Efforts in the Direction of Hilbert's Tenth Problem

Brian Tyrrell

St Peter's College

University of Oxford

Supervisor: Professor Damian Rössler

A thesis submitted for the degree of

Master of Science, Mathematics and Foundations of Computer Science

August 2018

Dedicated to the memory of Philip Dunphy.

Acknowledgements

First and foremost I'd like to thank my supervisor, Professor Damian Rössler, for his advisement and support over the last 5 months. I would also like to thank Professor Jochen Koenigsmann for encouraging me to study this area and for his mathematical insights and assistance along the way. Thanks to Nicolas Daans for sharing his ideas regarding universal definitions of global fields, and for sharing his thoughts on my thesis too.

My thanks to my parents for supporting me in everything I do; I will always appreciate your unwavering encouragement. Finally I would like to extend my thanks to the University of Oxford and the Mathematics department for having the resources available allowing me to undertake this project.

Abstract

The thesis we propose works to highlight efforts that have been made to determine the definability of $\mathbb{Z}$ in $\mathbb{Q}$. This is a gap yet to be fully filled in the field developed around (the open question of) Hilbert's 10th Problem over $\mathbb{Q}$.

Koenigsmann's recent paper on *Defining* $\mathbb{Z}$ *in* $\mathbb{Q}$ has contributed in three ways to the discussion of the definability of $\mathbb{Z}$ in $\mathbb{Q}$. It gives a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$, a $\forall\exists$-definition of $\mathbb{Z}$ in $\mathbb{Q}$, and a proof that the *Bombieri-Lang Conjecture* implies there is no existential definition of $\mathbb{Z}$ in $\mathbb{Q}$. The former two results have been translated to global function fields by Eisenträger & Morrison and Shlapentokh, respectively, however an existential definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ has yet to be realised.

In the course of this thesis we shall outline our interest in the relationship between $\mathbb{Z}$ and $\mathbb{F}_q[t]$, and motivate the definability questions from the perspective of Hilbert's 10th Problem. We will then excurse through the work of the aforementioned authors and their ilk and, finally, provide a shorter and simpler universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ than currently exists.

Contents

Chapter 1

Introduction

1.1 Hilbert's Tenth Problem

When originally posed by David Hilbert in 1900, his tenth problem took the following form [Hil00]:

> "Eine Diophantische Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.
>
> *Let a diophantine equation with any number of variables and with rational integer coefficients be given: one should present a procedure after which, by means of a finite number of operations, it can be decided whether the equation is solvable in rational integers.*"

In a more modern formulation, the problem is considered to be the following:

Problem. *Find an algorithm which takes as input any polynomial* $f \in \mathbb{Z}[x_1, \ldots, x_n]$ *and decides whether* $f(x_1, \ldots, x_n) = 0$ *has solutions in* $\mathbb{Z}^n$.

Number 10 in Hilbert's list of 23 problems published after his famous address to the International Congress of Mathematicians, these represented the pinnacle of unsolved mathematics and have had significant impact on the development of mathematics in the last century. Indeed, 70 years passed before Hilbert's 10th Problem (H10) was finally laid to rest. So strong was Hilbert's conviction that "*wir müssen wissen, wir werden wissen*"[1] he formulated his tenth problem to ask for the *presentation* of an

[1] "we must know, we will know".

algorithm; so it is remarkably significant and astounding that when Matiyasevich [Mat70] finally solved this problem in 1970, he answered it in the negative. The algorithm does not exist[2].

This result is colloquially known as the "DPRM Theorem" as Matiyasevich builds on the work of Davis, Putnam, and Robinson to complete his proof. While a beautiful survey article of Poonen [Poo08] outlines the relevant notions and historical collocation of DPRM, for us the question is answered so we continue on past it. If we wish to solve the (often-said) natural extension of H10, *Hilbert's 10th Problem over* $\mathbb{Q}$:

Problem. *Find an algorithm which takes as input any polynomial* $f \in \mathbb{Z}[x_1, \ldots, x_n]$ *and decides whether* $f(x_1, \ldots, x_n) = 0$ *has solutions in* $\mathbb{Q}^n$*,*

we find that logic and model-theoretic methods can tackle this question in a more modern fashion.

Translated to the language of model theory, the disproof of H10 has a more succinct presentation[3].

Theorem. *The existential first order theory* $\mathtt{Th}_\exists(\mathbb{Z})$ *of* $\mathbb{Z}$ *in the language of rings* $\mathcal{L}_{rings} = \{0, 1, +, -, \cdot\}$ *is undecidable.* ■

Therefore the analogous question of Hilbert's 10th Problem over $\mathbb{Q}$ (H10/$\mathbb{Q}$) in this format is:

Problem. *Determine the decidability of* $\mathtt{Th}_\exists(\mathbb{Q})$.

This problem has yet to be solved, though it is of interest to logicians, number theorists, and geometers alike; determining the decidability of $\mathtt{Th}_\exists(\mathbb{Q})$ is equivalent to determining when a variety defined over $\mathbb{Q}$ has a rational point. If one had an existential (sometimes called *diophantine*) definition of $\mathbb{Z}$ in $\mathbb{Q}$ then $\mathtt{Th}_\exists(\mathbb{Z})$ could be defined in $\mathtt{Th}_\exists(\mathbb{Q})$ making $\mathtt{Th}_\exists(\mathbb{Q})$ undecidable by H10. The most recent breakthrough in this area is due to Koenigsmann [Koe13]; in 2013 Koenigsmann delivered results which involve definitions of $\mathbb{Z}$ in $\mathbb{Q}$ in three ways. He first provided a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$, then provided a $\forall\exists$-definition (using just one universal quantifier) and finally proved, assuming the Bombieri-Lang conjecture, there is no existential definition of $\mathbb{Z}$ in $\mathbb{Q}$. (Note that this does not mean the decidability of $\mathtt{Th}_\exists(\mathbb{Q})$ has been answered if there is no existential definition of $\mathbb{Z}$ in $\mathbb{Q}$; rather, the most direct route has been cut off from us.)

In this thesis we will explore this problem tangentially. We do not know how to answer these questions of decidability and definability for $\mathbb{Z}$

[2]Not only this, but there exists a specific polynomial for which it is undecidable when the polynomial has integer solutions - see [Koe14, Cor. 3.14].

[3]More can be said about the interplay of these presentations of H10; cf. [Koe14].

and $\mathbb{Q}$, so let us move to another ring and field where answers are more forthcoming. Let $\mathbb{F}_q$ be a finite field of characteristic p and $q = p^n$ elements and let t be transcendental over $\mathbb{F}_q$. Instead of $\mathbb{Z}$ and $\mathbb{Q}$, we shall consider the ring of polynomials over a finite field, $\mathbb{F}_q[t]$, and its fraction field, $\mathbb{F}_q(t)$.

Why is it even remotely useful to be considering these structures in place of $\mathbb{Z}$ and $\mathbb{Q}$? The answer to this comes from a remarkable piece of number theory called the *function field analogy*.

1.2 The Function Field Analogy.

The Local-Global Principle of Hasse is not a theorem, rather a method of attack: in the roughest of terms one can state it as

Principle 1.2.1. *Prove a result over $\mathbb{Q}$ by proving it over $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p.*

By the Hasse-Minkowski Theorem [Ser73, Chapt. IV, §3] this principle is completely true for the problem of representing zero by quadratic forms, and many more examples exist in number theory of the Local-Global Principle in action (cf. [Con18b]). It is in this vein of thought the *function field analogy* exists: a notably strong correspondence between properties of $\mathbb{Z}$ and properties of $\mathbb{F}_q[t]$.

Principle 1.2.2. *A theorem true over $\mathbb{Z}$ has a corresponding theorem true over $\mathbb{F}_q[t]$, and vice versa.*

From immediate and basic algebraic number theory we see examples of this principle in action. Indeed, much of the first four chapters of [Ros02] is dedicated to noting this correspondence! In the preface, Rosen writes

> "Early on in the development of [elementary number theory] it was noticed that $\mathbb{Z}$ has many properties in common with $A = \mathbb{F}[T]$, the ring of polynomials over a finite field. Both rings are principle ideal domains, both have the property that the residue class ring of any nonzero ideal is finite, both rings gave infinitely many prime elements, and both rings have finitely many units. Thus, one is lead to suspect that many results which hold for $\mathbb{Z}$ have analogues of the ring A. This is indeed the case. The first four chapters of [[Ros02]] are devoted to illustrating this by presenting, for example, analogues of the little theorems of Fermat and Euler, Wilson's theorem, quadratic (and higher) reciprocity, the prime number theorem, and Dirichlet's theorem on primes in an arithmetic progression."

Furthermore, [Ros02, Chapt. 1–4] showcases a Chinese Remainder theorem, an Euler totient function, a Unique Factorisation theorem, a Riemann zeta function, a prime number theorem, a residue symbol, and a Dirichlet character function for function fields. Finally [Poo06, §2.6] displays a nice table highlighting a number field object and its function field analogue.

It is still not evident, however, why we write about these structures here. To that end we will remark that Hilbert's 10th Problem over $\mathbb{F}_q[t]$ and over $\mathbb{F}_q(t)$ are both solved: H10 over $\mathbb{F}_q(t)$ (with coefficients in $\mathbb{F}_q[t]$) is unsolvable by [Phe91, Vid94] and likewise with H10 over $\mathbb{F}_q[t]$ by [Den79]. There is also a speckling of results for H10 over other function fields, for which [Dem07] expounds. It is using this analogy we justify our curiosity regarding the definability of $\mathbb{Z}$ in $\mathbb{Q}$ in relation to $\mathbb{F}_q[t]$ and $\mathbb{F}_q(t)$:

Programme. *To answer* H10/$\mathbb{Q}$ *using* H10/$\mathbb{Z}$*, we can attempt to fully understand the connection between* H10/$\mathbb{F}_q(t)$ *and* H10/$\mathbb{F}_q[t]$*. One way to do this is to resolve all major definability questions of* $\mathbb{F}_q[t]$ *in* $\mathbb{F}_q(t)$*.*

Efforts in this direction must then cover three points, mirroring Koenigsmann's results:

(1) **A universal definition.** In [Koe13] Koenigsmann demonstrates a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$. Recently Eisenträger & Morrison [EM18] have produced a universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ using the class field theory developed by Park [Par13] which generalises Koenigsmann's methods. However, this result can be improved upon, which is the focus of *Section 4.3 & 4.4*.

(2) **A $\forall\exists$-definition.** In the same paper Koenigsmann gives a first order definition of $\mathbb{Z}$ in $\mathbb{Q}$ of the form $\forall\exists\ldots\exists(P \neq 0)$ where P is a polynomial with parameters from $\mathbb{Z}$ (i.e. "$P \neq 0$" is a quantifier-free formula of $\mathcal{L}_{\text{ring}}$). For function fields, Theorem 7.3 of [Shl15] demonstrates a $\forall\exists$-definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ using a single universal quantifier.

(3) **An existential definition.** In [Koe13], Koenigsmann puts forth an argument that the Bombieri-Lang conjecture implies $\mathbb{Z}$ is not *diophantine* over $\mathbb{Q}$. This means the following:

Definition 1.2.3. Let R be a ring. We say $A \subseteq R^m$ is *diophantine over* R if there exists a polynomial $p(x_1,\ldots,x_m,y_1,\ldots,y_n) \in R[x_1,\ldots,x_m,y_1,\ldots,y_n]$ such that

$$(a_1,\ldots,a_m) \in A \Leftrightarrow \exists r_1,\ldots,r_n \in R \text{ s.t. } p(a_1,\ldots,a_m,r_1,\ldots,r_n) = 0.$$

Note that it is often the case that "$\neq 0$" is positively existentially definable (e.g. in global fields, rings of integers, $\mathbb{Z}$, $\mathbb{F}_q[t]$, etc.) hence "existentially definable" and "diophantine" are often used interchangeably. The formulation of the Bombieri-Lang conjecture we use is:

Conjecture (Bombieri-Lang). *Let V be an absolutely irreducible affine or projective positive dimensional variety over $\mathbb{Q}$ such that $V(\mathbb{Q})$ is Zariski dense in V. Then so is*

$$\bigcup_{\phi: A \dashrightarrow V} \phi(A(\mathbb{Q})),$$

where $\phi : A \dashrightarrow V$ runs through all nontrivial $\mathbb{Q}$-rational maps from positive dimensional abelian varieties A defined over $\mathbb{Q}$, to V. ■

For function fields, it is still an open question whether $\mathbb{F}_q[t]$ is existentially definable in $\mathbb{F}_q(t)$.

1.3 A Plan of Action

There are more players to this game, however, than those that have been mentioned so far, both on the number field and function field teams. Consider *Figure 1.1:*

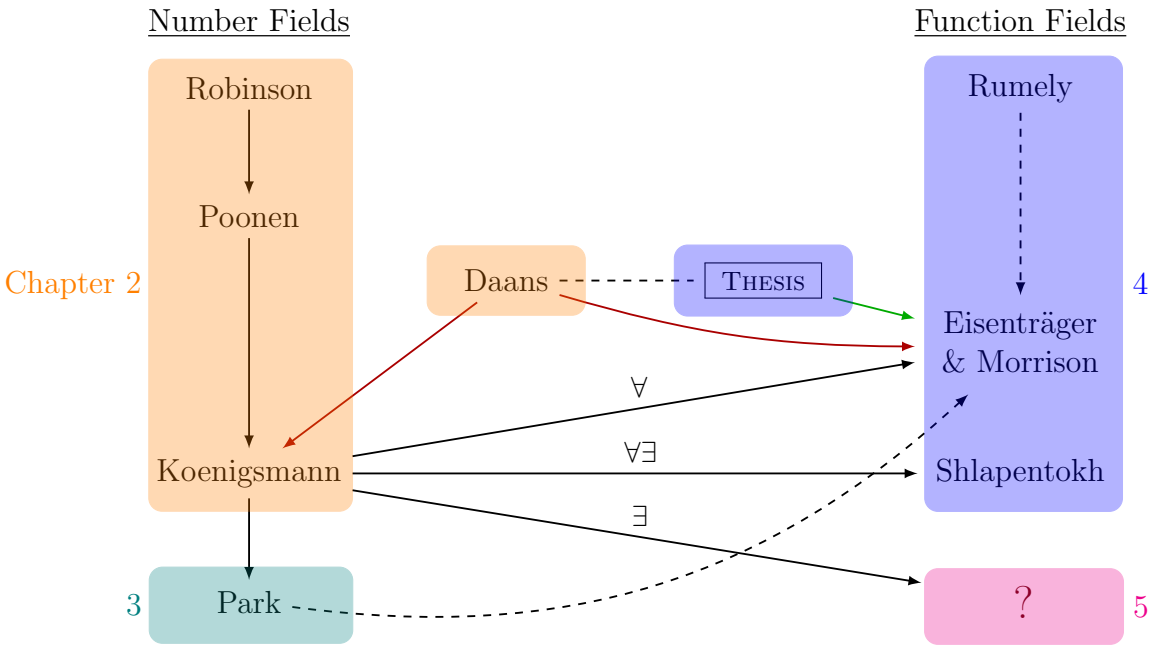

Figure 1.1: Outline of thesis.

The next chapter (*Chapter 2*) will begin with the genesis of the attempts to define $\mathbb{Z}$ in $\mathbb{Q}$; Robinson's 1949 definition and decades later Poonen's $\forall\exists$-definition (with two universal quantifiers), in *Section 2.1.2*. Koenigsmann's results (*Section 2.2*) follow next, and in this section we shall present an overview of Daans' universal definition of $\mathbb{Z}$ in $\mathbb{Q}$ (*Section 2.2.2*), which at the time of writing is the shortest universal definition of $\mathbb{Z}$ in $\mathbb{Q}$. The chapter ends with *Section 2.2.4:* Koenigsmann's answer to the diophantiness of $\mathbb{Z}$ in $\mathbb{Q}$ in the negative.

Chapter 3 is broken into two sections. The first, *Section 3.1*, is devoted to introducing the terminology and two main theorems of Class Field Theory: the *Reciprocity Law (Theorem 3.1.10)* and the *Existence Theorem (Theorem 3.1.12)*. The second section of the chapter closes the 'number fields' side of the thesis with Park's abstraction of Koenigsmann's universal definition to arbitrary number fields in *Section 3.2*.

We then begin working with function fields in *Chapter 4*. Rumely in 1980 provided the original first order definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ which influenced Eisenträger & Morrison's recent universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$; both of these results are discussed in *Section 4.1*. Eisenträger & Morrison's work is presented in *Section 4.2*, however this section is short as their work builds heavily on that of Park's, and uses some of the major results in class field theory. On the other hand, Daans' universal definition of $\mathbb{Z}$ in $\mathbb{Q}$ can be adapted to number fields and function fields, and this adaptation is presented in *Section 4.3*. The author has been successful in further refining Daans' method and a shorter universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$, again without relying on class field theory, is presented in *Section 4.4*. We round off this chapter with an analysis of Shlapentokh's work [Shl15], where in 2015 a $\forall\exists$-definition using a single universal quantifier was discovered for $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$.

Finally, the thesis draws to an end in *Chapter 5* with a discussion on the obstructions present to answering H10/$\mathbb{Q}$ using the undecidability of $\mathtt{Th}_\exists(\mathbb{Z})$ (*Section 5.1*) and how these obstructions are dealt with in the function field case (*Section 5.2*). It is still unknown whether $\mathbb{F}_q[t]$ is existentially definable in $\mathbb{F}_q(t)$, hence the "?" in *Figure 1.1*.

The reader is encouraged to refer to *Appendix A.2* for any function field terminology encountered that is unfamiliar to them. In addition to this, *Appendix A.1* holds a summary of the valuation theory that is required to explore this thesis.

Chapter 2

Number Fields

This chapter is devoted to number fields where we will excurse through the work of Robinson and Poonen and focus more heavily on the work of Koenigsmann and Daans. In particular it is their method of attack and style we will wish to adapt to the function field setting. We begin in 1949 with Julia Robinson.

2.1 From Humble Beginnings

As this is a subject concerned with the decidability of the theories of certain structures, we will of course make mention of the most famous result in this area.

Theorem (Gödel's 1st Incompleteness Theorem). $\mathtt{Th}(\langle \mathbb{N}; 0, 1, +, -, \cdot \rangle)$ *is undecidable.*

Proof. [Göd31]. ■

Corollary 2.1.1. $\mathtt{Th}(\langle \mathbb{Z}; 0, 1, +, -, \cdot \rangle)$ *is undecidable.*

Proof. Every natural number is definable in $\mathbb{Z}$ as the sum of four squares, thus if $\mathtt{Th}(\mathbb{Z})$ is decidable so must be $\mathtt{Th}(\mathbb{N})$; a contradiction. ■

Corollary 2.1.2. $\mathtt{Th}(\langle \mathbb{Q}; 0, 1, +, -, \cdot \rangle)$ *is undecidable.*

Proof. Robinson [Rob49] accomplished this by providing the first explicit definition of $\mathbb{Z}$ in $\mathbb{Q}$, from which the undecidability follows; if $\mathtt{Th}(\mathbb{Q})$ were decidable then as $\mathbb{Z}$ is definable one could create an algorithm for deciding $\mathtt{Th}(\mathbb{Z})$ using $\mathtt{Th}(\mathbb{Q})$, a contradiction to *Corollary 2.1.1.*

Let us state Robinson's definition. For $a, b \in \mathbb{Q}^\times$ and $k \in \mathbb{Q}$ let

$$\phi(a, b, k) := \exists x, y, z(2 + abk^2 + bz^2 = x^2 + ay^2),$$

and for $n \in \mathbb{Q}$ let

$$\psi(n) := \forall a, b \neq 0\Big(\big(\phi(a, b, 0) \wedge \forall k[\phi(a, b, k) \to \phi(a, b, k+1)]\big) \to \phi(a, b, n)\Big).$$

Then $\mathbb{Q} \models \psi(n) \Leftrightarrow n \in \mathbb{Z}$. The reverse implication is obvious by the principle of induction on $\mathbb{N}$, and noticing that $\psi(n) \Leftrightarrow \psi(-n)$. The forward implication is trickier, but follows by showing some integrality conditions at primes. For $k \in \mathbb{Q}$,

(1) For a prime $p \equiv 3 \mod 4$, $\phi(1, p, k) \Leftrightarrow v_p(k) \geq 0$ and $v_2(k) \geq 0$.

(2) For a prime $p \equiv 1 \mod 4$ and q a prime quadratic nonresidue mod p, $\phi(q, p, k) \Leftrightarrow v_p(k) \geq 0$ and $v_q(k) \geq 0$.

For a, b chosen as $1, p$ or q, p as above, it is the case

$$\phi(a, b, 0) \wedge \forall k[\phi(a, b, k) \to \phi(a, b, k + 1)]$$

hence $\psi(n)$ is equivalent to $\phi(1, p, n)$ or $\phi(q, p, n)$ for these a, b. Therefore $v_p(n) \geq 0$ for all primes p, meaning $n \in \mathbb{Z}$, as required. ■

Ten years later Robinson proved the same result in more general terms.

Theorem 2.1.3. *For any number field K, its ring of integers $\mathcal{O}_K$ is definable in K, and $\mathbb{Z}$ is definable in $\mathcal{O}_K$. Thus $\mathtt{Th}(\mathcal{O}_K)$ and $\mathtt{Th}(K)$ are undecidable.*

Proof. [Rob59]. ■

Consider the *positive arithmetical hierarchy* as defined in [Poo09a, §1.1]. Robinson's definition of $\mathbb{Z}$ in $\mathbb{Q}$ is a Π_4^+-formula, so it follows the Σ_5^+-theory of $\mathbb{Q}$ is undecidable. This result can be improved upon: Poonen [Poo09a] defines $\mathbb{Z}$ in $\mathbb{Q}$ using a Π_2^+-formula, making the theory $\mathtt{Th}_{\exists\forall\exists}(\mathbb{Q})$ undecidable once we take into account the negative answer to H10/$\mathbb{Z}$. How he achieves this is by introducing *quaternion algebras* to the playing field, instead of using (say) elliptic curves or valuation theory which at the time would have been the standard approach.

2.1.1 Quaternion Algebras

Definition 2.1.4. A *quaternion algebra over a field* F is a ring that is a four dimensional vector space over F with a basis $1, u, v, w$ with the following multiplicative relations: $u^2 \in F^\times$, $v^2 \in F^\times$, $uv = -vu = w$ and every $c \in F$ commutes with u and v. When $a = u^2$ and $b = v^2$ this ring is denote $\left(\frac{a,b}{F}\right)$ and is equal to $F + uF + vF + uvF$ as a vector space over F.

In this notation, Hamilton's quaternions $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$. It is standard notation to define

$$H_{a,b} := \left(\frac{a,b}{\mathbb{Q}}\right).$$

If we assume $\mathrm{char}(F) \neq 2$ then $\left(\frac{a,b}{F}\right)$ is noncommutative (so we shall assume this from now on). Another major definition we require is that of a *quaternionic basis*:

Definition 2.1.5. A basis of $\left(\frac{a,b}{F}\right)$ having the form $\{1, e_1, e_2, e_1e_2\}$ where $e_1^2 \in F^\times$, $e_2^2 \in F^\times$ and $e_1e_2 = -e_2e_1$ is called a *quaternionic basis* of $\left(\frac{a,b}{F}\right)$.

As these algebras are vector spaces, isomorphisms between bases result in isomorphisms between structures; for instance $\left(\frac{a,b}{F}\right) \cong \left(\frac{b,a}{F}\right)$ as $\{1, v, u, vu\}$ is a quaternionic basis of $\left(\frac{a,b}{F}\right)$ and $\left(\frac{b,a}{F}\right)$. From this fact we see

$$\left(\frac{a,b}{F}\right) \cong \left(\frac{a,-ab}{F}\right) \cong \left(\frac{b,-ab}{F}\right) \cong \left(\frac{ac^2,bd^2}{F}\right) \text{ for all } c,d \in F^\times$$

as well. This examination of bases allows us to prove $\left(\frac{a,1}{F}\right) \cong M_{2\times 2}(F)$ as vector spaces over F. From this we are inspired to define the following phenomenon:

Definition 2.1.6. Any quaternion algebra isomorphic to $M_{2\times 2}(F)$ is known as *split*. If $\left(\frac{a,b}{F}\right) \ncong M_{2\times 2}(F)$, then $\left(\frac{a,b}{F}\right)$ is *nonsplit*.

