring associated with $\mathfrak{p}$ is denoted by $\mathcal{O}_\mathfrak{p} := \{x \in K : v_\mathfrak{p}(x) \geq 0\}$. A *semilocal ring* in K is a finite intersection of local rings of K. Local rings of global fields are diophantine by the following lemma, first proved in [Shl94].

Lemma 2.1. *Let K be a global field, and let $\mathcal{O}_\mathfrak{p} \subseteq K$ be a local ring in K. Then $\mathcal{O}_\mathfrak{p}$ is diophantine over K.*

Proof. See [Shl94, Lemma 3.22]. □

If K is a global function field and S is a finite, nonempty set of primes of K, the *ring of S-integers* is

$$\mathcal{O}_S := \bigcap_{\mathfrak{p} \notin S} \mathcal{O}_\mathfrak{p}.$$

Then $\mathcal{O}_S$ is a Dedekind domain, and the primes of K not contained in S are in one-to-one correspondence with the maximal ideals in $\mathcal{O}_S$ by the map $\mathfrak{p} \mapsto \mathfrak{p} \cap \mathcal{O}_S$. Set $A := \mathcal{O}_S$; then there is a positive-characteristic analogue of the Hilbert class field of K, denoted K^A. The extension K^A is defined to be the maximal unramified abelian extension of K in which every prime of S splits completely. The extension K^A/K has finite degree over K and satisfies $\mathrm{Cl}(A) \simeq \mathrm{Gal}(K^A/K)$; see [Ros87]. For additional background on arithmetic in global function fields, see [Ros02].

2.1. The Artin map.

A *modulus* $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$ of K is a formal product of finitely many nonnegative powers of primes (both finite and infinite) of K. Given a modulus $\mathfrak{m}$ of K, let $\mathfrak{m}_0$ denote the finite part of $\mathfrak{m}$, and let $I(\mathfrak{m})$ denote the free abelian group generated by the finite primes of K such that $\mathfrak{m}(\mathfrak{p}) = 0$, i.e., those which do not divide $\mathfrak{m}$. The *support* of an element $\prod \mathfrak{p}^{e_\mathfrak{p}} \in I(\mathfrak{m})$ are the primes $\mathfrak{p}$ such that $e_\mathfrak{p} \neq 0$. Two elements of $I(\mathfrak{m})$ are *coprime* if their supports are disjoint. Define

$$K_\mathfrak{m} := \{x \in K : v_\mathfrak{p}(x) = 0 \text{ for all } \mathfrak{p} | \mathfrak{m}_0\}.$$

If $\mathfrak{p}|\mathfrak{m}$ is a real infinite prime, then it is associated with an embedding $K \to \mathbb{R}$. An element of $K^\times$ is *positive at* $\mathfrak{p}$ if its image under the embedding associated with $\mathfrak{p}$ is positive. We define

$$K_{\mathfrak{m},1} := \{x \in K^\times : v_\mathfrak{p}(x-1) \geq \mathfrak{m}(\mathfrak{p})\, \forall \mathfrak{p} | \mathfrak{m}_0 \text{ and positive at each real } \mathfrak{p}|\mathfrak{m}\}.$$

We have an embedding

$$K_{\mathfrak{m}} \to I(\mathfrak{m}),$$
$$x \mapsto (x) := \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}.$$

Denote the image of $K_{\mathfrak{m},1}$ in $I(\mathfrak{m})$ by $P(\mathfrak{m})$, and set $C(\mathfrak{m}) := I(\mathfrak{m})/P(\mathfrak{m})$.

Now suppose L/K is an abelian extension and that $\mathfrak{m}$ is a modulus of K containing the primes of K ramified in L. Given $\mathfrak{p}$ coprime to $\mathfrak{m}$, we denote the Frobenius of $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$ by $(\mathfrak{p}, L/K)$, and we define the Artin map for L/K:

$$\psi_{L/K} : I(\mathfrak{m}) \to \mathrm{Gal}(L/K),$$
$$\prod \mathfrak{p}_i^{e_i} \mapsto \prod (\mathfrak{p}, L/K)^{e_i}.$$

Let $I_K := I(1)$ denote the fractional ideals of K. Suppose that L/K is a finite extension. Given a prime $\mathfrak{P}$ of L, set $\mathfrak{p} := \mathfrak{P} \cap K$ and $f(\mathfrak{P}|\mathfrak{p}) := [\mathcal{O}_{\mathfrak{P}}/\mathfrak{P} : \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}]$. Then we have the relative ideal norm map

$$N_{L/K}(\mathfrak{P}) := \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})},$$

which we extend to I_L. Artin reciprocity lets us characterize the kernel of the Artin map.

Theorem 2.2 (Artin reciprocity)**.** *Suppose that L/K is a finite abelian extension. Then there is a modulus $\mathfrak{m}$ of K such that, if $\mathfrak{m}'$ is the modulus of L containing the primes of L above those dividing $\mathfrak{m}$,*

$$\psi_{L/K} : I(\mathfrak{m})/(P(\mathfrak{m}) \cdot N_{L/K}(I(\mathfrak{m}'))) \simeq \mathrm{Gal}(L/K)$$

is an isomorphism.

Such a modulus $\mathfrak{m}$ is called an *admissible modulus of K for L*.

2.2. **Ray class groups of rings of S-integers.** Suppose that K is a global function field and that S is a finite set of primes of K. Set $A := \mathcal{O}_S$. Suppose that $\mathfrak{m}$ is a modulus of K divisible by primes which are not in S. Then $M := \prod_{\mathfrak{p}|\mathfrak{m}} (\mathfrak{p} \cap A)^{v_{\mathfrak{p}}(\mathfrak{m})}$ is an ideal of A. Let $I_{\mathfrak{m}}(A)$ be the abelian group generated by primes of A which are coprime to M, let $P_{\mathfrak{m}}(A)$ be the image of $K_{\mathfrak{m},1}$ in $P_{\mathfrak{m}}(A)$, and let $\mathrm{Cl}_{\mathfrak{m}}(A) := I_{\mathfrak{m}}(A)/P_{\mathfrak{m}}(A)$. We have the following "folk theorems"; for proofs, see [Eis18, Corollary 2.8 and Theorem 2.9].

Theorem 2.3. *There is a finite abelian extension $K_{\mathfrak{m}}^A/K$ such that $\mathrm{Cl}_{\mathfrak{m}}(A) \simeq \mathrm{Gal}(K_{\mathfrak{m}}^A/K)$, where the isomorphism is the Artin map. Additionally, every class in $\mathrm{Cl}_{\mathfrak{m}}(A)$ contains infinitely many primes of A.*

We will need Theorem 2.3 in Section 4.

2.3. **The power residue symbol.** Now assume that K is a global field, that ℓ is a prime number coprime to the characteristic of K, and that K contains μ_ℓ, the ℓth roots of unity. Let $\omega \in \mu_\ell$ be a primitive root of unity. Let $a \in K^\times$. If $\mathfrak{p}$ is a finite prime of K such that $v_{\mathfrak{p}}(a) = 0$, and if $\alpha \in K(\sqrt[\ell]{a})$ is any root of $x^\ell - a$, then $(\mathfrak{p}, K(\sqrt[\ell]{a})/K)(\alpha)/\alpha$ is an ℓth root of unity and thus equals ω^s for some $0 \le s \le \ell - 1$. The value of s is independent of the choice of α. Define

$$\left(\frac{a}{\mathfrak{p}}\right)_\ell := \frac{(\mathfrak{p}, K(\sqrt[\ell]{a})/K)(\alpha)}{\alpha}$$

to be the *ℓth power residue symbol* for the prime $\mathfrak{p}$. Equivalently, $\omega^s = \left(\frac{a}{\mathfrak{p}}\right)_\ell$ is the unique ℓth root of unity satisfying

$$\alpha^{(|\mathbb{F}_\mathfrak{p}|-1)/\ell} \equiv \omega^s \pmod{\mathfrak{p}}.$$

This lets us compute the Frobenius of a prime $\mathfrak{p}$ coprime to $\mathfrak{m}$. The power residue symbol is multiplicative on $\mathcal{O}_\mathfrak{p}^\times$, and if $\left(\frac{a}{\mathfrak{p}}\right)_\ell = 1$, by Hensel's lemma, there exists a $b \in \mathcal{O}_\mathfrak{p}^\times$ such that $a \equiv b^\ell \pmod{\mathfrak{p}}$.

We will use a fixed compositum of two cyclic degree ℓ extensions of K in our diophantine definitions. Suppose that ℓ is a prime number and that $(\mathrm{char}(K), \ell) = 1$. Assume that a, b generate distinct, nontrivial subgroups in $K^\times/K^{\times\ell}$, and suppose that $\mathfrak{m}$ is a modulus of K containing the primes of K ramified in $L := K(\sqrt[\ell]{a}, \sqrt[\ell]{b})$. Then we have an isomorphism

$$\begin{aligned} \iota : \mathrm{Gal}(L/K) &\to \mu_\ell \times \mu_\ell, \\ \sigma &\mapsto \left(\frac{\sigma(\sqrt[\ell]{a})}{\sqrt[\ell]{a}}, \frac{\sigma(\sqrt[\ell]{b})}{\sqrt[\ell]{b}} \right). \end{aligned}$$

Thus for L/K, under the above identification, the Artin map is given by

$$\iota((\mathfrak{p}, L/K)) = \left(\left(\frac{a}{\mathfrak{p}}\right)_\ell, \left(\frac{b}{\mathfrak{p}}\right)_\ell \right).$$

2.4. **The Hilbert symbol.** Given a finite prime $\mathfrak{p}$ of K, we denote by $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$. Suppose that $(\mathrm{char}(K), n) = 1$. By Kummer theory and local class field theory, we have a nondegenerate pairing, called the Hilbert symbol,

$$(\cdot,\cdot)_{K_\mathfrak{p},n} : K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times n} \times K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times n} \to \mu_n$$

defined by

$$(\cdot,\cdot)_{K_\mathfrak{p},n} := \frac{(a, K_\mathfrak{p}(\sqrt[n]{b})/K_\mathfrak{p})(\sqrt[n]{b})}{\sqrt[n]{b}}.$$

This pairing satisfies $(a,b)_{K_\mathfrak{p},n} = 1$ if and only if a is a norm in $K(\sqrt[n]{b})$. We also have the following identity.

Theorem 2.4 (Hilbert reciprocity)**.** *For $a, b \in K$,*

$$\prod_\mathfrak{p} (a,b)_{K_\mathfrak{p},n} = 1.$$

Let $a, b \in K_\mathfrak{p}$. Let $R_\mathfrak{p} \subseteq K_\mathfrak{p}$ be the ring of integers of $K_\mathfrak{p}$, and let $\mathbb{F}_\mathfrak{p} := R_\mathfrak{p}/\mathfrak{p}$ be the residue field of $\mathfrak{p}$. Let $\mathrm{red}_\mathfrak{p} : R_\mathfrak{p} \to \mathbb{F}_\mathfrak{p}$ be the reduction map. We have the following formula for computing the Hilbert symbol when $(\mathrm{char}(\mathbb{F}_\mathfrak{p}), n) = 1$:

$$(a,b)_{K_\mathfrak{p},n} = \left((-1)^{v_\mathfrak{p}(a)v_\mathfrak{p}(b)} \,\mathrm{red}_\mathfrak{p}\left(\frac{a^{v_\mathfrak{p}(b)}}{b^{v_\mathfrak{p}(a)}} \right) \right)^{(|\mathbb{F}_\mathfrak{p}|-1)/n}. \tag{1}$$

Proof. This is a corollary to [Ser79, XIV.3, Proposition 8]. □

2.5. **Cyclic algebras.**

Definition 2.5. Let $n \in \mathbb{N}$, let K be a global field such that $(\mathrm{char}(K), n = 1)$, and let L/K be a finite cyclic extension of degree n. Let σ be a generator of $\mathrm{Gal}(L/K)$, and let $b \in K^\times$. The cyclic algebra associated with σ and b, denoted (σ, b), is generated by L and an element $T \in (\sigma, b)$ which satisfies

$$T^n = b, \qquad T \cdot s = \sigma(s) \cdot T$$

for all $s \in L$.

This is a degree n central simple algebra over K containing L as a commutative subalgebra, and it is split by L. If $(\mathrm{char}(K), n) = 1$ and if K contains the nth roots of unity μ_n, there is a simpler presentation of a degree n cyclic algebra.

Definition 2.6. Let $n \in \mathbb{N}$, and let K be a global field such that $(\mathrm{char}(K), n = 1)$ and that K contains a primitive nth root of unity ω. Let $a, b \in K^\times$. Define the cyclic K-algebra associated with a, b, and ω to be

$$(a, b)_\omega := \langle S, T \,|\, T^n = a, S^n = b, ST = \omega TS \rangle.$$

We are interested in these cyclic algebras because they are split if and only if their corresponding norm equations have rational solutions. We record the following theorem.

Theorem 2.7. *If K is a global field and σ generates $\mathrm{Gal}(L/K)$ for a cyclic extension L/K, the cyclic algebra (σ, b) is split if and only if b is a norm of L/K. If $(\mathrm{char}(K), n) = 1$ and K contains a primitive nth root of unity ω, then $(a, b)_\omega$ is split if and only if b is a norm of $K(\sqrt[n]{a})$.*

Proof. See [GS06, Corollaries 4.7.5 and 4.7.7]. □

We will also need the following theorem, proved in [Par13], on prescribing Hilbert symbols.

