Universally Defining Finitely Generated Subrings of Global Fields

Nicolas Daans

Received: November 13, 2020
Revised: November 20, 2021

Communicated by Michael Rathjen

Abstract. It is shown that any finitely generated subring of a global field has a universal first-order definition in its fraction field. This covers Koenigsmann's result for the ring of integers and its subsequent extensions to rings of integers in number fields and rings of S-integers in global function fields of odd characteristic. In this article a proof is presented which is uniform in all global fields, including the characteristic two case, where the result is entirely novel. Furthermore, the proposed method results in universal formulae requiring significantly fewer quantifiers than the formulae that can be derived through the previous approaches.

2020 Mathematics Subject Classification: Primary 11U99; Secondary 11R52
Keywords and Phrases: Diophantine set, definability, quaternion algebra, Hilbert 10

1 Introduction

It was recently shown by Koenigsmann that there is a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$ in the first-order language of rings [11]. That is, he showed that there exist a natural number m and a polynomial $F \in \mathbb{Q}[X, Y_1, \ldots, Y_m]$ such that

$$\mathbb{Z} = \{x \in \mathbb{Q} \mid \forall y_1, \ldots, y_m \in \mathbb{Q} : F(x, y_1, \ldots, y_m) \neq 0\}.$$

This builds on earlier work by Poonen, who had derived an $\forall\exists$-formula defining $\mathbb{Z}$ in $\mathbb{Q}$ [16]. That $\mathbb{Z}$ has a first-order definition in $\mathbb{Q}$ at all was already known long before and first shown by Robinson [17].
The purpose of this paper is to present a variation of Koenigsmann's construction. This adaptation not only shortens the proof and yields a simpler formula by removing

the need for many case distinctions, it also generalises directly to other global fields. Before stating our results in full generality, let us illustrate how the method applies for universally defining $\mathbb{Z}$ in $\mathbb{Q}$.

Let $\mathbb{P}$ be the set of prime numbers. For $p \in \mathbb{P}$, we denote by v_p the p-adic valuation on $\mathbb{Q}$, by $\mathbb{Z}_{(p)}$ the corresponding valuation ring of $\mathbb{Q}$, and by $p\mathbb{Z}_{(p)}$ its maximal ideal. One can easily obtain a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$ once one has found an existential definition of $\bigcup_{p\in\mathbb{P}} p\mathbb{Z}_{(p)}$ in $\mathbb{Q}$. Indeed, for $x \in \mathbb{Q}^\times$ one has

$$x \in \mathbb{Z} \;\Leftrightarrow\; x^{-1} \notin \bigcup_{p\in\mathbb{P}} p\mathbb{Z}_{(p)}.$$

To work our way towards an existential definition of $\bigcup_{p\in\mathbb{P}} p\mathbb{Z}_{(p)}$ in $\mathbb{Q}$, quaternion algebras over $\mathbb{Q}$ turn out to be a useful tool. Quaternion algebras were first introduced in this context in [16]. For a field K with $\mathrm{char}(K) \neq 2$ and $a, b \in K^\times$, write $(a, b)_K$ for the K-quaternion algebra with generators i, j such that $i^2 = a$, $j^2 = b$ and $ij + ji = 0$. To a given $a, b \in \mathbb{Q}^\times$, we associate the set

$$\Delta_{a,b} = \{p \in \mathbb{P} \mid (a, b)_{\mathbb{Q}_p} \text{ not split}\}.$$

This is a finite set of prime numbers also called the *ramification set* of the quaternion algebra $(a, b)_\mathbb{Q}$; it clearly depends only on the isomorphism class of $(a, b)_\mathbb{Q}$ as a $\mathbb{Q}$-algebra. In section 4 its computation and properties will be discussed. Now we define the subset

$$\Delta^c_{a,b} = \{p \in \Delta_{a,b} \mid v_p(c) \text{ is odd}\}$$

for $a, b, c \in \mathbb{Q}^\times$. In section 5 it will be shown that the subset of $\mathbb{Q}$

$$J^c_{a,b} = \bigcap_{p\in\Delta^c_{a,b}} p\mathbb{Z}_{(p)}$$

has an existential definition in $\mathbb{Q}$, uniformly in the parameters $a, b, c \in \mathbb{Q}^\times$. Here, we take the convention that $\bigcap \emptyset = \mathbb{Q}$. These sets were implicitly already introduced and given an existential definition by Koenigsmann [11], building on earlier work by Poonen [16].

To obtain a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$, it then remains to show that we can build an existential definition of $\bigcup_{p\in\mathbb{P}} p\mathbb{Z}_{(p)}$ by using the existentially definable sets $J^c_{a,b}$. Here we deviate substantially from the approach in [11]. Consider the following subset of $(\mathbb{Q}^\times)^2$:

$$\Phi = \{(1 + 4a^2, 2b) \mid a, b \in \mathbb{Z}^\times_{(2)}\}.$$

This set is existentially definable in $\mathbb{Q}$: to see this one can, for example, use that $2\mathbb{Z}_{(2)} = J^2_{2,5}$. We will see that

$$\bigcup_{p\in\mathbb{P}} p\mathbb{Z}_{(p)} = 2\mathbb{Z}_{(2)} \cup \bigcup_{(x,y)\in\Phi} (J^x_{x,y} \cap J^{2y}_{x,y}). \tag{1}$$

As the set on the right is existentially definable, this gives us the required existential definition for $\bigcup_{p\in\mathbb{P}} p\mathbb{Z}_{(p)}$ in $\mathbb{Q}$.

Let us explain why the inclusion from right to left holds. Take an arbitrary pair $(x, y) \in \Phi$. It is not hard to see that $2 \in \Delta_{x,y}$ (see Proposition 4.2). Furthermore, as $x > 0$, it is a well-known corollary of the Quadratic Reciprocity Law that $\Delta_{x,y}$ contains an even number of elements (Theorem 4.5); in particular we must have $\Delta_{x,y} \neq \{2\}$, so there exists a prime number $p \in \Delta_{x,y} \setminus \{2\}$. This implies $(x, y)_{\mathbb{Q}_p}$ is non-split, so that either $v_p(x)$ or $v_p(y) = v_p(2y)$ is odd (see Proposition 4.1); we conclude that $p \in \Delta^x_{x,y} \cup \Delta^{2y}_{x,y}$ and hence $(J^x_{x,y} \cap J^{2y}_{x,y}) \subseteq p\mathbb{Z}_{(p)}$. As this holds for arbitrary $(x, y) \in \Phi$, this shows the inclusion from right to left in (1).

For the other inclusion, the key point is to show that, given an odd prime p, one can find a pair $(x, y) \in \Phi$ such that $\Delta_{x,y} = \{2, p\}$. One possible approach is to first find a prime number $q \equiv 5 \bmod 8$ such that p is a non-square modulo q. For such q one has $\Delta_{q,2p} = \{2, p\}$ and $q = c^2 + 4d^2$ for certain $c, d \in \mathbb{Z} \setminus 2\mathbb{Z}$; hence one can set $x = q/c^2$, $y = 2p$. Having found x and y such that $\Delta_{x,y} = \{2, p\}$, we see that $\Delta^x_{x,y} \cup \Delta^{2y}_{x,y} = \{p\}$ and as such $J^x_{x,y} \cap J^{2y}_{x,y} = p\mathbb{Z}_{(p)}$. This concludes the proof of the inclusion from left to right.

With some adjustments a similar construction can be used in a more general context. For a global field K (i.e. a number field or a function field in one variable over a finite field) and a finite set S of valuations on K, define the *ring of S-integers* as the intersection of all valuation rings of K excluding those which are given by valuations in S. Our main result can be stated as follows:

THEOREM. *Let K be a global field, S a finite set of valuations on K. The ring of S-integers has a universal first-order definition in K with 37 quantifiers in the language of rings with constants for K.*

Without the quantitative bound, large parts of this result were already established by Park [14] for number fields and Eisenträger and Morrison [7] for global fields of odd characteristic. We recover these results with a uniform proof for all cases. This is because we reduce the number theoretic ingredients to just two statements. Firstly, that a quaternion algebra over a global field K which is split over all embeddings into $\mathbb{R}$ ramifies at an even number of primes (a fact known in the case $K = \mathbb{Q}$ as Hilbert's Reciprocity Law and closely related to the Quadratic Reciprocity Law). Secondly that conversely, for every finite set of primes of even cardinality of a global field K, there exists a quaternion algebra over K which ramifies precisely at these primes. To be able to also cover global fields of characteristic 2 in this article, for which the question has so far remained undiscussed in the literature, we will switch to a characteristic-independent parametrisation of quaternion algebras due to Albert, which we will state and briefly elaborate on in section 3.