Theorem 2.1.7. [Con18c]. *A quaternion algebra* $\left(\frac{a,b}{F}\right)$ *is either a division ring or is isomorphic to* $M_{2\times 2}(F)$. ■

One last piece of the puzzle, yet to be mentioned, are *primes*, or, more generally, *places* of a field (see *Appendix A.1* for a discussion of places and valuation theory). Let v be a place of a global field K and let K_v denote the completion of K at v. For any $a, b \in K_v^\times$ define the *Hilbert Symbol*:

$$(a,b)_v = \begin{cases} 1 & \text{if } ax^2 + by^2 = 1 \text{ has a solution in } K_v, \\ -1 & \text{o.w.} \end{cases}$$

Recall the definition of a *local field* (*Definition A.1.2*). Note that if K is a global field, and v a nontrivial place of K, then K_v is a local field.

Definition 2.1.8. We call a local field F *dyadic* if $\mathrm{char}(F) \neq 2$ yet its residue field is of characteristic two.

Lemma 2.1.9. *Now, some results linking the Hilbert symbol to the splitting of quaternion algebras. Assume in addition K_v is nondyadic and* $\mathrm{char}(K_v) \neq 2$.

(1) The quaternion algebra $\left(\frac{a,b}{K_v}\right)$ splits if and only if $(a,b)_v = 1$.

(2) $(a,b)_v = 1$ for almost all v.

(3) For $a, b \in K^\times$, $\prod_v (a,b)_v = 1$ (where the product is taken over all places of K).

Proof. See [Cha12, Theorem 1.13] for (1). For (2), for almost all finite places v, a and b are units of $\mathcal{O}_v = \{x \in K_v : v(x) \geq 0\}$, hence by [Cha12, Theorem 3.13] the algebra $\left(\frac{a,b}{K_v}\right)$ splits, so $(a,b)_v = 1$ for almost all v. (3) is an analogue to the product formula, known as *Hilbert's Reciprocity Law*. See [Daa18, Theorem 1.7.7] for a more technical presentation of this result. ■

[Ser79, Chapt. XIV, §3.8] presents a formula for calculating the Hilbert symbol:

Theorem 2.1.10. *Let K be a global field and $a, b \in K^\times$. Let v be a nonarchimedian place of K. Then*

$$(a,b)_v = \left((-1)^{v(a)v(b)} \,\mathrm{red}_v\left(\frac{a^{v(b)}}{b^{v(a)}}\right)\right)^{\frac{|\mathbb{F}_v|-1}{2}},$$

where $\mathbb{F}_v$ is the residue field of K_v. Moreover, if a is a v-adic unit, then

$$(a,b)_v = -1 \quad \Leftrightarrow \quad v(b) \text{ is odd and } \mathrm{red}_v(a) \text{ is a nonsquare of } \mathbb{F}_v. \quad ■$$

Returning to the interplay between primes and quaternion algebras, consider the following definition:

Definition 2.1.11. We say a quaternion algebra H is *ramified* at a place v if $H_v = H \otimes_F K_v$ is a division algebra.

The set of places at which H is ramified is denoted by $\mathrm{Ram}(H)$, and it is a finite set containing an even number of places (by Hilbert's Reciprocity Law). The product of $\mathrm{Ram}(H)$ is known as the *discriminant* of H.

The set $\mathrm{Ram}(H)$ appears in [Poo09a] in another guise, namely the set $\Delta_{a,b}$ of all prime numbers p which cause the quaternion algebra $H_{a,b}$ to ramify. This we shall see in the next section.

2.1.2 Poonen's Definition

Poonen introduces the following definitions at the beginning of [Poo09a]:

Definition 2.1.12.

- $\Delta_{a,b} := \{p \text{ prime} : H_{a,b} \otimes \mathbb{Q}_p \ncong M_{2\times 2}(\mathbb{Q}_p)\}$, as above.
- $S_{a,b} := \{2x_1 \in \mathbb{Q} : \exists x_2, x_3 x_4 \in \mathbb{Q} \text{ s.t. } x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1\}$, the set of traces of norm 1 elements of $H_{a,b}$.
- Let $S_{a,b}(\mathbb{Q}_p)$ be defined similarly for $H_{a,b} \otimes \mathbb{Q}_p$.
- $T_{a,b} := S_{a,b} + S_{a,b} + \{0, \ldots, 2309\}$.
- Consider the field extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. For $b \in \mathbb{F}_{q^2}$, define the trace and norm maps
$$\mathrm{Tr}(b) := b + b^q, \qquad \mathrm{Norm}(b) := b^{q+1}.$$
- $U_q := \mathrm{Tr}\left(\{b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q : \mathrm{Norm}(b) = 1\}\right)$. This is equivalently the set of $s \in \mathbb{F}_q$ making $x^2 - sx + 1$ irreducible in $\mathbb{F}_q[x]$.

How Poonen produces his result is via an application of the Hasse-Minkowski Local-Global Principle for $\mathbb{Q}$ and a clever way of diophantically representing $\mathbb{F}_q$.

Lemma 2.1.13.

(1) If $p \in \Delta_{a,b}$, then $\mathrm{red}_p^{-1}(U_p) \subseteq S_{a,b}(\mathbb{Q}_p) \subseteq \mathbb{Z}_p$.

(2) $S_{a,b} = \mathbb{Q} \cap \bigcap_p S_{a,b}(\mathbb{Q}_p)$.

(3) For q a prime power greater than 11, $\mathbb{F}_q = U_q + U_q$.

(4) If $a, b \in \mathbb{Q}^\times$ and either $a > 0$ or $b > 0$, then $T_{a,b} = \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)}$.

Proof. (1) is Lemma 2.1(ii) of [Poo09a]. (2) is the Hasse-Minkowski Local-Global Principle for $\mathbb{Q}$ in action. (3) and (4) are Lemmata 2.3 and 2.5 of [Poo09a], the latter a combination of (1), (2) & (3) of this lemma. ■

It is this last point that (essentially) allows us to conclude $\bigcap_{a,b \in \mathbb{Q}_{>0}} T_{a,b} = \mathbb{Z}$, and produce the following definition of $\mathbb{Z}$ in $\mathbb{Q}$:

Theorem 2.1.14. *The set $\mathbb{Z}$ equals the set of $t \in \mathbb{Q}$ for which the following Π_2^+-formula is true over $\mathbb{Q}$:*

$$\begin{aligned}
&(\forall a, b)(\exists a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4, x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4, n) \\
&\big((a + a_1^2 + a_2^2 + a_3^2 + a_4^2)(b + b_1^2 + b_2^2 + b_3^2 + b_4^2) \\
&\cdot \big[(x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 - 1)^2 + (y_1^2 - ay_2^2 - by_3^2 + aby_4^2 - 1)^2 \\
&\quad + n^2(n-1)^2 \cdots (n - 2309)^2 + (2x_1 + 2y_1 + n - t)^2\big] = 0\big).
\end{aligned}$$

Proof. Recall by Lagrange's Four Square Theorem, the set of a satisfying $a + a_1^2 + a_2^2 + a_3^2 + a_4^2 = 0$ for some $a_1, a_2, a_3, a_4 \in \mathbb{Q}$ are those $a \in \mathbb{Q}$ with $a \leq 0$. Thus

$$\begin{aligned}&(a + a_1^2 + a_2^2 + a_3^2 + a_4^2)(b + b_1^2 + b_2^2 + b_3^2 + b_4^2)\\ &\cdot \big[(x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 - 1)^2 + (y_1^2 - ay_2^2 - by_3^2 + aby_4^2 - 1)^2\\ &\quad + n^2(n-1)^2 \cdots (n-2309)^2 + (2x_1 + 2y_1 + n - t)^2\big] = 0\end{aligned}$$

is equivalent to

$$\begin{aligned}&\big(a \leq 0 \text{ or } b \leq 0\big) \text{ or}\\ &(x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 - 1)^2 + (y_1^2 - ay_2^2 - by_3^2 + aby_4^2 - 1)^2\\ &\quad + n^2(n-1)^2 \cdots (n-2309)^2 + (2x_1 + 2y_1 + n - t)^2\big] = 0\end{aligned}$$

which is in turn logically equivalent to

$$\begin{aligned}&a > 0 \wedge b > 0 \quad \rightarrow\\ &\text{Norm}(\bar{x}) = 1 \wedge \text{Norm}(\bar{y}) = 1 \wedge n \in \{0, \ldots, 2309\} \wedge t = 2x_1 + 2y_1 + n,\end{aligned}$$

that is,

$$a > 0 \wedge b > 0 \quad \rightarrow \quad t \in T_{a,b}.$$

Since $\bigcap_{a,b \in \mathbb{Q}_{>0}} T_{a,b} = \mathbb{Z}$, we are done. ■

Tidying up this definition, it is possible to define $\mathbb{Z}$ in $\mathbb{Q}$ using 2 universal and 7 existential quantifiers; $\mathbb{Z}$ is the set of those $t \in \mathbb{Q}$ such that

$$\begin{aligned}&(\forall a, b)(\exists x_1, x_2, x_3, x_4, y_2, y_3, y_4)\\ &\Bigg((a + x_1^2 + x_2^2 + x_3^2 + x_4^2)(b + x_1^2 + x_2^2 + x_3^2 + x_4^2)\\ &\cdot \Bigg[\big(x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 - 1\big)^2\\ &\quad + \prod_{n=0}^{2309} \big((n - t - 2x_1)^2 - 4ay_2^2 - 4by_3^2 + 4aby_4^2 - 4\big)^2\Bigg] = 0\Bigg).\end{aligned} \tag{2.1}$$

Poonen continues to extend this result to "big subrings" of $\mathbb{Q}$ and to a number field K in place of $\mathbb{Q}$, but the above proof is the crux of the matter and what Koenigsmann considers at the beginning of his paper.

2.2 Great Things

The first in Koenigsmann's trifecta of results is the universal definition of $\mathbb{Z}$ in $\mathbb{Q}$. The following results originate in [Koe13] (resp. [Koe16]) while an earlier draft of the paper [Koe10] contains some more detailed quantifier calculations.

2.2.1 Koenigsmann's Universal Definition

Koenigsmann lays out a four step process to achieving this universal definition. The first step, "Diophantine definition of quaternionic semi-local rings à la Poonen" does exactly what it claims: Poonen's definition (2.1) of $\mathbb{Z}$ in $\mathbb{Q}$ is modified to create a formula which, like (2.1) has two universal and 7 existential quantifiers but the degree of the polynomial involved decreases from 9244 to 8. Koenigsmann deviates from Poonen's terminology slightly to achieve this:

Definition 2.2.1.

- Let $\mathbb{P}$ be the set of rational primes and ∞ the infinite place of $\mathbb{Q}$ (see *Definition A.1.6*). Note $\mathbb{Q}_\infty := \mathbb{R}$.
- Let $a, b \in \mathbb{Q}^\times$. Now $\Delta_{a,b} := \{p \in \mathbb{P} \cup \{\infty\} : H_{a,b} \otimes \mathbb{Q}_p \ncong M_{2\times 2}(\mathbb{Q}_p)\}$.
- $T_{a,b} := S_{a,b} + S_{a,b}$ where $S_{a,b}$ is defined exactly as in *Definition 2.1.12*.
- $S_{a,b}(\mathbb{Q}_p)$ and $T_{a,b}(\mathbb{Q}_p)$ are defined as before.

Koenigsmann also gives a crucial explicit set of criteria for determining when a prime $p \in \mathbb{P} \cup \{\infty\}$ is a member of $\Delta_{a,b}$ or not; this is known as *Observation 5* ([Koe13]) which we replicate below for the sake of completeness.

Lemma 2.2.2. *Assume $a, b \in \mathbb{Q}^\times$ and $p \in \mathbb{P} \cup \{\infty\}$. Then $p \in \Delta_{a,b}$ if and only if:*

For $p = 2$: *After multiplying by suitable rational squares and integers $\equiv 1 \mod 8$ and, possibly, swapping a and b, the pair (a, b) is one of the following:*

(2, 3)	(3,3)	(5,6)	(6, 6)	(15, 15)
(2, 5)	(3, 10)	(5, 10)	(6, 15)	(15, 30)
(2, 6)	(3, 15)	(5, 30)	(10, 30)	(30, 30)
(2, 10)				

For $2 \neq p \in \mathbb{P}$**:**

$$v_p(a) \text{ is odd, } v_p(b) \text{ is even, and } \left(\frac{bp^{-v_p(b)}}{p}\right) = -1 \text{ or}$$
$$v_p(a) \text{ is even, } v_p(b) \text{ is odd, and } \left(\frac{ap^{-v_p(a)}}{p}\right) = -1 \text{ or}$$
$$v_p(a) \text{ is odd, } v_p(b) \text{ is odd, and } \left(\frac{-abp^{-v_p(ab)}}{p}\right) = -1.$$

For $p = \infty$**:** $\quad a < 0$ *and* $b < 0$.

Proof. These properties can be deduced from the computation of the Hilbert symbol $(a, b)_p$ as presented in [Ser73, Chapt. III Theorem 1]:

If we write $a = p^\alpha u$, $b = p^\beta v$, where u, v are p-adic units, then we have

$$(a, b)_p = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha \qquad \text{if } p \neq 2,$$
$$(a, b)_p = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)} \qquad \text{if } p = 2,$$

where $\epsilon(n)$ and $\omega(n)$ are the modulo 2 class of $\frac{n-1}{2}$ and $\frac{n^2-1}{8}$ respectively. ■

Remark 2.2.3. One can generalise *Lemma 2.2.2* to all local fields, as Daans does:

Lemma 2.2.4. [Daa18, Prop. 1.5.2]. *Suppose K is a nondyadic, nonarchimedian local field and* $\mathrm{char}(K) \neq 2$*. Let $\mathcal{O}$ be its valuation ring, v its corresponding valuation and π its uniformiser*[1]*. For $a, b \in K$ we have $\left(\frac{a,b}{K}\right)$ is nonsplit if and only if one of the following holds:*

(a) $v(a)$ is odd, $v(b)$ is even and $b\pi^{-v(b)}$ is a nonsquare modulo $\pi\mathcal{O}$.

(b) $v(b)$ is odd, $v(a)$ is even and $a\pi^{-v(a)}$ is a nonsquare modulo $\pi\mathcal{O}$.

(c) $v(a)$ and $v(b)$ are odd and $ab\pi^{-v(ab)}$ is a nonsquare modulo $\pi\mathcal{O}$.

□

The next step in Koenigsmann's paper is to reprove *Lemma 2.1.13*, taking great care to reprove *(4)* with the new definition of $T_{a,b}$, i.e. that

$$T_{a,b}\,(= S_{a,b} + S_{a,b}) = \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)}, \tag{2.2}$$

still. As a byproduct of this, a simpler Poonen-like definition arises:

[1] If $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}$, π is any fixed element of $\mathfrak{m} \setminus \mathfrak{m}^2$.

Theorem 2.2.5. *For any $t \in \mathbb{Q}$,*

$$\begin{aligned} t \in \mathbb{Q} \quad \Leftrightarrow \quad & (\forall a, b)(\exists x_1, x_2, x_3, x_4, y_2, y_3, y_4) \\ & \big((a + x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (b + x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot \\ & \big[(x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 - 1)^2 + \\ & ((t - 2x_1)^2 - 4ay_2^2 - 4by_3^2 + 4aby_4^2 - 4)^2\big] = 0\big). \end{aligned}$$

Proof. See the proofs of *Theorem 2.1.14* and [Poo09a, Theorem 4.1] for further explanation. ■

However *Theorem 2.2.5* was not the goal of Koenigsmann, merely a stepping stone. Step 2 of Koenigsmann's plan, "Towards a uniform diophantine definition of all $\mathbb{Z}_{(p)}$'s in $\mathbb{Q}$" begins with the following definitions:

Definition 2.2.6. Define the following sets: for $p, q \in \mathbb{Q}^\times$,

- $R_p^{[3]} := T_{-1,-p} + T_{2,-p}$,
- $R_p^{[5]} := T_{-2,-p} + T_{2,-p}$,
- $R_p^{[7]} := T_{-1,-p} + T_{-2,p}$,
- $R_p^{[1]} := T_{-2p,q} + T_{2p,q}$.

These sets are existentially definable in $\mathbb{Q}$ and moreover uniform in p and q. For $k = 1, 3, 5$ or 7, and $p \in \mathbb{Q}^\times$, define

- $\mathbb{P}^{[k]} := \{l \in \mathbb{P} : l \equiv k \mod 8\}$,
- $\mathbb{P}(p) := \{l \in \mathbb{P} : v_l(p) \text{ is odd}\}$, and $\mathbb{P}^{[k]}(p) := \mathbb{P}(p) \cap \mathbb{P}^{[k]}$.

These seemingly random allocation of sets in fact existentially define the localisations $\mathbb{Z}_{(p)}$ exactly: as a result of [Koe13, Prop. 10], if p is a prime and $p \equiv k \mod 8$ for $k = 3, 5, 7$ then $\mathbb{Z}_{(p)} = R_p^{[k]}$. Moreover if $p \equiv 1 \mod 8$ and q is a prime congruent to 3 mod 8 with $\left(\frac{p}{q}\right) = -1$, then $\mathbb{Z}_{(p)} = R_{p,q}^{[1]}$. Therefore

$$\mathbb{Z} = \mathbb{Z}_{(2)} \cap \bigcap_{p,q \in \mathbb{Q}^\times} (R_p^{[3]} \cap R_p^{[5]} \cap R_p^{[7]} \cap R_{p,q}^{[1]}),$$

where every set to the right hand side is defined existentially (as $\mathbb{Z}_{(2)} = T_{3,3} + T_{2,5}$).

The next step is showing that, for some of the $R_p^{[k]}$ and $R_{p,q}^{[1]}$ rings their *Jacobson radical* is also existentially defined.

Definition 2.2.7. The *Jacobson radical* of a ring R, denoted $J(R)$, is the intersection of all maximal ideals of R.

Koenigsmann achieves this in Corollary 15 and Proposition 16 of [Koe13] as follows:

Proposition 2.2.8. *Define for $k = 1, 3, 5$ and 7,*

$$\Phi_k := \{p \in \mathbb{Q}^{>0} \,:\, p \equiv k \bmod 8\,\mathbb{Z}_{(2)} \text{ and } \mathbb{P}(p) \subseteq \mathbb{P}^{[1]} \cup \mathbb{P}^{[k]}\},$$
$$\Psi := \{(p,q) \in \Phi_1 \times \Phi_3 : p \in 2 \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_q^{[3]}))\}.$$

(1) For $k = 1, 3, 5$ and 7, Φ_k is diophantine in $\mathbb{Q}$.

(2) If $k = 3, 5$ or 7 and if $p \in \Phi_k$ then

$$\{0\} \neq J(R_p^{[k]}) = \begin{cases} \bigcap_{l \in \Delta_{-1,-p} \cap \Delta_{2,-p}} l\,\mathbb{Z}_{(l)} & \text{if } k = 3, \\ \bigcap_{l \in \Delta_{-2,-p} \cap \Delta_{2,-p}} l\,\mathbb{Z}_{(l)} & \text{if } k = 5, \\ \bigcap_{l \in \Delta_{-1,-p} \cap \Delta_{-2,p}} l\,\mathbb{Z}_{(l)} & \text{if } k = 7. \end{cases}$$

In particular, in each of these cases the Jacobson radical is diophantine in $\mathbb{Q}$, defined by a formula uniform in p.

(3) Hence Ψ is diophantine in $\mathbb{Q}$.

(4) If $(p,q) \in \Psi$ then $J(R_{p,q}^{[1]}) = \bigcap_{l \in \Delta_{-2p,q} \cap \Delta_{2p,q}} l\,\mathbb{Z}_{(l)}$ and thus the Jacobson radical of $R_{p,q}^{[1]}$ is diophantine in $\mathbb{Q}$ too. ■

What remains now is to take all these existential definitions and convert them to something useful and universal, which is *Step 4* of Koenigmann's plan exactly. If $\Delta \subseteq \mathbb{P}$ is a finite set of primes, Koenigsmann defines for a "semilocal" (has finitely many maximal ideals) subring $R = \bigcap_{p \in \Delta} \mathbb{Z}_{(p)}$,

Definition 2.2.9. $\widetilde{R} := \{x \in \mathbb{Q} \,:\, \nexists y \in J(R) \text{ with } x \cdot y = 1\}$.

Clearly if $J(R)$ is diophantine then $\widetilde{R}$ is given by a universal formula. Moreover it can be shown $\widetilde{R} = \bigcup_{p \in \Delta} \mathbb{Z}_{(p)}$ (provided $\Delta \neq \emptyset$). This is the final nail in the coffin: using this set we have at last obtained a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$.

Theorem 2.2.10. ([Koe13, Prop. 18]).

(1) $\mathbb{Z} = \widetilde{\mathbb{Z}_{(2)}} \cap \left(\bigcap_{k=3,5,7} \bigcap_{p \in \Phi_k} \widetilde{R_p^{[k]}} \right) \cap \bigcap_{(p,q) \in \Psi} \widetilde{R_{p,q}^{[1]}}$.

(2) For any $t \in \mathbb{Q}$,

$$\begin{aligned} t \in \mathbb{Z} \quad \Leftrightarrow \quad & t \in \widetilde{\mathbb{Z}_{(2)}} \wedge \\ & \forall p \Big[\bigwedge_{k=3,5,7} (p \notin \Phi_k \vee t \in \widetilde{R_p^{[k]}}) \Big] \wedge \\ & \forall p, q \Big[(p,q) \notin \Psi \vee t \in \widetilde{R_{p,q}^{[1]}} \Big]. \end{aligned}$$

(3) There is a polynomial $g \in \mathbb{Z}[t; x_1, \ldots, x_{418}]$ of degree 28 such that, for any $t \in \mathbb{Q}$,

$$t \in \mathbb{Z} \quad \Leftrightarrow \quad \forall x_1, \ldots, x_{418} \in \mathbb{Q} \;\; g(t, x_1, \ldots, x_{418}) \neq 0.$$

Proof. (2) and (3) follow directly from (1); see [Koe10, Prop. 15(c)] for the degree and quantifier count in (3).

For (1), we can see $\mathbb{Z} \subseteq \widetilde{R_p^{[k]}}$ for $k = 3, 5, 7$ and $\mathbb{Z} \subseteq \widetilde{R_{p,q}^{[1]}}$ for $p \in \Phi_k$ and $(p, q) \in \Psi$ respectively [Koe13, Prop. 10, Corollary 15(b)]. As Φ_k and Ψ are nonempty, we conclude

$$\mathbb{Z} \subseteq \widetilde{\mathbb{Z}_{(2)}} \cap \left(\bigcap_{k=3,5,7} \bigcap_{p \in \Phi_k} \widetilde{R_p^{[k]}} \right) \cap \bigcap_{(p,q) \in \Psi} \widetilde{R_{p,q}^{[1]}}.$$

Recall that if p is a prime and $p \equiv k \mod 8$ for $k = 3, 5, 7$ then $\mathbb{Z}_{(p)} = R_p^{[k]} = \widetilde{R_p^{[k]}}$. Moreover if $p \equiv 1 \mod 8$ and q is a prime congruent to 3 mod 8 with $\left(\frac{p}{q}\right) = -1$, then $\mathbb{Z}_{(p)} = R_{p,q}^{[1]} = \widetilde{R_{p,q}^{[1]}}$. Therefore

$$\mathbb{Z} = \bigcap_{p \in \mathbb{P}} \mathbb{Z}_{(p)} \supseteq \widetilde{\mathbb{Z}_{(2)}} \cap \left(\bigcap_{k=3,5,7} \bigcap_{p \in \Phi_k} \widetilde{R_p^{[k]}} \right) \cap \bigcap_{(p,q) \in \Psi} \widetilde{R_{p,q}^{[1]}},$$

as required. ∎

The definition and use of the sets Φ_k, Ψ are ultimately unnecessary if our sole goal is to produce a universal definition, as Daans [Daa18] demonstrates.