Theorem 2.8. *Let n be a natural number, and let K be a global field containing μ_n and satisfying $(\mathrm{char}(K), n) = 1$. Let Σ denote the set of primes of K, and let Λ be a finite set of indices. Let $(a_i)_{i \in \Lambda}$ be a finite sequence of elements of $K^\times$, and suppose that $(\varepsilon_{i,\mathfrak{p}})_{i \in \Lambda, \mathfrak{p} \in \Sigma}$ is a family of elements of μ_n. There exists an $x \in K^\times$ satisfying $(a_i, x)_{K_\mathfrak{p}, n} = \varepsilon_{i,\mathfrak{p}}$ for all $i \in \Lambda$ and $\mathfrak{p} \in \Sigma$ if and only if the following conditions hold:*

1. *All but finitely many of the $\varepsilon_{i,\mathfrak{p}}$ are equal to 1.*
2. *For all $i \in \Lambda$, we have $\prod_{\mathfrak{p} \in \Sigma} \varepsilon_{i,\mathfrak{p}} = 1$.*
3. *For every $\mathfrak{p} \in \Sigma$, there exists an $x_\mathfrak{p} \in K^\times$ such that $(a_i, x_\mathfrak{p})_{K_\mathfrak{p}, n} = \varepsilon_{i,\mathfrak{p}}$.*

Proof. Theorem 3.7 of [Par13] is this theorem for $n = 2$. For general n and K containing μ_n with characteristic coprime to n, the same proof carries through, using [Par13, Proposition 3.5 and Lemma 3.6]. □

3. Cyclic algebras and diophantine semilocal rings in K

Throughout this section, assume that ℓ is a prime, that K is a global field, that $\mathrm{char}(K) \neq \ell$, and that $\omega \in K$ is a primitive ℓth root of unity. We then have, for $a, b \in K^\times$ and a prime $\mathfrak{p}$ of K,

$$(a, b)_{K_\mathfrak{p}, \ell} = 1 \iff (a, b)_\omega \otimes K_\mathfrak{p} \qquad \text{being split.}$$

Let F be a splitting field for $A := (a,b)_\omega$. For example, we can take $F = K(\sqrt[\ell]{b})$. We then have $A \otimes F \simeq M_\ell(F)$. Given $a \in A$, define the reduced norm $\mathrm{Nrd}(a)$ and the reduced trace $\mathrm{Trd}(a)$ to be the norm and trace, respectively, of the image of a in $M_\ell(F)$. If $a = \sum_{i,j=0}^{\ell} a_{ij} S^i T^j$, then $\mathrm{Nrd}(a)$ and $\mathrm{Trd}(a)$ are polynomials in the coefficients a_{ij} of a. Set

$$S_A := \{\mathrm{Trd}(a) : a \in A \text{ and } \mathrm{Nrd}(a) = 1\}.$$

Definition 3.1. Let $a, b \in K^\times$, and define

$$\Delta_{a,b} := \{\mathfrak{p} : (a,b)_\omega \otimes K_\mathfrak{p} \not\simeq M_\ell(K_\mathfrak{p})\}.$$

Also, define the semilocal ring

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

The set $\Delta_{a,b}$ is the set of primes where $(a,b)_\omega$ is not split; the set $\Delta_{a,b}$ is finite. The following proposition, which is a special case of [Dit17, Proposition 2.7] but which we record here for the reader, gives a diophantine definition of $T_{a,b}$.

Proposition 3.2. *Assume that $\ell \in \mathbb{N}$ is a prime, that K is a global field with $\mathrm{char}(K) \neq \ell$, and that $\omega \in K$ is a primitive ℓth root of unity. There exists a $B \in \mathbb{N}$ such that if $R \subseteq K$ is a finite set of representatives of*

$$\bigcup_{\mathfrak{p} : |\mathbb{F}_\mathfrak{p}| < B} \mathcal{O}_\mathfrak{p}/\mathfrak{p}\mathcal{O}_\mathfrak{p},$$

then

$$T_{a,b} = S_{(a,b)_\omega} + S_{(a,b)_\omega} + R.$$

Thus $T_{a,b}$ is diophantine over K.

Proof. This follows immediately from [Dit17, Proposition 2.7]. □

3.1. **Diophantine semilocal rings and their Jacobson radicals.** Again, fix a prime number ℓ, a global field K such that $\mathrm{char}(K) \neq \ell$, and a primitive ℓth root of unity $\omega \in K$. In this section, we will show that certain semilocal rings are diophantine. We will also show that their Jacobson radicals contain an ideal which is diophantine.

Lemma 3.3. *Let $a, b \in K^\times$. Then*

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

Proof. Suppose that $x \in K^{\times\ell} \cdot T_{a,b}^\times$. Then we can write $x = t^\ell \cdot u$ with $u \in T_{a,b}^\times$. Thus for any $\mathfrak{p} \in \Delta_{a,b}$,

$$v_\mathfrak{p}(x) = \ell \cdot v_\mathfrak{p}(t) + v_\mathfrak{p}(u) = \ell \cdot v_\mathfrak{p}(t).$$

Now suppose that $x \in \bigcap_{\mathfrak{p} \in \Delta_{a,b}} v_\mathfrak{p}^{-1}(\ell\mathbb{Z})$. Then for all $\mathfrak{p} \in \Delta_{a,b}$, there exists a $k_\mathfrak{p} \in \mathbb{Z}$ such that $v_\mathfrak{p}(x) = \ell \cdot k_\mathfrak{p}$. By weak approximation, there exists a $t \in K^\times$ such that $v_\mathfrak{p}(t) = k_\mathfrak{p}$ for each $\mathfrak{p} \in \Delta_{a,b}$. Then $v_\mathfrak{p}(x/t^\ell) = 0$ for each $\mathfrak{p} \in \Delta_{a,b}$, so $u := x/t^\ell \in T_{a,b}^\times$. Thus $x \in K^{\times\ell} T_{a,b}^\times$. □

Now suppose that $a, b, c \in K^\times$, and define

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

and for $p \in K^\times$, define

$$\mathbb{P}(p) := \{\mathfrak{p} : v_\mathfrak{p}(p) \not\equiv 0 \pmod{\ell}\}.$$

Lemma 3.4. *Suppose that $a, b, c \in K^\times$. Then*

$$I_{a,b}^c = \{x \in K : v_\mathfrak{p}(x) \text{ is positive and } v_\mathfrak{p}(x) \equiv v_\mathfrak{p}(c) \pmod{\ell} \text{ for } \mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(c), \\ \text{and } v_\mathfrak{p}(x), v_\mathfrak{p}(1-x) \equiv 0 \pmod{\ell} \text{ for } \mathfrak{p} \in \Delta_{a,b} \setminus \mathbb{P}(c)\}.$$

Proof. First, we will show that $I_{a,b}^c$ is contained on the right-hand side. Let $x \in I_{a,b}^c$. For all $\mathfrak{p} \in \Delta_{a,b}$, both $v_\mathfrak{p}(x/c)$ and $v_\mathfrak{p}(1-x)$ are divisible by ℓ by the previous lemma. For any $\mathfrak{p} \in \mathbb{P}(c)$, this implies that $v_\mathfrak{p}(x) \equiv v_\mathfrak{p}(c) \not\equiv 0 \pmod{\ell}$. In particular, $v_\mathfrak{p}(x) \neq 0$, so $v_\mathfrak{p}(1-x) = \min\{0, v_\mathfrak{p}(x)\}$. Because $v_\mathfrak{p}(1-x) \equiv 0 \pmod{\ell}$, it follows that $v_\mathfrak{p}(x) > 0$. If $\mathfrak{p} \notin \mathbb{P}(c)$, then $v_\mathfrak{p}(x) \equiv v_\mathfrak{p}(c) \equiv 0 \pmod{\ell}$.

Conversely, suppose that x is on the right-hand side. First, assume that $\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(c)$. Then $v_\mathfrak{p}(x) \equiv v_\mathfrak{p}(c) \pmod{\ell}$. We also have $v_\mathfrak{p}(1-x) = 0$ since $v_\mathfrak{p}(x) > 0$. For any prime $\mathfrak{p} \in \Delta_{a,b} \setminus \mathbb{P}(c)$, we have $v_\mathfrak{p}(x/c) \equiv 0 \pmod{\ell}$. It follows that $x \in c \cdot K^{\times \ell} \cdot T_{a,b}^\times$ by Lemma 3.3. We also have that $v_\mathfrak{p}(1-x) \equiv 0 \pmod{\ell}$ for all $\mathfrak{p} \in \Delta_{a,b} \setminus \mathbb{P}(c)$, so $1 - x \in K^{\times \ell} \cdot T_{a,b}^\times$, again by Lemma 3.3. □

Definition 3.5. For $a, b \in K^\times$, define

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

where $1 \leq k_\mathfrak{p} \leq \ell - 1$ is defined by

$$k_\mathfrak{p} = \max\left\{ v_\mathfrak{p}(a) - \ell \left\lfloor \frac{v_\mathfrak{p}(a)}{\ell} \right\rfloor, v_\mathfrak{p}(b) - \ell \left\lfloor \frac{v_\mathfrak{p}(b)}{\ell} \right\rfloor \right\}.$$

Lemma 3.6. *Let $a, b, c \in K^\times$. For $\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(c)$, set $r_\mathfrak{p} := v_\mathfrak{p}(c) - \ell \lfloor \frac{v_\mathfrak{p}(c)}{\ell} \rfloor$. Then*

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

In particular,

$$J_{a,b} = (I_{a,b}^a + I_{a,b}^a) \cap (I_{a,b}^b + I_{a,b}^b)$$

and is diophantine over K.

Proof. If $x, y \in I_{a,b}^c$, then, for any $\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(c)$,

$$v_\mathfrak{p}(x) \equiv v_\mathfrak{p}(y) \equiv r_\mathfrak{p} \pmod{\ell}$$

by Lemma 3.4. Also, $v_\mathfrak{p}(x) \geq r_\mathfrak{p}$ and $v_\mathfrak{p}(y) \geq r_\mathfrak{p}$ because $v_\mathfrak{p}(x), v_\mathfrak{p}(y) > 0$. Thus $x + y \in \bigcap_{\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(c)} \mathfrak{p}^{r_\mathfrak{p}} \mathcal{O}_\mathfrak{p}$.

Conversely, suppose that $z \in \bigcap_{\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(c)} \mathfrak{p}^{r_\mathfrak{p}} \mathcal{O}_\mathfrak{p}$, so $v_\mathfrak{p}(z) \geq r_\mathfrak{p}$ for each $\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(c)$. We will use weak approximation to show that there exists a $y \in K^\times$ such that $y, z - y \in I_{a,b}^c$. For the primes $\mathfrak{p} \in \Delta_{a,b}$, we require the following:

(1) If $\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(c)$ such that $v_\mathfrak{p}(z) > r_\mathfrak{p}$, then $v_\mathfrak{p}(y) = r_\mathfrak{p}$.
(2) If $\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(c)$ and $v_\mathfrak{p}(z) = r_\mathfrak{p}$, let $p \in \mathfrak{p}\mathcal{O}_\mathfrak{p} \setminus \mathfrak{p}^2 \mathcal{O}_\mathfrak{p}$, and write $z = p^{r_\mathfrak{p}} u$ with $u \in \mathcal{O}_\mathfrak{p}^\times$.
   (a) If $u \not\equiv 1 \pmod{\mathfrak{p}}$, we require that $y \equiv p^{r_\mathfrak{p}}(u-1) \pmod{\mathfrak{p}^{r_\mathfrak{p}+1}}$.

(b) If $u \equiv 1 \pmod{\mathfrak{p}}$, then $z = p^{r_\mathfrak{p}}(1+k)$ for some $k \in \mathfrak{p}\mathcal{O}_\mathfrak{p}$. Choose m such that $m\ell > v_\mathfrak{p}(k)$. We take $y \equiv p^{r_\mathfrak{p}}(1+k+p^{m\ell}) \pmod{\mathfrak{p}^{r_\mathfrak{p}+m\ell+1}}$.

(3) For $\mathfrak{p} \in \Delta_{a,b} \setminus \mathbb{P}(c)$, we require $v_\mathfrak{p}(y) < \min\{0, v_\mathfrak{p}(z)\}$ and $v_\mathfrak{p}(y) \equiv 0 \pmod{\ell}$ for $\mathfrak{p} \in \Delta_{a,b} \setminus \mathbb{P}(c)$.