The main theorem is first proven in section 6 without quantitative bounds. This way, steps which serve only to lower the number of quantifiers do not distract the reader from the structure of the argument. In section 7 we zoom in on how to obtain the bound on the number of quantifiers. The original method of [11], even just in the case

of defining $\mathbb{Z}$ in $\mathbb{Q}$, yields definitions with several hundreds of quantifiers.[1] The technique from the current article has been further improved in the case of defining $\mathbb{Z}$ in $\mathbb{Q}$ in a recent preprint by Sun and Zhang [19], leading to a definition with 32 quantifiers. Rings of S-integers in a global field K are finitely generated subrings of K which have K as their fraction field. In section 8 it will be explained how universal definability of arbitrary finitely generated subrings of K with fraction field K follows easily from universal definability of rings of S-integers. Here, however, we lose the bound on the number of quantifiers. Nevertheless, the most general result on universal definability of subrings of global fields we obtain can then be stated compactly as follows:

COROLLARY. *Let K be a global field. Any finitely generated subring R of K such that K is the fraction field of R has a universal first-order definition in K.*

ACKNOWLEDGEMENTS

I would like to thank Philip Dittmann for suggesting the approach in Section 8, as well as Jan Van Geel and Bjorn Poonen for pointing out Lemma 6.7.
This work grew out of my master thesis. It will also be part of my PhD thesis, prepared at the University of Antwerp under the supervision of Karim Johannes Becher and Philip Dittmann.
This work was supported by Fonds Wetenschappelijk Onderzoek - Vlaanderen (FWO) through PhD Fellowship fundamental research 51581, and by the FWO Odysseus programme (project *Explicit Methods in Quadratic Form Theory*).

2 LOGICAL PRELIMINARIES AND NOTATION

Let $\mathbb{N}$ denote the set of natural numbers, including 0. We will further use the notation $2\mathbb{N} = \{2n \mid n \in \mathbb{N}\}$.
We will use some basic standard terminology from mathematical logic when dealing with the syntax and semantics of statements in first-order language, as covered by many textbooks (e.g. [6, Chapter II-III]). We denote by $\mathcal{L}$ the first-order language of rings, that is the language consisting of three binary operation symbols $+, -, \cdot$ and two constant symbols $0, 1$. We denote by $\doteq$ the equality symbol in the language. Let R be a commutative ring and let $\mathcal{L}_R$ denote the language of rings extended with constant symbols for the elements of R. We interpret a commutative R-algebra K as an $\mathcal{L}_R$-structure via the action of R on K. The identity map makes any commutative ring R into an $\mathcal{L}_R$-structure in a canonical way.
Let $\varphi(X_1, \ldots, X_n)$ be an $\mathcal{L}_R$-formula in free variables $X_1, \ldots, X_n$. Given a commutative R-algebra K and a tuple $(x_1, \ldots, x_n) \in K^n$, we write $K \models \varphi(x_1, \ldots, x_n)$ if and only if, after substituting x_i for X_i for each $i \in \{1, \ldots, n\}$, the $\mathcal{L}_K$-statement $\varphi(x_1, \ldots, x_n)$ holds when evaluated in K. We call two $\mathcal{L}_R$-formulas

[1] The published version of [11] does not explicitly count the number of quantifiers. In an earlier preprint available online (https://archive.org/details/arxiv-1011.3424) it is claimed that a universal formula with 418 quantifiers is obtained. However, I was unable to replicate this count and reach the same final number.

φ_1 and φ_2 in free variables $X_1, \ldots, X_n$ *equivalent* if for any $\mathcal{L}_R$-structure K and for any $(x_1, \ldots, x_n) \in K^n$ we have $K \models \varphi_1(x_1, \ldots, x_n)$ if and only if $K \models \varphi_2(x_1, \ldots, x_n)$.

As we will only evaluate first-order formulas in commutative rings, there is no ambiguity in interpreting atomic $\mathcal{L}_R$-formulas as polynomial equalities with coefficients in R. Furthermore, we may identify $\mathcal{L}$ with $\mathcal{L}_\mathbb{Z}$, as every ring is a $\mathbb{Z}$-algebra in a unique way. Up to equivalence, every existential $\mathcal{L}_R$-formula $\varphi(X_1, \ldots, X_n)$ in free variables $X_1, \ldots, X_n$ can be written as

$$\exists Y_1, \ldots, Y_m \bigvee_{i=1}^{p} \left(\left(\bigwedge_{j=1}^{q_i} f_{i,j} \doteq 0 \right) \wedge \left(\bigwedge_{k=1}^{r_i} \neg(g_{i,k} \doteq 0) \right) \right) \tag{2}$$

for some $m, p, q_i, r_i \in \mathbb{N}$ and $f_{i,j}, g_{i,k} \in R[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ for all i, j, k. For the sake of brevity, we will call an existential $\mathcal{L}_R$-formula with m quantifiers an $\exists_m\mathcal{L}_R$*-formula*. By an $\exists\mathcal{L}_R$*-formula* we mean an $\exists_m\mathcal{L}_R$-formula for some $m \in \mathbb{N}$. If $p = q_1 = 1$ and $r_1 = 0$ (i.e. φ consists just of one polynomial equation), we call φ a *diophantine* $\mathcal{L}_R$*-formula*.

Given a subset $B \subseteq K^n$ and an $\mathcal{L}_R$-formula $\varphi(X_1, \ldots, X_n)$ such that

$$B = \{(x_1, \ldots, x_n) \in K^n \mid K \models \varphi(x_1, \ldots, x_n)\},$$

we say that φ *defines* B. A subset of K^n is said to have an *existential* (respectively *diophantine*) $\mathcal{L}_R$*-definition with* m *quantifiers* if it is equal to the set defined by some existential (respectively diophantine) $\mathcal{L}_R$-formula with m quantifiers. Instead of an existential $\mathcal{L}_R$-definition with m quantifiers, we write $\exists_m\mathcal{L}_R$*-definition* for short. Analogously, we define *universal* $\mathcal{L}_R$*-formulas* and *-definitions* with m quantifiers by replacing the existential quantifiers by universal quantifiers in (2) and we use the notation $\forall_m\mathcal{L}_R$. Note that a subset of K^n has a $\forall_m\mathcal{L}_R$-definition if and only if its complement in K^n has an $\exists_m\mathcal{L}_R$-definition.

It is clear that when ϕ and ψ are $\exists_{m_1}\mathcal{L}_R$- and $\exists_{m_2}\mathcal{L}_R$-formulas respectively, then $\phi \vee \psi$ is equivalent to an $\exists_m\mathcal{L}_R$-formula for $m = \max\{m_1, m_2\}$ and $\phi \wedge \psi$ is equivalent to an $\exists_{m_1+m_2}\mathcal{L}_R$-formula. This implies in particular that finite intersections and unions of $\exists\mathcal{L}_R$-definable subsets of K^n again have an $\exists\mathcal{L}_R$-definition.

In the rest of this article we will continue to work with general existential formulae instead of diophantine formulae, as the former are more natural to reason with. Furthermore, a well-known statement asserts that for a non-algebraically closed field K, every $\exists\mathcal{L}_K$-definable set is also definable by a diophantine $\mathcal{L}_K$-formula. Here is a version of this statement with quantitative bounds and a sketch of a proof for completeness.

PROPOSITION 2.1. *Let K be a field that is not algebraically closed, $m, n \in \mathbb{N}$, $B \subseteq K^n$ an $\exists_m\mathcal{L}_K$-definable set. Then B has a diophantine $\mathcal{L}_K$-definition in K^n with $m + 1$ quantifiers.*

Proof. We start from the general formula in (2) and subsequently replace it by formulas defining the same set B, eventually ending up with a diophantine formula

with $m+1$ quantifiers. Firstly, the observation that for $x_1, \dots, x_r \in K$ we have $x_1, \dots, x_r \neq 0$ if and only if $\exists y \in K : x_1 \cdots x_r y = 1$ allows us to pass to an equivalent $\exists_{m+1}\mathcal{L}$-formula without inequations, i.e. with $r_i = 0$ for all i. Secondly, letting $H(X,Y)$ be the form obtained by homogenising a non-constant univariate polynomial without roots over K – which exists precisely because K is not algebraically closed – one can convert a system of two equations into one equation by using that for all $x, y \in K$ one has $x = 0 = y$ if and only if $H(x,y) = 0$. Repeated application of this trick allows us to assume that $q_i = 1$ in (2) for all i. Finally, a finite disjunction of equations can be converted into one equation by using that for $x, y \in K$ one has $x = 0$ or $y = 0$ if and only if $xy = 0$, which lets us reduce to $p = 1$. □

Remark 2.2. In the above statement, one can even conclude that B has a diophantine $\mathcal{L}_K$-definition with m quantifiers as soon as $m \geq 1$, see [4, Corollary 4.12].