2.2.2 Daans' Universal Definition

Daans [Daa18] produces a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$ using the basics of [Koe13] however crucially he does not use the sets Φ_k and Ψ. This makes his definition vastly simpler. Begin with the following definition:

Definition 2.2.11. Define $J_{a,b} := \bigcap_{l\in\Delta} l\,\mathbb{Z}_{(l)}$, where

$$\Delta = \begin{cases} \Delta_{a,b} \setminus \{2,\infty\} & \text{if } 2 \in \Delta_{a,b} \text{ and } v_2(a), v_2(b) \text{ are even,} \\ \Delta_{a,b} \setminus \{\infty\} & \text{o.w.} \end{cases}$$

It can be proven that $\Delta = \Delta_{a,b} \cap (\mathbb{P}(a) \cup \mathbb{P}(b))$.

If we define $R_{a,b} := \bigcap_{l\in\Delta} \mathbb{Z}_{(l)}$ with Δ as above, then whenever $\Delta \neq \emptyset$, $R_{a,b}$ is a semilocal subring of $\mathbb{Q}$ with $J_{a,b}$ as its Jacobson radical. By [Koe13, Lemma 13(d)], $J_{a,b}$ is existentially definable, hence there is a universal definition for $\widetilde{R_{a,b}}$. The Jacobson radical here requires 122 quantifiers to define (see [Koe10] or [Daa18, Prop. 4.2.6]) so $\widetilde{R_{a,b}}$ requires $122 + 1 = 123$ universal quantifiers.

What is central to Daans' proof is his use of *Hilbert Reciprocity*. Recall the Hilbert symbol $(a,b)_p$ from §2.1.1, and the third result of *Lemma 2.1.9:*

Theorem 2.2.12. (Hilbert Reciprocity). *If $a, b \in \mathbb{Q}^\times$ then*

$$\prod_{p\in\mathbb{P}} (a,b)_p = 1. \qquad \blacksquare$$

Now, for one of Daans' main results:

Theorem 2.2.13. *We have*

$$\mathbb{Z} = \bigcap_{\substack{p,q>0 \\ q\in\mathbb{Q}^2\cdot T^\times_{-1,-1}}} \widetilde{R_{-p,-2q}}. \tag{2.3}$$

Hence there is a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$ using 146 quantifiers.

Proof. First, if $q \in \mathbb{Q}^2 \cdot T^\times_{-1,-1}$ then $q \in \mathbb{Q}^2 \cdot \mathbb{Z}^\times_{(2)}$ demonstrating $v_2(-2q) = 1$. Hence according to *Definition 2.2.11*, $\Delta = \Delta_{a,b} \setminus \{\infty\}$.

For any $p, q > 0$ the quaternion algebra $\left(\frac{-p,-2q}{\mathbb{R}}\right)$ is nonsplit as it is isomorphic to $\mathbb{H}$. This means precisely that $(-p,-2q)_\infty = -1$. By Hilbert Reciprocity we conclude $H_{-p,-2q}$ is nonsplit at some finite prime too. Therefore $\Delta = \Delta_{-p,-2q} \setminus \{\infty\}$ is nonempty and

$$\widetilde{R_{-p,-2q}} = \bigcup_{l\in\Delta} \mathbb{Z}_{(l)} \supseteq \mathbb{Z}$$

always. This demonstrates inclusion from left to right in (2.3).

On the other hand we wish to find parameters p, q satisfying $p, q > 0$ and $q \in \mathbb{Q}^2 \cdot T^\times_{-1,-1}$ such that $\widetilde{R_{-p,-2q}} = R_{-p,-2q} = \mathbb{Z}_{(l)}$ for any prime l. That is, we wish to find parameters p, q such that $\Delta_{-p,-2q} \setminus \{\infty\} = \{l\}$. Daans [Daa18, Theroem 4.6.3] produces a list to this effect:

- If $l = 2$, take $p = q = 1$.
- If $l \equiv 3, 7 \mod 8$, take $p = 1$, $q = l$.
- If $l \equiv 5 \mod 8$, take $p = l$, $q = 1$.
- If $l \equiv 1 \mod 8$, take $q = l$ and let p be a prime such that $p \equiv 5 \mod 8$ and $\left(\frac{p}{l}\right) = -1$.

On this last point, we exploit the Hilbert symbol formula in *Theorem 2.1.10:* as $-p$ is an l-adic unit,

$$(-p, -2l)_l = -1 \Leftrightarrow v_l(-2l) = 1 \text{ is odd and } \operatorname{red}_l(-p) \text{ is a nonsquare of } \mathbb{F}_l.$$

As $\left(\frac{-p}{l}\right) = \left(\frac{-1}{l}\right)\left(\frac{p}{l}\right) = 1 \cdot -1 = -1$, we conclude $\operatorname{red}_l(-p)$ is indeed a nonsquare of $\mathbb{F}_l$ hence $l \in \Delta_{-p,-2l}$ as required. Moreover, $2 \notin \Delta_{-p,-2l}$ by a similar calculation. Thus $\Delta_{-p,-2l} \setminus \{\infty\} = \{l\}$ in this case, as desired.

Therefore for each prime l there are adequate parameters p, q such that $\widetilde{R_{-p,-2q}} = R_{-p,-2q} = \mathbb{Z}_{(l)}$, meaning the RHS of (2.3) is a subset of $\bigcap_{l \in \mathbb{P}} \mathbb{Z}_{(l)} = \mathbb{Z}$, as required to prove equality.

This leads to a universal definition of 146 quantifiers as 123 are required for the ring $\widetilde{R_{-p,-2q}}$, a further 4 is required to express "$p > 0$" (by Lagrange's Four Square Theorem) and another 4 for "$q > 0$" and finally "$\mathbb{Q}^2 \cdot T^{\times}_{-1,-1}$" requires 15 existential quantifiers to define. ■

Remark 2.2.14. We can apply the general method of Daans later in the thesis to obtain a new universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$. Thus it is worth highlighting the main steps in the above proof.

The main goal is to find a set of conditions D on parameters a, b such that:

(1) If a, b satisfies D this forces $\Delta = \Delta_{a,b} \setminus \{\infty\}$.

(2) If a, b satisfy D, then $(a, b)_\infty = -1$. Equivalently, Δ is always nonempty.

(3) For each prime $\mathfrak{p}$, one can find a, b satisfying D such that $\Delta = \{\mathfrak{p}\}$. Equivalently, there exist a, b satisfying D such that

$$(a, b)_{\mathfrak{p}} = -1 \text{ and } (a, b)_{\mathfrak{q}} = 1 \text{ for all primes } \mathfrak{q} \neq \mathfrak{p}.$$

Then we obtain a universal definition, which in *Theorem 2.2.13* is:

(4) $t \in \mathbb{Z} \quad \Leftrightarrow \quad \forall a, b \in \mathbb{Q}\ ((a, b) \notin D \vee t \in \widetilde{R_{a,b}})$. □

If it is the case that Φ_k and Ψ are inessential to produce a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$, why bother?

As Koenigsmann demonstrates in §3 of [Koe13], these sets give rise to new (and old) diophantine predicates in $\mathbb{Q}$; in Proposition 20 (b) & (e) Koenigsmann exhibits the set of nonsquares of $\mathbb{Q}$ ($\{x \in \mathbb{Q} : x \notin \mathbb{Q}^2\}$) and the set of those rational numbers outside the image of any norm map[2] ($\{(x,y) \in \mathbb{Q}^2 : x \notin \mathrm{Norm}(y)\}$) are diophantine.

The former of these sets (for a general number field K) was the focus of a 2009 paper of Poonen's where he proved the set $K^\times \setminus K^{\times 2}$ is diophantine using highly nontrivial properties of Châtelet surfaces and the Brauer-Manin obstruction to the Hasse Principle ([Poo09b]). However, using the sets Φ_k and Ψ Koenigsmann gives an *elementary* proof that the set of nonsquares of $\mathbb{Q}$ is diophantine and moreover gives an explicit formula for the set.

The sets Φ_k and Ψ are also crucial to Koenigsmann's $\forall\exists$-definition of $\mathbb{Z}$ in $\mathbb{Q}$ of one universal quantifier, as we shall see in the next section.

2.2.3 Koenigsmann's $\forall\exists$-Definition

In this section Koenigsmann first replaces the set "$R^{[1]}_{p,q}$" with "$R^{[1]}_p$":

Lemma 2.2.15. *Assume $p \in \Phi_1$ and define*

$$R^{[1]}_p := \{x \in \mathbb{Q} : \exists q \text{ s.t. } (p,q) \in \Psi,\ q \in (R^{[1]}_{p,q})^\times \text{ and } x \in R^{[1]}_{p,q}\}.$$

Then $R^{[1]}_p$ is diophantine in $\mathbb{Q}$ and $R^{[1]}_p = \bigcup_{l \in \mathbb{P}(p)} \mathbb{Z}_{(l)}$. In particular, if p is a prime $\equiv 1$ mod 8 then $R^{[1]}_p = \mathbb{Z}_{(p)}$.

Proof. [Koe13, Lemma 19]. Note that the 'in particular' property is the same as that mentioned on page 15 for the sets $R^{[k]}_p$, $k = 3, 5$, or 7. ■

Theorem 2.2.16. *For all $t \in \mathbb{Q}$, $t \in \mathbb{Z}$ if and only if*

$$\forall p \left(t \in \mathbb{Z}_{(2)} \wedge \begin{cases} \big(p \in \mathbb{Q}^2 \cdot (2 + 4\,\mathbb{Z}_{(2)})\big) \\ \bigvee_{k=1,3,5,7} \begin{cases} \big(p \neq 0 \wedge p \in \mathbb{Q}^2 \cdot (k + 8\,\mathbb{Z}_{(2)})\big) \\ \wedge \big((p \notin \Phi_k) \vee p \in \mathbb{Q}^2 \vee \big(p \in \Phi_k \setminus \mathbb{Q}^2 \wedge t \in R^{[k]}_p\big)\big) \end{cases} \end{cases} \right)$$

Proof. First note that this formula for $\mathbb{Z}$ is indeed of the shape $\forall\exists$ as there is one universal quantifier ($\forall p$) at the beginning and everything defined

[2] $\mathrm{Norm} : \mathbb{Q}(\sqrt{y}) \to \mathbb{Q}\,;\ a + b\sqrt{y} \mapsto a^2 - yb^2$.

thereafter is existential: under the assumption $p \in \mathbb{Q}^2 \cdot (k + 8\,\mathbb{Z}_{(2)})$, '$p \notin \Phi_k$' becomes equivalent to

$$p \notin \mathbb{Z}_{(2)}^{\times} \vee \big(p \in k + \mathbb{Z}_{(2)} \wedge p \notin \Phi_k\big),$$

which is diophantine by [Koe13, Prop. 20(c)]. Also '$p \in \Phi_k \setminus \mathbb{Q}^2$' is diophantine by [Koe13, Prop. 20(b)]. So this is indeed a $\forall\exists$-formula with one universal quantifier[3].

Now the question becomes: is this formula accurate? Denote the formula in question by (✤). If $t \in \mathbb{Z}$ then $t \in \mathbb{Z}_{(2)}$ and $t \in R_p^{[k]}$ for all $p \in \Phi_k \setminus \mathbb{Q}^2$ and $k = 1, 3, 5, 7$ (by [Koe13, Prop. 10, Corollary 15, Lemma 19]), hence t satisfies (✤). Also for all odd primes $p \in \mathbb{P}$, if $p \equiv k \mod 8$ then $R_p^{[k]} = \mathbb{Z}_{(p)}$, therefore

$$(✤) \subseteq \bigcap_p \mathbb{Z}_{(p)} = \mathbb{Z},$$

as required. ■

2.2.4 Koenigsmann's Existential Definition

Now for something of a different flavour: a result of Koenigsmann's final section of [Koe13], that $\mathbb{Z}$ is *not* diophantine in $\mathbb{Q}$ (provided the Bombieri-Lang conjecture is true). The version of the Bombieri-Lang conjecture we will use is the following:

Conjecture (Bombieri-Lang). *Let V be an absolutely irreducible affine or projective positive dimensional variety over $\mathbb{Q}$ such that $V(\mathbb{Q})$ is $\mathbb{Q}$-Zariski dense in V. Then so is*

$$\bigcup_{\phi : A \dashrightarrow V} \phi(A(\mathbb{Q})),$$

where the $\phi : A \dashrightarrow V$ run through all nontrivial $\mathbb{Q}$-rational maps from positive dimensional abelian varieties A defined over $\mathbb{Q}$, to V. ■

This conjecture is based on [HS00, §F.5.2] in the special case of varieties over $\mathbb{Q}$. Koenigsmann also makes note that "...our reading of 'nontrivial' in the Conjecture implies that there are such $\phi : A \dashrightarrow V$ over $\mathbb{Q}$ for which $\phi(A(\mathbb{Q}))$ is infinite (it is certainly in the spirit of the conjecture that the $\phi(A(\mathbb{Q}))$ account for $V(\mathbb{Q})$ being dense in V but, strictly speaking, this reading gives a slightly stronger, though equally plausible, conjecture)."

[3] And 1109 existential quantifiers by [Koe10, Corollary 18].

In order to obtain the desired result we must deal with the following lemma which, in layman's terms, posits that (for hypersurfaces V) if $V(\mathbb{Q})$ is Zariski dense in V then there are not many points of $V(\mathbb{Q})$ with integer first coordinate:

Lemma 2.2.17. *Assume the Bombieri-Lang Conjecture as presented above. Let $f \in \mathbb{Q}[x_1, \ldots, x_{n+1}] \setminus \mathbb{Q}[x_1, \ldots, x_n]$ be absolutely irreducible and let $V = V(f) \subseteq \mathbb{A}^{n+1}$ be the affine hypersurface defined over $\mathbb{Q}$ by f. Assume that $V(\mathbb{Q})$ is Zariski dense in V and denote by $\pi : \mathbb{A}^{n+1} \to \mathbb{A}$ the projection map to the first coordinate. Then*

$$V(\mathbb{Q}) \cap \pi^{-1}(\mathbb{Q} \setminus \mathbb{Z})$$

is also Zariski dense in V.

Proof. This is [Koe13, Lemma 22]. For any $g \in \mathbb{Q}[x_1, \ldots, x_n] \setminus \{0\}$ by the Bombieri-Lang conjecture there exists an abelian variety A and rational map $\phi : A \dashrightarrow V$ both defined over $\mathbb{Q}$ such that $\phi(A(\mathbb{Q})) \setminus V(g)(\mathbb{Q})$ is infinite (we consider $V(g)$ as a subset of $\mathbb{A}^{n+1}$). We may assume that $\pi(\phi(A(\mathbb{Q})) \setminus V(g)(\mathbb{Q}))$ is infinite and the pole divisor $D = (\pi \circ \phi)_\infty$ is what is known as 'ample'[4] (we may need to compose ϕ with another rational map to do so).

By [Fal91, Corollary 6.2] there are only finitely many $P \in A(\mathbb{Q}) \setminus D(\mathbb{Q})$ with $\pi(\phi(P)) \in \mathbb{Z}$, so $(\phi(A(\mathbb{Q})) \setminus V(g)(\mathbb{Q})) \cap \pi^{-1}(\mathbb{Z})$ is finite meaning

$$(V(\mathbb{Q}) \setminus V(g)(\mathbb{Q})) \cap \pi^{-1}(\mathbb{Q} \setminus \mathbb{Z}) \neq \emptyset,$$

as recall $\phi(A(\mathbb{Q})) \subseteq V(\mathbb{Q})$. As g was arbitrary we conclude $V(\mathbb{Q}) \cap \pi^{-1}(\mathbb{Q} \setminus \mathbb{Z})$ is Zariski dense in V, as required. ■

The following theorem has been proven model-theoretically in [Koe10] and algebraically in [Koe13]. Although the former takes longer to prove, the author is partial to it.

Theorem 2.2.18. *Assume the Bombieri-Lang conjecture as above. Then there is no infinite subset of $\mathbb{Z}$ existentially definable in $\mathbb{Q}$; in particular, $\mathbb{Z}$ is not diophantine in $\mathbb{Q}$.*

Proof. Suppose $A \subseteq \mathbb{Z}$ is infinite and defined in $\mathbb{Q}$ by an existential formula $\phi_A(x)$. Let $\mathbb{Q}^*$ be a countable proper elementary extension of $\mathbb{Q}$, realising the type $\{\phi_A(x) \wedge x \neq a : a \in A\}$ (given by the Compactness Theorem; here we use A is infinite). Suppose ζ_1 witnesses this type. Note ζ_1 is a nonstandard natural number.

[4]See *Definition A.2.2* for 'divisor' and [HS00, §A.3.2] for 'ample'.

The map $\mathbb{N} \to \mathbb{N}; n \mapsto 2^n$ is definable in $\mathbb{N}$, hence $\mathbb{Q}$. Thus $\zeta_2 := 2^{\zeta_1}$ is a nonstandard natural number as well. The elements $\zeta_1, \zeta_2, \ldots, \zeta_{i+1} := 2^{\zeta_i}, \ldots$ are algebraically independent over $\mathbb{Q}$, and they form a countable transcendence base of $\mathbb{Q}^*$ over $\mathbb{Q}$. Finally, set $A^* := \phi_A(\mathbb{Q}^*)$ and notice $\zeta_1 \in A^*$ by design.

Let $K = \mathbb{Q}(\zeta_1, \zeta_2, \ldots)$. As $\mathbb{Q}^*$ is countable we find $\alpha_i \in \mathbb{Q}^*$, $i \in \mathbb{N}$ such that

$$K(\alpha_1) \subseteq K(\alpha_2) \subseteq \cdots \quad \text{with} \bigcup_{i=1}^{\infty} K(\alpha_i) = \mathbb{Q}^*,$$

where in addition we make the standard assumption that, for each $i \in \mathbb{N}$ the minimal polynomial of α_i is of the form $f_i(\zeta_1, \ldots, \zeta_i, z) \in K[z]$ with coefficients in $\mathbb{Q}$. As $\mathbb{Q}$ is relatively algebraically closed in $\mathbb{Q}^*$, all the polynomials $f_i \in \mathbb{Q}[x_1, \ldots, x_i, z]$ are absolutely irreducible over $\mathbb{Q}$.

Consider the following set of formulae in the free variables $x_1, x_2, \ldots$:

$$\begin{aligned} p :=& \{g(x_1, \ldots, x_i) \neq 0 : g \in \mathbb{Q}[x_1, \ldots, x_i] \setminus \{0\}, i \in \mathbb{N}\} \\ & \cup \{\exists z f_i(x_1, \ldots, x_i, z) = 0 : i \in \mathbb{N}\} \\ & \cup \{x_1 \in \mathbb{Q} \setminus \mathbb{Z}\}. \end{aligned}$$

Note this last condition is (existentially) definable by the results of *Chapter 2*.

Claim: *p is finitely realisable in $\mathbb{Q}$.*
Let $p_0 \subseteq p$ be finite and let k be the highest index occurring in p_0 among the formulae from the second line above. Since the $K(\alpha_j)$ are linearly ordered by inclusion, if $\exists z f_k(x_1, \ldots, x_k, z) = 0$ then $\exists z f_i(x_1, \ldots, x_i, z) = 0$ for all $i < k$. Hence we need only check that $V(f_k)(\mathbb{Q}) \cap \pi^{-1}(\mathbb{Q} \setminus \mathbb{Z})$ is $\mathbb{Q}$-Zariski dense in $V(f_k)$; this will follow from *Lemma 2.2.17* provided $V(f_k)(\mathbb{Q})$ is $\mathbb{Q}$-Zariski dense in $V(f_k)$. We know that it is, as $(\zeta_1, \ldots, \zeta_k, \alpha_k) \in V(f_k)(\mathbb{Q}^*)$, so if $V(f_k)(\mathbb{Q}) \setminus V(g) = \emptyset$ with $g \in \mathbb{Q}[x_1, \ldots, x_k]$, then $g(\zeta_1, \ldots, \zeta_k) = 0$ in $\mathbb{Q}^*$ and $\zeta_1, \ldots, \zeta_k$ are algebraically independent over $\mathbb{Q}$; a contradiction.

Therefore by Compactness we can realise p in some elementary extension $\mathbb{Q}^{**}$ of $\mathbb{Q}$. Calling the realising ω-tuple in $\mathbb{Q}^{**}$ again $\zeta_1, \zeta_2, \ldots$ our construction yields that $\mathbb{Q}^*$ can be realised as a subfield of $\mathbb{Q}^{**}$. Finally note that $\zeta_1 \in A^* \subseteq \mathbb{Z}^*$ and $\zeta_1 \notin \mathbb{Z}^{**}$, hence $\zeta_1 \notin A^{**} := \phi_A(\mathbb{Q}^{**})$. But ϕ_A is an existential formula so its realisations should pass from the structure $\mathbb{Q}^*$ to its superstructure $\mathbb{Q}^{**}$; a contradiction. Therefore A has no existential definition in $\mathbb{Q}$, as required. ■

Remark 2.2.19. We will revisit existential definitions (this time, for function fields) in *Chapter 5*. □

Chapter 3

Class Field Theory: An Introduction

Definition 3.0.1. A *global field* is a field which is either an *(algebraic) number field* (a finite field extension of $\mathbb{Q}$) or a *global function field* (a finite field extension of $\mathbb{F}_q(t)$).

The results of §2.2.1 have been generalised to global fields; to number fields by Park [Par13] and to global function fields by Eisenträger & Morrison [EM18]. In order to tackle Park's and Eisenträger & Morrison's work we must first present the basic definitions and main theorems of *class field theory*. It is important that the reader be familiar with the terminology covered in *Appendices A.1 & A.2* before examining the next section.

We will primarily operate from Milne's book [Mil13], and all results mentioned without proof can be found in Takagi's landmark paper [Tak20][1].

3.1 The Main Theorems of Class Field Theory

Let K be a number field (initially). We state the following definition in a general fashion, but one can see how it applies for $F = K$ and $A = \mathcal{O}_K$:

Definition 3.1.1. Let A be a Dedekind domain with field of fractions F. A *fractional ideal* I of F is a set of the form

$$I = \tfrac{1}{a}J, \quad \text{where } a \in A \text{ and } J \text{ is an ideal}^2 \text{ of } A.$$

[1] See [Con18a, Theorem 5.6] for a list of major class field theory results due to [Tak20].

[2] Sometimes called an *integral ideal* to distinguish from fractional ideals.

One can show the set of all fractional ideals of K forms a group (cf. [Neu99, I 3.8]). The group of fractional ideals of K is denoted I_K. For a finite set S of primes of K we define I_K^S to be the subgroup of I_K generated by prime ideals *not* in S. To elaborate further, each element $\mathfrak{a}$ of I_K^S factors uniquely as

$$\mathfrak{a} = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_s^{n_s}, \quad \mathfrak{p}_i \notin S, \quad n_i \in \mathbb{Z}\,.$$

I_K^S is thus the free abelian group generated by the prime ideals not in S.

Define

$$\begin{aligned} K^S &= \{a \in K^\times : \ \mathrm{ord}_\mathfrak{p}(a) = 0 \text{ for all finite } \mathfrak{p} \in S\} \\ &= \{a \in K^\times : (a) \in I_K^S\} \text{ where } (a) = a\mathcal{O}_K, \end{aligned}$$

and let $i : K^S \to I_K^S$ be the canonical map $a \mapsto (a)$. *Lemma 1.1* of [Mil13, Chapt. V] demonstrates there is an exact sequence

$$0 \longrightarrow \mathcal{O}_K^\times \xrightarrow{p_1} K^S \xrightarrow{\ i\ } I_K^S \xrightarrow{p_2} I_K/i(K^\times) \longrightarrow 0$$

where p_1 is the natural inclusion and p_2 is the natural inclusion composed with the natural projection. The group $\mathcal{C}_K = I_K/i(K^\times)$ with the multiplication operation

$$\text{for all } \mathfrak{a},\, \mathfrak{b} \in I_K \qquad \mathfrak{a}i(K^\times) \cdot \mathfrak{b}i(K^\times) = (\mathfrak{a}\mathfrak{b})i(K^\times)$$

(sometimes this is written in the equivalence class notation: $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$)

is known as the *(full) ideal class group of* K. Not only is p_2 surjective but moreover every class in $\mathcal{C}_K$ can be represented by an *integral* ideal in I_K^S.