We claim that $y, z-y \in I_{a,b}^c$. For $\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(c)$, by construction we have that $v_\mathfrak{p}(y)$ is positive and congruent to $r_\mathfrak{p}$ modulo ℓ. For $\mathfrak{p} \in \Delta_{a,b} \setminus \mathbb{P}(c)$, (3) ensures that $v_\mathfrak{p}(y) = v_\mathfrak{p}(1-y) \equiv 0 \pmod{\ell}$. Thus $y \in I_{a,b}^c$. We will now show that $z-y \in I_{a,b}^c$. First, we claim that, for $\mathfrak{p} \in \Delta_{a,b} \cap \mathbb{P}(c)$, $v_\mathfrak{p}(z-y) > 0$ and $v_\mathfrak{p}(z-y) \equiv v_\mathfrak{p}(c) \pmod{\ell}$. We have that $v_\mathfrak{p}(z-y) \geq \min\{v_\mathfrak{p}(z), v_\mathfrak{p}(y)\} > 0$. Additionally, we have $v_\mathfrak{p}(z-y) \equiv r_\mathfrak{p} \pmod{\ell}$ by (1) and (2) above, and by definition, $v_\mathfrak{p}(c) \equiv r_\mathfrak{p} \pmod{\ell}$. For $\mathfrak{p} \in \Delta_{a,b} \setminus \mathbb{P}(c)$, because $v_\mathfrak{p}(y) \equiv 0 \pmod{\ell}$ and $v_\mathfrak{p}(y) < v_\mathfrak{p}(z)$, it follows that $v_\mathfrak{p}(z-y) = v_\mathfrak{p}(y) \equiv 0 \pmod{\ell}$. Finally, from $v_\mathfrak{p}(z-y) < 0$, it follows that

$$v_\mathfrak{p}(1-(z-y)) = v_\mathfrak{p}(z-y) = v_\mathfrak{p}(y) \equiv 0 \pmod{\ell}.$$

We conclude that $z = y + (z-y) \in I_{a,b}^c + I_{a,b}^c$ by Lemma 3.4. □

3.2. **Partitioning the primes of K.** One main step in the proof that the non-norms are diophantine is to partition the primes of a finite number of sets. We partition the primes using ray classes for a fixed abelian extension of K, which we now describe. The following proposition outlines the properties of this extension.

Proposition 3.7. *Suppose that ℓ is an odd prime number and that K is a global field containing a primitive ℓth root of unity and that* $\mathrm{char}(K) \neq \ell$. *There exist $a, b \in K^\times$ satisfying the following conditions:*

(i) *(a) and (b) are coprime.*
(ii) *a, b generate distinct, nontrivial subgroups of $K^\times/K^{\times\ell}$.*
(iii) *If K is a number field, $a, b \in 1 + \ell^3\mathcal{O}_K$.*
(iv) *For every subfield M of $L := K(\sqrt[\ell]{a}, \sqrt[\ell]{b})/K$ containing K, there is a finite prime of K ramified in M.*

Proof. First, assume that K is a number field. Fix a prime $\mathfrak{p}_0$ of K which does not divide $\ell\mathcal{O}_K$. There exists $a \in K^\times$ such that $a \in 1 + \ell^3\mathcal{O}_K$ and $v_{\mathfrak{p}_0}(a) = 1$. To choose b, fix a different prime $\mathfrak{p}_1 \neq \mathfrak{p}_0$ not dividing $\ell\mathcal{O}_K$. There exists a $b \in K^\times$ such that

- $b \in 1 + \ell^3\mathcal{O}_K$,
- $v_\mathfrak{p}(b) = 0$ for any $\mathfrak{p}|(a)$,
- and $v_{\mathfrak{p}_1}(b) = 1$.

If K is a global function field, similarly, choose two primes $\mathfrak{p}_0, \mathfrak{p}_1 \neq \mathfrak{q}$ and $a, b \in K^\times$ such that $v_{\mathfrak{p}_0}(a) = 1$, that $v_{\mathfrak{p}_1}(a) = 0$, that $v_{\mathfrak{p}'}(b) = 0$ if $\mathfrak{p}'|(a)$, and that $v_{\mathfrak{p}_1}(b) = 1$.

Thus (i) is satisfied because b is chosen so that (b) is coprime to (a). We also have (ii) holding because $v_{\mathfrak{p}_0}(a) \not\equiv 0 \pmod{\ell}$ and $v_{\mathfrak{p}_1}(b) \not\equiv 0 \pmod{\ell}$, so both a and b generate nontrivial subgroups of $K^\times/K^{\times\ell}$. These subgroups are distinct because $v_{\mathfrak{p}_0}(a^m/b^n) \not\equiv 0 \pmod{\ell}$ for $1 \leq m, n \leq \ell - 1$. By construction, (iii) holds as well if K is a number field.

We now show that (iv) holds. Indeed, every intermediate extension is of the form $K(\sqrt[n]{a}), K(\sqrt[\ell]{b})$, or $K(\sqrt[\ell]{ab^j})$ for some $j = 1, 2, \ldots, \ell - 1$, and each ramifies at either $\mathfrak{p}_0$ or $\mathfrak{p}_1$. □

Proposition 3.8. *Set $L := K(\sqrt[\ell]{a}, \sqrt[\ell]{b})$, where a, b are chosen so that they satisfy conditions* (i)–(iv) *of Proposition* 3.7. *Set $A := \mathcal{O}_K$ if K is a number field, and if*

K is a global function field, suppose that $\mathfrak{q}$ is a prime of K which is unramified in L, and set $A := \mathcal{O}_{\{\mathfrak{q}\}}$. Given $\sigma \in \mathrm{Gal}(L/K)$ and an ideal class $\mathcal{C} \in \mathrm{Cl}(A)$, there exists a prime $\mathfrak{p}$ of K unramified in L such that $(\mathfrak{p}, L/K) = \sigma$ and $\mathfrak{p} \cap A \in \mathcal{C}$.

Proof. We first prove the proposition if K is a number field. Let H denote the Hilbert class field of K. We claim that H and L are linearly disjoint, i.e., $H \cap L = K$. This is true because all intermediate fields between K and L are ramified at some prime of K. Thus

$$\mathrm{Gal}(HL/K) \simeq \mathrm{Gal}(L/K) \times \mathrm{Cl}(K),$$

so the proposition follows by the Chebotarev density theorem.

If K is a global function field and $\mathfrak{q}$ is a prime of K which is unramified in L, the same argument works by replacing H with K^A, the maximal unramified abelian extension of K in which $\mathfrak{q}$ splits completely. □

We now fix $a, b \in K^\times$ as in Proposition 3.7 and fix an admissible modulus $\mathfrak{m}$ of K for L whose support contains all primes in the support of (ℓab). We need to fix two extra constants $c, d \in K$.

Lemma 3.9. *Let $\omega \in K$ be a primitive ℓth root of unity. There exist $c, d \in K^\times$ such that $(a, c)_{K_\mathfrak{p}, \ell} = \omega$ for each prime $\mathfrak{p} \in \mathbb{P}(a)$, $(b, d)_{K_\mathfrak{q}, \ell} = \omega$ for each prime $\mathfrak{q} \in \mathbb{P}(b)$, and*

$$(\mathbb{P}(a) \cup \mathbb{P}(b)) \cap \mathbb{P}(c) = (\mathbb{P}(a) \cup \mathbb{P}(b)) \cap \mathbb{P}(d) = \emptyset.$$

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the primes of $\mathbb{P}(a)$. If $r \not\equiv 0 \pmod{\ell}$, then choose primes $\mathfrak{p}_{r+1}, \ldots, \mathfrak{p}_s$ such that for $r+1 \le t \le s$, $\mathfrak{p}_t$ is coprime to (a) and (b), $\left(\frac{a}{\mathfrak{p}_t}\right)_\ell = \omega$, and $s \equiv 0 \pmod{\ell}$. Set $P := \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ in this case, and set $P := \mathbb{P}(a)$ otherwise. For each prime $\mathfrak{p} \in \mathbb{P}(a) \cup \mathbb{P}(b)$, let $x_\mathfrak{p} \in K^\times$ satisfy $v_\mathfrak{q}(x_\mathfrak{p}) = 0$ for each $\mathfrak{q} \in \mathbb{P}(a) \cup \mathbb{P}(b)$, and let $\left(\frac{x_\mathfrak{p}}{\mathfrak{p}}\right)_\ell = \omega$. Then we will use Theorem 2.8 to show that there exists a $c \in K^\times$ such that

- $(a, c)_{K_\mathfrak{p}, \ell} = \omega$ for each $\mathfrak{p} \in P$;
- $(a, c)_{K_\mathfrak{p}, \ell} = 1$ for all other primes $\mathfrak{p}$ of K; and
- for each $\mathfrak{p} \in \mathbb{P}(a)$, $(x_\mathfrak{p}, c)_{K_\mathfrak{q}, \ell} = 1$ for all primes $\mathfrak{q}$ of K.

It is clear that conditions (1) and (2) of Theorem 2.8 are satisfied, and now we show the existence of local elements. Let $\mathfrak{p} \in \mathbb{P}(a)$, and let $k_\mathfrak{p}$ be the multiplicative inverse of $v_\mathfrak{p}(a)$ modulo ℓ. Then we can choose $c_\mathfrak{p} \in K^\times$ such that $v_\mathfrak{q}(c_\mathfrak{p}) = 0$ for each $\mathfrak{q} \in \mathbb{P}(a)$, and such that $\left(\frac{c_\mathfrak{p}}{\mathfrak{p}}\right)_\ell = \omega^{k_\mathfrak{p}}$. Then

$$(a, c_\mathfrak{p})_{K_\mathfrak{p}, \ell} = (\omega^{k_\mathfrak{p}})^{v_\mathfrak{p}(a)} = \omega$$

by equation 1. For each $\mathfrak{q} \in \mathbb{P}(a)$, because $x_\mathfrak{q}$ and $c_\mathfrak{p}$ are $\mathfrak{q}$-adic units, we have $(x_\mathfrak{q}, c_\mathfrak{p})_{K_\mathfrak{q}, \ell} = 1$. If $\mathfrak{p} \in P \setminus \mathbb{P}(a)$, we can choose any $c_\mathfrak{p} \in K^\times$ such that $v_\mathfrak{p}(c_\mathfrak{p}) = 1$ and $v_\mathfrak{q}(c_\mathfrak{p}) = 0$ for any $\mathfrak{q} \in \mathbb{P}(a)$. Then

$$(a, c_\mathfrak{p})_{K_\mathfrak{p}, \ell} = \left(\frac{a}{\mathfrak{p}}\right)_\ell = \omega,$$

again by equation 1, and

$$(x_\mathfrak{q}, c_\mathfrak{p})_{K_\mathfrak{p}, \ell} = 1$$

because $x_\mathfrak{q}, c_\mathfrak{p}$ are $\mathfrak{q}$-adic units for each $\mathfrak{q} \in \mathbb{P}(a)$. For any prime $\mathfrak{p} \notin P$, let $c_\mathfrak{p}$ be a $\mathfrak{p}$-adic ℓth power; then $(a, c_\mathfrak{p})_{K_\mathfrak{p}, n} = 1 = (x_\mathfrak{q}, c_\mathfrak{p})_{K_\mathfrak{q}, \ell}$ for each $\mathfrak{q} \in \mathbb{P}(a)$. Finally, let

$\mathfrak{p}$ be a prime not in P. Then we choose a $c_\mathfrak{p} \in K$ which is a $\mathfrak{p}$-adic ℓth power, so $(a, c_\mathfrak{p})_{K_\mathfrak{p},\ell} = 1 = (x_\mathfrak{q}, c_\mathfrak{p})_{K_\mathfrak{q},\ell}$ for each $\mathfrak{q} \in \mathbb{P}(a)$.

Finally, we observe that the third item implies that, for each $\mathfrak{p} \in \mathbb{P}(a) \cup \mathbb{P}(b)$, $\mathfrak{p} \notin \mathbb{P}(c)$ by equation 1. The proof for the existence of d is similar. □

We now fix a primitive ℓth root of unity $\omega \in K$ and constants $c, d \in K$ with the properties guaranteed by Lemma 3.9. Enlarge the modulus $\mathfrak{m}$ of K for L by any primes $\mathfrak{p}$ dividing (c) or (d) and any primes $\mathfrak{p}$ such that $(a, c)_{K_\mathfrak{p},\ell} \neq 1$ or $(b, d)_{K_\mathfrak{p},\ell} \neq 1$.

We will connect the splitting behavior of primes of K in L with ramification of cyclic algebras over K. We identify $\mathrm{Gal}(L/K) \simeq \mu_\ell \times \mu_\ell$; let ω be a generator of μ_ℓ. First, we partition $\mathrm{Gal}(L/K)$ depending on whether the restriction of $\sigma \in \mathrm{Gal}(L/K)$ to $K(\sqrt[\ell]{a})$ or $K(\sqrt[\ell]{b})$ is trivial or not.

Definition 3.10.

- $C_{(1,1)} := \{(1, 1)\}$.
- $C_{(-1,-1)} := \{(\omega^i, \omega^j) : i, j \neq 0\}$.
- $C_{(1,-1)} := \{(1, \omega^j) : j \neq 0\}$.
- $C_{(-1,1)} := \{(\omega^i, 1) : i \neq 0\}$.