3 Quaternion algebras

A *quaternion algebra* over K is by definition a 4-dimensional central simple K-algebra. It follows from Wedderburn's Theorem [15, Corollary 3.5.a] that such an algebra is either a division algebra, in which case we call it *non-split*, or isomorphic to the ring of 2×2 matrices over K, in which case we call it *split*. When Q is a quaternion algebra over K and L/K is a field extension, then $Q \otimes_K L$ is a quaternion algebra over L [18, 8.5.1]. We denote this algebra by Q_L and say that Q *splits over* L, or that L *splits* Q, if Q_L is split.

Given $a, b \in K$ with $b(1+4a) \neq 0$, we define the 4-dimensional K-algebra $[a,b)_K = K \oplus Ku \oplus Kv \oplus Kuv$ with $u^2 - u = a$, $v^2 = b$ and $uv + vu = v$. This is a K-quaternion algebra and one can show that all quaternion algebras over K are of this form for some a and b. (See [1, Section IX.10].)

Given $a, b \in K^\times$, we define the 4-dimensional K-algebra $(a,b)_K = K \oplus Ki \oplus Kj \oplus Kij$ with $i^2 = a, j^2 = b$ and $ij + ji = 0$. If $\mathrm{char}(K) \neq 2$ this is a K-quaternion algebra and one can show that all quaternion algebras over K are of this form for some a and b. Furthermore, one has $[a,b)_K \cong (1+4a, b)_K$ by mapping v to j and u to $\frac{i+1}{2}$. (See [1, Section IX.10])

We denote by Trd and Nrd the *reduced trace map* and the *reduced norm map* on Q respectively. See [18, Section 8.5] for basic properties of these two functions. If $Q = [a,b)_K$ and $x = x_1 + x_2 u + x_3 v + x_4 uv$ for some $x_1, \dots, x_4 \in K$, then one has

$$\mathrm{Trd}(x) = 2x_1 + x_2 \quad \text{and} \quad \mathrm{Nrd}(x) = x_1^2 + x_1 x_2 - a x_2^2 - b(x_3^2 + x_3 x_4 - a x_4^2).$$

If $Q = (a,b)_K$, $\mathrm{char}(K) \neq 2$ and $x = x_1 + x_2 i + x_3 j + x_4 ij$ for $x_1, \dots, x_4 \in K$, then

$$\mathrm{Trd}(x) = 2x_1 \quad \text{and} \quad \mathrm{Nrd}(x) = x_1^2 - a x_2^2 - b x_3^2 + ab x_4^2.$$

Here are some results on quaternion algebras that will be used later.

Proposition 3.1. *Let K be a field, $a, b \in K$.*

1. *Assume* $b(1+4a) \neq 0$. *The quaternion algebra* $[a,b)_K$ *is split if and only if* $b = x^2 + xy - ay^2$ *for some* $x, y \in K$.

2. *Assume* $ab \neq 0$ *and* $\mathrm{char}(K) \neq 2$. *The quaternion algebra* $(a,b)_K$ *is split if and only if* $b = x^2 - ay^2$ *for some* $x, y \in K$.

Proof. See [1, Theorem IX.10.26 and Theorem IX.10.27]. □

PROPOSITION 3.2. *Let* K *be a field and* Q *a quaternion algebra over* K. *Suppose* $d \in K$ *is such that the splitting field of* $X^2 - X - d$ *splits* Q. *Then there exists* $b \in K$ *such that* $Q \cong [d,b)_K$.

Proof. One can easily see that $\mathbb{M}_2(K) \cong [d,1)_K$ by considering the matrices

$$u = \begin{bmatrix} 0 & d \\ 1 & 1 \end{bmatrix} \quad \text{and} \quad v = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$$

and verifying that they satisfy $u^2 - u = d$, $v^2 = 1$ and $uv + vu = v$. Thus when Q is split, we can set $b = 1$. If Q is non-split, the result can be derived from a straightforward application of the Skolem-Noether theorem, see e.g. [15, Proposition 15.1.a]. □

LEMMA 3.3. *For any* $a, b \in \mathbb{R}$ *with* $b \neq 0$, $[a^2, b)_{\mathbb{R}}$ *is split.*

Proof. We have $[a^2,b)_{\mathbb{R}} \cong (1+4a^2, b)_{\mathbb{R}}$ and $1 + 4a^2$ is a square in $\mathbb{R}$. Now invoke Proposition 3.1. □

4 LOCAL AND GLOBAL FIELDS

By a *local field* we will mean the fraction field of a complete discrete valuation ring with finite residue field. We call the corresponding $\mathbb{Z}$-valuation on this field the *canonical valuation* of the local field. Note that a finite extension of a local field is again local. The reader is referred to [8] for an overview on valuation theory.

PROPOSITION 4.1. *Let* K *be a local field. Let* v *be its canonical valuation and let* F *be the residue field.*

(a) If $\mathrm{char}(F) \neq 2$ *and* $a, b \in K^\times$ *are such that* $(a,b)_K$ *is a division algebra, then at least one of* $v(a)$ *and* $v(b)$ *is odd.*

(b) If $a, b \in K$ *are such that* $b(1+4a) \neq 0$ *and* $[a,b)_K$ *is a division algebra, then* $v(a) \leq 0$. *If additionally* $v(a) = 0$, *then at least one of* $v(1+4a)$ *and* $v(b)$ *is odd.*

Proof. We denote by $\mathcal{O}$ the valuation ring of v and by $\mathfrak{m}$ its maximal ideal.
Assume $\mathrm{char}(F) \neq 2$ and that $v(a)$ and $v(b)$ are both even; after multiplying a and b with a square – which does not change the isomorphism class of $(a,b)_K$ – we may assume $v(a) = v(b) = 0$. Then a and b are non-zero modulo $\mathfrak{m}$, whereby the equation

$b = X^2 - aY^2$ has a solution modulo $\mathfrak{m}$ [13, 62:1] and by Hensel's Lemma [8, Theorem 1.3.1] it then has a solution over K, whence $(a,b)_K$ is split by Proposition 3.1. This shows part (a).
If $\mathrm{char}(F) \neq 2$, then also $\mathrm{char}(K) \neq 2$, whereby $[a,b)_K \cong (1+4a,b)_K$ and part (b) follows from part (a): if $v(a) > 0$, then $1+4a$ is a square in K by Hensel's Lemma. Assume for the rest of the proof that $\mathrm{char}(F) = 2$.
We may multiply b by a square and assume without loss of generality that $v(b) \in \{0,1\}$. If either $v(a) > 0$ or $v(a) = v(b) = 0$, then we can find a non-zero $y \in \mathcal{O}$ such that $a + by^2 \equiv 0 \bmod \mathfrak{m}$, as F is a finite field and of characteristic 2, whereby every element of $\mathcal{O}$ is a square modulo $\mathfrak{m}$. Then the polynomial $X^2 - X - a - by^2$ has a simple root modulo $\mathfrak{m}$; by Hensel's Lemma it then has a root in K, i.e. there exists an $x \in K$ with $0 = x^2 - x - a - by^2$ and thus

$$b = \left(\frac{x}{y}\right)^2 + \left(\frac{x}{y}\right)\left(\frac{-1}{y}\right) - a\left(\frac{-1}{y}\right)^2,$$

whereby $[a,b)_K$ is split in light of Proposition 3.1. □

PROPOSITION 4.2. *Let K be a local field with canonical discrete valuation ring $\mathcal{O}$ and residue field F. Let $d \in \mathcal{O}$ be such that $X^2 - X - d$ is irreducible over the residue field. Then for all $b \in K^\times$ we have that $[d,b)_K$ is split if and only if $v(b)$ is even.*

Proof. Note that $v(1+4d) = 0$, otherwise $X^2 - X - d$ would be reducible over the residue field. Hence, if $v(b)$ is even, it follows from Proposition 4.1 that $[d,b)_K$ is split.
The form $X^2 - XY - Y^2 d$ has no non-trivial zeroes over F. Thus the form can only represent elements of K of even value under v. Hence if $v(b)$ is odd, there cannot be $x, y \in K$ with $b = x^2 + xy - y^2 d$, whereby $[d,b)_K$ is non-split in light of Proposition 3.1. □