The next important concept is that of a *modulus*:

Definition 3.1.2. A *modulus* for K is a function $m : \{\text{primes of } K\} \to \mathbb{Z}$ such that

(1) $m(\mathfrak{p}) \geq 0$ for all primes $\mathfrak{p}$ and $m(\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p}$,

(2) if $\mathfrak{p}$ is real, then $m(\mathfrak{p}) \in \{0, 1\}$,

(3) if $\mathfrak{p}$ is complex, then $m(\mathfrak{p}) = 0$.

One generally writes $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{m(\mathfrak{p})}$ and calls this ideal a modulus, too. It can also be written as $\mathfrak{m} = \mathfrak{m}_\infty\, \mathfrak{m}_0$ where $\mathfrak{m}_\infty$ is a product of real primes and $\mathfrak{m}_0$ is a product of prime ideals (hence is an ideal of $\mathcal{O}_K$).

Given a modulus $\mathfrak{m}$ we define $K_{\mathfrak{m},1}$ to be the set of $a \in K^\times$ such that

$$\mathrm{ord}_\mathfrak{p}(a - 1) \geq m(\mathfrak{p}) \qquad \text{for all finite } \mathfrak{p} \mid \mathfrak{m},$$

$$\sigma_{\mathfrak{p}}(a) > 0 \qquad \text{for all real } \mathfrak{p} \mid \mathfrak{m},$$

where $\sigma_{\mathfrak{p}}$ is the embedding $\sigma_{\mathfrak{p}} : K \hookrightarrow \mathbb{R}$.

Let $S(\mathfrak{m})$ be the set of primes dividing $\mathfrak{m}$. Then for a finite $\mathfrak{p} \in S(\mathfrak{m})$ and $a \in K_{\mathfrak{m},1}$, $\mathrm{ord}_{\mathfrak{p}}(a-1) > 0 = \mathrm{ord}_{\mathfrak{p}}(1)$, hence by the nonarchimedian property $\mathrm{ord}_{\mathfrak{p}}(a) = 0$. For an infinite $\mathfrak{p} \in S(\mathfrak{m})$, $\mathrm{ord}_{\mathfrak{p}}(a) = 0$ immediately. We conclude there is a well-defined injection

$$i : K_{m,1} \to I_K^{S(\mathfrak{m})}, \qquad a \longmapsto (a).$$

Definition 3.1.3. The quotient of this map, $\mathcal{C}_{\mathfrak{m}} = I_K^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1})$, is known as the *ray class group (modulo* $\mathfrak{m}$*).*

We can also show ([Mil13, Prop. 1.6]) that every class in $\mathcal{C}_{\mathfrak{m}}$ is represented by an integral ideal $\mathfrak{a}$, and two integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ represent the same class in $\mathcal{C}_{\mathfrak{m}}$ if and only if there exist nonzero $a, b \in \mathcal{O}_K$ such that $a\mathfrak{a} = b\mathfrak{b}$, and also $a \equiv b \equiv 1 \mod \mathfrak{m}_0$ and a and b have the same sign for every real prime $\mathfrak{p} \mid \mathfrak{m}$. Thus, this is some generalisation of the full ideal class group $\mathcal{C}_K$ (if $\mathfrak{m} = 1$ then $\mathcal{C}_{\mathfrak{m}} = \mathcal{C}_K$ trivially).

Definition 3.1.4. If $\mathfrak{m} = \mathfrak{m}_0$, a product of finite primes, then $\mathcal{C}_{\mathfrak{m}}$ is known as the *narrow class group.*

Class groups have a direct connection to Galois groups of abelian extensions. One of the most important elements of the Galois group of a finite Galois extension of K is the *Frobenius element*, which concerns *unramified primes.*

Definition 3.1.5. ([Neu99, Chapt. I §9]). Let L be a finite Galois extension of K and let $\mathfrak{p}$ be a prime ideal of K. Suppose $\mathfrak{P}$ is a prime ideal of L *lying over* $\mathfrak{p}$ (i.e. $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$). Consider the natural map

$$\theta : D(\mathfrak{P}) \to \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_K/\mathfrak{p}), \qquad \sigma \mapsto (\alpha \mapsto \sigma(\alpha) \mod \mathfrak{p}),$$

where $D(\mathfrak{P})$ is the stabiliser of $\mathfrak{P}$ in $\mathrm{Gal}(L/K)$ (also known as the *decomposition group of* $\mathfrak{P}$ *over* K). There is an exact sequence

$$1 \to I(\mathfrak{P}) \to D(\mathfrak{P}) \xrightarrow{\theta} \mathrm{Gal}(\mathcal{O}_L/\mathfrak{P} \,/\, \mathcal{O}_K/\mathfrak{p}) \to 1,$$

where $I(\mathfrak{P})$, the kernel of θ, is the *inertia group of* $\mathfrak{P}$ *over* K. We say $\mathfrak{P}$ is *unramified* over $\mathfrak{p}$ if the inertia group is trivial. Otherwise, $\mathfrak{P}$ *ramifies*[3].

It can be shown that only finitely many primes of K may ramify in L [Neu99, Chapt. I (8.4)]. Now let $\mathfrak{B}$ be a prime ideal of L, unramified and lying over a prime ideal $\mathfrak{p}$ of K.

[3]One can define ramification in a more general context - see [Neu99, Chapt. I §8].

Definition 3.1.6. An element $\sigma \in \mathrm{Aut}(L/K)$ satisfying $\sigma\mathfrak{B} = \mathfrak{B}$ and, for all $\alpha \in \mathcal{O}_L$, $\sigma\alpha \equiv \alpha^{\#\mathcal{O}_K/\mathfrak{p}} \mod \mathfrak{B}$ is known as the *Frobenius element at* $\mathfrak{B}$ and denoted $(\mathfrak{B}, L/K)$.

One of the major results of Galois theory is the next theorem:

Theorem 3.1.7. *If L is a finite Galois extension over K, for all prime ideals $\mathfrak{p}$ of K if $\mathfrak{B}$ is an unramified prime ideal of L lying over $\mathfrak{p}$ then $(\mathfrak{B}, L/K)$ exists and is unique.*

Proof. By *Definition 3.1.5*, $D(\mathfrak{P}) \cong \mathrm{Gal}(\mathcal{O}_L/\mathfrak{B} \,/\, \mathcal{O}_K/\mathfrak{p})$ hence $D(\mathfrak{B})$ is cyclic with a canonical generator, namely the Frobenius map $x \mapsto x^{\#\mathcal{O}_K/\mathfrak{p}}$ of $\mathrm{Gal}(\mathcal{O}_L/\mathfrak{B} \,/\, \mathcal{O}_K/\mathfrak{p})$. This element of $D(\mathfrak{B})$ is $(\mathfrak{B}, L/K)$ exactly. ■

Moreover, as $\mathrm{Gal}(L/K)$ acts transitively on the primes dividing $\mathfrak{p}$, the set $\{(\mathfrak{B}, L/K) : \mathfrak{B}|\,\mathfrak{p}\}$ is a conjugacy class in $\mathrm{Gal}(L/K)$ which we shall denote $(\mathfrak{p}, L/K)$. We pause here to note that if L/K is abelian, $(\mathfrak{p}, L/K)$ contains only one element (so is treated as an element of $\mathrm{Gal}(L/K)$ itself).

Excitingly, this brings us to the two main theorems in class field theory, both of which concern the *Artin map.*

Definition 3.1.8. For every finite set S of primes of K containing all primes which ramify in L, we can define a homomorphism

$$\psi_{L/K} : I_K^S \to \mathrm{Gal}(L/K), \qquad \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_t^{n_t} \longmapsto \prod_{i=1}^{t} (\mathfrak{p}_i, L/K)^{n_i},$$

known as the *(global) Artin map*, or the *reciprocity map.*

Definition 3.1.9. If S is a finite set of primes of K, a homomorphism $\psi : I_K^S \to G$ *admits a modulus* $\mathfrak{m}$ if there exists a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) \supset S$ such that $\psi(i(K_{\mathfrak{m},1})) = 0$. (So ψ admits $\mathfrak{m}$ if and only if it factors through $\mathcal{C}_{\mathfrak{m}}$.)

The first main theorem is known as the *reciprocity law*:

Theorem 3.1.10. Reciprocity Law. *Let L be a finite abelian extension of K and S be the set of primes of K which ramify in L. Then the Artin map $\psi_{L/K} : I_K^S \to \mathrm{Gal}(L/K)$ admits a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$ and it defines an isomorphism*

$$I_K^{S(\mathfrak{m})}/i(K_{m,1}) \cdot \mathrm{Norm}(I_L^{S(\mathfrak{m})}) \xrightarrow{\cong} \mathrm{Gal}(L/K),$$

where the norm map $\mathrm{Norm}_{L/K} = \mathrm{Norm} : I_L \to I_K$ is the unique homomorphism such that for any prime ideal $\mathfrak{B}$ of L lying over $\mathfrak{p}$ of K, $\mathrm{Norm}(\mathfrak{B}) = \mathfrak{p}^{f(\mathfrak{B}/\mathfrak{p})}$, where $f(\mathfrak{B}/\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{B} : \mathcal{O}_K/\mathfrak{p}]$ is the inertia degree of $\mathfrak{B}$ over $\mathfrak{p}$. ■

Now, write $I_K^{\mathfrak{m}}$ for $I_K^{S(\mathfrak{m})}$ and $I_L^{\mathfrak{m}}$ for $I_L^{S(\mathfrak{m})'}$ where $S(\mathfrak{m})'$ contains the prime ideals of L lying over a prime in $S(\mathfrak{m})$.

Definition 3.1.11. A subgroup H of $I_K^{\mathfrak{m}}$ is called a *congruence subgroup (modulo $\mathfrak{m}$)* if $i(K_{\mathfrak{m},1}) \subseteq H \subseteq I_K^{\mathfrak{m}}$.

The second main theorem of class field theory is the *Existence Theorem*:

Theorem 3.1.12. Existence Theorem. *Let $\mathfrak{m}$ be a modulus. For every congruence subgroup H modulo $\mathfrak{m}$, there exists a finite abelian extension L/K such that $H = i(K_{\mathfrak{m},1}) \cdot \mathrm{Norm}_{L/K}(I_L^{\mathfrak{m}})$ and the set of primes ramifying in L is precisely $S(\mathfrak{m})$.* ■

This is known as the "Existence Theorem" as in particular it asserts the existence of an important abelian extension of K, called the *ray class field (modulo $\mathfrak{m}$)* and denoted $K_{\mathfrak{m}}$. This extension satisfies the following properties, listed in [Cla18]:

(1) There is a canonical isomorphism $\mathcal{C}_{\mathfrak{m}} = I_K^{\mathfrak{m}}/i(K_{\mathfrak{m},1}) \cong \mathrm{Gal}(K_{\mathfrak{m}}/K)$. This follows from the *Existence Theorem* and *Reciprocity Law* (*Theorems 3.1.12 & 3.1.10*) by choosing $H = i(K_{\mathfrak{m},1})$. Thus, there is a correspondence between the ray class group and ray class field of a modulus $\mathfrak{m}$.

(2) In the number field case, $K_{\mathfrak{m}}/K$ is a finite extension. The ray class field of a function field contains the extension $\overline{\mathbb{F}_q}$ of the constant field, hence is an infinite extension. Later, this will be an important distinction.

(3) The extension $K_{\mathfrak{m}}$ ramifies only at primes dividing the modulus.

(4) If $\mathfrak{m} \mid \mathfrak{m}'$ then $K_{\mathfrak{m}} \subseteq K_{\mathfrak{m}'}$.

According to [Cla18], "the divisibility relation endows the moduli with the structure of a directed set (a partially ordered set in which any pair of elements is less than or equal to some third element). Therefore by [item (4)] the ray class fields form a directed system of fields". Within this directed system we may take a limit and obtain:

(5) $\lim_{\to \mathfrak{m}} K_{\mathfrak{m}} = K^{ab}$, the maximal abelian extension of K. In other words, every finite abelian extension of K is contained in some ray class field.

For a field $L \subseteq K_{\mathfrak{m}}$, define

$$\mathrm{Norm}(\mathcal{C}_{L,\mathfrak{m}}) = i(K_{\mathfrak{m},1}) \cdot \mathrm{Norm}(I_L^{\mathfrak{m}}) \qquad \mod i(K_{\mathfrak{m},1}).$$

Corollary 3.1.13. *Fix a modulus* $\mathfrak{m}$*. There is a 1-to-1 correspondence*

$$\{\textit{abelian extensions of } K \textit{ contained in } K_{\mathfrak{m}}\} \leftrightarrow \{\textit{subgroups of } \mathcal{C}_{\mathfrak{m}}\},$$

given by $L \mapsto \mathrm{Norm}(\mathcal{C}_{L,\mathfrak{m}})$*. Moreover,*

$$\begin{aligned} L_1 \subseteq L_2 &\iff \mathrm{Norm}(\mathcal{C}_{L_1,\mathfrak{m}}) \supseteq \mathrm{Norm}(\mathcal{C}_{L_2,\mathfrak{m}}), \\ \mathrm{Norm}(\mathcal{C}_{L_1\cdot L_2,\mathfrak{m}}) &= \mathrm{Norm}(\mathcal{C}_{L_1,\mathfrak{m}}) \cap \mathrm{Norm}(\mathcal{C}_{L_2,\mathfrak{m}}), \\ \mathrm{Norm}(\mathcal{C}_{L_1\cap L_2,\mathfrak{m}}) &= \mathrm{Norm}(\mathcal{C}_{L_1,\mathfrak{m}}) \cdot \mathrm{Norm}(\mathcal{C}_{L_2,\mathfrak{m}}). \end{aligned}$$

■

We shall finally reap the benefits of class field theory after we introduce one more concept; that of a *conductor*.

Let L/K be an abelian extension and $\psi_{L/K} : I_K^{S(\mathfrak{n})} \to \mathrm{Gal}(L/K)$ be the Artin map for a modulus $\mathfrak{n}$. We say *Artin Reciprocity holds for* $\mathfrak{n}$ if ψ factors through $\mathcal{C}_{\mathfrak{n}}$; equivalently if $i(K_{\mathfrak{n},1}) \subseteq \mathrm{Ker}(\psi)$.

Definition 3.1.14. The *conductor* of L/K, denoted $\mathfrak{f}(L/K)$, is the highest common factor of all moduli for which Artin reciprocity holds. Equivalently[4],

$$f(L/K) = \gcd\{\mathfrak{m} \,:\, K_{\mathfrak{m}} \supseteq L\}.$$

Due to the Reciprocity Law, there is a modulus $\mathfrak{m}$ with $S(\mathfrak{m})$ equal to the set of primes of K which ramify in L, such that the kernel of the Artin map $\psi_{L/K} : I^{S(\mathfrak{m})} \to \mathrm{Gal}(L/K)$ contains $i(K_{\mathfrak{m},1})$. So $\mathfrak{f}(L/K)$ is always nontrivial. Moreover, Artin reciprocity holds for $\mathfrak{f}(L/K)$ so it is then the *smallest* modulus such that $\psi_{L/K}$ factors through $\mathcal{C}_{\mathfrak{f}(L/K)}$. By its definition then the conductor is divisible exactly by the primes ramifying in L.

Lemma 3.1.15. *The subfields of the ray class field* $K_{\mathfrak{m}}$ *containing* K *are those with conductor* $\mathfrak{f} \mid \mathfrak{m}$*.*

Proof. Note that if $K_{\mathfrak{m}} \supseteq L \supseteq K$ then $f(L/K) | f(K_{\mathfrak{m}}/K)$ and by definition $f(K_{\mathfrak{m}}/K) \mid \mathfrak{m}$. ■

We are now ready to reap what we have sown.

Example 3.1.16. Let $K = \mathbb{Q}(\sqrt{m})$ where m is a square-free integer. Identify $\mathrm{Gal}(K/\mathbb{Q})$ with $\{\pm 1\}$. The modulus $\mathfrak{m} = 4|m|\infty$ is admissible for this extension ([Con18a, Ex. 5.8]), so the Artin map is the homomorphism determined by

$$\psi_{K/\mathbb{Q}} : I_{\mathbb{Q}}^{S(\mathfrak{m})} \to \mathrm{Gal}(K/\mathbb{Q}); \text{ esp. for } p \in \mathbb{Z} \text{ a prime, } p \mapsto (p, \mathbb{Q}(\sqrt{m})/\mathbb{Q}).$$

Assume $p \neq 2$ (which we can do by choice of $\mathfrak{m}$). In order to compute this Frobenius element we break into two cases:

[4] cf. [Cla18, (RC5)].

Case 1: $m \equiv a^2 \mod p$. Then the ideal $p\mathcal{O}_K$ splits; $p\mathcal{O}_K = (p, \sqrt{m} + a)(p, \sqrt{m} - a) = \mathfrak{B}^+\mathfrak{B}^-$ by [Mil17, Theorem 3.41]. As $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, the conjugacy class $\{(\mathfrak{B}, K/\mathbb{Q}) : \mathfrak{B}|p\}$ has size one, so $(p, K/\mathbb{Q}) = (\mathfrak{B}^+, K/\mathbb{Q}) = (\mathfrak{B}^-, K/\mathbb{Q})$. The Frobenius element satisfies

(1) $\sigma\mathfrak{B}^+ = \mathfrak{B}^+$,

(2) For all $\alpha \in \mathcal{O}_K$, $\sigma\alpha \equiv \alpha^p \mod \mathfrak{B}^+$,

hence $(p, K/\mathbb{Q}) = a + b\sqrt{m} \mapsto a + b\sqrt{m}$ "=" 1.

Case 2: If m is not a square mod p, then $p\mathcal{O}_K = (p)$ is inert by [Mil17, Theorem 3.41]. The Frobenius element must satisfy

(1) $\sigma p = p$ (trivial, as $\mathrm{Gal}(K/\mathbb{Q})$ fixes p),

(2) For all $\alpha \in \mathcal{O}_K$, $\sigma\alpha \equiv \alpha^p \mod p$,

By use of Fermat's Little Theorem, we see $(p, K/\mathbb{Q}) = a + b\sqrt{m} \mapsto a - b\sqrt{m}$ "=" -1.

Therefore $(p, K/\mathbb{Q}) = 1 \Leftrightarrow \left(\frac{m}{p}\right) = 1$, and so $\psi_{K/\mathbb{Q}} : p \mapsto \left(\frac{m}{p}\right)$, where $\left(\frac{m}{p}\right)$ is the Legendre symbol. We have just demonstrated the Legendre symbol is subsumed by the Artin map. □

In fact, the Reciprocity Law of *Theorem 3.1.10* also contains the usual Quadratic Reciprocity Law:

Example 3.1.17. (*See* [Con18a, Ex. 6.5]). Let p be an odd prime. Define $p^* = (-1)^{\frac{p-1}{2}} p$. This guarantees $p^* \equiv 1 \mod 4$ and thus for $K = \mathbb{Q}(\sqrt{p^*})$, 2 does not ramify in K. The Artin map $\psi_{K/\mathbb{Q}} : I_{\mathbb{Q}}^{p\infty} \to \mathrm{Gal}(K/\mathbb{Q})$ maps any odd prime q to $(q, K/\mathbb{Q})$. As the conductor $\mathfrak{f}(K/\mathbb{Q}) = p\infty$, $\psi_{K/\mathbb{Q}}$ admits the modulus $p\infty$. By the Reciprocity Law (*Theorem 3.1.10*), $i(K_{p\infty,1}) \subseteq \mathrm{Ker}(\psi_{K/\mathbb{Q}})$. Identifying $I_{\mathbb{Q}}^{p\infty}/i(K_{p\infty,1})$ with $(\mathbb{Z}/p\mathbb{Z})^\times$ and $\mathrm{Gal}(K/\mathbb{Q})$ with $\{\pm 1\}$ again, the Artin map is a homomorphism

$$(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}, \quad q \mod p \mapsto \left(\frac{p^*}{q}\right),$$

by the previous example. However, it can be shown the only homomorphism from $(\mathbb{Z}/p\mathbb{Z})^\times$ onto $\{\pm 1\}$ is the Legendre map

$\left(\frac{\cdot}{p}\right) : x \mod p \mapsto \left(\frac{x}{p}\right)$, hence $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$. Using the formula

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}},$$

we obtain the Quadratic Reciprocity Law

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

exactly. □

Not only does the Artin Reciprocity Law generalise the Quadratic Reciprocity Law, it generalises Hilbert's Reciprocity Law of $\prod_v (a,b)_v = 1$ for $a, b \in \mathbb{Q}^\times$. This is covered by Conrad [Con18a, §7] working off of [Has30]. This coincidentally relates back to Hilbert's list of 23 problems, where Artin's reciprocity map for *abelian* extensions of $\mathbb{Q}$ is accepted as a partial solution to the 9th problem:

Conjecture (Hilbert's 9th Problem). *Find the most general law of the Quadratic Reciprocity Theorem in any algebraic number field.* ■

According to [Con18a], "three themes in number theory at the end of the 19th century led to class field theory: relations between abelian extensions and ideal class groups, density theorems for primes . . . and reciprocity laws". We have seen the study of the Artin map is the study of reciprocity laws, and we have seen one connection between abelian extensions and ideal class groups (*Corollary 3.1.13*). Here is another, which one could argue motivated the existence of the whole subject (or, at least, motivated Hilbert):

Theorem 3.1.18. (Kronecker-Weber). *Every finite abelian extension of* $\mathbb{Q}$ *lies in a cyclotomic field* $\mathbb{Q}(\zeta_m)$ *for some* m.

Hilbert was deeply interested in this theorem. It was he who gave the first complete proof in 1896 [Hil96], and included its generalisation as one of his 23 problems published in 1900:

Conjecture (Hilbert's 12th Problem). *Extend the Kronecker-Weber theorem on abelian extensions of the rational numbers to any base number field.* ■

Remarkably, the Kronecker-Weber Theorem can be deduced from the Artin Reciprocity Law.

Proof of the Kronecker-Weber Theorem: Let m be a positive integer. The ray class group for $\mathfrak{m} = m\infty$ is $\mathcal{C}_\mathfrak{m} = I_\mathbb{Q}^\mathfrak{m}/i(\mathbb{Q}_{\mathfrak{m},1}) \cong (\mathbb{Z}/m\,\mathbb{Z})^\times$, hence the ray class field $L_\mathfrak{m}$ is the field where

$$\mathrm{Gal}(L_\mathfrak{m}/\,\mathbb{Q}) \cong \mathcal{C}_\mathfrak{m} \cong (\mathbb{Z}/m\,\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\,\mathbb{Q}),$$

so $L_\mathfrak{m} = \mathbb{Q}(\zeta_m)$. Every abelian extension of $\mathbb{Q}$ has conductor dividing $\mathfrak{m}$ for some m, hence by *Lemma 3.1.15* is contained in $\mathbb{Q}(\zeta_m)$ as required. ■

The final concern of 19th century number theory which led to class field theory was determining the density of primes (both in $\mathbb{Q}$ and its extensions). Remarkably, one can show that every element of the Galois group of a finite extension of number field L/K has (infinitely many) representations as a Frobenius element for some prime of K:

Theorem 3.1.19. Chebotarev's Density Theorem. *Let L/K be a finite extension of number fields with Galois group G and let C be a conjugacy class in G. Then the set of prime ideals of K such that $(\mathfrak{p}, L/K) = C$ has density $\frac{|C|}{|G|}$ in the set of all prime ideals of K. In particular,*

(1) If G is abelian, then for a fixed $\tau \in G$, the set of prime ideals $\mathfrak{p}$ of K with $(\mathfrak{p}, L/K) = \tau$ has density $\frac{1}{|G|}$.