Now we partition the primes of K depending on whether or not they split completely in $K(\sqrt[\ell]{a})$ or $K(\sqrt[\ell]{b})$. For a prime $\mathfrak{p}$ of K and $p \in K^\times$ and for $i, j = \pm 1$, set

$$\mathbb{P}^{i,j} := \{\mathfrak{p} : \psi_{L/K}(\mathfrak{p}) \in C_{i,j}\}$$

and

$$\mathbb{P}^{i,j}(p) := \mathbb{P}(p) \cap \mathbb{P}^{i,j}.$$

Proposition 3.11. *Suppose that $a, b, c, d \in K^\times$ and that a modulus $\mathfrak{m}$ are as above. Given $p \in I(\mathfrak{m})$, we have*

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

$$\mathbb{P}^{(-1,1)}(p) = \left(\bigcap_{k=0}^{\ell-1} \Delta_{ab^k,p}\right) \cap \left(\bigcap_{k=1}^{\ell-1} \Delta_{a,c^k p}\right),$$

$$\mathbb{P}^{(1,-1)}(p) = \left(\bigcap_{k=1}^{\ell-1} \Delta_{a^k b,p}\right) \cap \left(\bigcap_{k=1}^{\ell-1} \Delta_{b,d^k p}\right).$$

Proof. We will begin with the first equality. First, no primes $\mathfrak{p}|\mathfrak{m}$ occur in $\Delta_{a,p} \cap \Delta_{b,p}$ since if $(a, p)_{K_\mathfrak{p},\ell} \neq 1$, we must have $\mathfrak{p} \nmid \ell$ and $v_\mathfrak{p}(a) \not\equiv 0 \pmod{\ell}$. But then, because $(a), (b)$ are coprime, we have $(b, p)_{K_\mathfrak{p},\ell} = 1$. Now suppose $\mathfrak{p} \nmid \mathfrak{m}$; then we have $v_\mathfrak{p}(a) = v_\mathfrak{p}(b) = 0$. From equation 1, $(a, p)_{K_\mathfrak{p},\ell} = \left(\frac{a^{v_\mathfrak{p}(p)}}{\mathfrak{p}}\right)_\ell \neq 1$ if and only if $\mathfrak{p} \in \mathbb{P}(p)$ and $\left(\frac{a}{\mathfrak{p}}\right)_\ell \neq 1$. Similarly, $(b, p)_{K_\mathfrak{p},\ell} = \left(\frac{b}{\mathfrak{p}}\right)_\ell^{v_\mathfrak{p}(p)}$ is not 1 if and only if $\mathfrak{p} \in \mathbb{P}(p)$ and $\left(\frac{b}{\mathfrak{p}}\right)_\ell \neq 1$. Because $\psi_{L/K}(\mathfrak{p}) = \left(\left(\frac{a}{\mathfrak{p}}\right)_\ell, \left(\frac{b}{\mathfrak{p}}\right)_\ell\right)$, for any $\mathfrak{p} \nmid \mathfrak{m}$, we have $\mathfrak{p} \in \Delta_{a,p} \cap \Delta_{b,p}$ if and only if $\mathfrak{p} \in \mathbb{P}^{(-1,-1)}(p)$.

Now we will prove the second equality, as the proof of the third equality is similar to this case. Assume first that $\mathfrak{p} \in \mathbb{P}^{(-1,1)}(p)$; we will show that $\mathfrak{p}$ is on the right-hand side of the second equality. We compute $(a, p)_{K_\mathfrak{p},\ell} \neq 1$ and $(b, p)_{K_\mathfrak{p},\ell} = 1$. Thus for every integer $0 \leq k \leq \ell - 1$, we have $(ab^k, p)_{K_\mathfrak{p},\ell} \neq 1$ and

hence $\mathfrak{p} \in \bigcap_{k=0}^{\ell-1} \Delta_{ab^k,p}$. We also note that $(a,c)_{K_\mathfrak{p},\ell} = 1$ by the construction of c in the proof of Lemma 3.9. Thus for $0 \leq k \leq \ell-1$, $\mathfrak{p} \in \Delta_{a,c^k p}$.

Now we will show the reverse inclusion. Suppose that $\mathfrak{p}|\mathfrak{m}$. We will show that $\mathfrak{p}$ is not in the set on the right-hand side in the second equality. First, if K is a number field and $\mathfrak{p}|\ell\mathcal{O}_K$, we have $(a,p)_{K_\mathfrak{p},\ell} = 1$ because a is a $\mathfrak{p}$-adic ℓth power. If $\mathfrak{p} \in \mathbb{P}(a)$, then $(a,c)_{K_\mathfrak{p},\ell} = \omega$. If, additionally, $(a,p)_{K_\mathfrak{p},\ell} \neq 1$, then there is some $1 \leq k \leq \ell-1$ such that

$$(a, c^k p)_{K_\mathfrak{p},\ell} = (a,p)_{K_\mathfrak{p},\ell}(a,c)^k_{K_\mathfrak{p},\ell} = 1,$$

and thus $\mathfrak{p} \notin \bigcap_{k=0}^{\ell-1} \Delta_{a,c^k p}$. If $\mathfrak{p}|\mathfrak{m}$ but $\mathfrak{p} \notin \mathbb{P}(a)$, then $(a,p)_{K_\mathfrak{p},\ell} = 1$ since $v_\mathfrak{p}(a) \equiv 0 \pmod{\ell}$ and $v_\mathfrak{p}(p) = 0$. Thus $\mathfrak{p} \notin \Delta_{a,p}$, so we conclude that the right-hand side in the second equality contains no primes dividing $\mathfrak{m}$. If $\mathfrak{p}$ does not divide $\mathfrak{m}$ and $\mathfrak{p} \in \bigcap_{k=0}^{\ell-1} \Delta_{ab^k,p}$, then $\mathfrak{p} \in \mathbb{P}^{(-1,1)}(p)$. Indeed, because $(a,p)_{K_\mathfrak{p},\ell} \neq 1$, we must have $\mathfrak{p} \in \mathbb{P}(p)$ and $\psi_{L/K}(\mathfrak{p}) \in C_{-1,-1} \cup C_{-1,1}$. We must have $(b,p)_{K_\mathfrak{p},\ell} = 1$, because otherwise, for some $1 \leq k \leq \ell-1$, we would have $(ab^k,p)_{K_\mathfrak{p},\ell} = 1$. Thus $\psi_{L/K}(\mathfrak{p}) \in C_{-1,1}$, so $\mathfrak{p} \in \mathbb{P}^{(-1,1)}(p)$. □

4. Controlling integrality with cyclic algebras

We maintain the notation of the previous section: K is a global field, ℓ is an odd prime, K contains μ_ℓ, we choose $a,b,c,d \in K^\times$ and the extension L/K so that they satisfy the properties guaranteed by Proposition 3.7 and Lemma 3.9, and $\mathfrak{m}$ is an admissible modulus of K for L containing the primes dividing $(\ell),(a),(b),(c)$, and (d). Below, we define the semilocal rings of K which are diophantine and whose primes will have a certain splitting behavior in L/K.

Definition 4.1. Let $p,q \in K^\times$, and define

$$\begin{aligned} R_p^{(-1,-1)} &:= T_{a,p} + T_{b,p}, \\ R_p^{(-1,1)} &:= \sum_{k=0}^{\ell-1} T_{ab^k,p} + T_{a,c^k p}, \\ R_p^{(1,-1)} &:= \sum_{k=0}^{\ell-1} T_{a^k b,p} + T_{b,d^k p}, \\ R_{p,q}^{(1,1)} &:= T_{ap,q} + T_{bp,q}. \end{aligned}$$

Proposition 4.2. *Let $p \in K^\times$ such that $(p) \in I(\mathfrak{m})$. Then*

$$\begin{aligned} R_p^{(-1,-1)} &= \bigcap_{\mathfrak{p} \in \mathbb{P}^{(-1,-1)}(p)} \mathcal{O}_\mathfrak{p}, \\ R_p^{(-1,1)} &= \bigcap_{\mathfrak{p} \in \mathbb{P}^{(-1,1)}(p)} \mathcal{O}_\mathfrak{p}, \\ R_p^{(1,-1)} &= \bigcap_{\mathfrak{p} \in \mathbb{P}^{(1,-1)}(p)} \mathcal{O}_\mathfrak{p}. \end{aligned}$$

Proof. The proof follows from Definitions 4.1 and 3.1 and Corollary 3.11. □

4.1. **Integrality at $\mathfrak{p}$ with $\psi_{L/K}(\mathfrak{p}) \neq (1,1)$.** We now define the sets which will let us parametrize a family of diophantine semilocal rings whose primes all are contained in the same union of ray classes for the modulus $\mathfrak{m}$.

Definition 4.3. For $i, j = \pm 1$, define

$$\Phi_{(i,j)} := \{p \in K^\times : (p) \in I(\mathfrak{m}), \psi_{L/K}((p)) \in C_{(i,j)}, \mathbb{P}(p) \subseteq \mathbb{P}^{(1,1)} \cup \mathbb{P}^{(i,j)}\}.$$

Definition 4.4. Let $(i,j) \in \{(-1,-1),(1,-1),(-1,1)\}$. For $\mathfrak{p} \in \mathbb{P}^{(i,j)}(p)$, define $r_\mathfrak{p} := v_\mathfrak{p}(p) - \ell\lfloor \frac{v_\mathfrak{p}(p)}{\ell} \rfloor$ and

$$J_p^{(i,j)} := \bigcap_{\mathfrak{p} \in \mathbb{P}^{(i,j)}(p)} \mathfrak{p}^{r_\mathfrak{p}} \mathcal{O}_\mathfrak{p}.$$

Remark 4.5. If $\mathfrak{p} \in \mathbb{P}^{(i,j)}(p)$, then $v_\mathfrak{p}(p) \not\equiv 0 \pmod{\ell}$, so $r_\mathfrak{p} := v_\mathfrak{p}(p) - \ell\lfloor \frac{v_\mathfrak{p}(p)}{\ell} \rfloor$ satisfies $1 \leq r_\mathfrak{p} \leq \ell - 1$. Additionally, if $(i,j) \in \{(-1,-1),(1,-1),(-1,1)\}$, then $J_p^{(i,j)}$ is contained in the Jacobson radical $J(R_p^{(i,j)})$ of $R_p^{(i,j)}$. In particular, any element of $J_p^{(i,j)}$ is integral at all primes of $\mathbb{P}^{(i,j)}(p)$.

Lemma 4.6.

(a) *For $i, j = \pm 1$, $\Phi_{(i,j)}$ is diophantine over K.*
(b) *For $(i,j) \neq (1,1)$, given $p \in \Phi_{(i,j)}$, $\mathbb{P}^{(i,j)}(p)$ is nonempty. Furthermore, $J_p^{(i,j)}$ is diophantine.*
(c) *For $(i,j) \neq (1,1)$, given $\mathfrak{p}$ with $\psi_{L/K}(\mathfrak{p}) \in C_{(i,j)}$, there exists a $p \in \Phi_{(i,j)}$ with $\mathbb{P}^{(i,j)}(p) = \{\mathfrak{p}\}$. Additionally, $v_\mathfrak{p}(p) \equiv 1 \pmod{\ell}$, so $J_p^{(i,j)} = J(R_p^{(i,j)})$, the Jacobson radical of $R_p^{(i,j)}$.*

Proof. To prove (a), we will first show that $\{p : (p) \in I(\mathfrak{m})\}$ is diophantine over K. First, the local rings $\mathcal{O}_\mathfrak{p}$ are all diophantine over K. Choose $t \in K$ with $v_\mathfrak{p}(t) = 1$; then $\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}\mathcal{O}_\mathfrak{p} = t^{\mathfrak{m}(\mathfrak{p})}\mathcal{O}_\mathfrak{p}$ is also diophantine over K. We have $K_{\mathfrak{m},1}$ being diophantine over K because

$$K_{\mathfrak{m},1} = \bigcap_{\mathfrak{p} | \mathfrak{m}_0} 1 + \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}\mathcal{O}_\mathfrak{p},$$

and $\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}\mathcal{O}_\mathfrak{p}$ is diophantine over K by [Shl94, Lemma 3.22]. Next, we claim that $\{p : (p) \in I(\mathfrak{m})\}$ is a finite union of $K^\times$-translates of $K_{\mathfrak{m},1}$. This is because $C(\mathfrak{m})$ is finite if K is a number field, and because the subgroup of degree 0 classes of $C(\mathfrak{m})$ is finite if K is a global function field. Thus $\{p : (p) \in I(\mathfrak{m})\}$ is diophantine over K because $K_{\mathfrak{m},1}$ is diophantine over K.

Now observe that $\mathbb{P}(p) \subseteq \mathbb{P}^{(1,1)} \cup \mathbb{P}^{(i,j)}$ if and only if $\mathbb{P}^{(i',j')}(p) = \emptyset$ for $(i',j') \neq (1,1),(i,j)$. This is equivalent to requiring that p is in $(R_p^{(i',j')})^\times \cap (R_p^{(i'',j'')})^\times$, where $(i',j'),(i'',j'')$ are the elements of $\{(\pm 1, \pm 1)\}$ which are not $(1,1)$ or (i,j). Thus $\{p : \mathbb{P}(p) \subseteq \mathbb{P}^{(1,1)} \cup \mathbb{P}^{(i,j)}\}$ is diophantine over K because $(R_p^{(i',j')})^\times$ is diophantine over K by Definition 4.1 and Proposition 3.2.

Now we prove (b). Let $(p) = \prod \mathfrak{p}_s^{e_s}$ be the factorization of (p). Then for each s, we have $\psi_{L/K}(\mathfrak{p}_s) \in C_{(i,j)}$ or $\psi_{L/K}(\mathfrak{p}_s) \in C_{(1,1)}$. Observe that, for some s, we must have $\psi_{L/K}(\mathfrak{p}_s) \in C_{(i,j)}$ and $e_i \not\equiv 0 \pmod{\ell}$ because otherwise $\psi_{L/K}((p)) = (1,1)$. We conclude that $\mathfrak{p}_s \in \mathbb{P}^{(i,j)}(p)$. We now use Lemma 3.6 to show that $J_p^{(i,j)} \subseteq$

$J(R_p^{(i,j)})$ is diophantine over K. If $(i,j) = (-1,-1)$, then $\mathbb{P}^{(-1,-1)}(p) = \Delta_{a,p} \cap \Delta_{b,p}$ and $J_p^{(-1,-1)} = J_{a,p} + J_{b,p}$. For $(i,j) = (-1,1)$, we have that

$$\mathbb{P}^{(-1,1)}(p) = \bigcap_{k=0}^{\ell-1} \Delta_{ab^k,p} \cap \Delta_{a,c^k p},$$

and hence

$$J_p^{(-1,1)} = \sum_{k=0}^{\ell-1} J_{ab^k,p} + J_{a,c^k p},$$

by Proposition 3.11 and Definition 3.5. We have a similar expression for $J(R_p^{(1,-1)})$. Thus $J_p^{(i,j)}$ is diophantine by Lemma 3.6 for $(i,j) \neq (1,1)$.