PROPOSITION 4.3. *Let K be a local field. For every quadratic field extension L/K and any quaternion algebra Q over K, Q_L is split.*

Proof. See [15, Section 17.10]. □

We call a finite extension of $\mathbb{Q}$ a *number field* and a function field in one variable over a finite field a *global function field*. By a *global field* we mean either a number field or a global function field.
Given a field K, we consider the set of $\mathbb{Z}$-valuations on K, which we denote by $\mathcal{V}_K$. Given $v \in \mathcal{V}_K$, we may denote by $\mathcal{O}_v$ the valuation ring of K corresponding to the valuation v and by $\mathfrak{m}_v$ the maximal ideal of $\mathcal{O}_v$. We write K_v for the fraction field of the completion of $\mathcal{O}_v$.
Note that if K is a global field, then the completion of any discrete valuation ring has a fraction field which is a local field. Furthermore, for all $x \in K^\times$ there exist only finitely many $v \in \mathcal{V}_K$ with $v(x) \neq 0$.
Given a quaternion algebra Q defined over a field K, we call Q *nonreal* if Q is split over every real closure of K. By definition, if K does not have real closures, all

quaternion algebras over Q are nonreal. A quaternion algebra Q over a global field is nonreal if and only if Q is split over every embedding into $\mathbb{R}$.
Let Q be a quaternion algebra over K. We define the *ramification set* of Q as

$$\Delta Q = \{v \in \mathcal{V}_K \mid Q_{K_v} \text{ is not split}\}.$$

The sets $\Delta_{a,b}$ from the introduction (for $a, b \in \mathbb{Q}^\times$) correspond to $\Delta((a,b)_{\mathbb{Q}})$ in this new notation.

THEOREM 4.4 (Albert-Brauer-Hasse-Noether). *Let K be a global field and Q a nonreal quaternion algebra over K. Then $\Delta Q = \emptyset$ if and only if Q is split.*

Proof. See [12, Theorem 8.1.17]. □

THEOREM 4.5 (Hilbert Reciprocity). *Let K be a global field. If Q is a nonreal quaternion algebra over K, then $|\Delta Q| \in 2\mathbb{N}$. Conversely, given any subset $S \subseteq \mathcal{V}_K$ with $|S| \in 2\mathbb{N}$, there exists a nonreal quaternion algebra Q over K with $\Delta Q = S$.*

Proof. See [12, Theorem 8.1.17]. □

We can derive a more explicit form of the second part of the last theorem.

COROLLARY 4.6. *Let K be a global field. Let $S \subseteq \mathcal{V}_K$ be such that $|S| \in 2\mathbb{N}$. Let $d \in K$ be such that $1 + 4d \neq 0$ and suppose that for all $v \in S$, the polynomial $X^2 - X - d$ is irreducible over K_v. Then there exists $b \in K^\times$ such that $\Delta([d,b)_K) = S$ and $[d,b)_K$ is nonreal.*

Proof. By Theorem 4.5 there exists a nonreal K-quaternion algebra Q such that $\Delta Q = S$. Let L be the splitting field of $X^2 - X - d$ over K. Clearly Q_L is again nonreal. We show that $\Delta(Q_L) = \emptyset$; this implies via Theorem 4.4 that Q_L splits, and then the statement follows from Proposition 3.2.
Consider a $\mathbb{Z}$-valuation w of L. Then $L_w \cong LK_v$ for some $\mathbb{Z}$-valuation v of K. If $v \notin S$, then by the choice of Q, Q_{K_v} is split, so also Q_{L_w} is split. On the other hand, if $v \in S$, L_w/K_v is a quadratic extension by the assumption that $X^2 - X - d$ is irreducible over $K_\mathfrak{p}$. Proposition 4.3 then implies that L_w splits Q. We conclude that, for all $\mathbb{Z}$-valuations w of L, Q_{L_w} is split. This shows that $\Delta(Q_L) = \emptyset$. □

For later use, we also mention an instance of the classical Weak Approximation Theorem from valuation theory.

THEOREM 4.7 (Weak Approximation). *Let K be a field, $v_1, \ldots, v_n$ pairwise distinct $\mathbb{Z}$-valuations on K. Then for any $a_1, \ldots, a_n \in K$ and $\gamma_1, \ldots, \gamma_n \in \mathbb{Z}$ there exists an $x \in K$ with*

$$v_i(x - a_i) > \gamma_i \quad \text{for all } i \in \{1, \ldots, n\}.$$

Proof. See [8, Theorem 2.4.1]; using that distinct $\mathbb{Z}$-valuations are trivially independent by [8, Corollary 2.3.2]. □

5 SEMILOCAL SUBRINGS

Let Q, Q' be quaternion algebras over K and L/K a quadratic field extension. Consider the following subsets of K:

$$S(Q) = \{\mathrm{Trd}(x) \mid x \in Q \setminus K, \mathrm{Nrd}(x) = 1\},$$
$$T(Q, Q') = \bigcap\{\mathcal{O}_v \mid v \in \Delta(Q) \cap \Delta(Q')\}.$$

We will write $T(Q)$ instead of $T(Q, Q)$. We will see that these sets have good $\exists\mathcal{L}_K$-definitions (see Lemma 5.2). They were introduced in the context of defining subrings of global fields by Poonen in [16] and Koenigsmann in [11].
Throughout this article, when dealing with subsets of a field K, we take the convention that $\bigcap \emptyset = K$.

THEOREM 5.1. *Let Q, Q' be nonreal quaternion algebras over a global field K. Then*

$$T(Q, Q') = S(Q) + S(Q').$$

Proof. In [5, Proposition 2.9] a proof is given in the case $Q = Q'$; by inspection one sees how the proof can be easily modified to cover the general case. □

For a subset A of a field K, denote $A^{-1} = \{x \in K^\times \mid x^{-1} \in A\}$ and $A^\times = A \cap A^{-1}$.

LEMMA 5.2. *There exist $\exists_7\mathcal{L}$-formulas $\varphi_1, \varphi_2, \varphi_3$ in the variables (X, A, B, A', B') such that, for all global fields K and for all $a, b, a', b' \in K$ with $(1 + 4a)b'(1 + 4a')b' \neq 0$ and such that $[a, b)_K$ and $[a', b')_K$ are nonreal, we have*

$$T([a, b)_K, [a', b')_K) = \{x \in K \mid K \models \varphi_1(x, a, b, a', b')\},$$
$$T([a, b)_K, [a', b')_K)^{-1} = \{x \in K \mid K \models \varphi_2(x, a, b, a', b')\},$$
$$T([a, b)_K, [a', b')_K)^\times = \{x \in K \mid K \models \varphi_3(x, a, b, a', b')\}.$$

Proof. By the formulas for reduced trace and norm given in the third section, we have for $a, b \in K$ with $(1 + 4a)b \neq 0$ that

$$S([a, b)_K) = \left\{ t \in K \;\middle|\; \begin{array}{l} \exists x_1, x_3, x_4 \in K : (x_1^2 + x_1(t - 2x_1) - a(t - 2x_1)^2 \\ -b(x_3^2 + x_3x_4 - ax_4^2) = 1) \end{array} \right\}.$$

Thus there is an $\exists_3\mathcal{L}$-formula taking a and b as parameters defining $S([a, b)_K)$. As such, there is an $\exists_7\mathcal{L}$-formula φ_1 defining $T([a, b)_K, [a', b')_K)$, since for $x \in K$ one has

$$x \in T([a, b)_K, [a', b')_K) \Leftrightarrow \exists y \in K : (y \in S([a, b)_K) \text{ and } x - y \in S([a', b')_K)).$$

To find φ_2, one expresses that $x \neq 0$, subtitutes $\frac{1}{x}$ for x into φ_1 and then clears denominators. For φ_3, it suffices to express that $x \neq 0$, substitute $\frac{x^2+1}{x}$ for x in φ_1

and clear denominators. Indeed we have for nonreal quaternion algebras $Q = [a, b)_K$ and $Q' = [a', b')_K$ that

$$T(Q, Q')^\times = \bigcap \{\mathcal{O}_v^\times \mid v \in \Delta(Q) \cap \Delta(Q')\}.$$

For a valuation $v \in \mathcal{V}_K$ and $x \in K^\times$, it is easy to see that $x \in \mathcal{O}_v^\times$ if and only if $\frac{x^2+1}{x} \in \mathcal{O}_v$. Hence $x \in T(Q, Q')^\times$ if and only if $\frac{x^2+1}{x} \in T(Q, Q')$. □