(2) For any $\sigma \in G$, there are infinitely many primes $\mathfrak{p}$ of K with $(\mathfrak{p}, L/K) = \sigma$.

(3) The set of prime elements which completely split in L has density $\frac{1}{|G|}$.

Proof. The density theorem for an abelian extension L/K is a consequence of applying the surjective homomorphism $\mathcal{C}_\mathfrak{m} \to \mathrm{Gal}(L/K)$ (from *Theorem 3.1.10*) to a result of Milne ([Mil13, Theorem 2.5]) noting the primes of K are equidistributed amongst the classes of $\mathcal{C}_\mathfrak{m}$. Milne also remarks that the nonabelian case can be derived from the abelian one [Mil13, Chapt. VIII].

(1) is clear and (2) follows from the infinitude of primes of K. For (3), note that if $\mathfrak{p}$ splits completely in L if and only if $(\mathfrak{p}, L/K)$ is trivial (cf. the proof of *Lemma 3.1.22*, yet to appear) so $|C| = 1$. ■

Chebotarev's theorem is a generalisation of Dirichlet's theorem on arithmetic progressions; Dirichlet's theorem now follows very easily:

Corollary 3.1.20. (Dirichlet's Theorem on Arithmetic Progressions). *For coprime $a, d \in \mathbb{Z}$, there are infinitely many primes in the arithmetic progression $a, a+d, a+2d, \ldots$.*

Proof. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_d)$. Consider the conjugacy class $C = \{\zeta_d \mapsto \zeta_d^a\}$. The density of those primes p with $(p, \mathbb{Q}(\zeta_d)/\mathbb{Q}) = C$ is positive, hence there exist an infinitude of primes congruent to a modulo d, as required. ■

The final important object we will introduce for class field theory is the *Hilbert class field*.

Definition 3.1.21. The ray class group for the modulus $\mathfrak{m} = 1$ is the full ideal class group, and the corresponding ray class field is known as the *Hilbert class field*; it is the maximal abelian extension H of K that is unramified at *all* primes[5].

As a consequence of this definition, the full ideal class group of K is $\mathcal{C}_K \cong \mathrm{Gal}(H/K)$ so $[H : K] = h_K$, the class number of K.

Recall that $\mathcal{O}_K$ is a principal ideal domain if and only if $h_K = 1$; it is often said that the larger (than 1) h_K is, the "further away" $\mathcal{O}_K$ is to being a principal ideal domain. In fact, this notion can be made precise using the Hilbert class field.

Lemma 3.1.22. *The prime ideals of K which split completely in H are exactly the principal ideals.*

Proof. If $\mathfrak{p}$ a prime ideal of K splits completely, then $\mathfrak{p}\,\mathcal{O}_H = \mathfrak{B}_1 \dots \mathfrak{B}_{h_K}$ and each inertia degree $f_i = 1, 1 \leq i \leq h_K$. Therefore for each i, $f_i = [\mathcal{O}_H/\mathfrak{B}_i : \mathcal{O}_K/\mathfrak{p}] = 1$ so the Galois groups $\mathrm{Gal}(\mathcal{O}_H/\mathfrak{B}_i \,/\, \mathcal{O}_K/\mathfrak{p}) \cong \{1\}$, hence for each i the decomposition groups $D(\mathfrak{B}_i) \cong \{1\}$ meaning the Frobenius element $(\mathfrak{p}, H/K)$ is trivial. Thus $\mathfrak{p}$ is principal, by the Artin map isomorphism $\mathcal{C}_K \cong \mathrm{Gal}(H/K)$.

On the other hand, if $\mathfrak{p}$ is a principal ideal of K then the Frobenius element $(\mathfrak{p}, H/K)$ is trivial (by the Artin map again) so the Galois groups $\mathrm{Gal}(\mathcal{O}_H/\mathfrak{B}_i \,/\, \mathcal{O}_K/\mathfrak{p})$ for $1 \leq i \leq \frac{[H:K]}{f_i}$ are trivial, meaning $f_i = [\mathcal{O}_H/\mathfrak{B}_i : \mathcal{O}_K/\mathfrak{p}] = 1$ for all i. As H/K is Galois and $\mathfrak{p}$ is unramified, we conclude $\mathfrak{p}$ splits completely as required. ■

Corollary 3.1.23. *The density of the principal primes in K is $\frac{1}{h_K}$.*

Proof. By the Chebotarev Density Theorem (*Theorem 3.1.19 (3)*), the set of prime numbers which split in H has density

$$\frac{1}{|\,\mathrm{Gal}(H/K)|} = \frac{1}{|\mathcal{C}_K|} = \frac{1}{h_K}.$$

[5]This includes the real primes, where a real prime is unramified if it remains real in the extension. A complex prime cannot ramify.

However, as *Lemma 3.1.22* demonstrates, the set of prime ideals which split completely in H is exactly the set of principal prime ideals in K. Therefore the density of the principal primes in K is $\frac{1}{h_K}$, as required. ■

Remark 3.1.24. Recall for a number field K, $\mathcal{O}_K$ is a principal ideal domain if and only if it is a unique factorisation domain. Thus, $\frac{1}{h_K}$ also measures how far from "unique factorisation" K is. □

The last phenomenon surrounding the Hilbert class field we will mention is sometimes called *principalization*; the situation where an extension of algebraic number field forces ideals of the lower field's ring of integers to become principal in the extension:

Theorem 3.1.25. (Principal Ideal Theorem). *Every ideal in K becomes principal in the Hilbert class field of K.*

Proof. See [Mil13, Theorem 3.17]. ■

We are now ready to give Park's universal definition of the ring of integers in a number field.

3.2 Park's Universal Definition

The first step in Park's definition of the ring of integers $\mathcal{O}_K$ in a number field K is setting up the relevant quaternion algebra machinery, in the style of Poonen and Koenigsmann. This time, however, since the primes and valuations we deal with may be more complicated (and some may be redundant) we deal directly with *places* instead of *primes*.

Notation A. See [Par13].

- Let $\mathbb{P}$ be the set of finite places of K and let $\mathbb{P} \cup \infty$ be the set of all places of K, both finite and infinite.
- 'Prime ideals of K' and their corresponding valuations are mentioned interchangeably, as according to *Appendix A.1*.
- $H_{a,b}$, $S_{a,b}$, $T_{a,b}$, U_v (previously U_p), $S_{a,b}(K_v)$ and $T_{a,b}(K_v)$ are defined as in *Definition 2.2.1*.
- $\Delta_{a,b} := \{v \in \mathbb{P} \cup \infty : H_{a,b} \otimes K_v \text{ does not split}\}$.

- For a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ and its associated valuation v, $\mathcal{O}_v$ is the set of elements in the completion K_v whose valuations are nonnegative. In the context of a given $a, b \in K$, for an infinite place v, we define

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

- Denote by $(\mathcal{O}_K)_\mathfrak{p}$ the localisation of $\mathcal{O}_K$ at $\mathfrak{p}$.

Using the same machinery as in [Koe13] or [Poo09a], we conclude for any $a, b \in K^\times$ such that $v(a) > 0$ or $v(b) > 0$ for each real archimedian place v, $T_{a,b} = \bigcap_{\mathfrak{p} \in \Delta_{a,b}} (\mathcal{O}_K)_\mathfrak{p}$ ([Par13, Prop. 2.3]; cf. (2.2) of this thesis).

The next step in [Koe13] was to produce a uniform diophantine definition of all $\mathbb{Z}_{(p)}$'s in $\mathbb{Q}$ using the congruence class of p modulo 8. As these "modulo 8" congruence classes cannot be replicated in general number fields, Park uses class field theory (in particular, ray classes) in their stead.

To obtain a uniform definition of the ring of integers of a number field as the intersection of localised rings as Park does [Par13, §3.3] we will fix the following notation:

Definition 3.2.1. Let a, b be totally positive[6] elements of $K^\times$ whose images in $K^\times/K^{\times 2}$ are independent. Let

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

be the Artin map. Denote by $\mathfrak{m}$ an admissible modulus to the extension $K(\sqrt{a}, \sqrt{b})/K$. Partition the set of primes of K as follows:

- $\mathbb{P}^{[i,j]} := \{\text{prime ideals } \mathfrak{p} \text{ of } K : \psi(\mathfrak{p}) = (i, j)\}$, where $i, j \in \{\pm 1\}$.
- $\mathbb{P}^{[i,j]}(p) := \{\text{primes } \mathfrak{p} \in \mathbb{P}^{[i,j]} : v_\mathfrak{p}(p) \text{ is odd}\}$.

Sometimes 'σ' is used in place of '$[i, j]$' in the superscript of $\mathbb{P}$.

With a **careful** choice of $a, b \in K^\times$, there is a direct correspondence between the sets of primes $\mathbb{P}^\sigma(p)$ and $\Delta_{x,p} \cap \Delta_{y,p}$ for x, y combinations of a, b:

Lemma 3.2.2. *Choosing a, b according to* [Par13, Lemma 3.19]*,*

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

■

[6] An element is *totally positive* if it is a square in $K_\mathfrak{p}$ for every infinite prime $\mathfrak{p}$.

From this point forward, fix a and b as in [Par13, Lemma 3.19]. The above lemma leads us to a definition strikingly similar to *Definition 2.2.6*:

Definition 3.2.3.

- $R_p^{[-1,-1]} := T_{a,p} + T_{b,p} = \bigcap_{\mathfrak{p}\in\Delta_{a,p}\cap\Delta_{b,p}}(\mathcal{O}_K)_\mathfrak{p} = \bigcap_{\mathfrak{p}\in\mathbb{P}^{[-1,-1]}(p)}(\mathcal{O}_K)_\mathfrak{p}$.
- $R_p^{[1,-1]} := T_{ab,p} + T_{b,p} = \bigcap_{\mathfrak{p}\in\Delta_{ab,p}\cap\Delta_{b,p}}(\mathcal{O}_K)_\mathfrak{p} = \bigcap_{\mathfrak{p}\in\mathbb{P}^{[1,-1]}(p)}(\mathcal{O}_K)_\mathfrak{p}$.
- $R_p^{[-1,1]} := T_{a,p} + T_{ab,p} = \bigcap_{\mathfrak{p}\in\Delta_{a,p}\cap\Delta_{ab,p}}(\mathcal{O}_K)_\mathfrak{p} = \bigcap_{\mathfrak{p}\in\mathbb{P}^{[-1,1]}(p)}(\mathcal{O}_K)_\mathfrak{p}$.
- $R_p^{[1,1]} := T_{ap,q} + T_{bp,q} = \bigcap_{\mathfrak{p}\in\Delta_{ap,q}\cap\Delta_{bp,q}}(\mathcal{O}_K)_\mathfrak{p}$.

As a result of this definition, once again[7] we have a representation of $\mathcal{O}_K$ in terms of the R_p^σ:

Proposition 3.2.4. *Let $(K^\times)^+$ denote the set of totally positive elements of K. Then*

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

Proof. Note that $\mathcal{O}_K = \bigcap_\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$ where $\mathfrak{p}$ ranges over all finite primes of $\mathcal{O}_K$. This proposition follows from *Lemmata 3.11 & 3.12* of [Par13]. ■

The next three sections of Park's paper are devoted to the Jacobson radical and attempting to create conditions which impose integrality at each finite place of K. This results in the following definition and proposition:

Definition 3.2.5. For each $\sigma \in \mathrm{Gal}(K(\sqrt{a},\sqrt{b})/K)$,

$$\begin{aligned}
&\Phi_\sigma := \{p \in K^\times : (p) \in I^{S(\mathfrak{m})},\ \psi((p)) = \sigma, \text{ and } \mathbb{P}(p) \subseteq \mathbb{P}^{[1,1]} \cup \mathbb{P}^\sigma\},\\
&\widetilde{\Phi_\sigma} := K^{\times 2}\cdot\Phi_\sigma,\\
&\Psi := \Bigg\{(p,q) \in \widetilde{\Phi_{(1,1)}} \times \widetilde{\Phi_{(-1,-1)}} :\ \prod_{\mathfrak{p}|\mathfrak{m}}(ap,q)_\mathfrak{p} = -1 \text{ and}\\
&\qquad\qquad p \in a\cdot K^{\times 2}\cdot(1 + J(R_q^{[-1,-1]}))\Bigg\}.
\end{aligned}$$

Proposition 3.2.6.

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

[7] See just before *Definition 2.2.7*.

(2) For any $p \in \Phi_\sigma$ and $\sigma \in \mathrm{Gal}(K(\sqrt{a},\sqrt{b})/K)$ with $\sigma \neq (1,1)$, $\mathbb{P}^\sigma(p) \neq \emptyset$. Also for $(p,q) \in \Psi$, $\Delta_{ap,q} \cap \Delta_{bp,q} \cap I^{S(\mathfrak{m})} \neq \emptyset$.

(3) The Jacobson radical $J(R_p^\sigma)$ is diophantine for $p \in \Phi_\sigma$, $\sigma \neq (1,1)$. For $(p,q) \in \Psi$, $J(R_{p,q}^{[1,1]})$ is diophantine.

(4) Hence Ψ is diophantine.

(5) For $\sigma \in \mathrm{Gal}(K(\sqrt{a},\sqrt{b})/K)$ with $\sigma \neq (1,1)$, if $\mathfrak{p} \nmid \mathfrak{m}_0$ is a prime ideal of K satisfying $\psi(\mathfrak{p}) = \sigma$ then there exists $p \in \Phi_\sigma$ such that $\mathfrak{p} \in \mathbb{P}^\sigma(p)$. Similarly if $\psi(\mathfrak{p}) = (1,1)$ then there exists $(p,q) \in \Psi$ such that $\Delta_{ap,q} \cap \Delta_{bp,q} = \{\mathfrak{p}\}$.

Proof. See *Lemmata 3.22, 3.23 & 3.25* of [Par13]. ■

Note that *(2)* is important as it demonstrates $\mathcal{O}_K \subseteq R_p^\sigma$ for all $p \in \Phi_\sigma$ and $\mathcal{O}_K \subseteq R_{p,q}^{[1,1]}$ for $(p,q) \in \Psi$.

Remark 3.2.7. The parallel drawn between *Definition 3.2.5* and Koenigsmann's Φ_k, Ψ is immediate. Also, *Proposition 3.2.6* is a combination of Corollary 15 and Proposition 16 of [Koe13] exactly. □

We put everything together in §4 of [Par13]. There, we have the theorem below. Recall the definition of the *Jacobson radical* of a semilocal ring R (*Definition 2.2.7*) and the notation

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

Theorem 3.2.8. ([Par13, Theorem 4.2]) *For any number field K,*

$$\mathcal{O}_K = \bigcap_{\mathfrak{p}|\mathfrak{m}_0} \widetilde{(\mathcal{O}_K)_\mathfrak{p}} \cap \left(\bigcap_{\sigma \neq (1,1)} \bigcap_{p \in \Phi_\sigma} \widetilde{R_p^\sigma} \right) \cap \bigcap_{(p,q)\in\Psi} \widetilde{R_{p,q}^{[1,1]}}. \tag{3.1}$$

Proof. The argument relies on *Proposition 3.2.6* in two ways: first, all the sets $\mathbb{P}^\sigma(p)$ and $\Delta_{ap,q} \cap \Delta_{bp,q}$ are nonempty for $p \in \Phi_\sigma$ and $(p,q) \in \Psi$ respectively, by *Proposition 3.2.6 (2)*. This means $\mathcal{O}_K$ is a subset of the RHS of (3.1). Second, we need to indicate that (for $\sigma \neq (1,1)$) we can always find $p, p' \in \Phi_\sigma$ such that

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

for $\mathfrak{p}_0 \nmid \mathfrak{m}_0$ - i.e. that integrality at $\mathfrak{p}_0$ is imposed. This can be done precisely by *Proposition 3.2.6 (5)*. Suppose $\psi(\mathfrak{p}_0) = (-1,-1)$. Choose

$p \in \Phi_{(-1,-1)}$ such that $\mathfrak{p}_0 \in \mathbb{P}^{(-1,-1)}(p)$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the rest of the primes in $\Delta_{a,p} \cap \Delta_{b,p}$. By our choice of a, b we may choose a prime ideal $\mathfrak{q}$ in the ideal class of $\mathfrak{p}_0^{-1}$ with $\psi(\mathfrak{q}) = (1,1)$ and $\mathfrak{q}$ distinct from $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ (cf. [Par13, Lemma 3.19]). Let $(p') = \mathfrak{p}_0\mathfrak{q}$; then $p' \in \Phi_{(-1,-1)}$ by construction and $\mathbb{P}^{(-1,-1)}(p) \cap \mathbb{P}^{(-1,-1)}(p') = \{\mathfrak{p}_0\}$ as desired. The argument is the same if $\psi(\mathfrak{p}_0) = (1,-1)$ or $(-1,1)$.

If $\psi(\mathfrak{p}_0) = (1,1)$ we show the analogous result using *Proposition 3.2.6 (5)* again:

$$\text{there exists } (p,q) \in \Psi \text{ s.t. } \bigcup_{\mathfrak{p} \in \Delta_{ap,q} \cap \Delta_{bp,q}} (\mathcal{O}_K)_{\mathfrak{p}} = (\mathcal{O}_K)_{\mathfrak{p}_0},$$

meaning once again integrality at $\mathfrak{p}_0$ is imposed, as is required to prove the equality (3.1). ■

Corollary 3.2.9. *For any number field K, $\mathcal{O}_K$ is defined in K by a universal first-order $\mathcal{L}_{rings}$-formula.*

Proof. Note that $\bigcap_{\mathfrak{p}|\mathfrak{m}_0} \widetilde{(\mathcal{O}_K)_{\mathfrak{p}}}$ is universally definable, as $J((\mathcal{O}_K)_{\mathfrak{p}}) = \mathfrak{p}$ is diophantine by [Eis03a, Theorem 5.15] (using the trick $v_{\mathfrak{p}}(x) > 0 \Leftrightarrow v_{\mathfrak{p}}\left(\frac{x}{\pi}\right) \geq 0$, where π is a uniformiser of $\mathfrak{p}$).

From this result, and the diophantiness results of *Proposition 3.2.6*, we conclude everything to the RHS of (3.1) is universally definable. Then by *Theorem 3.2.8*, $\mathcal{O}_K$ can be universally defined in K, as required ■

The proof of this result also concludes the paper. What is remarkable about this result is the similarities we see when we apply the same techniques to function fields, as we do in the next chapter.

Remark 3.2.10. Can we apply the same method as Daans from *Section 2.2.2* to obtain a universal definition without the class field theory fuss? Unfortunately, an immediate application will not work. If we make the natural assumption that '$p > 0$' means 'p is a square' or even 'p is the sum of four squares', then it is no longer guaranteed that $\left(\frac{-p,-2q}{K_\infty}\right)$ is nonsplit for ∞ an infinite prime of K. Indeed, if $K = \mathbb{Q}(i)$ then $K_\infty = \mathbb{C}$ and all quaternion algebras over $\mathbb{C}$ are split. Therefore Daans' definition fails in the general case. However, a *modification* to his original method will work and produce significant results. See *Section 4.3* for a discussion on what modifications need be made.

Remark 4.4.11 also discusses why the author's short universal definition for function fields cannot be immediately applied to number fields. □

Chapter 4

Function Fields

This chapter will be structurally and mathematically similar to *Chapter 2:* we will first briefly analyse Rumely's early results on defining $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ [Rum80], then pass to the more modern universal definition of the ring of S-integers $\mathcal{O}_S$ in a global function field K (see *Definition 4.1.4*) by Eisenträger & Morrison and Daans. The author then shares his own improvement on these results: a shorter universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ using the methods of §2.2.2. We conclude with a $\forall\exists$-definition of $\mathcal{O}_S$ in K with a single universal quantifier (the analogy of §2.2.3) due to Shlapentokh, however this appears quite out of left field as Shlapentokh does not use the techniques outlined in *Chapter 2*, §3.2 or §4.2.

In this chapter the language we consider for function fields is $\mathcal{L}_{\text{rings}} \cup \{t\}$. Once again the reader is referred to *Appendix A.2* if unfamiliar function field terminology is encountered.

4.1 In the Beginning...

Rumely made a contribution to the area of undecidability and definability in global function fields in 1980, where the following results are a subset of his paper [Rum80]:

Theorem 4.1.1.

I. Every valuation ring (archimedian and nonarchimedian alike) of every global field is definable.

II. There is a sentence of $\mathcal{L}_{rings}$ which distinguishes number fields from function fields.

III. If K is a function field then $\mathtt{Th}(K)$ defines its field of constants $\mathbb{F}$, the polynomial ring $\mathbb{F}[t]$ and a model of $\mathbb{N}$ given by the powers of t.

This last result has the following consequence:

IV. The theory of global (function) fields is essentially undecidable[1]. ■

Rumely's tactics are completely different to what we have discussed before in the case of Poonen, Koenigsmann and Park; as his work predates the introduction of quaternion algebras to this field he instead focuses more on the *Hasse Norm Theorem* and *Artin's Reciprocity Law* ([Rum80, Prop. C & D]). This mirrors Robinson's proof of the undecidability of $\mathtt{Th}(\mathbb{Q})$ (*Corollary 2.1.2*) where the active local-global principle was the *Hasse-Minkowski Theorem* (replaced in [Rum80] by the *Hasse Norm Theorem*) and the theory of quadratic forms were used (replaced by the theory of *norm forms*, controlled by Artin's Reciprocity Law).

Note that the defining formulae for *Theorem 4.1.1 (I), (III)* are neither universal nor existential nor of the form "$\forall \ldots \exists \ldots$". The sentence of *Theorem 4.1.1 (II)* is in some sense exactly what one might expect; it is based on the fact that the field of constants of any function field K (characteristic $\neq 2$) is definable in K, while if K is a number field there is no substructure which is a subfield to $\mathcal{O}_K$, like $\mathbb{F}$ is to $\mathbb{F}[t]$. Finally, *Theorem 4.1.1 (IV)* follows from the ability to define $\mathbb{F}[t]$ in K and Raphael Robinson's construction of a model of $\mathbb{N}$ in $\mathbb{F}[t]$ using powers of t (reproduced in [Rum80, §4]).

Nearly 40 years later our picture is clearer yet still incomplete. By the results of Hilbert's 10th Problem discussed in *Chapter 1*, we now know the existential theories of $\mathbb{F}_q[t]$ and $\mathbb{F}_q(t)$ are undecidable as well[2]. In fact, the existential theory of any algebraic function field K is undecidable [Shl96, Eis03b]. It still eludes us, however, whether $\mathbb{F}_q[t]$ is diophantine in $\mathbb{F}_q(t)$ and, until very recently, it eluded us whether $\mathbb{F}_q[t]$ is universally definable in $\mathbb{F}_q(t)$.

Eisenträger & Morrison [EM18] answered this latter question in the positive in 2018; they generalise Rumely's result and improve on Shlapentokh's definition [Shl15] which requires one change of quantifier. They prove three results in the paper, all generalisations of Koenigsmann's results to global function fields, using Park's class-field-theoretic methods. Their second and third results are the following:

[1] Recall that a theory is *essentially undecidable* if every consistent extension of it is undecidable too. Robinson arithmetic is essentially undecidable, hence every theory which includes or interprets it is (essentially) undecidable too - which is used in *Theorem 4.1.1 (IV)*. For example, the theory of fields is undecidable but not essentially undecidable, as ACF admits QE.

[2] We will emphasise here that the theories are in a language containing t.

Theorem 4.1.2. ([EM18, Theorem 1.2]). *Let K be a global field with* $\mathrm{char}(K) \neq 2$. *Then*

$$\{(x, y) \in K^\times \times K^\times : x \notin \mathrm{Norm}(K(\sqrt{y}))\},$$

is diophantine over K.[3] ■

Theorem 4.1.3. ([EM18, Theorem 1.4]). *Let K be a global field with* $\mathrm{char}(K) \neq 2$. *Then $K^\times \setminus K^{\times 2}$ is diophantine over K.* ■

Originally established in [Poo09b] and proven using elementary means in [Koe13] for $K = \mathbb{Q}$, here *Theorem 4.1.3* is reproven using techniques more in line with Park's setup.