Finally, we prove (c). If K is a global function field, let $\mathfrak{p}_0 \nmid \mathfrak{m}$ satisfy $\psi_{L/K}(\mathfrak{p}_0) = (1,1)$, and set $A := \mathcal{O}_{\{\mathfrak{p}_0\}}$. If K is a number field, let $A = \mathcal{O}_K$. Suppose that $\psi_{L/K}(\mathfrak{p}) \in C_{(i,j)}$, and let $\mathfrak{q}$ be an ideal of K such that $\mathfrak{q} \cap A$ is in the ideal class of $(\mathfrak{p} \cap A)^{-1}$ in $\mathrm{Cl}(A)$ and such that $\psi_{L/K}(\mathfrak{q}) = (1,1)$; such an ideal exists by Proposition 3.8. Then

$$(\mathfrak{p} \cap A)(\mathfrak{q} \cap A) = pA$$

for some $p \in K^\times$. It follows that $(p) \in I(\mathfrak{m})$, $\psi_{L/K}((p)) = \psi_{L/K}(\mathfrak{p}) \in C_{(i,j)}$, and $\mathbb{P}(p) \subseteq \mathbb{P}^{(1,1)} \cup \mathbb{P}^{(i,j)}$, so we conclude that $\mathbb{P}^{(i,j)}(p) = \{\mathfrak{p}\}$. Additionally, $v_{\mathfrak{p}}(p) = 1$, so $J_p^{(i,j)} = \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$. □

4.2. **Integrality at $\mathfrak{p}$ with $\psi_{L/K}(\mathfrak{p}) = (1,1)$.**

Lemma 4.7. *Suppose that $\mathfrak{p}_0, \mathfrak{q}_0$ are distinct primes of K coprime to $\mathfrak{m}$. Set $A := \mathcal{O}_K$ if K is a number field, and $A := \mathcal{O}_{\{\mathfrak{q}_0\}}$ if K is a global function field. For any $\zeta \in \mu_\ell \subseteq K$, and $\sigma \in \mathrm{Gal}(L/K)$, there are infinitely many $q \in K^\times$ such that*

(i) *$(q) \in I(\mathfrak{m})$ and $\psi_{L/K}(\mathfrak{q}) = \sigma$;*
(ii) *qA is a prime ideal of A, so if K is a global function field, there is a prime $\mathfrak{q}$ of K such that $qA = \mathfrak{q} \cap A$;*
(iii) *$\left(\frac{q}{\mathfrak{p}_0}\right)_\ell = \zeta$.*

Proof. The proof is similar to that of [Par13, Lemma] if K is a number field, or [Eis18, Lemma 3.15] if K is a global function field. We outline the proof here.

We have an isomorphism

$$K_{\mathfrak{m}}/K_{\mathfrak{m},1} \to \left(A/\prod_{\mathfrak{p}|\mathfrak{m}} (\mathfrak{p} \cap A)^{v_{\mathfrak{p}}(\mathfrak{m})}\right)^\times$$

defined by writing $x = y/z$ for some $y, z \in A \cap K_{\mathfrak{m}}$, and then mapping

$$y/z \mapsto yz^{-1} \mod \prod_{\mathfrak{p}|\mathfrak{m}} (\mathfrak{p} \cap A)^{v_{\mathfrak{p}}(\mathfrak{m})}.$$

We then have

$$K_{\mathfrak{m}\mathfrak{p}_0}/K_{\mathfrak{m}\mathfrak{p}_0,1} \simeq A/(\mathfrak{p}_0 \cap A) \times K_{\mathfrak{m}}/K_{\mathfrak{m},1}$$

by the Chinese remainder theorem. We also note that $K_{\mathfrak{m}}/K_{\mathfrak{m},1}$ is isomorphic to the group of principal classes in $C_{\mathfrak{m}}$ via the mapping $p \mapsto (p)$. By Proposition 3.8, there is a prime $\mathfrak{q}'$ of K such that $\mathfrak{q}' \cap A$ is in the principal ideal class and $\psi_{L/K}(\mathfrak{q}') = \sigma$. Then there exists a $q' \in K^\times$ such that $q'A = \mathfrak{q}' \cap A$ and $\psi_{L/K}((q')) = \sigma$. Let

$s \in K^\times$ satisfy $\left(\frac{a}{\mathfrak{p}_0}\right)_\ell = \zeta$. By the above isomorphism, there is some $x \in K_{\mathfrak{m}}$ which maps to (q', s). Then there are infinitely many primes $\mathfrak{q}$ of K such that $\mathfrak{q} \cap A$ is in the ideal class of xA and thus are principle ideals, say, of the form qA. Any such q satisfies the three properties of the lemma. □

We will need the well-known fact that $K_{\mathfrak{p}}^\times / K_{\mathfrak{p}}^{\times \ell}$ is finite for any prime $\mathfrak{p}$ of K and any prime number ℓ. We sketch the proof below.

Lemma 4.8. *Let ℓ be a prime number, let K be a global field satisfying* $\mathrm{char}(K) \neq \ell$*, and let $\mathfrak{p}$ be a prime of K. Then $K_{\mathfrak{p}}^\times / K_{\mathfrak{p}}^{\times \ell}$ is finite.*

Proof. Let $\pi \in K_{\mathfrak{p}}$ be a uniformizer for $R_{\mathfrak{p}}$. Then $K_{\mathfrak{p}}^{\times \ell} = \pi^\ell \cdot R_{\mathfrak{p}}^{\times \ell}$, so it suffices to show that $R_{\mathfrak{p}}^{\times \ell}$ has finite index in $R_{\mathfrak{p}}^\times$. Let e be the absolute ramification index, meaning that $\pi^e R_{\mathfrak{p}} = \ell R_{\mathfrak{p}}$. By Hensel's lemma, if $\alpha \in 1 + \mathfrak{p}^{2e+1} R_{\mathfrak{p}}$, then α is an ℓth power: let $f(x) = x^\ell - \alpha$; then

$$|f(1)|_{\mathfrak{p}} \leq \frac{1}{\ell^{2e+1}} < \frac{1}{\ell^{2e}} = |\ell|_{\mathfrak{p}}^2 = |f'(1)|_{\mathfrak{p}}^2.$$

Thus $1 + \mathfrak{p}^{2e+1} R_{\mathfrak{p}} \subseteq R_{\mathfrak{p}}^{\times \ell}$. Also, $1 + \mathfrak{p}^{2e+1} R_{\mathfrak{p}}$ is an open neighborhood of 1 in the profinite group $R_{\mathfrak{p}}^\times$ and hence has finite index. Thus it also has finite index in $R_{\mathfrak{p}}^{\times \ell}$. □

We will next show that, for a fixed prime $\mathfrak{p}$ of K, $(x, y)_{K_{\mathfrak{p}}, \ell} \neq 1$ cuts out a diophantine subset of $K^\times \times K^\times$.

Lemma 4.9. *Assume that ℓ is an odd prime, that K is a global field with* $\mathrm{char}(K) \neq \ell$*, and that $\mathfrak{p}$ is a prime of K. Then*

$$\{(x, y) \in K^\times \times K^\times : (x, y)_{K_{\mathfrak{p}}, \ell} \neq 1\}$$

is diophantine over K.

Proof. There exist $s_1, \ldots, s_m \in K^\times$ which are a complete set of representatives for $K_{\mathfrak{p}}^\times / K_{\mathfrak{p}}^{\times \ell}$ by Lemma 4.8. If $\pi \in K_{\mathfrak{p}}$ is a uniformizer, let e be the absolute ramification index, meaning that $\pi^e R_{\mathfrak{p}} = \ell R_{\mathfrak{p}}$. Now define $S_j := s_j \cdot K^{\times \ell} \cdot (1 + \mathfrak{p}^{2e+1} \mathcal{O}_{\mathfrak{p}})$. We have

$$K^\times = \bigcup_j S_j.$$

Given $x, y \in K^\times$, there exist $z_i, z_j \in K_{\mathfrak{p}}^{\times \ell}$ such that $x = z_i s_i$ and $y = z_j s_j$. Then we compute $(x, y)_{K_{\mathfrak{p}}, \ell} = (s_i, s_j)_{K_{\mathfrak{p}}, \ell}$ by the linearity and nondegeneracy of the Hilbert symbol. Thus

$$\{(x, y) \in K^\times \times K^\times : (x, y)_{\mathfrak{p}} \neq 1\} = \bigcup_{i_j, i_k : (s_{i_j}, s_{i_k})_{K_{\mathfrak{p}}, \ell} \neq 1} S_i \times S_j,$$

and this set is diophantine over K. □

We need the following sets for our diophantine definitions of semilocal rings in K whose primes split completely in L.

Definition 4.10. Letting $(i, j) = (\pm 1, \pm 1)$,

$$\widetilde{\Phi_{(i,j)}} := K^{\times \ell} \cdot \Phi_{(i,j)}.$$

$$\Psi := \left\{ (p,q) \in \widetilde{\Phi_{(1,1)}} \times \widetilde{\Phi_{(-1,-1)}} \mid \prod_{\mathfrak{p}\mid\mathfrak{m}} (ap,q)_{K_\mathfrak{p},\ell} \neq 1 \text{ and } p \in a^{\ell-1} \cdot K^{\times\ell}(1 + J_p^{(-1,-1)}) \right\}.$$

Lemma 4.11.

(a) $\widetilde{\Phi_{(i,j)}}$ *and* Ψ *are diophantine over* K.
(b) *If* $(p,q) \in \Psi$, *then* $\Delta_{ap,q} \cap \Delta_{bp,q}$ *is nonempty. Moreover, the Jacobson radical* $J(R_{p,q}^{(1,1)})$ *contains* $J_{p,q}^{(1,1)}$, *which is diophantine over* K.
(c) *Given* $\mathfrak{p}_0$ *with* $\psi_{L/K}(\mathfrak{p}_0) = (1,1)$, *there exists* $(p,q) \in \Psi$ *such that* $\Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}_0\}$ *and* $v_{\mathfrak{p}_0}(p) \equiv 1 \pmod{\ell}$. *Moreover,* $J(R_{p,q}^{(1,1)}) = J_{ap,q} + J_{bp,q}$ *and thus is diophantine over* K.

Proof. We have $\widetilde{\Phi_{(i,j)}}$ being diophantine over K by Lemma 4.6(a), and together with Lemma 4.6(b) and Lemma 4.9, we conclude that Ψ is diophantine over K as well.

We now prove (b). Let $(p,q) \in \Psi$. Then there is some prime $\mathfrak{p} \nmid \mathfrak{m}$ such that $(ap,q) \neq 1$ by Hilbert reciprocity. Then either $v_\mathfrak{p}(ap)$ or $v_\mathfrak{p}(q)$ is not divisible by ℓ. Because $\mathfrak{p} \nmid \mathfrak{m}$, we have $\mathfrak{p} \in \mathbb{P}(p) \cup \mathbb{P}(q)$, and consequently $\mathfrak{p} \in \mathbb{P}^{(1,1)} \cup \mathbb{P}^{(-1,-1)}$. We claim that $\mathfrak{p} \in \mathbb{P}^{(1,1)}$, so we assume toward a contradiction that $\mathfrak{p} \in \mathbb{P}^{(-1,-1)}$. Then $\mathfrak{p} \in \mathbb{P}^{(-1,-1)}(q)$, and $p \in a^{\ell-1} \cdot K^{\times\ell} \cdot (1 + \mathfrak{p}\mathcal{O}_\mathfrak{p})$. Thus $ap \in K_\mathfrak{p}^{\times\ell}$ by Hensel's lemma, and $(ap,q)_{K_\mathfrak{p},\ell} = 1$, which is a contradiction. Thus $\mathfrak{p} \in \mathbb{P}^{(1,1)}$.

Now we observe that $(a,q)_{K_\mathfrak{p},\ell} = (b,q)_{K_\mathfrak{p},\ell} = 1$, and hence $(p,q)_{K_\mathfrak{p},\ell} \neq 1$. Thus $(bp,q)_{K_\mathfrak{p},\ell} \neq 1$ as well. We conclude that $\mathfrak{p} \in \Delta_{ap,q} \cap \Delta_{bp,q}$.

In this case, $J_{ap,q} + J_{bp,q}$ is diophantine and is contained in (but not necessarily equal to) the Jacobson radical of $R_{p,q}^{(1,1)}$. We have

$$J_{ap,q} + J_{bp,q} = \bigcap_{\mathfrak{p} \in \Delta_{ap,q} + \Delta_{bp,q}} \mathfrak{p}^{r_\mathfrak{p}} \mathcal{O}_\mathfrak{p},$$

where $r_\mathfrak{p} = \max\{v_\mathfrak{p}(p) - \ell\lfloor \frac{v_\mathfrak{p}(p)}{\ell} \rfloor, v_\mathfrak{p}(q) - \ell\lfloor \frac{v_\mathfrak{p}(q)}{\ell} \rfloor\}$.