PROPOSITION 5.3. *Let K be a global field. Let S be a non-empty, finite subset of $\mathcal{V}_K$. Then the subsets $\bigcap_{v\in S} \mathcal{O}_v$ and $\bigcap_{v\in S} \mathcal{O}_v^\times$ have $\exists_7\mathcal{L}_K$-definitions.*

Proof. We can find two finite sets $S_1, S_2 \subseteq \mathcal{V}_K$ of even cardinality such that $S_1 \cap S_2 = S$; by Theorem 4.5 we can find nonreal K-quaternion algebras Q_1 and Q_2 such that $\Delta(Q_1) = S_1$ and $\Delta(Q_2) = S_2$. We obtain that $\bigcap_{v\in S} \mathcal{O}_v = T(Q_1, Q_2)$; by Lemma 5.2 this set and $T(Q_1, Q_2)^\times$ have an $\exists_7\mathcal{L}_K$-definition. □

For $c \in K^\times$, we define the following finite subsets of $\mathcal{V}_K$:

$$\mathsf{Odd}(c) = \{v \in \mathcal{V}_K \mid v(c) \text{ is odd}\}$$
$$\mathsf{Neg}(c) = \{v \in \mathcal{V}_K \mid v(c) < 0\}.$$

For a quaternion algebra Q over K and an element $c \in K^\times$ we define the following subsets of K:

$$\square K = \{x \in K \mid \exists y \in K : x = y^2\},$$
$$J^c(Q) = \bigcap \{\mathfrak{m}_v \mid v \in \Delta Q \cap \mathsf{Odd}(c)\},$$
$$H^c(Q) = \bigcap \{\mathfrak{m}_v^{-v(c)} \mid v \in \Delta Q \cap \mathsf{Neg}(c)\}.$$

The sets $J^c_{a,b}$ from the introduction (for $a, b, c \in \mathbb{Q}^\times$) correspond to $J^c((a, b)_\mathbb{Q})$ in this notation. The sets $H^c(Q)$ will in the end only play a role when considering global fields of characteristic 2, but in this section we make no assumptions on the characteristic.

LEMMA 5.4. *Let K be a field, $S \subseteq \mathcal{V}_K$ finite , $R = \bigcap_{v\in S} \mathcal{O}_v$. For $c \in K^\times$ we have*

$$(c \cdot \square K \cap (1 - \square K \cdot R^\times)) \cdot R = \bigcap \{\mathfrak{m}_v \mid v \in S \cap \mathsf{Odd}(c)\},$$
$$(c^{-1} \cdot R + c \cdot R^{-1})^{-1} \cup \{0\} = \bigcap \{\mathfrak{m}_v^{-v(c)} \mid v \in S \cap \mathsf{Neg}(c)\}.$$

Proof. First we observe that, by Weak Approximation, we have

$$\square K \cdot R^\times = \bigcap_{v\in S} v^{-1}(2\mathbb{Z}).$$

Let $x \in K^\times$ be arbitrary. Let us consider $v \in S \cap \mathsf{Odd}(c)$. If $x \in c \cdot \square K$ then $v(x)$ is odd, and if additionally $x \in 1 - \square K \cdot R^\times$, then it follows that $v(x)$ is strictly positive.

Therefore if $x \in c \cdot \square K \cap (1 - \square K \cdot R^\times)$, then $x \in \bigcap\{\mathfrak{m}_v \mid v \in S \cap \mathsf{Odd}(c)\}$, whereby also $Rx \subseteq \bigcap\{\mathfrak{m}_v \mid v \in S \cap \mathsf{Odd}(c)\}$. This proves the left-to-right inclusion in the first equality.
For the other inclusion, let us consider $x \in \bigcap\{\mathfrak{m}_v \mid v \in S \cap \mathsf{Odd}(c)\}$. By Weak Approximation, there exists $z \in K$ such that for all $v \in S \cap \mathsf{Odd}(c)$ we have $v(cz^2) = 1$ and for all $v \in S \setminus \mathsf{Odd}(c)$ we have $v(cz^2) < \min\{0, v(x)\}$. Then $cz^2 \in (c \cdot \square K \cap (1 - \square K \cdot R^\times))$ and $v(cz^2) < v(x)$ for all $v \in S$, whereby $\frac{x}{cz^2} \in R$. Thus we have $x \in (c \cdot \square K \cap (1 - \square K \cdot R^\times)) \cdot R$.
We now give a proof of the second equality. Let $x \in (c^{-1}R + cR^{-1})^{-1}$. Then $x^{-1} = c^{-1}t' + ct^{-1}$ for some $t' \in R$, $t \in R \setminus \{0\}$. For $v \in S \cap \mathsf{Neg}(c)$, we have $R \subseteq \mathcal{O}_v$, $v(c^{-1}t') = -v(c) + v(t') > 0$ and $v(ct^{-1}) = v(c) - v(t) < 0$, hence

$$v(x^{-1}) = \min\{v(c^{-1}t'), v(ct^{-1})\} = v(c) - v(t) \leq v(c),$$

whereby $v(x) \geq -v(c)$. This shows the left-to-right inclusion of the second equality in the statement.
Now let $x \in \bigcap\{\mathfrak{m}^{-v(c)} \mid v \in S \cap \mathsf{Neg}(c)\}$ with $x \neq 0$. Then $v(x) \geq -v(c) > 0$ for all $v \in S \cap \mathsf{Neg}(c)$. We will show that for any $v \in S$ we can find $t_v, t'_v \in \mathcal{O}_v$ with $t_v \neq 0$ such that $t'_v = cx^{-1} - c^2 t_v^{-1}$. Once this is shown, it follows by Weak Approximation that there exist $t, t' \in \bigcap_{v \in S} \mathcal{O}_v = R$, $t \neq 0$ such that $t' = cx^{-1} - c^2 t^{-1}$, whereby we will have that $x = (c^{-1}t' + ct^{-1})^{-1}$, as we want to show.
Let us consider $v \in S$. Assume first that $v(x) \geq -v(c)$. In this case we take $t_v = xc$ and $t'_v = 0$. Now suppose that $v(x) < -v(c)$. By our assumption on x this is only possible when $v(c) \geq 0$. In this case we take $t_v = 1$ and $t'_v = c(x^{-1} - c)$. □

PROPOSITION 5.5. *There exist an $\exists_{16}\mathcal{L}$-formula $\phi_1(X, A, B)$ and an $\exists_{15}\mathcal{L}$-formula ϕ_2 in the variables (X, A, B) such that, for all global fields K and $a, b, c \in K$ with $(1 + 4a)bc \neq 0$ such that $[a, b)_K$ is nonreal, we have*

$$J^c([a, b)_K) = \{x \in K \mid K \models \phi_1(x, a, b, c)\},$$
$$H^c([a, b)_K) = \{x \in K \mid K \models \phi_2(x, a, b, c)\}.$$

Proof. By Lemma 5.4 we have that

$$J^c([a, b)_K) = (c \cdot \square K \cap (1 - \square K \cdot T([a, b)_K)^\times)) \cdot T([a, b)_K),$$
$$H^c([a, b)_K) = (c^{-1} \cdot T([a, b)_K) + c \cdot T([a, b)_K)^{-1})^{-1} \cup \{0\}.$$

For $x \in K$ we have that $x \in \square K \cdot T([a, b)_K)^\times$ if and only if

$$\exists q \in K^\times : xq^2 \in T([a, b)_K)^\times \cup \{0\}$$

which by Lemma 5.2 can be described with an $\exists_8\mathcal{L}$-formula.
For $x \in K$ we have that $x \in J^c([a, b)_K)$ if and only if

$$\exists y \in K^\times : \frac{x}{cy^2} \in T([a, b)_K) \text{ and } 1 - cy^2 \in \square K \cdot T([a, b)_K)^\times.$$

Hence, invoking Lemma 5.2 and clearing denominators to express that $\frac{x}{cy^2} \in T([a,b)_K)$, we find an $\exists_{16}\mathcal{L}$-formula for ϕ_1.
To see that $H^c(Q_{a,b})$ can be described with an $\exists_{15}\mathcal{L}$-formula, note that for $x \in K^\times$ we have that $x \in H^c([a,b)_K)$ if and only if

$$\exists y \in K^\times : cy \in T([a,b)_K) \text{ and } \frac{1-xy}{cx} \in T([a,b)_K)^{-1},$$

and then invoke Lemma 5.2 and clear denominators. □

6 RINGS OF S-INTEGERS

For the remainder of this article, let K be a global field. For a set $S \subseteq \mathcal{V}_K$, we define the set

$$\mathcal{O}_S = \{x \in K \mid \forall v \in \mathcal{V}_K \setminus S : v(x) \geq 0\} = \bigcap_{v \in \mathcal{V}_K \setminus S} \mathcal{O}_v.$$

If S is a finite set, we call $\mathcal{O}_S$ *the ring of S-integers*.