However, it is their first result which is of principle interest to us and the focus of the next section. Recall:

Definition 4.1.4. Denote by $v_\mathfrak{p}$ the valuation corresponding to the prime $\mathfrak{p}$. For S a finite set of primes of a global function field K, define $\mathcal{O}_S$ to be the ring

$$\mathcal{O}_S := \{x \in K : v_\mathfrak{p}(x) \geq 0 \text{ for all primes } \mathfrak{p} \notin S\}.$$

The reader would do well to recall as well *Remark A.1.10;* that all primes of a global function field are considered to be finite.

Theorem 4.1.5. ([EM18, Theorem 1.2]). *Let K be a global function field of odd characteristic and let S be a finite nonempty set of primes of K. Then $\mathcal{O}_S$ is first-order universally definable in K.*

In particular for $K = \mathbb{F}_q(t)$ and $S = \{\infty\}$[4]*, $\mathcal{O}_S = \mathbb{F}_q[t]$ is universally definable in $\mathbb{F}_q(t)$.* ■

4.2 Eisenträger & Morrison's Universal Definition

Eisenträger & Morrison's universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ is based on the same idea present in [Koe13], [Par13] and even [Poo09a]; use certain diophantine-definable rings, parameterised by $K^\times$, to encode 'integrality' at some finite set of primes. However, although we prove analogous results to Koenigsmann and Park, we cannot use the latter's arguments exactly.

For instance, although most of the results of §3.1 apply to global function fields (cf. [EM18, §2]), we cannot use [Par13, Lemma 3.19] or the

[3] This generalises [Koe13, Prop. 20(e)] from $K = \mathbb{Q}$ to global fields.

[4] The prime at infinity; see *Definition A.1.9.*

$a, b \in K^\times$ that result from it (thus scrapping the whole biquadratic extension $K(\sqrt{a}, \sqrt{b})$). This is because, as part of Park's choice of $a, b \in K^\times$, we use the Chebotarev density theorem on the extension H/K where H is the Hilbert class field of K. For number fields, this is allowed, however for function fields the Hilbert class field is an infinite field extension hence the Chebotarev density theory cannot be applied.

Our work-around, *Lemmata 3.8 & 3.10* of [EM18], does not use the Hilbert class field but instead a smaller field extension with Hilbert class field-like features. For the sake of completeness, here are those lemmata, condensed into one result:

Lemma 4.2.1. *Let K be a global function field and S be a finite set of primes in $S_K = \mathbb{P}$, the set of all primes of K. We can choose $a, b \in K^\times$ so that the following hold:*

(1) The images of a, b in $K^\times/K^{\times 2}$ are distinct.

(2) Any admissible modulus $\mathfrak{m}$ for $K(\sqrt{a}, \sqrt{b})/K$ is divisible by the primes of S.[5]

(3) Given a finite set of primes $S' \subseteq S_K$ disjoint from S, an ideal class $\overline{I}$ in $\mathcal{C}_{\mathcal{O}_{S'}}$, and an element $\sigma \in \mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K)$ there exists a prime $\mathfrak{q}$ of K such that $\mathfrak{q} \cap \mathcal{O}_{S'}$ is in the ideal class $\overline{I}$, $\mathfrak{q} \in I^{\mathfrak{m}}$ and $\psi(\mathfrak{q}) = \sigma$.

(4) As fractional ideals, $(a), (b)$ are coprime.

We can also choose $c, d \in K^\times$ such that

(5) $\Delta_{a,c} = \mathbb{P}(a)$ or $\Delta_{a,c} = \mathbb{P}(a) \cup \{\mathfrak{p}_a\}$, where $\mathfrak{p}_a$ is coprime to $(a), (b)$.

(6) $\Delta_{b,d} = \mathbb{P}(b)$ or $\Delta_{b,d} = \mathbb{P}(b) \cup \{\mathfrak{p}_b\}$, where $\mathfrak{p}_b$ is coprime to $(a), (b)$ and $\mathfrak{p}_a$. ■

Finally, we shall fix an admissible modulus $\mathfrak{m}$ for $K(\sqrt{a}, \sqrt{b})/K$ such that $\mathfrak{m}$ contains all primes dividing $(a), (b), (c)$ and (d) along with any other primes $\mathfrak{p}$ such that $(a, c)_\mathfrak{p} = -1$ or $(b, d)_\mathfrak{p} = -1$.

This choice of $a, b, c, d \in K^\times$ allows Eisenträger & Morrison to sweep through the rest of Park's paper with relative ease in a stunning display of mathematical grace and symmetry. For instance, *Lemma 3.2.2* of §3.2 becomes, in this context;

Lemma 4.2.2. *Choose a, b, c, d according to* Lemma 4.2.1. *Let $p \in K^\times$ such that (p) and $\mathfrak{m}$ are coprime. Then*

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

[5] This in particular is vital to their paper.

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

This leads us to a definition strikingly similar to *Definition 3.2.3:*

Definition 4.2.3. For $p, q \in K^\times$,

(1) $R_p^{[-1,-1]} := \bigcap_{\mathfrak{p} \in \Delta_{a,p} \cap \Delta_{b,p}} (\mathcal{O}_K)_\mathfrak{p} \qquad \left(= \bigcap_{\mathfrak{p} \in \mathbb{P}^{[-1,-1]}(p)} (\mathcal{O}_K)_\mathfrak{p} \right).$

(2) $R_p^{[1,-1]} := \bigcap_{\mathfrak{p} \in \Delta_{ab,p} \cap \Delta_{b,p} \cap \Delta_{a,cp}} (\mathcal{O}_K)_\mathfrak{p} \quad \left(= \bigcap_{\mathfrak{p} \in \mathbb{P}^{[1,-1]}(p)} (\mathcal{O}_K)_\mathfrak{p} \right).$

(3) $R_p^{[-1,1]} := \bigcap_{\mathfrak{p} \in \Delta_{a,p} \cap \Delta_{ab,p} \cap \Delta_{b,dp}} (\mathcal{O}_K)_\mathfrak{p} \quad \left(= \bigcap_{\mathfrak{p} \in \mathbb{P}^{[-1,1]}(p)} (\mathcal{O}_K)_\mathfrak{p} \right).$

(4) $R_p^{[1,1]} := \bigcap_{\mathfrak{p} \in \Delta_{ap,q} \cap \Delta_{bp,q}} (\mathcal{O}_K)_\mathfrak{p}.$

(where the second equality in items (1)-(3) holds only when (p) and $\mathfrak{m}$ are coprime.)

Now define Ψ, Φ_σ for $\sigma \neq (1,1)$ exactly the same as in [Par13] (*Definition 3.2.5*). Then, in a series of lemmata ([EM18, Lemmata 3.14, 3.15 & 3.17]) Eisenträger & Morrison recreate *Proposition 3.2.6* exactly, which leads us to the following theorem: the precise near replication of [Par13, Theorem 4.2], i.e. *Theorem 3.2.8:*

Theorem 4.2.4. ([EM18, Theorem 3.20]) *For any global function field K and finite set of primes $S \subset S_K$, with $\mathfrak{m}$ chosen as before,*

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

Corollary 4.2.5. *For any global function field K with $\mathrm{char}(K) \neq 2$, and any nonempty finite set of primes S of K, $\mathcal{O}_S$ is definable in K by a universal formula.*

Proof.

$$\begin{aligned} \text{For } f \in K, \qquad f \in \mathcal{O}_S \quad \Leftrightarrow \quad & f \in \bigcap_{\mathfrak{p} \,|\, \mathfrak{m},\ \mathfrak{p} \notin S} \widetilde{\mathcal{O}_\mathfrak{p}} \\ & \wedge \forall p \bigwedge_{\sigma \neq (1,1)} (p \notin \Phi_\sigma \vee f \in \widetilde{R_p^\sigma}) \\ & \wedge \forall p, q \left((p,q) \notin \Psi_K \vee f \in \widetilde{R_{p,q}^{(1,1)}} \right). \quad \blacksquare \end{aligned}$$

This is more or less the same definition which would result if K was a number field, i.e. from *Corollary 3.2.9*. Note the number of quantifiers needed for a universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ would be no less than 418, the number needed for Koenigsmann's definition (*Theorem 2.2.10 (3)*).

4.3 Daans Strikes Again

In §4.4 of [Daa18], Daans modifies the method he uses to produce a universal definition of $\mathbb{Z}$ in $\mathbb{Q}$, to construct a universal definition of $\mathcal{O}_K$ in K for *any global field* K. This modification he does in two ways.

(A) *Theorem 2.2.13* is not how the result appears in [Daa18]; using the same proof the following is shown instead. Using the notation defined in *Definition 2.2.11*,

Theorem 4.3.1. [Daa18, Theorem 4.3.3].

$$\bigcup_{l\in\mathbb{P}} l\,\mathbb{Z}_{(l)} = \bigcup_{\substack{p,q>0\\ q\in\mathbb{Q}^2\cdot T^{\times}_{-1,-1}}} J_{-p,-2q}. \qquad \blacksquare$$

To fabricate a universal definition from this, Daans has the following proposition. Let $\mathbb{P}$ be the set of finite primes (prime ideals) of K.

Proposition 4.3.2. *Let K be a global field and let $T \subseteq \mathbb{P}$ be a nonempty set of primes. Suppose that $\bigcup_{\mathfrak{p}\in T} \mathfrak{p}(\mathcal{O}_K)_{\mathfrak{p}}$ has a positive existential definition in K with n quantifiers. Then $\bigcap_{\mathfrak{p}\in T}(\mathcal{O}_K)_{\mathfrak{p}}$ has a universal definition in K with $n+1$ quantifiers.*

Proof. This is Proposition 4.1.1 of [Daa18]. Let $\phi(t)$ be the existential formula defining $\bigcup_{\mathfrak{p}\in T} \mathfrak{p}(\mathcal{O}_K)_{\mathfrak{p}}$. Then

$$\bigcap_{\mathfrak{p}\in T}(\mathcal{O}_K)_{\mathfrak{p}} = \{x \in K : K \models \forall u(x\cdot u = 1 \to \neg\phi(u))\}.$$

$\blacksquare$

Notice the similarity between this definition and *Definition 2.2.9*. In abstract terms, we are showing that for a subring R of K containing $\mathcal{O}_K$, R has a universal definition when $J(R)$ has an existential definition. This was the motivating idea behind Koenigsmann's universal definition of $\mathbb{Z}$ in $\mathbb{Q}$.

(B) For Daans' method (*Remark 2.2.14*) one of the main underlying ideas is to force all quaternion algebras satisfying the conditions of D to be nonsplit at ∞. For a general global field, the behaviour of ∞ could be quite erratic - to counteract this, Daans adapts his method so that the set of conditions he considers, denoted Φ_u^S, deliberately forces all quaternion algebras at infinity to split, yet all quaternion algebras at primes of S to be nonsplit. We change (1) & (2) of *Remark 2.2.14* as follows:

(1') If a, b satisfies $D = \Phi_u^S$ this forces $\Delta = \Delta_{a,b} \setminus (S \cup \mathbb{P}_\infty)$, where $\mathbb{P}_\infty$ is the set of infinite primes of K (empty when K is a global function field).

(2') If a, b satisfy $D = \Phi_u^S$, then $(a, b)_\mathfrak{q} = 1$ for all $\mathfrak{q} \in \mathbb{P}_\infty$. Also if a, b satisfy D then $(a, b)_\mathfrak{p} = -1$ for all $\mathfrak{p} \in S$.

Let us expand on (B). Let K be a global field of characteristic not equal to[6] 2. We wish to find a universal definition of $\mathcal{O}_S$ in K, where $S \subseteq \mathbb{P}$. We will first show that S can be taken to have odd cardinality.

Proposition 4.3.3. *Let $S \subseteq S' \subseteq \mathbb{P}$ and suppose $S' \setminus S$ is finite. If $\bigcup_{\mathfrak{p} \in \mathbb{P} \setminus S'} \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$ has a positive existential definition with n quantifiers, then $\bigcup_{\mathfrak{p} \in \mathbb{P} \setminus S} \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$ has a positive existential definition with $\max\{n, 15\}$ quantifiers.*

Proof. See [Daa18, Prop. 4.4.1]. Note

$$\bigcup_{\mathfrak{p} \in \mathbb{P} \setminus S} \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p} = \bigcup_{\mathfrak{p} \in \mathbb{P} \setminus S'} \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p} \cup \bigcup_{\mathfrak{p} \in S' \setminus S} \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p},$$

and the union of positive existentially defined sets is again positive existential. The number of quantifiers needed to define $\bigcup_{\mathfrak{p} \in \mathbb{P} \setminus S} \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$ is the maximum of the number needed for $\bigcup_{\mathfrak{p} \in \mathbb{P} \setminus S'} \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$, which is n, and $\bigcup_{\mathfrak{p} \in S' \setminus S} \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$, which is 15, by [Daa18, Corollary 4.1.3]; the generalisation of defining $\mathbb{Z}_{(p)}$ in $\mathbb{Q}$ (see [Koe13, Prop. 10]). ■

So we will assume from this point without loss of generality that $|S|$ is odd. Let $\mathbb{P}^{[2]}$ be the set of dyadic primes, where a prime $\mathfrak{p}$ is dyadic if $K_\mathfrak{p}$ is a dyadic field (recall *Definition 2.1.8*). Define the following notation:

Definition 4.3.4. For a finite prime $\mathfrak{p}$ of K and $a \in (\mathcal{O}_K)_\mathfrak{p}^\times$, define

$$a \otimes \mathfrak{p} \quad \Leftrightarrow \quad \begin{cases} \text{if } \mathfrak{p} \notin \mathbb{P}^{[2]}, \ a \text{ is a nonsquare modulo } \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}, \\ \text{if } \mathfrak{p} \in \mathbb{P}^{[2]}, \ a \text{ is a nonsquare modulo } 4\,\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}, \\ \qquad\qquad \text{but } \textit{is} \text{ a square modulo } 4(\mathcal{O}_K)_\mathfrak{p}. \end{cases}$$

[6] See *Remark 4.3.11* for the characteristic 2 case.

Finally, $\Xi(S) := \{a \in K^\times : a \otimes \mathfrak{p} \text{ for all } \mathfrak{p} \in S\}$.

Lemma 4.3.5. *For any finite set of finite primes S, $\Xi(S)$ is nonempty.*

Proof. See [Daa18, Lemma 4.4.2] for details. This follows from applying the *Weak Approximation Theorem* [Mil17, Theorem 7.20]: if $|\cdot|_1, \ldots, |\cdot|_n$ are nontrivial inequivalent norms of a field F, and $a_1, \ldots, a_n \in F$, then for every $\epsilon > 0$ there exists $a \in F$ such that $|a - a_i|_i < \epsilon$, for $1 \leq i \leq n$. ■

By Siegel's Theorem [Lam05, Chapt. XI Cor. 1.5], the totally positive elements of K are exactly those elements which can be written as the sum of four squares. Moreover, if K has no real infinite primes then every element is totally positive. Let "$a > 0$" denote "a is nonzero and the sum of 4 squares" if K has real infinite primes and "a is nonzero" otherwise.

Lemma 4.3.6. [Daa18, Lemma 4.4.3]. *Let S be a nonempty, finite set of finite primes of K. Let $u \in \bigcap_{\mathfrak{p}\in S}(\mathcal{O}_K)_\mathfrak{p}^\times$. Then the set*

$$\Phi_u^S = \{(a,b) \in K^2 : a > 0,\, b \in (\mathcal{O}_K)_\mathfrak{p}^\times,\, a \equiv u \mod \prod_{\mathfrak{p}\in S} 4\,\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}\}$$

has a positive existential definition with 49 quantifiers. Moreover, the number of quantifiers can be reduced by 4 if K is nonreal, by 3 if $|S|$ is odd but at least 3, and by 24 if $|S|$ is even. ■

We have now arrived at the main theorem for this section. Recalling *Definition 2.2.11*, define $J_{a,b}^c := \bigcap_{\mathfrak{p}\in\Delta\cap\mathbb{P}(c)} \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$. This also has a positive existential definition of 61 quantifiers (cf. [Daa18, Prop. 4.2.6] & [Koe10, Lemma 11]).

Theorem 4.3.7. *Let S be a finite set of finite primes of K of odd cardinality. Let $\pi \in K^\times$ be an element such that $S \subseteq \mathbb{P}(\pi)$. Let u, c be parameters such that*

(i) $u \in \Xi(S)$,

(ii) for all $\mathfrak{p} \in S$, $v_\mathfrak{p}(c) = 0$ and for all $\mathfrak{p} \in \mathbb{P}^{[2]} \cup \mathbb{P}(\pi) \setminus S$, $v_\mathfrak{p}(c) = 1$.[7]

Then

$$\bigcup_{\mathfrak{p}\in\mathbb{P}\setminus S} \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p} = \bigcup_{(a,b)\in\Phi_u^S} (J_{a,b\pi}^a \cap J_{a,b\pi}^b \cap J_{a,b\pi}^c).$$

In particular, the set $\bigcup_{\mathfrak{p}\in\mathbb{P}\setminus S} \mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$ has a positive existential definition in K.

[7]Such a u, π and c exist by Weak Approximation.

Proof. We will show the equality holds; that $\bigcup_{(a,b)\in\Phi_u^S}(J^a_{a,b\pi}\cap J^b_{a,b\pi}\cap J^c_{a,b\pi})$ has a positive existential definition in K follows from *Lemma 4.3.6* given $J^x_{a,b\pi}$ is positive-existentially definable.

First, let $\Delta = \Delta_{a,b\pi}\cap(\mathbb{P}(a)\cup\mathbb{P}(b)\cup\mathbb{P}(c))$. For $(a,b)\in\Phi_u^S$, $a>0$ hence a is a square in all completions of K at infinite primes, meaning $(a,b)_\mathfrak{q} = (1,b)_\mathfrak{q} = 1$ for all $\mathfrak{q}\in\mathbb{P}_\infty$. Therefore $\Delta_{a,b\pi}$ contains no infinite primes. When a,b and c satisfy the conditions of the theorem, $(\mathbb{P}(a)\cup\mathbb{P}(b)\cup\mathbb{P}(c))\cap S=\emptyset$ and $\mathbb{P}(\pi)\setminus S\subseteq\mathbb{P}(c)$. By the former property, $\Delta\subseteq\Delta_{a,b\pi}\setminus S$. By the latter, used in conjunction with *Lemma 2.2.4*, $\Delta_{a,b\pi}\setminus S\subseteq\Delta$. We conclude

$$\Delta = \Delta_{a,b\pi}\setminus S = \Delta_{a,b\pi}\setminus(S\cup\mathbb{P}_\infty),$$

which is (1') of the modified *Remark 2.2.14* complete. Therefore

$$J^a_{a,b\pi}\cap J^b_{a,b\pi}\cap J^c_{a,b\pi} = \bigcap_{\mathfrak{p}\in\Delta_{a,b\pi}\cap(\mathbb{P}(a)\cup\mathbb{P}(b)\cup\mathbb{P}(c))}\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p} \quad = \bigcap_{\mathfrak{p}\in\Delta}\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p},$$

and we now wish to prove

$$\bigcup_{\mathfrak{p}\in\mathbb{P}\setminus S}\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p} = \bigcup_{(a,b)\in\Phi_u^S}\left(\bigcap_{\mathfrak{p}\in\Delta}\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}\right).$$

For the inclusion from left to right, we must show Δ is nonempty (modified *Remark 2.2.14* (2')). However as $u\in\Xi(S)$, $a\equiv u \mod \prod_{\mathfrak{p}\in S}4\,\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$, and $b\in\bigcap_{\mathfrak{p}\in S}(\mathcal{O}_K)_\mathfrak{p}^\times$, by *Lemma 2.2.4 (b)* it is the case $S\subseteq\Delta_{a,b\pi}$. As $|S|$ is odd, we conclude by Hilbert Reciprocity that Δ is nonempty.

Finally, as per *Remark 2.2.14 (3)* we must show for all $\mathfrak{q}\in\mathbb{P}\setminus S$ there exists $(a,b)\in\Phi_u^S$ such that $(a,b)_\mathfrak{q}=-1$. Fix $\mathfrak{q}\in\mathbb{P}\setminus S$. By Weak Approximation we can choose a such that

- $a>0$,
- $a\equiv u \mod \prod_{\mathfrak{p}\in S}4\,\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$,
- and $a\otimes\mathfrak{q}$.

Due to [Daa18, Theorem 1.7.10], there exists $b'\neq 0$ such that $\Delta_{a,b'\pi} = S\cup\{\mathfrak{q}\}$. As $v_\mathfrak{p}(a)$ is even for all[8] $\mathfrak{p}\in S$, by *Lemma 2.2.4 (b)* again we see $v_\mathfrak{p}(b'\pi)=v_\mathfrak{p}(\pi)+v_\mathfrak{p}(b')$ must be odd. Thus $v_\mathfrak{p}(b')$ must be even, for all $\mathfrak{p}\in S$. Multiply b' by an appropriate square γ such that $b=b'\gamma\in\bigcap_{\mathfrak{p}\in S}(\mathcal{O}_K)_\mathfrak{p}^\times$. Then $(a,b)\in\Phi_u^S$ as desired and $\Delta=\Delta_{a,b\pi}\setminus S=\Delta_{a,b'\pi}\setminus S=\{\mathfrak{q}\}$ as required. ■

[8]By assumption $u\in\bigcap_{\mathfrak{p}\in S}(\mathcal{O}_K)_\mathfrak{p}^\times$ and $a\equiv u \mod \prod_{\mathfrak{p}\in S}4\,\mathfrak{p}(\mathcal{O}_K)_\mathfrak{p}$.

Remark 4.3.8. If one can find $\pi \in K^\times$ such that $S = \mathbb{P}(\pi)$ (as one can do in fields of class number 1, e.g. $K = \mathbb{F}_q(t)$, when $S \neq \{\infty\}$) then for all $S \subseteq \mathbb{P}$, one can define $\mathcal{O}_S$ in K without the need for the parameter c as follows:

If needed, expand S to S' such that $\mathbb{P}^{[2]} \subseteq S'$. Choose $\pi' \in K^\times$ such that $S' = \mathbb{P}(\pi')$. Then the set $\mathbb{P}^{[2]} \cup \mathbb{P}(\pi') \setminus S$ is empty. In the second paragraph of the above proof we see there is no need for c; $\Delta = \Delta_{a,b\pi} \setminus S$ still. Therefore $J^c_{a,b\pi}$ is unnecessary in this case.