We move on to part (c). Suppose that $\mathfrak{p}_0$ is a prime of K with $\mathfrak{p} \not| \mathfrak{m}$ and $\psi_{L/K}(\mathfrak{p}_0) = (1,1)$. We will now construct $(p,q) \in \Psi$ such that $\Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}_0\}$. We begin by choosing our candidate for q. If K is a number field, set $A := \mathcal{O}_K$, and if K is a global function field, let $\mathfrak{p}_1 \neq \mathfrak{p}_0$ be a prime of K such that $\psi_{L/K}(\mathfrak{p}_1) = (1,1)$, and set $A := \mathcal{O}_{\{\mathfrak{p}_1\}}$. Let $\zeta \in \mu_\ell$ be a primitive ℓth root of unity. Then by Lemma 4.7, there exist infinitely many $q \in K^\times$ such that $\psi_{L/K}((q)) = (\zeta,\zeta)$, $\left(\frac{q}{\mathfrak{p}_0}\right)_\ell = \zeta$, and qA is a prime ideal of A, so $qA = \mathfrak{q} \cap A$ for some finite prime $\mathfrak{q}$ of K. We then have $\{\mathfrak{q}\} = \Delta_{a,q} \cap \Delta_{b,q}$ by Lemma 3.11. We note that this choice of q implies that $q \in \widetilde{\Phi_{(-1,-1)}}$.

For each $\mathfrak{p}|\mathfrak{m}$, by Lemma 4.8, there is a finite generating set $E_\mathfrak{p} \subseteq K$ for $K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times\ell}$. Using the Chinese remainder theorem, we can assume that, for each $e \in E_\mathfrak{p}$, $e \equiv 1 \pmod{\mathfrak{p}_0}$. By Hensel's lemma, $e \in K_{\mathfrak{p}_0}^{\times\ell}$ for each e. Finally, fix $e_0 \in K^\times$ such that $\left(\frac{e_0}{\mathfrak{p}_0}\right)_\ell = 1$ and $\left(\frac{e_0}{\mathfrak{q}}\right)_\ell = \zeta$.

We now construct p. Using Theorem 2.8, there exists a $p \in K^\times$ with the following prescribed Hilbert symbols:

	$\mathfrak{p}_0$	$\mathfrak{q}$	all other primes
$e \in E_\mathfrak{p}$, $\mathfrak{p}\vert\mathfrak{m}$	1	1	1
e_0	1	1	1
q	ζ	$\zeta^{\ell-1}$	1
a	1	1	1
b	1	1	1

Clearly, the Hilbert symbol is 1 for almost all $\mathfrak{p}$. Also, across any row, the product of the symbols is 1. We now must show that, for each $\mathfrak{p}$, there exists an element of $K^\times$ satisfying the prescription. First, we will do the $\mathfrak{q}$ column: we claim that $a^{\ell-1}$ satisfies all of the prescriptions. For each $x \in \{a, b, e_0\} \cup E_\mathfrak{p}$, x and a are $\mathfrak{q}$-adic units, and hence $(x, a)_{K_\mathfrak{q},\ell} = 1$. Since $\psi_{L/K}((q)) = (\zeta, \zeta)$ and $v_\mathfrak{q}(q) = 1$, we have $(a^{\ell-1}, q)_{K_\mathfrak{q},\ell} = \zeta^{\ell-1}$. For the $\mathfrak{p}_0$ column, we take $x \in \mathfrak{p}_0 \setminus \mathfrak{p}_0^2$ so that in particular, $v_\mathfrak{p}(x) = 1$. We then have $(x, q)_{K_{\mathfrak{p}_0},\ell} = \left(\frac{q}{\mathfrak{p}_0}\right)_\ell = \zeta$. For $\mathfrak{p}\vert\mathfrak{m}$, as mentioned above, $E_\mathfrak{p} \subseteq K_{\mathfrak{p}_0}^{\times\ell}$, so $(x, e)_{K_{\mathfrak{p}_0},\ell} = 1$. For e_0, we compute $(x, e_0)_{K_\mathfrak{p},\ell} = \left(\frac{e_0}{\mathfrak{p}_0}\right)_\ell = 1$. Finally, $(x, a)_{K_{\mathfrak{p}_0},\ell} = (x, b)_{K_{\mathfrak{p}_0}\ell} = 1$ because

$$(1, 1) = \psi_{L/K}(\mathfrak{p}_0) = \left(\left(\frac{a}{\mathfrak{p}_0}\right)_\ell, \left(\frac{b}{\mathfrak{p}_0}\right)_\ell\right).$$

By Theorem 2.8, there exists a $p \in K^\times$ satisfying the prescribed Hilbert symbols above.

We now claim that p has the following properties:

(1) For each $\mathfrak{p}\vert\mathfrak{m}$ and $e \in E_\mathfrak{p}$, $(e, p)_{K_\mathfrak{p},\ell} = 1$.
(2) $(e_0, p)_{K_{\mathfrak{p}_0},\ell} = 1$ and $(q, p)_{K_{\mathfrak{p}_0},\ell} = \zeta$.
(3) For $\mathfrak{p} \nmid \mathfrak{m}$, $(a, p)_{K_\mathfrak{p},\ell} = (b, p)_{K_\mathfrak{p},\ell} = 1$.
(4) $(q, p)_{K_{\mathfrak{p}_0},\ell} = \zeta^{\ell-1}$.
(5) $\prod_{\mathfrak{p}\vert\mathfrak{m}} (ap, q)_{K_\mathfrak{p},\ell} = \zeta$.

Conditions (1) through (4) follow immediately from the above table. For condition (5), we compute

$$\begin{aligned}
\prod_{\mathfrak{p}\vert\mathfrak{m}} (ap, q)_{K_\mathfrak{p},\ell} &= \prod_{\mathfrak{p}\vert\mathfrak{m}} (a, q)_{K_\mathfrak{p},\ell} (p, q)_{K_\mathfrak{p},\ell} \\
&= \prod_{\mathfrak{p}\vert\mathfrak{m}} (a, q)_{K_\mathfrak{p},\ell} \\
&= \left(\prod_{\mathfrak{p}\nmid\mathfrak{m}} (a, q)_{K_\mathfrak{p},\ell}\right)^{-1} \\
&= (a, q)_{K_\mathfrak{q},\ell}^{-1} \\
&= \zeta^{\ell-1},
\end{aligned}$$

where the second equality follows from $(p, q)_{K_\mathfrak{p}} = 1$ for $\mathfrak{p}\vert\mathfrak{m}$ by the construction of p, the third follows from Hilbert reciprocity, the fourth is a computation using the fact that $\mathbb{P}(q) = \{\mathfrak{q}, \mathfrak{p}_1\}$ and using equation 1, and the fifth follows from $\psi_{L/K}((q)) = (\zeta, \zeta)$.

We claim that $(p,q) \in \Psi$. First, we will show that $v_{\mathfrak{p}}(p) \equiv 0 \pmod{\ell}$ for each $\mathfrak{p}|\mathfrak{m}$. For all $e \in E_{\mathfrak{p}}$, a generating set for $K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times \ell}$, we have $(e,p)_{K_{\mathfrak{p}},\ell} = 1$ by (1). Then by the nondegeneracy of the Hilbert symbol as a pairing on $K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times \ell}$, we have $p \in K_{\mathfrak{p}}^{\times \ell}$, and hence $v_{\mathfrak{p}}(p) \equiv 0 \pmod{\ell}$, for each $\mathfrak{p}|\mathfrak{m}$. By weak approximation, there exists an $r \in K^{\times}$ such that $v_{\mathfrak{p}}(r^{\ell}p) = 0$ for each $\mathfrak{p}|\mathfrak{m}$, so we may assume that $(p) \in I_{\mathfrak{m}}$. From $(a,p)_{K_{\mathfrak{p}},\ell} = (b,p)_{K_{\mathfrak{p}},\ell} = 1$ for each $\mathfrak{p} \nmid \mathfrak{m}$ and by 1, it follows that any prime $\mathfrak{p}$ dividing (p) to a power $e_{\mathfrak{p}} \not\equiv 0 \pmod{\ell}$ must satisfy $\psi_{L/K}(\mathfrak{p}) = (1,1)$. Thus $\psi_{L/K}((p)) = (1,1)$ as well, so $p \in \widetilde{\phi_{(1,1)}}$. By construction of q, we have $q \in \phi_{(-1,-1)}$, and by (5), $\prod_{\mathfrak{p}|\mathfrak{m}}(ap,q)_{K_{\mathfrak{p}},\ell} \neq 1$. Now we claim that $ap \in K_{\mathfrak{q}}^{\times \ell}$. Because e_0 and a are $\mathfrak{q}$-adic units, $(e_0,a)_{K_{\mathfrak{q}},\ell} = 1$, and by (2), $(e_0,p)_{K_{\mathfrak{q}},\ell} = 1$, so $(ap,e_0)_{K_{\mathfrak{q}},\ell} = 1$. Thus $v_{\mathfrak{q}}(ap) \equiv 0 \pmod{\ell}$, again by equation 1. Similarly, we have $(ap,q)_{\mathfrak{q}} = 1$. Because q and e_0 generate $K_{\mathfrak{q}}^{\times}/K_{\mathfrak{q}}^{\times \ell}$, and again using the nondegeneracy of the Hilbert symbol, we conclude that $ap \in K_{\mathfrak{q}}^{\times \ell}$. We have $R_q^{(-1,-1)} = \mathcal{O}_{\mathfrak{q}}$ and $J(R_q^{(-1,-1)}) = \mathfrak{q}\mathcal{O}_{\mathfrak{q}}$, so by Hensel's lemma, we conclude that $K^{\times} \cap K_{\mathfrak{q}}^{\times \ell} = 1 + J(R_q^{(-1,-1)})$ and that $ap \in 1 + J(R_q^{(-1,-1)})$. Hence $p \in a^{\ell-1}K^{\times \ell}(1 + J(R_q^{(-1,-1)}))$, as claimed. Thus $(p,q) \in \Psi$.

Finally, we show that $\Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}_0\}$. Because $(a,q)_{K_{\mathfrak{p}_0},\ell} = (b,q)_{K_{\mathfrak{p}_0},\ell} = 1$ and $(p,q)_{K_{\mathfrak{p}_0},\ell} = \zeta$, we have

$$(ap,q)_{K_{\mathfrak{p}_0},\ell} = (bp,q)_{K_{\mathfrak{p}_0},\ell} = \zeta \neq 1,$$

so $\mathfrak{p}_0 \in \Delta_{ap,q} \cap \Delta_{bp,q}$. As observed above, $(ap,q)_{K_{\mathfrak{q}},\ell} = 1$, so $\mathfrak{q} \notin \Delta_{ap,q} \cap \Delta_{bp,q}$. If $\mathfrak{p} \neq \mathfrak{p}_0, \mathfrak{q}$ is any other prime not dividing $\mathfrak{m}$, we have $(q,a)_{K_{\mathfrak{p}},\ell} = 1$ and $(q,p)_{K_{\mathfrak{p}},\ell} = 1$, so $(q,ap)_{K_{\mathfrak{p}},\ell} = 1$. If K is a number field and $\mathfrak{p}|(\ell)$, then because $a \in K_{\mathfrak{p}}^{\times \ell}$, we have $(a,q)_{K_{\mathfrak{p}},\ell} = 1$. Also, $(p,q)_{K_{\mathfrak{p}},\ell} = 1$ by construction of p, so $(ap,q)_{K_{\mathfrak{p}},\ell} = 1$. If $\mathfrak{p}|\mathfrak{m}$ but does not divide (ℓ), we again have $(p,q)_{K_{\mathfrak{p}},\ell} = 1$. On the other hand, at most one of $(a,q)_{K_{\mathfrak{p}},\ell}$ or $(b,q)_{K_{\mathfrak{p}},\ell}$ cannot equal 1 because (a) and (b) are coprime. Thus $\mathfrak{p} \notin \Delta_{ap,q} \cap \Delta_{bp,q}$, so $\{\mathfrak{p}_0\} = \Delta_{ap,q} \cap \Delta_{bp,q}$. □

5. Proof of main theorem

Lemma 5.1. *Assume that ℓ is an odd prime, that K is a global field with* $\operatorname{char}(K) \neq \ell$*, and that $\zeta \in K$ is a primitive ℓth root of unity. Let $\mathfrak{p}$ be a prime of K. Also, assume that $s \in K^{\times}$ satisfies $v_{\mathfrak{p}}(s) = 0$ and $\left(\frac{s}{\mathfrak{p}}\right)_{\ell} = \zeta \neq 1$. Then the set*

$$s \cdot K^{\times \ell} \cdot (1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}})$$

has the elements of K such that $v_{\mathfrak{p}}(x) \equiv 0 \pmod{\ell}$, and there exists a $t \in K^{\times}$ such that $v_{\mathfrak{p}}(xt^{\ell}) = 0$ and $\left(\frac{xt^{\ell}}{\mathfrak{p}}\right)_{\ell} = \zeta$.