PROPOSITION 6.1. *Let $V \subseteq \mathcal{V}_K$ be non-empty. Suppose that the set $\bigcup_{v\in V} \mathfrak{m}_v$ has a $\exists_n\mathcal{L}_K$-definition. Then $\bigcap_{v\in V} \mathcal{O}_v$ has a $\forall_n\mathcal{L}_K$-definition.*

Proof. This follows from the observation that

$$\bigcap_{v\in V} \mathcal{O}_v = \left(K \setminus \left(\bigcup_{v\in V} \mathfrak{m}_v\right)^{-1}\right) \cup \{0\}.$$

□

COROLLARY 6.2. *Let $S \subseteq \mathcal{V}_K$ be finite and non-empty. Then $\bigcup_{v\in S} \mathfrak{m}_v$ has an $\exists_7\mathcal{L}_K$-definition and $\bigcap_{v\in S} \mathcal{O}_v$ has a $\forall_7\mathcal{L}_K$-definition in K.*

Proof. The second statement follows from the first one by Proposition 6.1. By Proposition 5.3, for every $v \in \mathcal{V}_K$, $\mathcal{O}_v$ has an $\exists_7\mathcal{L}_K$-definition. Then the same holds for $\mathfrak{m}_v$: fix an arbitrary $\pi \in \mathfrak{m}_v \setminus \mathfrak{m}_{(v)}^2$; we have $\mathfrak{m}_v = \pi\mathcal{O}_v$, whence $x \in \mathfrak{m}_v$ if and only if $\frac{x}{\pi} \in \mathcal{O}_v$. If every $\mathfrak{m}_v$ has an $\exists_7\mathcal{L}_K$-definition, then so does a finite union of such sets. □

We will show that for any finite set $S \subseteq \mathcal{V}_K$, there is an $\exists\mathcal{L}_K$-definition of

$$\bigcup_{v\in\mathcal{V}_K\setminus S} \mathfrak{m}_v$$

in K. From this we will obtain a $\forall\mathcal{L}_K$-definition of $\mathcal{O}_S$ via Proposition 6.1.
In particular, setting $S = \emptyset$, we find a universal definition of the ring of integers $\mathcal{O}_K$ in a number field K. However, even if one is only interested in the case $S = \emptyset$, it will be crucial in the proof to also allow S to be non-empty.

LEMMA 6.3. *Let $V \subseteq V' \subseteq \mathcal{V}_K$ and suppose that $V' \setminus V$ is finite. Assume that $\bigcup_{v\in\mathcal{V}_K\setminus V'} \mathfrak{m}_v$ has an $\exists_n\mathcal{L}_K$-definition. Then the set $\bigcup_{v\in\mathcal{V}_K\setminus V} \mathfrak{m}_v$ has an $\exists_m\mathcal{L}_K$-definition with $m = \max\{n, 7\}$.*

Proof. Since we know from Corollary 6.2 that $\bigcup_{v\in V'\setminus V} \mathfrak{m}_v$ has an $\exists_7\mathcal{L}_K$-definition, we obtain that the set $\bigcup_{v\in\mathcal{V}_K\setminus V} \mathfrak{m}_v$ has an $\exists_{\max\{n,7\}}\mathcal{L}_K$-definition by observing that

$$\bigcup_{v\in\mathcal{V}_K\setminus V} \mathfrak{m}_v = \bigcup_{v\in\mathcal{V}_K\setminus V'} \mathfrak{m}_v \cup \bigcup_{v\in V'\setminus V} \mathfrak{m}_v.$$

□

In particular, to prove that $\bigcup_{v\in\mathcal{V}_K\setminus S} \mathfrak{m}_v$ has an $\exists\mathcal{L}_K$-definition for all finite sets S, it is enough to show this for sufficiently large sets S of finite cardinality.
Let $S \subseteq \mathcal{V}_K$ be a non-empty finite set, and $u \in \bigcap_{v\in S} \mathcal{O}_v^\times$. Define the set

$$\Phi_u^S = \left\{ (a, b) \in K^2 \;\middle|\; b \in \bigcap_{v\in S} \mathcal{O}_v^\times, a \equiv u \bmod \prod_{v\in S} \mathfrak{m}_v \right\}.$$

LEMMA 6.4. *Let $S \subseteq \mathcal{V}_K$ be a non-empty finite set and $u \in \bigcap_{v\in S} \mathcal{O}_v^\times$. Then the set Φ_u^S has a $\exists_{14}\mathcal{L}_K$-definition in K^2.*

Proof. By Proposition 5.3 $\bigcap_{v\in S} \mathcal{O}_v^\times$ has a $\exists_7\mathcal{L}_K$-definition. By Weak Approximation, fix an element $\pi \in K^\times$ with $\pi \in \mathfrak{m}_v \setminus \mathfrak{m}_v^2$ for all $v \in S$. The condition that $a \equiv u \bmod \prod_{v\in S} \mathfrak{m}_v$ can be rewritten as $a - u \in \pi \bigcap_{v\in S} \mathcal{O}_v$. By Proposition 5.3 this can be described by an $\exists_7\mathcal{L}_K$-formula. This brings the total to $7 + 7 = 14$ quantifiers. □

LEMMA 6.5. *Let F be a finite field. There exists $u \in F$ such that $X^2 - X - u^2$ is irreducible over F.*

Proof. If $\mathrm{char}(F) = 2$, then every element is a square and the statement becomes trivial, as F has a separable quadratic extension. Suppose now that $\mathrm{char}(F) \neq 2$; we need to show that there exists $u \in F$ such that the discriminant $1+4u^2$ is not a square. To this end, take any $b \in F$ which is not a square. Using that every element is a sum of two squares in F [13, 62:1], write $b = c^2 + d^2$ for some $c, d \in F$. Then $u = \frac{d}{2c}$ does the trick, as $1 + 4u^2 = \frac{b}{c^2}$ is not a square. □

LEMMA 6.6. *Let K be a global field. Let $\pi \in K^\times$ be such that $S = \mathsf{Odd}(\pi)$ has odd cardinality. Let $u \in K^\times$ be such that for all $v \in S$, $v(u) = 0$ and $X^2 - X - u^2$ is irreducible over $\mathcal{O}_v/\mathfrak{m}_v$.*
If $\mathrm{char}(K) = 2$, then we have

$$\bigcup_{v\in\mathcal{V}_K\setminus S} \mathfrak{m}_v = \bigcup_{(a,b)\in\Phi_u^S} (J^b([a^2, b\pi)_K) \cap H^a([a^2, b\pi)_K)).$$

If $\mathrm{char}(K) \neq 2$ *and* S *contains all (finitely many) valuations* $v \in \mathcal{V}_K$ *with* $v(2) > 0$*, then we have*

$$\bigcup_{v \in \mathcal{V}_K \setminus S} \mathfrak{m}_v = \bigcup_{(a,b) \in \Phi_u^S} (J^{1+4a^2}([a^2, b\pi)_K) \cap J^b([a^2, b\pi)_K)).$$

Proof. We start by showing the right-to-left inclusion in both cases. Take an arbitrary $(a, b) \in \Phi_u^S$. By the definition of Φ_u^S we have for all $v \in S$ that $v(a) = 0$, $v(b\pi) = v(b) + v(\pi) \equiv 0 + 1 \bmod 2$ and $X^2 - X - a^2$ is irreducible over $\mathcal{O}_v/\mathfrak{m}_v$. It follows by Proposition 4.2 that $S \subseteq \Delta[a^2, b\pi)_K$. By Lemma 3.3 $[a^2, b\pi)_K$ is nonreal. As $|S|$ is odd, Hilbert Reciprocity (Theorem 4.5) tells us that there exists $w \in \Delta[a^2, b\pi)_K \setminus S$. By part (b) of Proposition 4.1 at least one of the following holds:

(i) $2w(a) = w(a^2) < 0$. In this case, $H^a([a^2, b\pi)_K) \subseteq \mathfrak{m}_w$.