In private correspondence with the author, Daans shared the following conjecture:

Conjecture 4.3.9. *Let K be a global field and S a finite set of finite primes. There exists $\pi \in K$ such that $S \subseteq \mathbb{P}(\pi)$ and $|\mathbb{P}(\pi)|$ is odd.* ■

A consequence of this conjecture, using the same argument as above, is that the element c (and thus the set $J^c_{a,b\pi}$) is always unnecessary in defining $\mathcal{O}_S$ in K. □

Remark 4.3.10. *Theorem 4.3.7* produces a universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ with 167 quantifiers as follows:

First note c is not needed by *Remark 4.3.8*. Let S be some set of finite primes of $\mathbb{F}_q(t)$ of cardinality 5. By *Lemma 4.3.6* the number of quantifiers needed for Φ^S_u is $49 - 4 - 3 = 42$, as $\mathbb{F}_q(t)$ is nonreal and $|S| \geq 3$. The total number of quantifiers needed to define $\mathcal{O}_S$ in $\mathbb{F}_q(t)$ is $1 + 2 + 42 + 61 + 61 = 167$, by the formula

$$x \in \mathcal{O}_S \Leftrightarrow \forall u \Big(x \cdot u = 1 \to \neg \big(\exists a, b ((a,b) \in \Phi^S_u \wedge x \in J^a_{a,b\pi} \wedge x \in J^b_{a,b\pi}) \big) \Big)$$

(cf. *Proposition 4.3.2* with $T = \mathbb{P} \setminus S$). Then by *Proposition 4.3.3*, $\mathbb{F}_q[t]$ also has a universal definition in $\mathbb{F}_q(t)$ with 167 quantifiers. □

Remark 4.3.11. Daans also demonstrates there is a universal definition of $\mathcal{O}_S$ in K for K a global field of characteristic 2 and S any finite set of finite primes [Daa18, §4.5]. He uses central simple algebras to do this (an introduction to which is given in [GS06]). □

4.4 A New Universal Definition

We will now provide a shorter universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ than appears in [EM18] and [Daa18] (with a loss of generality, however; Eisenträger

& Morrison's and Daans' universal definitions apply to any ring of S-integers $\mathcal{O}_S$). We will remain in the case $\mathrm{char}(\mathbb{F}_q) \neq 2$. We first need the following lemma:

Lemma 4.4.1. *Any nonsquare of $\mathbb{F}_q(\!(1/t)\!)$ is of the form $1/t\,c^2$, $f c^2$, or $f/t\,c^2$ where $c \in \mathbb{F}_q(\!(1/t)\!)$ and $f \in \mathbb{F}_q$ is a nonsquare.*

Proof. This is [Daa18, Prop. 1.4.5] exactly. For an explicit proof see *Appendix B.* ■

Lemma 4.4.2. *The quaternion algebra $H_{f,g/t}(\mathbb{F}_q(\!(1/t)\!)) = \left(\frac{f,\, g/t}{\mathbb{F}_q(\!(1/t)\!)}\right)$ is nonsplit, where $f, g \in \mathbb{F}_q$ and f is a nonsquare.*

Proof. We will use an equality found in [EM18]: for a $\mathfrak{p}$-adic unit a,

$$(a,b)_{\mathfrak{p}} = -1 \quad \Leftrightarrow \quad v_{\mathfrak{p}}(b) \text{ is odd and } \mathrm{red}_{\mathfrak{p}}(a) \text{ is a nonsquare of } \mathbb{F}_{\mathfrak{p}}.$$

Thus $(f, g/t)_\infty = -1$ if and only if $v_\infty(g/t) = 1$ is odd and $f \in \mathbb{F}_q$ is a nonsquare (as it was chosen to be). Hence $H_{f,g/t}(\mathbb{F}_q(\!(1/t)\!))$ is nonsplit, as desired. Note this also means $H_{f/t,g}(\mathbb{F}_q(\!(1/t)\!))$ is nonsplit too. ■

Now for some results concerning primes, and nonsquares of the base field $\mathbb{F}_q$. Recall the residue field $\mathbb{F}_{f(t)}$ and residue map $\mathrm{red}_{f(t)}$ from *Appendix A.2.* We will use the Legendre symbol, which in this context is defined as:

Definition 4.4.3. Let $f(t) \in \mathbb{F}_q[t]$ be a prime (that is, the monic and irreducible polynomial corresponding to the principal prime ideal $\mathfrak{p}$) and $g(t) \in \mathbb{F}_q[t]$, where $f(t) \nmid g(t)$. Then

$$\left(\frac{g(t)}{f(t)}\right) := \begin{cases} 1 & \text{if } \mathrm{red}_{f(t)}(g(t)) \text{ is a square of } \mathbb{F}_{f(t)}, \\ -1 & \text{if } \mathrm{red}_{f(t)}(g(t)) \text{ is a nonsquare of } \mathbb{F}_{f(t)}. \end{cases}$$

Lemma 4.4.4. *Let $f(t) \in \mathbb{F}_q[t]$ be a prime and $g \in \mathbb{F}_q$ be nonsquare. If $\deg(f)$ is odd, then $\left(\frac{g}{f(t)}\right) = -1$ still. If $\deg(f)$ is even, then $\left(\frac{g}{f(t)}\right) = 1$.*

Proof. This follows from the formula

$$\left(\frac{g}{f(t)}\right) = g^{\frac{q-1}{2}\cdot \deg(f)} = (-1)^{\deg(f)}$$

of [Ros02, Prop. 3.2]. ■

Lemma 4.4.5. *Given a prime $f(t) \in \mathbb{F}_q[t]$, one can choose $g \in \mathbb{F}_q$ nonsquare and $d(t)$ a prime of $\mathbb{F}_q[t]$ of opposite parity in degree to $f(t)$ such that $\mathrm{red}_{f(t)}(gd(t))$ is a nonsquare of $\mathbb{F}_{f(t)}$.*

Proof. We will assume that g is chosen according to *Lemma 4.4.4*. We wish to find a polynomial $d(t)$ which is monic, irreducible, of degree of opposite parity to $\deg(f)$ and congruent to either a square or nonsquare, modulo $f(t)$. By Dirichlet's Theorem on primes in arithmetic progressions [Ros02, Chapt. 4], there are infinitely many primes equivalent to $c(t)$ mod $f(t)$ for any $c(t) \in \mathbb{F}_{f(t)}$. Moreover, for N large enough, there is a prime of degree N in this arithmetic progression [Ros02, Theorem 4.8].

Therefore if $f(t)$ is of odd degree then we can choose $d(t)$ to be monic, irreducible, of even degree and $d(t) \equiv c(t)^2 \mod f(t)$, where $c(t) \not\equiv 0 \mod f(t)$. If $f(t)$ has even degree then we can choose $d(t)$ to be monic, irreducible, of odd degree and $d(t) \equiv c(t) \mod f(t)$ where $c(t) \in \mathbb{F}_{f(t)}$ is a nonsquare, as required. ∎

These lemmata will contribute to the next result. Before this, some notation. Let $\phi(a)$ denote the formula "the degree of a is even and the leading coefficient of a is a square". Note that an element $a \in \mathbb{F}_q(t)$ satisfies ϕ if and only if a is a square in $\mathbb{F}_q(\!(1/t)\!)$, by *Lemma B.0.1* of *Appendix B*.

If $f_1, \ldots, f_r$ are the nonsquare elements of $\mathbb{F}_q$, let $\psi(a,b)$ denote

$$\begin{aligned}\exists c, d\Big(&\text{“}c \text{ and } d \text{ are of opposite parity in degree”}\\ &\wedge \Big[\big\{\phi(c) \wedge (a = f_1 c \vee \cdots \vee a = f_r c) \wedge b \in \mathbb{F}_q \cdot d\big\}\\ &\vee \ \big\{\phi(d) \wedge (b = f_1 d \vee \cdots \vee b = f_r d) \wedge a \in \mathbb{F}_q \cdot c\big\}\Big]\Big).\end{aligned}$$

Finally define

Definition 4.4.6. $D := \{(a,b) \in \mathbb{F}_q(t) \times \mathbb{F}_q(t) : \psi(a,b)\}$.

The complicated choice of $\psi(a,b)$ will be justified in the upcoming theorem.

Remark 4.4.7. In order to create this universal definition we will employ Daans' method of defining $\mathbb{Z}$ in $\mathbb{Q}$, with a twist. Recall that this was a 4 step process, centred around a set of conditions D on parameters a, b such that:

(1) If a, b satisfies D this forces $\Delta = \Delta_{a,b} \setminus \{\infty\}$.

(2) If a, b satisfy D, then $(a,b)_\infty = -1$. Equivalently, Δ is always nonempty.

(3) For each prime $\mathfrak{p}$, one can find a, b satisfying D such that $\Delta = \{\mathfrak{p}\}$. Equivalently, there exist a, b satisfying D such that

$$(a,b)_{\mathfrak{p}} = -1 \text{ and } (a,b)_{\mathfrak{q}} = 1 \text{ for all primes } \mathfrak{q} \neq \mathfrak{p}.$$

To accommodate the fact that all primes of $\mathbb{F}_q(t)$ are finite (see *Remark A.1.10*) we will have to modify (1), in order for the upcoming $\widetilde{R}_{a,b}$ to still have a universal definition by [EM18]:

(1') If a, b satisfies D this forces $\Delta = \Delta_{a,b}$.

Then we will obtain a universal definition as follows:

(4) $t \in \mathbb{F}_q[t] \cup (\mathbb{F}_q[t])_\infty \quad \Leftrightarrow \quad \forall a, b \in \mathbb{F}_q(t)\ ((a,b) \notin D \vee t \in \widetilde{R_{a,b}})$.

I claim that the aforementioned D, defined by $\psi(a,b)$, satisfies (1'), (2) & (3). Let us explore. □

Theorem 4.4.8. *We have*

$$\mathbb{F}_q[t] \cup (\mathbb{F}_q[t])_\infty = \bigcap_{(a,b)\in D} \widetilde{R_{a,b}},$$

where

$$R_{a,b} := \bigcap_{\mathfrak{p}\in\Delta_{a,b}\cap(\mathbb{P}(a)\cup\mathbb{P}(b))} (\mathbb{F}_q[t])_{\mathfrak{p}}, \qquad \widetilde{R_{a,b}} = \bigcup_{\mathfrak{p}\in\Delta_{a,b}\cap(\mathbb{P}(a)\cup\mathbb{P}(b))} (\mathbb{F}_q[t])_{\mathfrak{p}}.$$

Proof. By [EM18, Lemma 3.19], $\widetilde{R_{a,b}}$ has a universal definition, provided $\Delta_{a,b} \cap (\mathbb{P}(a) \cup \mathbb{P}(b)) \neq \emptyset$.

Consider this set of primes in more detail.

$$\begin{aligned} \mathfrak{p} \in \Delta_{a,b} \quad &\Leftrightarrow \quad (a,b)_{\mathfrak{p}} = -1 \\ &\Leftrightarrow \quad \left((-1)^{v_{\mathfrak{p}}(a)v_{\mathfrak{p}}(b)} \operatorname{red}_{\mathfrak{p}}\left(\frac{a^{v_{\mathfrak{p}}(b)}}{b^{v_{\mathfrak{p}}(a)}}\right)\right)^{\frac{\#\mathbb{F}_{\mathfrak{p}}-1}{2}} = -1. \end{aligned}$$

If $\mathfrak{p} \notin \mathbb{P}(a) \cup \mathbb{P}(b)$ then $v_{\mathfrak{p}}(a)$ and $v_{\mathfrak{p}}(b)$ are both even. Assume one of them is nonzero.[9]

$$\Leftrightarrow \quad \left(\operatorname{red}_{\mathfrak{p}}(c)^2\right)^{\frac{\#\mathbb{F}_{\mathfrak{p}}-1}{2}} = -1$$

[9] If both are 0, $c = 1$ and $\operatorname{red}_{\mathfrak{p}}(c)^{\frac{\#\mathbb{F}_q-1}{2}} = 1$, a contradiction too.

$$\Leftrightarrow \quad \operatorname{red}_{\mathfrak{p}}(c)^{\#\mathbb{F}_{\mathfrak{p}}-1} = -1,$$

however $\operatorname{red}_{\mathfrak{p}}(c)$ must satisfy the equation $x^{\#\mathbb{F}_{\mathfrak{p}}} = x$ of a finite field; with our assumption of a noneven characteristic, we have a contradiction. Thus

$$\Delta \quad = \quad \Delta_{a,b} \cap (\mathbb{P}(a) \cup \mathbb{P}(b)) \quad = \quad \Delta_{a,b}. \qquad (\textit{Remark 4.4.7 (1').})$$

According to our general strategy, we next must prove $\Delta_{a,b}$ is nonempty for $(a,b) \in D$; *Remark 4.4.7 (2).*

Any nonsquare of $\mathbb{F}_q(t)_\infty = \mathbb{F}_q(\!(1/t)\!)$ is of the form $1/t\,c^2$, $f c^2$, or $f/t\,c^2$ for $c \in \mathbb{F}_q(\!(1/t)\!)$ and $f \in \mathbb{F}_q$ a nonsquare, by *Lemma 4.4.1.* For $(a,b) \in D$ considered as elements of $\mathbb{F}_q(\!(1/t)\!)$, there are at most 9 possible classes for (a,b) modulo squares of $\mathbb{F}_q(\!(1/t)\!)$:

$$\begin{array}{ccc} (1/t, 1/t) & (1/t, f) & (1/t, f/t) \\ (f, 1/t) & (f, g) & (f, g/t) \\ (f/t, 1/t) & (f/t, g) & (f/t, g/t) \end{array}$$

for $f, g \in \mathbb{F}_q$ nonsquares. However out of these possible scenarios, only four are allowed by choice of a and b: $(f, g/t), (f/t, g), (1/t, f)$ and $(f, 1/t)$. By the rules of quaternionic bases (cf. [Con18c, Definition 4.1]) we conclude $H_{a,b}(\mathbb{F}_q(\!(1/t)\!))$ is nonsplit for any such a, b if $H_{f,g/t}(\mathbb{F}_q(\!(1/t)\!))$ is nonsplit. However by *Lemma 4.4.2* we know this is nonsplit.

This demonstrates for all $(a,b) \in D$, $\infty \in \Delta_{a,b}$. As well as this, by Hilbert Reciprocity we conclude the quaternion algebra given by (a,b) must be nonsplit at some finite prime too, meaning $\Delta_{a,b} \setminus \{\infty\}$ is nonempty. This allows us to conclude $\mathbb{F}_q[t] \cup (\mathbb{F}_q[t])_\infty \subseteq \widetilde{R_{a,b}}$ for each $(a,b) \in D$, therefore

$$\mathbb{F}_q[t] \cup (\mathbb{F}_q[t])_\infty \subseteq \bigcap_{(a,b)\in D} \widetilde{R_{a,b}}.$$

We will now show the reverse inclusion, à la *Remark 4.4.7 (3).* Consider the prime ideals of $\mathbb{F}_q[t]$; these are principal ideals $\mathfrak{p} = (f(t))$ with $f(t) \in \mathbb{F}_q[t]$ a monic and irreducible polynomial.

Set $a = zf(t)$ where $z \in \mathbb{F}_q$ is a nonsquare (chosen later). Set $b = gd(t)$ according to *Lemma 4.4.5.* By this choice of a and b, $(a,b)_{f(t)} = -1$ as $v_{f(t)}(a)$ is odd and $\operatorname{red}_{f(t)}(b)$ is a nonsquare of $\mathbb{F}_{\mathfrak{p}}$. Also, for any prime $\mathfrak{q} \neq \mathfrak{p}$, $\mathfrak{q} \neq \infty$, $v_{\mathfrak{q}}(a) = 0$ and b is either a $\mathfrak{q}$-unit (in which case $(a,b)_{\mathfrak{q}} = 1$) or $\mathfrak{q} = (d(t))$ (from *Lemma 4.4.5*). In this case,

$$(a,b)_{d(t)} = \left((-1)^{v(a)v(b)} \operatorname{red}_{d(t)} \left(\frac{a^{v(b)}}{b^{v(a)}}\right)\right)^{\frac{q^{\deg d}-1}{2}}$$

$$= \mathrm{red}_{d(t)}(zf(t))^{\frac{q^{\deg d}-1}{2}}$$
$$= \left(\tfrac{zf(t)}{d(t)}\right) = \left(\tfrac{z}{d(t)}\right)\left(\tfrac{f(t)}{d(t)}\right).$$

By the law of Quadratic Reciprocity,

$$\left(\tfrac{d(t)}{f(t)}\right)\left(\tfrac{f(t)}{d(t)}\right) = (-1)^{\frac{q^{\deg f}-1}{2}\frac{q^{\deg d}-1}{2}} = 1,$$

as f and d have opposite parity in degree (and q is not a power of 2). Consider the following two cases.

Case 1: f has odd degree. Then $\left(\tfrac{d(t)}{f(t)}\right) = 1$ by *Lemma 4.4.5*, meaning $\left(\tfrac{f(t)}{d(t)}\right) = 1$. Now choose $z \in \mathbb{F}_q$ nonsquare such that $\left(\tfrac{z}{d(t)}\right) = 1$ (cf. *Lemma 4.4.4*). Then

$$(a,b)_{d(t)} = \left(\tfrac{z}{d(t)}\right)\left(\tfrac{f(t)}{d(t)}\right) = (1)(1) = 1.$$

Case 2: f has even degree. Then $\left(\tfrac{d(t)}{f(t)}\right) = -1$ by *Lemma 4.4.5*, meaning $\left(\tfrac{f(t)}{d(t)}\right) = -1$. Now choose $z \in \mathbb{F}_q$ nonsquare such that $\left(\tfrac{z}{d(t)}\right) = -1$ still (cf. *Lemma 4.4.4*). Then

$$(a,b)_{d(t)} = \left(\tfrac{z}{d(t)}\right)\left(\tfrac{f(t)}{d(t)}\right) = (-1)(-1) = 1.$$

In either case, we conclude $(a,b)_{d(t)} = 1$. So by choice of a and b, $\mathfrak{p} = (f(t))$ and naturally ∞ are the only primes at which the algebra $H_{a,b}(\mathbb{F}_q(t)_{\mathfrak{p}})$ is nonsplit. Moreover by design $(a,b) \in D$ so $\Delta_{a,b} = \{\mathfrak{p}, \infty\}$ as required. ■

Remark 4.4.9. We will show now that D of *Theorem 4.4.8* is diophantine.

Consider $\phi(c)$: "the degree of c is even and the leading coefficient of c is a square". This is captured by

$$\exists f\Big(\deg(c) = \deg(f^2) \wedge \exists g\big(\deg(c) > \deg(g) \wedge c = f^2 + g\big)\Big)$$
$$\Leftrightarrow\ \exists f\big(\deg(c) = \deg(f^2) \wedge \deg(c) \geq \deg(t(c - f^2))\big)$$
$$\Leftrightarrow\ \exists f\big(\deg(f^2) \geq \deg(t(c - f^2))\big)$$

What if we additionally wanted to say "d is of odd degree"? This would be

$$\exists f\big(\deg(f^2) \geq \deg(t(c - f^2))\big) \wedge \exists h\big(\deg(f^2) = \deg(th^2 d)\big)$$

$\Leftrightarrow \exists f, h\big(\deg(th^2d) \geq \deg(t(c-f^2))\big) \wedge \exists g\big(\deg(g) < \deg(f^2) \wedge f^2 = k \cdot th^2d + g\big)$
for some $k \in \mathbb{F}_q$,
$\Leftrightarrow \exists f, h\big(\deg(th^2d) \geq \deg(t(c-f^2)) \wedge \deg(f^2) \geq \deg(t(f^2 - k \cdot th^2d))\big)$
for some $k \in \mathbb{F}_q$.

Let $\mathbb{F}_q = \{k_1, \ldots, k_q\}$. Let $\chi(c,d)$ denote

$$\exists f, h\big(\deg(th^2d) \geq \deg(t(c-f^2)) \wedge \big\{\deg(f^2) \geq \deg(t(f^2 - k_1 \cdot th^2d)) \\ \vee \deg(f^2) \geq \deg(t(f^2 - k_2 \cdot th^2d)) \vee \cdots \vee \deg(f^2) \geq \deg(t(f^2 - k_q \cdot th^2d))\big\}\big).$$

Then, by the above argument, "the degree of c is even, the degree of d is odd, and the leading coefficient of c is a square" is represented by this formula.

Recall $\psi(a,b)$ denotes

$$\exists c, d\Big(\text{"}c \text{ and } d \text{ are of opposite parity in degree"} \\ \wedge \Big[\big\{\phi(c) \wedge (a = f_1 c \vee \cdots \vee a = f_r c) \wedge b \in \mathbb{F}_q \cdot d\big\} \\ \vee \ \big\{\phi(d) \wedge (b = f_1 d \vee \cdots \vee b = f_r d) \wedge a \in \mathbb{F}_q \cdot c\big\}\Big]\Big).$$

This formula is equivalent to

$$\chi(f_1 a, b) \vee \cdots \vee \chi(f_r a, b) \vee \chi(f_1 b, a) \vee \cdots \vee \chi(f_r b, a). \tag{4.1}$$

"$\deg(A) \geq \deg(B)$" is equivalent to "$v_\infty(\frac{B}{A}) \geq 0$". By [Eis03a, Theorem 5.15], the set $\{z \in K : v_\mathfrak{p}(z) \geq 0\}$ is diophantine (and requires 9 quantifiers to define), therefore $\psi(a,b)$ is indeed diophantine and moreover requires $2 + 9 + 9 = 20$ quantifiers according to (4.1). □

Corollary 4.4.10. *There is a universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ given by 145 quantifiers.*

Proof. By *Remark 4.4.7 (4)*, we have

$$f(t) \in \mathbb{F}_q[t] \cup (\mathbb{F}_q[t])_\infty \Leftrightarrow \forall a, b\left((a,b) \notin D \vee f(t) \in \widetilde{R_{a,b}}\right). \tag{4.2}$$

By [EM18, Lemma 3.19], $\widetilde{R_{a,b}}$ is universally defined, hence as D is diophantine, (4.2) is indeed a universal formula for $\mathbb{F}_q[t] \cup (\mathbb{F}_q[t])_\infty$. Denote this formula by $\Phi(f)$.

Recall that the number of quantifiers needed to define $\widetilde{R_{a,b}}$ is one more than is required to define its Jacobson radical, which is $2 + 8 \cdot 15 = 122$

by [Par13, Lemma 3.17]. Thus the number of universal quantifiers need to define $\mathbb{F}_q[t] \cup (\mathbb{F}_q[t])_\infty$ in $\mathbb{F}_q(t)$ using (4.2) is at most $2+20+122+1 = 145$.

What about the definition of $\mathbb{F}_q[t]$? This is simply

$$f(t) \in \mathbb{F}_q[t] \quad \Leftrightarrow \quad \Phi(f(t)) \wedge (\deg(f(t)) > 0 \vee f(t) = k_1 \vee \cdots \vee f(t) = k_q)\,,$$

where $k_1, \ldots, k_q$ are the elements of $\mathbb{F}_q$. Note that "$\deg(f) > 0$" is universally defined by 9 quantifiers ([Eis03a, Theorem 5.15]) and thus $\mathbb{F}_q[t]$ is universally defined in $\mathbb{F}_q(t)$ by $\max\{145, 9\} = 145$ quantifiers, as required.

This definition requires the use of elements of $\mathbb{F}_q$ as parameters; alternatively one could instead include the constant α in the language $\mathcal{L}_{\text{rings}} \cup \{t\}$ where $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Or one could declare the language to be $\mathcal{L}_{\text{rings}} \cup \{t\}$ and define α as part of D (using one additional existential quantifier). ■

Remark 4.4.11. As we are able to take Daans' method in defining $\mathbb{Z}$ over $\mathbb{Q}$ and apply it to function fields, we might wonder if the same can be done for number fields, as Park's work also builds on Koenigsmann's and has great similarities to Eisenträger & Morrison's result. We can say at the least that the set of conditions D of *Definition 4.4.6* cannot be directly applied in their current form to number fields; $\psi(a, b)$ relies on the finite field $\mathbb{F}_q$ of which there is no definable analogy in a number field K (cf. *Theorem 4.1.1 (II)*). Therefore this definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ will fail to define $\mathcal{O}_K$ in K. □

4.5 Shlapentokh's ∀∃-Definition

We shall outline part of [Shl15] which gives (when simplified) a ∀∃-definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ using one universal quantifier:

Theorem 4.5.1. *Let K be a global function field. $\mathbb{F}_q[t]$ has a definition (with parameters) over K of the form $\forall\exists\ldots\exists(P = 0)$ where P is a polynomial over K and only one variable is in the range of the universal quantifier.*

In particular, for $K = \mathbb{F}_q(t)$, there is a ∀∃-definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ with a single universal quantifier.

Shlapentokh uses the following notation (in addition to *Appendix A.2*):

Notation B.

- Let r be a rational prime and ζ_r be a primitive r^{th} root of unity. Suppose $\mathbb{F}_q$ has an extension of degree r and let $\zeta_r \in \mathbb{F}_q$.

- Let $\mathfrak{p}_\infty$ be the pole of t.
- Let o be the smallest positive integer such that for some prime $\mathfrak{a}$ it is the case $\operatorname{ord}_{\mathfrak{a}} t = o$.