Proof. Suppose that $x \in s \cdot K^{\times \ell} \cdot (1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}})$. Then there exist $p \in \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ and $t \in K^{\times}$ such that $x = st^{\ell}(1+p)$. Thus $v_{\mathfrak{p}}(x) = \ell v_{\mathfrak{p}}(t)$, so $v_{\mathfrak{p}}(x/t^{\ell}) = 0$. We compute

$$\left(\frac{xt^{-\ell}}{\mathfrak{p}}\right)_{\ell} = \left(\frac{s(1+p)}{\mathfrak{p}}\right)_{\ell} = \left(\frac{s}{\mathfrak{p}}\right)_{\ell}.$$

Conversely, suppose that there exists a $t \in K^{\times}$ with $v_{\mathfrak{p}}(xt^{\ell}) = 0$ and $\left(\frac{xt^{\ell}}{\mathfrak{p}}\right)_{\ell} = \zeta$. Then $\left(\frac{xt^{\ell}s^{-1}}{\mathfrak{p}}\right)_{\ell} = 1$, so there exists some $u \in \mathcal{O}_{\mathfrak{p}}$ with $xt^{\ell}s^{-1} \equiv u^{\ell} \mod \mathfrak{p}$. We conclude that $x \in s \cdot K^{\ell} \cdot (1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}})$. □

We will now prove Theorem 1.3, which states that if ℓ is an odd prime, K is a global field with $\mathrm{char}(K) \neq \ell$, and K contains μ_ℓ, then

$$\{(x,y) \in K^\times \times K^\times : x \text{ is not a norm of } K(y^{1/\ell})\}$$

is diophantine over K.

Proof. We find that, given $x, y \in K^\times$, x is not a norm in $K(\sqrt[\ell]{y})/K$ if and only if it fails to be a relative local norm by the Hasse norm theorem. This happens if and only if there exists a prime $\mathfrak{p}$ of K such that $(a,b)_{K_\mathfrak{p},\ell} \neq 1$. Fix $a, b \in K^\times$ and a modulus $\mathfrak{m}$ of K for $L := K(\sqrt[\ell]{a}, \sqrt[\ell]{b})$ as in Proposition 3.7. Define $s_{(-1,-1)} := a =: s_{(-1,1)}$ and $s_{(1,-1)} := b$. We will show that there is a prime $\mathfrak{p}$ of K such that $(x,y)_{K_\mathfrak{p},\ell} \neq 1$ if and only if one of the following conditions is satisfied:

- $\exists\, \mathfrak{p} | \mathfrak{m}$ such that $(x,y)_{K_\mathfrak{p},\ell} \neq 1$,
- $\bigvee_{(i,j)\neq(1,1)} \exists p \in \Phi_{(i,j)}$ such that

$$\left(\left(x \in \bigcup_{r=1}^{\ell-1} p^r \cdot K^{\times\ell} \cdot (R_p^{(i,j)})^\times\right) \wedge \left(\bigvee_{\substack{0\leq c\leq \ell-1\\ 1\leq d\leq \ell-1}} x^c y^d \in \bigcup_{k=1}^{\ell-1} s_{(i,j)}^k \cdot K^{\times\ell} \cdot (1 + J_p^{(i,j)})\right)\right)$$
$$\vee \left(\left(y \in \bigcup_{r=1}^{\ell-1} p^r \cdot K^{\times\ell} \cdot (R_p^{(i,j)})^\times\right) \wedge \left(\bigvee_{\substack{1\leq c\leq \ell-1\\ 0\leq d\leq \ell-1}} x^c y^d \in \bigcup_{k=1}^{\ell-1} s_{(i,j)}^k \cdot K^{\times\ell} \cdot (1 + J_p^{(i,j)})\right)\right),$$

- $\exists (p,q) \in \Psi_K$ such that $q \in (R_{p,q}^{(1,1)})^\times$ and

$$\left(\left(x \in \bigcup_{r=1}^{\ell-1} p^r \cdot K^{\times\ell} \cdot (R_{p,q}^{(1,1)})^\times\right) \wedge \left(\bigvee_{\substack{0\leq c\leq \ell-1\\ 1\leq d\leq \ell-1}} x^c y^d \in \bigcup_{k=1}^{\ell-1} q^k \cdot K^{\times\ell} \cdot (1 + J_{ap,q} + J_{bp,q}))\right)\right)$$
$$\vee \left(\left(y \in \bigcup_{r=1}^{\ell-1} p^r \cdot K^{\times\ell} \cdot (R_{p,q}^{(1,1)})^\times\right) \wedge \left(\bigvee_{\substack{1\leq c\leq \ell-1\\ 0\leq d\leq \ell-1}} x^c y^d \in \bigcup_{k=1}^{\ell-1} q^k \cdot K^{\times\ell} \cdot (1 + J_{ap,q} + J_{bp,q})\right)\right).$$

This will imply the theorem because the sets above are all diophantine over K by Lemmas 4.6 and 4.11, Definition 4.1, and Proposition 3.2.

We now prove the claim. Suppose that x is not a norm of $K(\sqrt[\ell]{y})$; then there exists a prime $\mathfrak{p}$ such that $(x,y)_{K_\mathfrak{p},\ell} \neq 1$. We will show that one of the above conditions on x and y is satisfied. If $\mathfrak{p}|\mathfrak{m}$, then the first condition holds and we are done, so assume otherwise.

First, suppose that $\mathfrak{p} \nmid \mathfrak{m}$ satisfies $\psi_{L/K}(\mathfrak{p}) \in C_{i,j}$ with $(i,j) \neq (1,1)$. By equation 1, we have $v_\mathfrak{p}(x) \not\equiv 0 \pmod{\ell}$ or $v_\mathfrak{p}(y) \not\equiv 0 \pmod{\ell}$. Assume first that $v_\mathfrak{p}(x) \not\equiv 0 \pmod{\ell}$. Then by Lemma 4.6(b), there exists a $p \in \Phi_{(i,j)}$ such that $v_\mathfrak{p}(p) = 1$ and $\mathbb{P}^{(i,j)}(p) = \{\mathfrak{p}\}$. Then there exists $1 \leq r \leq \ell - 1$ such that $v_\mathfrak{p}(x) \equiv v_\mathfrak{p}(p^r) \pmod{\ell}$. Observe that since $\psi_{L/K}(\mathfrak{p}) \neq (1,1)$, we must have $\left(\frac{s_{(i,j)}}{\mathfrak{p}}\right)_\ell \neq 1$.

Thus

$$x \in p^r \cdot K^{\times \ell} \cdot \mathcal{O}_{\mathfrak{p}}^{\times} = p^r \cdot K^{\times \ell} \cdot (R_p^{(i,j)})^{\times},$$

where the equality follows from Definition 4.1. Since $(x,y)_{K_{\mathfrak{p}},\ell} \neq 1$, we must have $\left(\frac{x^{v_{\mathfrak{p}}(y)} y^{-v_{\mathfrak{p}}(x)}}{\mathfrak{p}}\right)_{\ell} \neq 1$, which implies that

$$x^{v_{\mathfrak{p}}(y)} y^{-v_{\mathfrak{p}}(x)} \in s_{(i,j)}^k \cdot K^{\times \ell} \cdot (1 + J(R_p^{(i,j)}))$$

for some $k = 1, \ldots, n-1$ by Lemma 5.1. Writing $v_{\mathfrak{p}}(x) = \ell q_1 + r_1$, $v_{\mathfrak{p}}(y) = \ell q_2 + r_2$ with $1 \leq r_1 \leq \ell - 1$, $0 \leq r_2 \leq \ell - 1$, we have

$$x^{r_2} y^{\ell - r_1} \in s_{(i,j)}^k \cdot K^{\times \ell} \cdot (1 + J(R_p^{(i,j)})).$$

The argument for when $v_{\mathfrak{p}}(x) \equiv 0 \pmod{\ell}$ and $v_{\mathfrak{p}}(y) \not\equiv 0 \mod \ell$ is similar.

Now suppose that $(x,y)_{K_{\mathfrak{p}},\ell} \neq 1$ for a prime $\mathfrak{p} \in C_{(1,1)}$. Then using Lemma 4.11(c), there exist $(p,q) \in \Psi$ such that $\Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}\}$. Moreover, by the proof of Lemma 4.11(c), q can be chosen such that $v_{\mathfrak{p}}(q) = 0$ and $\left(\frac{q}{\mathfrak{p}}\right)_{\ell} \neq 1$, and p satisfies $v_{\mathfrak{p}}(p) \not\equiv 0 \pmod{\ell}$. Then

$$q \in \mathcal{O}_{\mathfrak{p}}^{\times} = (R_{p,q}^{(1,1)})^{\times},$$

and assuming first that $v_{\mathfrak{p}}(x) \not\equiv 0 \pmod{\ell}$, it follows that there exists $1 \leq r \leq \ell - 1$ such that

$$x \in p^r \cdot K^{\times \ell} \cdot (R_{p,q}^{(1,1)})^{\times}.$$

By arguing as in the case with $\psi_{L/K}(\mathfrak{p}) \neq (1,1)$, we conclude that

$$x^c y^d \in q^k \cdot K^{\times \ell} \cdot (1 + J(R_{p,q}^{(1,1)})).$$

The case in which $v_{\mathfrak{p}}(y) \not\equiv 0 \pmod{\ell}$ again is similar.

Now, conversely, suppose that one of the three conditions holds. There is nothing to show whether the first condition holds, so suppose that the second holds. Without loss of generality, for some $(i,j) \neq (1,1)$, there exists a $p \in \Phi_{(i,j)}$ such that

$$x \in p^r \cdot K^{\times \ell} \cdot (R_p^{(i,j)})^{\times} \subseteq p^r \cdot K^{\times \ell} \cdot (\mathcal{O}_{\mathfrak{p}})^{\times}. \tag{2}$$

This implies that

$$v_{\mathfrak{p}}(x) \equiv v_{\mathfrak{p}}(p^r) \not\equiv 0 \pmod{\ell}.$$

By Lemma 4.6(b), $\mathbb{P}^{(i,j)}(p) \neq \emptyset$ and thus contains some prime $\mathfrak{p}$; we will now compute $(x,y)_{K_{\mathfrak{p}},\ell}$. For some $0 \leq c \leq \ell - 1$ and $1 \leq d, k \leq \ell - 1$, we have

$$x^c y^d \in s_{(i,j)}^k \cdot K^{\times \ell} \cdot (1 + J(R_p^{(i,j)})) \subseteq s_{(i,j)}^k \cdot K^{\times \ell} \cdot (1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}}). \tag{$\star$}$$

It follows that $(x,y)_{K_{\mathfrak{p}},\ell} \neq 1$ if and only if $(x,y)_{K_{\mathfrak{p}},\ell}^d \neq 1$ since $1 \leq d \leq \ell - 1$; thus we will show that $(x,y)_{K_{\mathfrak{p}},\ell}^d \neq 1$.

We compute

$$\begin{aligned}(x,y)_{K_{\mathfrak{p}},\ell}^d &= (x,x)_{K_{\mathfrak{p}},\ell}^c (x,y)_{K_{\mathfrak{p}},\ell}^d \\ &= (x, x^c y^d)_{K_{\mathfrak{p}},\ell}.\end{aligned}$$

The first equality follows because $(x,x)_{K_{\mathfrak{p}},\ell} = 1$, and the second follows from linearity of the Hilbert symbol. Possibly by multiplying $x^c y^d$ by an ℓth power of $K^{\times}$, we can assume $v_{\mathfrak{p}}(x^c y^d) = 0$. Because $v_{\mathfrak{p}}(x^c y^d) = 0$, we have $(x, x^c y^d)_{K_{\mathfrak{p}},\ell} = \left(\frac{x^c y^d}{\mathfrak{p}}\right)_{\ell}^{v_{\mathfrak{p}}(x)}$ by equation 1.

Because of equation ($\star$) and by Hensel's lemma, there exists a $z \in K_{\mathfrak{p}}^{\times \ell}$ such that $x^c y^d z = s_{(i,j)}^k$. This implies that $(x, x^c y^d)_{K_{\mathfrak{p}},\ell} = (x, s_{(i,j)})_{K_{\mathfrak{p}},\ell}$, and $(x, s_{(i,j)})_{K_{\mathfrak{p}},\ell} \neq 1$ by Lemma 5.1. Combining the above computations, we see that $(x,y)_{K_{\mathfrak{p}},\ell} \neq 1$.

Now suppose that the third condition holds. By Lemma 4.11(b), $\Delta_{ap,q} \cap \Delta_{bp,q} \neq \emptyset$, so it contains some prime $\mathfrak{p}$. We claim that $(x,y)_{K_{\mathfrak{p}},\ell} = 1$. Without loss of generality and by the same reasoning as above, $x \in p^r \cdot K^{\times \ell} \cdot (\mathcal{O}_{\mathfrak{p}})^\times$, and $x^c y^d \in q^k \cdot K^{\times \ell} \cdot (1 + \mathfrak{p}\mathcal{O}_{\mathfrak{p}})$ for some c satisfying $0 \leq c \leq \ell - 1$, and for some r, d, k satisfying $1 \leq r, d, k \leq \ell - 1$. Because $(ap, q)_{K_{\mathfrak{p}},\ell} \neq 1$ and $v_{\mathfrak{p}}(q) = 0$, we must have $\left(\frac{q}{\mathfrak{p}}\right)_\ell \neq 1$. The same argument and similar computations to the above give us $(x,y)_{K_{\mathfrak{p}},\ell} \neq 1$, now with q playing the role of $s_{(i,j)}$. □

We now prove Corollary 1.4 using Theorem 1.3, the Hasse norm theorem, and local class field theory.