(ii) $w(1 + 4a^2)$ is odd. In this case, $J^{1+4a^2}([a^2, b\pi)_K) \subseteq \mathfrak{m}_w$.

(iii) $w(b\pi)$ is odd, whereby $w(b)$ is odd (since $w \notin S = \mathsf{Odd}(\pi)$) and thus $J^b([a^2, b\pi)_K) \subseteq \mathfrak{m}_w$.

Note that case (ii) does not occur if $\mathrm{char}(K) = 2$. If case (i) occurs and $w(2) = 0$, then by part (a) of Proposition 4.1 also either (ii) or (iii) occurs. We conclude that $J^b([a^2, b\pi)_K) \cap H^a([a^2, b\pi)_K) \subseteq \mathfrak{m}_w$ if $\mathrm{char}(K) = 2$, and $J^b([a^2, b\pi)_K) \cap J^{1+4a^2}([a^2, b\pi)_K) \subseteq \mathfrak{m}_w$ if $w(2) = 0$. As this argument works for general $(a, b) \in \Phi_u^S$, this shows the right-to-left inclusion in each of the two cases.
To show the inclusion from left to right in both cases, it suffices to show that for any given $w \in \mathcal{V}_K \setminus S$ there exist $(a, b) \in \Phi_u^S$ such that $\Delta[a^2, b\pi)_K = S \cup \{w\}$. Indeed, having found such (a, b) one has for all $v \in S$ that $v(1 + 4a^2) = v(a) = v(b) = 0$, from which it follows that $\mathfrak{m}_w \subseteq J^{1+4a^2}([a^2, b\pi)_K) \cap J^b([a^2, b\pi)_K) \cap H^a([a^2, b\pi)_K)$. Given $w \in \mathcal{V}_K \setminus S$, by Lemma 6.5 and Weak Approximation there exists $a \in K^\times$ such that $a \equiv u \bmod \prod_{v \in S} \mathfrak{m}_v$, $w(a) = 0$ and $X^2 - X - a^2$ is irreducible over $\mathcal{O}_{(w)}/\mathfrak{m}_{(w)}$. By Corollary 4.6 we can find $b \in K^\times$ such that $\Delta[a^2, b\pi)_K = S \cup \{w\}$. Proposition 4.2 tells us that $v(b\pi) = v(b) + v(\pi)$ is odd for all $v \in S$, whereby $v(b)$ is even. Hence by Weak Approximation we may multiply b by an appropriate square and assume without loss of generality that $b \in \bigcap_{v \in S} \mathcal{O}_v^\times$. Then $(a, b) \in \Phi_u^S$ and $\Delta[a^2, b\pi)_K = S \cup \{w\}$, whereby we are done. □

LEMMA 6.7. *Let* K *be a global field,* $S \subseteq \mathcal{V}_K$ *finite. There exists* $\pi \in K^\times$ *such that* $S \subseteq \mathsf{Odd}(\pi)$ *and* $\mathsf{Odd}(\pi)$ *has odd cardinality.*

Proof. If needed, we enlarge S to be a set of even cardinality. It follows from results of class field theory - more specifically a generalisation of Dirichlet's theorem on arithmetic progressions as formulated e.g. in [2, A.10] - that there exist infinitely many $v \in \mathcal{V}_K$ such that $S \cup \{v\} = \mathsf{Odd}(\pi)$ for some $\pi \in K^\times$. □

THEOREM 6.8. *Let* K *be a global field and* S *a finite subset of* $\mathcal{V}_K$*. The set* $\bigcup_{v \in \mathcal{V}_K \setminus S} \mathfrak{m}_v$ *has an* $\exists\mathcal{L}_K$*-definition in* K*. Furthermore,* $\mathcal{O}_S$ *has a* $\forall\mathcal{L}_K$*-definition in* K*.*

Proof. By Lemma 6.7 there exists $\pi \in K^\times$ such that $S \subseteq S' = \mathsf{Odd}(\pi)$ and S' has odd cardinality. By Weak Approximation and Lemma 6.5 we can find $u \in K$ such that for all $v \in S'$ one has $v(u) = 0$ and $X^2 - X - u^2$ irreducible over $\mathcal{O}_v/\mathfrak{m}_v$.
By Proposition 5.5 and Lemma 6.4, the sets $\bigcup\{J^b([a^2, b\pi)_K) \cap H^a([a^2, b\pi)_K) \mid (a,b) \in \Phi_u^{S'}\}$ and $\bigcup\{J^{1+4a^2}([a^2, b\pi)_K) \cap J^b([a^2, b\pi)_K) \mid (a,b) \in \Phi_u^{S'}\}$ have $\exists\mathcal{L}_K$-definitions, hence by Lemma 6.6 one has that $\bigcup_{v\in\mathcal{V}_K\setminus S'} \mathfrak{m}_v$ has an $\exists\mathcal{L}_K$-definition. By Lemma 6.3 we know that also $\bigcup_{v\in\mathcal{V}_K\setminus S} \mathfrak{m}_v$ has an $\exists\mathcal{L}_K$-definition. The second part now follows from Proposition 6.1. □

Remark 6.9. A variation of Lemma 6.6 can be proven which does not require invoking additional results from class field theory (as in Lemma 6.7) to find an appropriate element π, but instead requires introducing another auxiliary parameter. This approach can be found in an earlier preprint of this article, available via https://arxiv.org/abs/1812.04372v4 (Lemma 6.6).

7 Quantifier count and optimisation

As explained in the proof of Theorem 6.8, the equality in Lemma 6.6 gives rise to an $\exists\mathcal{L}_K$-definition of $\bigcup_{v\in\mathcal{V}_K\setminus S} \mathfrak{m}_v$, which then leads to a $\forall\mathcal{L}_K$-definition of $\mathcal{O}_S$ via Proposition 6.1. We can count the number of quantifiers in the definition obtained:

1. By Proposition 5.5 the sets $J^d(Q_{a^2,b})$ (for $d = 1 + 4a^2, b$) and $H^a(Q_{a^2,b})$ can be defined with $\exists\mathcal{L}$-formulas with 16 and 15 quantifiers, respectively. This implies that the intersections
$$J^b([a^2, b\pi)_K) \cap J^{1+4a^2}([a^2, b\pi)_K) \quad \text{and} \quad J^b([a^2, b\pi)_K) \cap H^a([a^2, b\pi)_K)$$
can be defined with $16 + 16 = 32$ and $16 + 15 = 31$ quantifiers respectively.
2. By Lemma 6.4 the set Φ_u^S needs 14 quantifiers to define.
3. In total this yields a definition for
$$\bigcup_{v\in\mathcal{V}_K\setminus S} \mathfrak{m}_v$$
with $2 + 14 + 32 = 48$ quantifiers if $\mathrm{char}(K) \neq 2$, or $2 + 14 + 31 = 47$ quantifiers if $\mathrm{char}(K) = 2$.

This bound can be improved, using a result for reducing the number of quantifiers needed when taking a conjunction of existential formulas.

Theorem 7.1. *Let K be a field which is finitely generated over a perfect field. For any $m_1, m_2, n \in \mathbb{N}$ with $m_1, m_2 \geq 1$ and subsets $D_1, D_2 \subseteq K^n$ which are $\exists_{m_1}\mathcal{L}_K$-definable and $\exists_{m_2}\mathcal{L}_K$-definable respectively, the intersection $D_1 \cap D_2$ is $\exists_{m_1+m_2-1}\mathcal{L}_K$-definable.*

Proof. This is [4, Theorem 1.4]. In [19, Theorem 1.2] a special case of this result is shown for $K = \mathbb{Q}$ for the same purposes as we use it, yielding a very explicit formula. □

PROPOSITION 7.2. *The set $\bigcup_{v\in\mathcal{V}_K\setminus S}\mathfrak{m}_v$ has an $\exists_{37}\mathcal{L}_K$-definition in K. When $\mathrm{char}(K) = 2$, it also has an $\exists_{36}\mathcal{L}_K$-definition in K.*

Proof. This follows by going through the quantifier count at the beginning of the section and applying Theorem 7.1 every time a conjunction of existential formulas is taken in the construction. This means that consecutively Lemma 5.2, Proposition 5.3, Proposition 5.5 and Lemma 6.4 need to be reproven to obtain the required number of quantifiers. In particular, the sets $T([a^2, b)_K)$ are $\exists_6\mathcal{L}_K$-definable, and the sets $J^d([a^2, b)_K)$ and $H^a([a^2, b)_K)$ are $\exists_{13}\mathcal{L}_K$-definable and $\exists_{12}\mathcal{L}_K$-definable respectively. A finite intersection of valuation rings $\bigcap_{v\in S}\mathcal{O}_v$ is $\exists_6\mathcal{L}_K$-definable, whereby Φ_u^S is $\exists_{11}\mathcal{L}_K$-definable. The reader can verify these claims and that these eventually lead to the claimed number of quantifiers by counting the number of times conjunctions of existential formulas are taken in the construction of all these formulas. □

8 FINITELY GENERATED SUBRINGS

Theorem 6.8 shows us that rings of S-integers (with $S \subseteq \mathcal{V}_K$ finite) have a universal definition in their fraction field. What follows is a sketch on how to obtain from this a universal definition for any finitely generated ring in its global fraction field K.
For the rest of this section, let R be a domain with a global field K as its fraction field. Let R' be the integral closure of R in K.