Proof of Corollary 1.4. Assume that n is a square-free natural number, that K is a global field with $(\mathrm{char}(K), n) = 1$, and that K contains μ_n, the nth roots of unity. Let $n = \prod_{i=1}^r \ell_i$, where the ℓ_i are the distinct r primes dividing n. We will show that

$$\{(x,y) \in K^\times \times K^\times : x \text{ is not a norm of } K(\sqrt[n]{y})/K\}$$

is equal to

$$\bigcup_{i=1}^r \{(x,y) \in K^\times \times K^\times : x \text{ is not a norm of } K(\sqrt[\ell_i]{y})/K\}.$$

After showing this, Corollary 1.4 follows from Theorem 1.3 and [Eis18, Theorem 1.3] if $2|n$ because the finite union of diophantine sets is diophantine.

Given a cyclic extension M of K of degree n and $\alpha \in K$, we find that $M = K(\alpha^{1/n})$ is the compositum of the fields $L_i := K(\alpha^{1/\ell_i})$. We note that M/K, and hence each L_i/K, satisfies the Hasse norm principle. Let $\mathcal{P}$ be a prime of M, and let $\mathfrak{P}_i$ be the corresponding prime below $\mathcal{P}$ in L_i for each i. Let $\mathfrak{p}$ be the prime of K below $\mathcal{P}$. Then

$$M_{\mathcal{P}} = (L_1)_{\mathfrak{P}_i} \cdots (L_r)_{\mathfrak{P}_r}.$$

Since $M_{\mathcal{P}}/K_{\mathfrak{p}}$ is cyclic and hence abelian, by local class field theory we have

$$N_{M_{\mathcal{P}}/K_{\mathfrak{p}}}(M_{\mathcal{P}}^\times) = \bigcap_{i=1}^r N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(L_{\mathfrak{P}_i}^\times).$$

Each L_i/K is cyclic, so it satisfies the Hasse norm principle; we thus conclude that

$$\begin{aligned}
N_{M/K}(M^\times) &= K^\times \cap \bigcap_{\mathfrak{P}} N_{M_{\mathcal{P}}/K_{\mathfrak{p}}}(M_{\mathcal{P}}^\times) && \text{by the Hasse norm principle} \\
&= K^\times \cap \bigcap_{\mathfrak{P}} \bigcap_{i=1}^r N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(L_{\mathfrak{P}_i}^\times) && \text{by local class field theory} \\
&= K^\times \cap \bigcap_{i=1}^r \bigcap_{\mathfrak{P}_i} N_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(L_{\mathfrak{P}_i}^\times) \\
&= K^\times \cap \bigcap_{i=1}^r N_{L_i/K}(L_i^\times) && \text{again by the Hasse norm principle.}
\end{aligned}$$

Thus

$$\{(x,y) \in K^\times \times K^\times : x \text{ is not a norm of } K(y^{1/n})\}$$

is equal to

$$\bigcup_{i=1}^{r} \{(x,y) \in K^\times \times K^\times : x \text{ is not a norm of } K(y^{1/l_i})\}.$$

This is a finite union of sets diophantine over K by Theorem 1.3 if l_i is odd, and by [Eis18, Theorem 1.3] if l_i is 2. □

6. Non-nth powers are diophantine

In this section, we prove Corollary 1.5. This was proved in [CTVG15] for when K is a number field.

Corollary 6.1. *Let $n > 1 \in \mathbb{N}$, and let K be a global field with $(\mathrm{char}(K), n) = 1$. Then $K^\times \setminus K^{\times n}$ is diophantine over K.*

Proof. It suffices to prove this for n prime and K containing a primitive nth root of unity, as observed in [VAV12, CTVG15], which we now assume. Because the Hilbert symbol

$$(\cdot,\cdot)_{K_\mathfrak{p},n} : K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times n} \times K_\mathfrak{p}^\times / K_\mathfrak{p}^{\times n} \to \mu_n$$

is a nondegenerate pairing, we have $x \in K^\times \setminus K^{\times n}$ if and only if there exists a $y \in K^\times$ such that $(x,y)_{K_\mathfrak{p},n} \neq 1$. This holds if and only if there exists a $y \in K^\times$ such that x is not a norm of $K(\sqrt[n]{y})/K$. Set

$$D := \{(x,y) \in K^\times \times K^\times : x \text{ is not a norm of } K(\sqrt[n]{y})/K\}.$$

Putting this together, we see that

$$K^\times \setminus K^{\times n} = \{x \in K^\times : \exists y \in K^\times \text{ s.t. } (x,y) \in D\},$$

so $K^\times \setminus K^{\times n}$ is diophantine over K by Theorem 1.3. □

7. Nonnorms of cyclic extensions

We will first prove Theorem 1.6 in the case in which $n = \ell$ is a prime, K contains μ_ℓ, the primitive ℓth root of unity, and $\mathrm{char}(K) \neq \ell$, and we will then show how the theorem for $n > 1$ square free and fields K not containing μ_n follows. Recall that, for a finite field extension L/K of degree n, a *norm form for L/K* is a homogeneous polynomial f of degree n in the n variables $t_1, \ldots, t_n$ (thought of as ranging over K) such that there is a K-basis $b_1, \ldots, b_n$ of L satisfying

$$f(t_1, \ldots, t_n) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma\left(\sum_i t_i b_i\right)$$

for any $t_1, \ldots, t_n \in K$.

Proof of Theorem 1.6. Assume that ℓ is a prime number, that K is a global field with $\mathrm{char}(K) \neq \ell$, and that K contains μ_ℓ, the primitive ℓth roots of unity. Set $d = \binom{2\ell-1}{\ell}$ and

$$D := \{(x,y) \in K^\times \times K^\times : x \text{ is not a norm of } K(\sqrt[\ell]{y})/K\}.$$

Consider a cyclic extension $L = K(y^{1/\ell})$ of K for $y \in K^\times$, and the K-basis $\{y^{(i-1)/\ell}\}$, $i = 1, \dots, \ell$, of L. Then every other basis of L/K is of the form

$$w_i = \sum_j b_{ij} y^{(j-1)/\ell}$$

for some matrix $(b_{ij}) \in \mathrm{GL}_\ell(K)$. Then

$$N_{L/K}(t_1, \dots, t_\ell) = N_{L/K}\left(\sum_i t_i \left(\sum_j b_{ij} y^{(j-1)/\ell}\right)\right),$$

as a polynomial in the variables t_i, has coefficients $f_s \in K[y, b_{11}, \dots, b_{\ell\ell}]$. Thus

$$\begin{aligned}(x, a_1, \dots, a_d) \in D(\ell, K) \iff \exists b_{ij}, y \in K \text{ for } i, j = 1, \dots, \ell \text{ such that} \\ \bullet\ f_s(y, b_{11}, \dots, b_{\ell\ell}) = a_s, \\ \bullet\ (b_{ij}) \in \mathrm{GL}_\ell(K), \text{ and} \\ \bullet\ (x, y) \in D.\end{aligned}$$

Thus $D(\ell, K)$ is diophantine over K because each condition in the above list defines a diophantine set over K. The first two are clearly diophantine, and the third is, by Theorem 1.3, if ℓ is odd, and by [Eis18, Theorem 1.3] if $\ell = 2$. This proves the theorem in the case in which K contains μ_ℓ, the ℓth roots of unity.

Now suppose that K does not contain the ℓth roots of unity. Let $\omega \in \overline{K}$ be a primitive ℓth root of unity in an algebraic closure $\overline{K}/K$, and set $M := K(\omega)$. If L/K is a cyclic extension of degree ℓ, a basis of L/K is also a basis of ML/M since M and L are both Galois over K and $M \cap L = K$. Thus a norm form for L/K is also a norm form of ML/M when viewing the variables as ranging over M rather than K.

We now show that $D(\ell, K)$ is diophantine over K. We have $(x, \vec{a}) \in D(\ell, K)$ if and only if there is a cyclic extension L/K such that $f_{\vec{a}}$ is a norm form of L/K, and if σ generates $\mathrm{Gal}(L/K)$, the cyclic algebra (σ, x) is not split. Let τ be a generator of $\mathrm{Gal}(ML/M)$ with $\tau|_L = \sigma$. Since the map

$$\begin{aligned}Br(K) &\to Br(M), \\ [A] &\mapsto [A \otimes_K L]\end{aligned}$$

is multiplication by $[M : K] = \ell - 1$ on the level of Brauer classes, and since

$$(\sigma, x) \otimes_K M \simeq (\tau, x),$$

we find that (σ, x) is split if and only if (τ, x) is split, as $\ell - 1$ is coprime to ℓ. Thus $(x, \vec{a}) \in D(\ell, K)$ if and only if $(x, \vec{a}) \in D(\ell, M)$, which is diophantine over M. Let $g \in M[s, t_1, \dots, t_d, u_1 \dots, u_m]$ be a polynomial which gives a diophantine definition of $D(\ell, M)$ over M, meaning that

$$\begin{aligned}(x', a_1', \dots, a_d') \in M \times M^d \iff \exists r_1, \dots, r_m \\ \in M \text{ s.t. } f(x', a_1', \dots, a_d', r_1, \dots, r_m) = 0.\end{aligned}$$

Such a polynomial exists by our proof of the theorem above for global fields containing the ℓth roots of unity. Write the coefficients of f as K-linear combinations in $\omega^i, i = 0, \dots, \ell - 1$, and let $f_i \in K[s, t_1, \dots, t_d, u_1, \dots, u_m]$ be the polynomial which is the coefficient of ω^i in f. Then $f_0, \dots, f_{\ell-1}$ give a diophantine definition

of $D(\ell, K)$ over K. This proves the theorem for a global field K with $\mathrm{char}(K) \neq \ell$, where $n = \ell$ is a prime.

Finally, if n is square free and K is a global field with $(\mathrm{char}(K), n) = 1$, we can reduce Theorem 1.6 to the case in which n is prime, just as we did in the proof of Corollary 1.4. Let $n = \ell_1 \cdots \ell_r$ be the prime factorization of n; then cyclic extensions L/K of degree n are the compositum of cyclic extensions L_i/K of degree ℓ_i. An element x of K is not a norm of L/K if and only if x is not a norm of L_i/K for some i, $1 \leq i \leq r$. Hence

$$D(n, K) = \bigcup_{i=1}^{r} D(\ell_i, K),$$

and we see that $D(n, K)$ is diophantine over K because each $D(\ell_i, K)$ is diophantine over K by the above argument for $n = \ell$ prime. This finishes the proof of the theorem. □

Acknowledgments

I would like to thank Philip Dittman for pointing out a mistake in a previous version of this work, and for his comments and suggestions. I would also like to thank the anonymous referees for their careful reading, corrections, and suggestions.

References

[CTVG15] J.-L. Colliot-Thélène and J. Van Geel, *Le complémentaire des puissances n-ièmes dans un corps de nombres est un ensemble diophantien* (French, with English and Dutch summaries), Compos. Math. **151** (2015), no. 10, 1965–1980, DOI 10.1112/S0010437X15007368. MR3414391

[Dit17] P. Dittmann, *Irreducibility of polynomials over global fields is diophantine*, Compos. Math. **154** (2018), no. 4, 761–772, DOI 10.1112/S0010437X17007977. MR3778193

[DPR61] M. Davis, H. Putnam, and J. Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436, DOI 10.2307/1970289. MR0133227

[Eis05] K. Eisenträger, *Integrality at a prime for global fields and the perfect closure of global fields of characteristic $p > 2$*, J. Number Theory **114** (2005), no. 1, 170–181, DOI 10.1016/j.jnt.2005.02.008. MR2163911

[Eis18] K. Eisenträger and T. Morrison, *Universally and existentially definabile subsets of global fields*, Math. Res. Lett. **25** (2018), no. 4, 1173–1204. MR3882159

[GS06] P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, Cambridge, England, 2006. MR2266528

[Koe16] J. Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Ann. of Math. (2) **183** (2016), no. 1, 73–93, DOI 10.4007/annals.2016.183.1.2. MR3432581

[Mat70] Ju. V. Matiyasevich, *The Diophantineness of enumerable sets* (Russian), Dokl. Akad. Nauk SSSR **191** (1970), 279–282. MR0258744

[Par13] J. Park, *A universal first-order formula defining the ring of integers in a number field*, Math. Res. Lett. **20** (2013), no. 5, 961–980, DOI 10.4310/MRL.2013.v20.n5.a12. MR3207365

[Poo09a] B. Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131** (2009), no. 3, 675–682, DOI 10.1353/ajm.0.0057. MR2530851

[Poo09b] B. Poonen, *The set of nonsquares in a number field is Diophantine*, Math. Res. Lett. **16** (2009), no. 1, 165–170, DOI 10.4310/MRL.2009.v16.n1.a16. MR2480570

[Rob49] J. Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114, DOI 10.2307/2266510. MR0031446

[Ros87] M. Rosen, *The Hilbert class field in function fields*, Exposition. Math. **5** (1987), no. 4, 365–378. MR917350

[Ros02] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR1876657

[Ser79] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York–Berlin, 1979. Translated from the French by Marvin Jay Greenberg. MR554237

[Shl94] A. Shlapentokh, *Diophantine classes of holomorphy rings of global fields*, J. Algebra **169** (1994), no. 1, 139–175, DOI 10.1006/jabr.1994.1276. MR1296586

[VAV12] A. Várilly-Alvarado and B. Viray, *Higher-dimensional analogs of Châtelet surfaces*, Bull. Lond. Math. Soc. **44** (2012), no. 1, 125–135, DOI 10.1112/blms/bdr075. MR2881330

Institute for Quantum Computing, The University of Waterloo, 200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada

Email address: travis.morrison@uwaterloo.ca