LEMMA 8.1. *Let $S = \{v \in \mathcal{V}_K \mid R \not\subseteq \mathcal{O}_v\}$. The following hold:*

1. *For any non-zero ideal I of R, R/I is a finite ring.*
2. *$R' = \mathcal{O}_S$.*

Furthermore, if R is finitely generated, then the set S is finite.

Proof. Let $p = \mathrm{char}(K)$. Set $R_0 = \mathbb{Z}$ if $p = 0$; if $p > 0$, let R_0 be a fixed subring of R isomorphic to $\mathbb{F}_p[T]$. Let $K_0 = \mathrm{Frac}(R_0)$. Note that R_0 is a principal ideal domain and K/K_0 is a finite extension; by the Krull-Akizuki Theorem [3, Proposition VII.2.5.5] R is a noetherian ring of Krull dimension 1 and R' is a Dedekind domain. Furthermore, for any non-zero ideal I of R, $I_0 = I \cap R_0$ is non-zero and R/I is a finitely generated R_0/I_0-module. But R_0/I_0 is a finite ring, whereby also R/I is finite. This concludes the proof of the first part.
Clearly by definition $R \subseteq \mathcal{O}_S$ and hence also $R' \subseteq \mathcal{O}_S$, as the latter is integrally closed. Since R' is a Dedekind domain, it is the intersection of the discrete valuation rings in which it is contained [9, Proposition 2.1]; hence $R' = \mathcal{O}_S$ by construction.
Finally, assume that R is generated as a ring by $b_1, \ldots, b_n \in K$. Then S consists precisely of those $v \in \mathcal{V}_K$ for which $v(b_i) < 0$ for at least one $i \in \{1, \ldots, n\}$. There are only finitely many such valuations. □

Remark 8.2. One can show that an integral domain with global fraction field K is finitely generated if and only if it is contained in $\mathcal{O}_S$ for some finite set $S \subseteq \mathcal{V}_K$.

LEMMA 8.3. *Assume that R is finitely generated. There exists $r \in R \setminus \{0\}$ such that $rR' \subseteq R$.*

Proof. As R is finitely generated as a $\mathbb{Z}$-algebra, its integral closure R' is finitely generated as an R-module [10, Corollary 7.7.4]. Let $R' = Ra_1 + \ldots + Ra_n$ for $a_1, \ldots, a_n \in R'$. Since R and R' have the same fraction field, we have that for all i, there exists an $r_i \in R \setminus \{0\}$ such that $r_i a_i \in R$; setting $r = r_1 \cdots r_n$ now yields $rR' \subseteq R$. □

THEOREM 8.4. *Assume that R is finitely generated. Then R has a $\forall\mathcal{L}_K$-definition in K.*

Proof. By Lemma 8.3 there exists an $r \in R \setminus \{0\}$ such that $rR' \subseteq R$. As rR' is a non-zero ideal of R, R/rR' is finite by the first part of Lemma 8.1. Thus, there exist $y_1, \ldots, y_n \in R$ such that $R = \bigcup_{i=1}^{n}(y_i + rR')$. We have by the second part of Lemma 8.1 that R' is a ring of S-integers; it follows from Theorem 6.8 that it has a $\forall\mathcal{L}_K$-definition in K. Since a finite union of $\forall\mathcal{L}_K$-definable sets is again $\forall\mathcal{L}_K$-definable; we conclude that R is $\forall\mathcal{L}_K$-definable in K. □

Remark 8.5. This method does not give us any uniform bound on the number of quantifiers needed to define a finitely generated subring of a global field in its fraction field. To see that this is the case, consider for a non-zero $n \in \mathbb{N}$ the subring $\mathbb{Z}[ni]$ of $\mathbb{Q}[i]$ where $i^2 = -1$. Then the integral closure of $\mathbb{Z}[ni]$ in $\mathbb{Q}[i]$ is $\mathbb{Z}[i]$. One verifies that

$$\forall r \in \mathbb{Z}[i] : (r\mathbb{Z}[i] \subseteq \mathbb{Z}[ni] \Rightarrow |\mathbb{Z}[ni]/r\mathbb{Z}[i]| \geq n).$$

Indeed, whenever $r \in \mathbb{Z}[i]$ satisfies $a\mathbb{Z}[i] \subseteq \mathbb{Z}[ni]$, then we must have $r \in n\mathbb{Z}[i]$. And $|\mathbb{Z}[ni]/n\mathbb{Z}[i]| = n$. If $\mathbb{Z}[i]$ has a $\forall_m\mathcal{L}_{\mathbb{Q}[i]}$-definition in $\mathbb{Q}[i]$, the technique from Theorem 8.4 gives us a $\forall_{nm}\mathcal{L}_{\mathbb{Q}[i]}$-definition for $\mathbb{Z}[ni]$ in $\mathbb{Q}[i]$.

QUESTION 8.6. *Can we give a uniform bound on the number of quantifiers needed to universally define a finitely generated subring of a global field in its fraction field?*

QUESTION 8.7. *Let R be a finitely generated domain. Does R have a universal definition in its fraction field?*

REFERENCES

[1] Albert, A. A., *Structure of Algebras*. American Mathematical Society, 1939.

[2] Bass, H., Milnor, J., and Serre, J.-P., Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_n ($n \geq 2$). *Inst. Hautes Études Sci. Publ. Math. 33* (1967), 59–137.

[3] Bourbaki, N., *Algèbre Commutative: Chapitres 5 à 7*. Éléments de Mathématique. Springer, 2006.

[4] Daans, N., Dittmann, P., and Fehm, A., Existential rank and essential dimension of diophantine sets, preprint, 2021, arXiv:2102.06941.

[5] Dittmann, P., Irreducibility of polynomials over number fields is diophantine. *Compos. Math. 154* (2018), 761–772.

[6] Ebbinghaus, H.-D., Flum, J., and Thomas, W., *Mathematical Logic*, second ed. Springer, 1994.

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

[8] Engler, A. J. and Prestel, A., *Valued Fields.* Springer, 2005.

[9] Fröhlich, A., Chapter 1: Local fields. In *Algebraic Number Theory*. Academic Press Inc. (London) Ltd., 1967, 1–42.

[10] Grothendieck, A., *Éléments de Géometrie Algébrique. IV: Étude locale des schémas et des morphismes de schémas*. (Séconde partie) (rédigés avec la collaboration de Jean Dieudonné). Publications Mathémathiques de l'I.H.É.S., 1965.

[11] Koenigsmann, J., Defining $\mathbb{Z}$ in $\mathbb{Q}$. *Ann. Math. (2) 183* (2016), no. 1, 73–93.

[12] Neukirch, J., Schmidt, A., and Wingberg, K., *Cohomology of Number Fields*, second ed. Springer, 2008.

[13] O'Meara, T., *Introduction to Quadratic Forms*. Springer, 2000.

[14] Park, J., A universal first-order formula defining the ring of integers in a number field. *Math. Res. Lett. 20* (2013), no. 5, 961–980.

[15] Pierce, R. S., *Associative Algebras*. Springer, 1982.

[16] Poonen, B., Characterizing integers among rational numbers with a universal-existential formula. *Amer. J. Math. 131* (2009), 675–682.

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

[18] Scharlau, W., *Quadratic and Hermitian Forms*. Springer, 1985.

[19] Zhang, G.-R. and Sun, Z.-W., $\mathbb{Q} \setminus \mathbb{Z}$ is diophantine over $\mathbb{Q}$ with 32 unknowns, preprint, 2021, arXiv:2104.02520.

Nicolas Daans
Universiteit Antwerpen
Departement Wiskunde
Campus Middelheim - G, M.G.105
Middelheimlaan 1
2020 Antwerpen
Belgium
nicolas.daans@uantwerpen.be