Suppose $f \in \mathbb{F}_q(t)$ is given. Consider the following first order statement, which we will denote as $\mathfrak{S}$, in the language $\mathcal{L}_{\text{rings}} \cup \{t\}$:

$$\forall c \in \mathbb{F}_q(t)\ \exists v, \hat{v}, \widetilde{t}, \widetilde{v} \in \mathbb{F}_q(t),$$

$$\Bigg(\exists \bar{s} \in \mathbb{Z}_{>0} \text{ s.t. } f^{p^{\bar{s}}} = f \tag{A1}$$

$$\vee \operatorname{ord}_{\mathfrak{p}_\infty} c > \operatorname{ord}_{\mathfrak{p}_\infty} t \tag{A2}$$

$$\vee \left(\exists s' \in \mathbb{Z}_{\geq 0} \text{ s.t. } v = t^{p^{s'}} \ \wedge \ \operatorname{ord}_{\mathfrak{p}_\infty} v^p < \operatorname{ord}_{\mathfrak{p}_\infty} c < \operatorname{ord}_{\mathfrak{p}_\infty} v\right)\Bigg) \tag{A3}$$

$$\bigvee$$

$$\Bigg(\exists s, \hat{s}, \widetilde{s} \in \mathbb{Z}_{\geq 0} \text{ s.t. } v = t^{p^s} \wedge \widetilde{v} = \widetilde{t}^{p^s} \wedge \hat{v} = t^{p^{\hat{s}}} \wedge \frac{\widetilde{v}^o}{\widetilde{t}^o} = \left(\frac{\hat{v}}{t}\right)^{p^{\widetilde{s}}} \tag{B1}$$

$$\wedge \operatorname{ord}_{\mathfrak{p}_\infty} c = \operatorname{ord}_{\mathfrak{p}_\infty} v \tag{B2}$$

$$\wedge \operatorname{ord}_{\mathfrak{p}} f \geq 0 \text{ for all } \mathfrak{p} \text{ s.t. } \operatorname{ord}_{\mathfrak{p}} t > 0 \tag{B3}$$

$$\wedge \exists y \in L_i(\sqrt[r]{c}) \text{ s.t. } \operatorname{Norm}_{L_i(\sqrt[r]{c})/L_i}(y) = t^i \frac{f^{rp^{\hat{s}}} - f^r}{t^{p^{\hat{s}}} - t}, \tag{B4}$$

$$\text{for some } i \in \{0, \ldots, r-1\}\Bigg),$$

where for each i, the field

$$L_i = \mathbb{F}_q(t)\left(\sqrt[r]{1 + \left(t^i \tfrac{f^{rp^{\hat{s}}} - f^r}{t^{p^{\hat{s}}} - t}\right)^{-1}}, \sqrt[r]{1 + (c + c^{-1})\left(t^i \tfrac{f^{rp^{\hat{s}}} - f^r}{t^{p^{\hat{s}}} - t}\right)^{-1}}\right).$$

Note that the norm equations of (B4) can also be written in polynomial format, as can all the $\operatorname{ord}_{\mathfrak{p}}$ statements for any prime $\mathfrak{p}$ of a global field (cf. [Eis03a, Theorem 5.15]). One might be wary of the quantifier "$\exists s \in \mathbb{Z}_{\geq 0}$" however [Shl15, Lemma 5.6] demonstrates this has a diophantine definition in $\mathbb{F}_q(t)$. Hence $\mathfrak{S}$ is a first order sentence in the given language. In fact, $\mathfrak{S}$ is of the form $\forall\exists \ldots \exists(P = 0)$ where P is a polynomial over $\mathbb{F}_q(t)$.

Before Shlapentokh tackles *Theorem 4.5.1*, she opens with the 'easier' case of $q = p$, i.e. the field $\mathbb{F}_p(t)$ where p is prime.

Lemma 4.5.2. *$\mathbb{F}_p[t]$ has a first order definition in $\mathbb{F}_p(t)$. Let r be a rational prime, and define*

$$F = \Bigg\{ y \in \mathbb{F}_p(t) : \forall m \in \mathbb{Z}_{>0}, \forall \text{ primes } \mathfrak{p} \neq \mathfrak{p}_\infty, \operatorname{ord}_{\mathfrak{p}} \frac{y^{rp^m} - y^r}{t^{p^m} - t} \geq 0 \vee \operatorname{ord}_{\mathfrak{p}} \frac{y^{rp^m} - y^r}{t^{p^m} - t} \equiv 0 \mod r \Bigg\}.$$

Then $F = \mathbb{F}_p[t]$.

Proof. If y is a polynomial in t, then for all $m \in \mathbb{Z}_{>0}$, $\frac{y^{rp^m} - y^r}{t^{p^m} - t}$ is a polynomial in t ([Shl15, Lemma 5.10]). Hence $\operatorname{ord}_{\mathfrak{p}} \frac{y^{rp^m} - y^r}{t^{p^m} - t} \geq 0$ for all primes $\mathfrak{p}$ for such y and thus $y \in F$.

On the other hand, for any prime $\mathfrak{p} \neq \mathfrak{p}_\infty$ of $\mathbb{F}_p(t)$, there exists $m_0 \in \mathbb{Z}_{\geq 0}$ such that $\operatorname{ord}_{\mathfrak{p}}(t^{p^m} - t) = 1$ for all integers m such that $m_0 | m$. Thus for this prime,

$$\operatorname{ord}_{\mathfrak{p}} \frac{y^{qp^m} - y^q}{t^{p^m} - t} = qp^m \operatorname{ord}_{\mathfrak{p}} y - 1,$$

so if $\operatorname{ord}_{\mathfrak{p}} y < 0$ it is the case

$$\operatorname{ord}_{\mathfrak{p}} \frac{y^{qp^m} - y^q}{t^{p^m} - t} < 0 \text{ and } \operatorname{ord}_{\mathfrak{p}} \frac{y^{qp^m} - y^q}{t^{p^m} - t} \not\equiv 0 \mod r,$$

thus $y \notin F$. So F is the polynomial ring $\mathbb{F}_p[t]$ exactly, as required. ∎

Remark 4.5.3. To switch from $\mathbb{F}_p[t]$ to $\mathbb{F}_q[t]$, where $q = p^n$, we allow for all m above to be divisible by n. However, there is still the problem of quantifying over $\mathbb{Z}_{>0}$ in $\mathbb{F}_q(t)$. To fix this inaccuracy, we can instead use the following definition of F:

$$\begin{aligned} F = \Bigg\{ & y \in \mathbb{F}_p(t) : \forall c \in \mathbb{F}_p(t), \forall \text{ primes } \mathfrak{p} \neq \mathfrak{p}_\infty, \\ & \big(\operatorname{ord}_{\mathfrak{p}_\infty} c \geq 0 \quad \vee & \text{(C1)} \\ & \exists t^{p^m} \text{ s.t. } \operatorname{ord}_{\mathfrak{p}_\infty} t^{p^{m+1}} < \operatorname{ord}_{\mathfrak{p}_\infty} c < \operatorname{ord}_{\mathfrak{p}_\infty} t^{p^m} \big) & \text{(C2)} \\ & \bigvee \\ & \Big(\exists t^{p^{\tilde{m}}} \text{ s.t. } \operatorname{ord}_{\mathfrak{p}_\infty} c = \operatorname{ord}_{\mathfrak{p}_\infty} t^{p^{\tilde{m}}} \quad \wedge & \text{(D1)} \\ & \operatorname{ord}_{\mathfrak{p}} \frac{y^{rp^{\tilde{m}}} - y^r}{t^{p^{\tilde{m}}} - t} \geq 0 \vee \operatorname{ord}_{\mathfrak{p}} \frac{y^{rp^{\tilde{m}}} - y^r}{t^{p^{\tilde{m}}} - t} \equiv 0 \mod r \Big) \Bigg\}. & \text{(D2)} \end{aligned}$$

Together (C1), (C2) and (D1) replace the quantifier "$\forall m \in \mathbb{Z}_{>0}$" by ensuring only adequate values of $t^{p^{\tilde{m}}}$ pass to (D2).

Not only is this formulation of F equivalent to that of *Lemma 4.5.2*, we see (C1) is similar to (A2) and (C2) is equivalent to (A3) of $\mathfrak{S}$. (A1) of $\mathfrak{S}$ simply determines if $f \in \mathbb{F}_q$, so is quite harmless and can be ignored. Also note that in $\mathfrak{S}$, "$\exists t^{p^{\tilde{m}}}$" of the above definition of F is replaced by "$\exists s \in \mathbb{Z}_{\geq 0}$ s.t. $v = t^{p^s}$" as by [Shl15, Lemma 5.6] this articulation ensures diophantiness. The condition (D2) is replaced in $\mathfrak{S}$ by (B3) and (B4). This is tricky and invokes the *Strong Approximation Theorem* to allow us to reuse the universally quantified c instead of "$\forall$ primes $\mathfrak{p} \neq \mathfrak{p}_\infty$" [Shl15, Prop. 3.9 & 3.10]. Finally, note that all requirements of the order at a single prime can be stated existentially [Eis03a, Theorem 5.15]. □

Remark 4.5.4. If we assume $\mathfrak{S}$ to be true about $f \in \mathbb{F}_q(t)$ and assume f is nonconstant, and c doesn't satisfy (A2) and (A3), then (B1) implies $\widetilde{t}^{o(p^s-1)} = t^{p^{\tilde{s}}(p^{\hat{s}}-1)}$. Thus $\mathfrak{a}$ must be a zero of $\widetilde{t}$ (where $\operatorname{ord}_{\mathfrak{a}} t = o$) and

$$o(p^s - 1) \operatorname{ord}_{\mathfrak{a}} \widetilde{t} = op^{\tilde{s}}(p^{\hat{s}} - 1).$$

From this we conclude $(p^s - 1)|(p^{\hat{s}} - 1)$ and $s|\hat{s}$. This will be useful to us later on. □

We now approach the result mentioned at the beginning of the section.

Proposition 4.5.5. *$\mathbb{F}_q[t]$ is definable over $\mathbb{F}_q(t)$ by a $\forall\exists$-formula using a single universal quantifier.*

Proof. As we have argued above, $\mathfrak{S}$ can be expressed by a Π_2^+-formula using a single universal quantifier. We shall show this defines $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$.

Let $f \in \mathbb{F}_q(t)$ and assume $\mathfrak{S}$ is true about f. Suppose for the purpose of contradiction it is the case that for some prime $\mathfrak{q}$, $\operatorname{ord}_{\mathfrak{q}} f < 0$. Then there are three cases:

Case 1: $\operatorname{ord}_{\mathfrak{q}} t > 0$.

Case 2: $\operatorname{ord}_{\mathfrak{q}} t = 0$.

Case 3: $\operatorname{ord}_{\mathfrak{q}} t < 0$.

By (B3) **Case 1** is immediately eliminated. Suppose we are in **Case 2**; $\operatorname{ord}_{\mathfrak{q}} t = 0$. Let u be the smallest positive integer such that $\operatorname{ord}_{\mathfrak{q}}(t^{p^u} - t) > 0$; such an u exists by [Shl15, Prop. 5.7]. Then let $c \in \mathbb{F}_q(t)$ be such that c is not an r^{th} power modulo $\mathfrak{q}$ and $\operatorname{ord}_{\mathfrak{p}_\infty} c = p^s$ with $u|s$ (such an element exists by [Shl15, Lemma 7.2]). (B2) and (B4) of $\mathfrak{S}$ will hold for such a c.

On the other hand, we know $s|\hat{s}$ by *Remark 4.5.4*, so $u|\hat{s}$. As $\operatorname{ord}_{\mathfrak{q}} f < 0$, it follows $\operatorname{ord}_{\mathfrak{q}} t^i \frac{f^{qp^{\hat{s}}} - f^q}{t^{p^{\hat{s}}} - t} < 0$ for $i = 0, \ldots, r-1$ and $\operatorname{ord}_{\mathfrak{q}} t^i \frac{f^{qp^{\hat{s}}} - f^q}{t^{p^{\hat{s}}} - t}$

$\not\equiv 0 \mod r$, by [Shl15, Prop. 5.7]. However, then (B4) contradicts [Shl15, Prop. 3.10] exactly.

As a result only **Case 3** is permitted to occur; all poles of f are poles of t. As $f \in \mathbb{F}_q(t)$ we conclude in fact $f \in \mathbb{F}_q[t]$ as desired.

Now assuming $f \in \mathbb{F}_q[t]$, we shall show $\mathfrak{S}$ is true of f. WLOG assume f is nonconstant (so (A1) of $\mathfrak{S}$ does not hold) and let $c \in \mathbb{F}_q(t)$. Let s_1, s_2 be positive integers such that $o | p^{s_1}(p^{s_2} - 1)$.

If for all $s \in \mathbb{Z}_{\geq 0}$ it is the case $\mathrm{ord}_{\mathfrak{p}_\infty} c \neq -p^s$ then either (A2) or (A3) is true, and thus $\mathfrak{S}$ holds. Assume otherwise, that

$$\exists s \in \mathbb{Z}_{\geq 0} \text{ s.t. } \mathrm{ord}_{\mathfrak{p}_\infty} c = -p^s.$$

Let $\hat{s}$ be a multiple of sns_2 (recalling that $q = p^n$) and let $\widetilde{s} = s_1$. Notice from this assignment that $o(p^s - 1) | p^{\widetilde{s}}(p^{\hat{s}} - 1)$. Lastly, set

$$w = \frac{p^{\widetilde{s}}(p^{\hat{s}} - 1)}{o(p^s - 1)} \qquad \text{and} \qquad \widetilde{t} = t^w.$$

Note that, by design, now (B1) and (B2) are true. Also note (B3) is true by virtue of the fact $f \in \mathbb{F}_q[t]$.

Finally, as $\mathbb{F}_{p^{\hat{s}}}$ contains the coefficients of f, by [Shl15, Lemma 5.10] $\frac{f^{rp^{\hat{s}}} - f^r}{t^{p^{\hat{s}}} - t}$ is a polynomial and for some $j \in \{0, \ldots, r-1\}$, $t^j \frac{f^{rp^{\hat{s}}} - f^r}{t^{p^{\hat{s}}} - t}$ has degree divisible by r (hence $\mathrm{ord}_{\mathfrak{p}_\infty} t^j \frac{f^{rp^{\hat{s}}} - f^r}{t^{p^{\hat{s}}} - t} \equiv 0 \mod r$). Therefore by [Shl15, Prop. 3.10] there exists $y \in L_j(\sqrt[r]{c})$ such that $\mathbf{N}_{L_j(\sqrt[r]{c})/L_j}(y) = t^j \frac{f^{rp^{\hat{s}}} - f^r}{t^{p^{\hat{s}}} - t}$, which is (B4) exactly. This concludes the theorem. ■

We can extend this result to an arbitrary global function field and prove *Theorem 4.5.1* as follows: let K be a finite extension of $\mathbb{F}_q(t)$. Revise *Notation B:*

Notation C.

- Let $\mathfrak{p}_{K,\infty}$ be a prime of K which is a pole of t.
- Let e be the ramification degree of $\mathfrak{p}_{K,\infty}$ over $\mathbb{F}_q(t)$ (the size of the inertia group in *Definition 3.1.5*).
- Let o be the smallest positive integer such that for some K-prime $\mathfrak{a}_K$ we have $\mathrm{ord}_{\mathfrak{a}_K} t = o$.
- Let $E(t)$ be the polynomial divisible by all primes which ramify in $K/\mathbb{F}_q(t)$ and are not poles of t.

We can assume WLOG t is not a p^{th} power in K (otherwise t can be replaced by a parameter w, where w is not a p^{th} power, and the polynomial ring of t can be existentially defined in the polynomial ring of w).

We need to modify statements of $\mathfrak{S}$ to reflect the extension K. Let $\mathfrak{S}'$ be the first order statement:

$$\forall c \in K\ \exists v, \hat{v}, \widetilde{t}, \widetilde{v} \in K,$$

$$\Bigg(\exists \bar{s} \in \mathbb{Z}_{>0} \text{ s.t. } f^{p^{\bar{s}}} = f \tag{A1}$$

$$\vee\ \operatorname{ord}_{\mathfrak{p}_{K,\infty}} c > e \operatorname{ord}_{\mathfrak{p}_{K,\infty}} t \tag{A2}$$

$$\vee\ (\exists s' \in \mathbb{Z}_{\geq 0} \text{ s.t. } v = t^{p^{s'}} \wedge e \operatorname{ord}_{\mathfrak{p}_{K,\infty}} v^p < \operatorname{ord}_{\mathfrak{p}_{K,\infty}} c < e \operatorname{ord}_{\mathfrak{p}_{K,\infty}} v) \Bigg) \tag{A3}$$

$$\bigvee$$

$$\Bigg(\exists s, \hat{s}, \widetilde{s} \in \mathbb{Z}_{\geq 0} \text{ s.t. } v = t^{p^s} \wedge \widetilde{v} = \widetilde{t}^{p^s} \wedge \hat{v} = t^{p^{\hat{s}}} \wedge \frac{\widetilde{v}^o}{\widetilde{t}^o} = \left(\frac{\hat{v}}{t}\right)^{p^{\bar{s}}} \tag{B1}$$

$$\wedge \operatorname{ord}_{\mathfrak{p}_{K,\infty}} c = e \operatorname{ord}_{\mathfrak{p}_{K,\infty}} v \tag{B2}$$

$$\wedge \operatorname{ord}_{\mathfrak{p}_K} f \geq 0 \text{ for all } \mathfrak{p}_K \text{ s.t. } \operatorname{ord}_{\mathfrak{p}_K} t > 0 \tag{B3}$$

$$\wedge \operatorname{ord}_{\mathfrak{p}_K} f \geq 0 \text{ for all } \mathfrak{p}_K \text{ ramifying in the extension } K/\mathbb{F}_q(t) \tag{B4}$$
$$\text{which are not poles of } t$$

$$\wedge\ \bar{f} = E(t)^r f + 1 \tag{B5}$$

$$\wedge \operatorname{ord}_{\mathfrak{p}_K} t^i \frac{f^{rp^{\hat{s}}} - f^r}{t^{p^{\hat{s}}} - t} \geq 0 \wedge \operatorname{ord}_{\mathfrak{p}_K} t^i \frac{\bar{f}^{rp^{\hat{s}}} - \bar{f}^r}{t^{p^{\hat{s}}} - t} \geq 0 \text{ for all } K\text{-primes} \tag{B6}$$
$$\mathfrak{p}_K \text{ ramifying in the extension } K/\mathbb{F}_q(t) \text{ which are not poles of } t,$$
$$\text{for all } i = 0, \ldots, r-1$$

$$\wedge\ \exists y \in L_i(\sqrt[r]{c}) \text{ s.t. } \mathbf{N}_{L_i(\sqrt[r]{c})/L_i}(y) = t^i \frac{f^{rp^{\hat{s}}} - f^r}{t^{p^{\hat{s}}} - t}, \tag{B7}$$
$$\text{for some } i \in \{0, \ldots, r-1\}$$

$$\wedge\ \exists y \in \overline{L_i}(\sqrt[r]{c}) \text{ s.t. } \mathbf{N}_{\overline{L_i}(\sqrt[r]{c})/\overline{L_i}}(y) = t^i \frac{\bar{f}^{rp^{\hat{s}}} - \bar{f}^r}{t^{p^{\hat{s}}} - t}, \tag{B8}$$
$$\text{for some } i \in \{0, \ldots, r-1\} \Bigg)$$

where for each i, the field

$$L_i = \mathbb{F}_q(t) \left(\sqrt[r]{1 + \left(t^i \tfrac{f^{rp^{\hat{s}}} - f^r}{t^{p^{\hat{s}}} - t} \right)^{-1}}, \sqrt[r]{1 + (c + c^{-1}) \left(t^i \tfrac{f^{rp^{\hat{s}}} - f^r}{t^{p^{\hat{s}}} - t} \right)^{-1}} \right),$$

and

$$\overline{L_i} = \mathbb{F}_q(t)\left(\sqrt[r]{1+\left(t^i\frac{\bar{f}^{rp^{\hat{s}}}-\bar{f}^r}{t^{p^{\hat{s}}}-t}\right)^{-1}}, \sqrt[r]{1+(c+c^{-1})\left(t^i\frac{\bar{f}^{rp^{\hat{s}}}-\bar{f}^r}{t^{p^{\hat{s}}}-t}\right)^{-1}}\right).$$

Theorem 4.5.6. *$\mathbb{F}_q[t]$ is definable over K by a $\forall\exists$-formula using a single universal quantifier.*

Proof. In the same way that $\mathfrak{S}$ was a Π_2^+-formula with a single universal quantifier, so too is $\mathfrak{S}'$. The proof that $\mathfrak{S}'$ is a first order statement defining $\mathbb{F}_q[t]$ in K is [Shl15, Theorem 7.3]; in short, if f satisfies $\mathfrak{S}'$ then we apply the same argument as in the proof of *Proposition 4.5.5*, with some minor extra arguments to compensate for ramification in $K/\mathbb{F}_q(t)$. The 'Weak Vertical Method' [Shl07, §10.1] allows us to deduce $f^r \in \mathbb{F}_q(t)$ from $f \in K$. Combining this with the fact[10] that the only poles of f are poles of t, we conclude f^r is a polynomial. In the same fashion we deduce $\bar{f}^r$ (defined at (B5)) is a polynomial.

If $\bar{f} \notin \mathbb{F}_q(t)$, yet $\bar{f}^r \in \mathbb{F}_q[t]$, then clearly $\bar{f}^r$ is not an r^{th} power in $\mathbb{F}_q(t)$. Therefore for some prime $\mathfrak{p}_0$ of $\mathbb{F}_q(t)$, $\operatorname{ord}_{\mathfrak{p}_0}\bar{f}^r \not\equiv 0 \bmod r$, hence by [Shl15, Lemma 3.4] $\mathfrak{p}_0$ is ramified in the extension $\mathbb{F}_q(t)(\bar{f})/\mathbb{F}_q(t)$. Since $\mathbb{F}_q(t)(\bar{f}) \subseteq K$, $\mathfrak{p}_0$ ramifies in K too. However, by design $E(t)$ is divisible by every prime ramifying in the extension $K/\mathbb{F}_q(t)$ and not a pole of t, and we have proven f has poles at poles of t only, so $\bar{f}$, and hence $\bar{f}^r$, cannot have a zero or pole at any prime ramifying in the extension $K/\mathbb{F}_q(t)$ as $\bar{f} = E(t)^r f + 1$. This is a contradiction to the existence of $\mathfrak{p}_0$. Accordingly $\bar{f}^r$ *is* an r^{th} power in $\mathbb{F}_q[t]$, so $\bar{f} \in \mathbb{F}_q[t]$, and from this we see $f \in \mathbb{F}_q(t)$, again with poles only at poles of t, thus $f \in \mathbb{F}_q[t]$ as required. ■

We conclude that, although Shlapentokh does not appeal to the same basic quaternionic techniques as Koenigsmann, Park, or Eisenträger & Morrison [Koe13, Par13, EM18], she still produces the analogous $\forall\exists$-definition for $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$, as asserted.

[10] See **Case 3** of the proof of *Proposition 4.5.5*.

Chapter 5

An Existential Question

5.1 A Rational Obstruction

We have seen in *Section 2.2.4* that the Bombieri-Lang conjecture is an obstruction to an existential definition of $\mathbb{Z}$ in $\mathbb{Q}$. However, this is unfortunately not the only obstruction - an older conjecture of Mazur [Maz92] also blocks the path to a diophantine definition of $\mathbb{Z}$ in $\mathbb{Q}$:

Conjecture (Mazur). *If X is a variety over $\mathbb{Q}$, then the (real) topological closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ has at most finitely many connected components.* ■

Here the topology of $X(\mathbb{R})$ is the subspace topology inherited from $\mathbb{R}^n$. A direct consequence (cf. [Poo03, Prop. 12.11]) of this conjecture is what the author refers to as the *Diophantine Mazur Conjecture:*

Conjecture (Diophantine Mazur Conjecture). *If X is any algebraic set and S is a diophantine subset of $X(\mathbb{Q})$ then the closure of S in $X(\mathbb{R})$ has at most finitely many connected components.* ■

Corollary 5.1.1. *If $\mathbb{Z}$ is diophantine over $\mathbb{Q}$, then Mazur's Conjecture is false.* ■

Of course, giving a diophantine definition of $\mathbb{Z}$ in $\mathbb{Q}$ is not the only way to embed H10/$\mathbb{Z}$ as a subproblem of H10/$\mathbb{Q}$; by a similar argument to that made in *Chapter 1*, if we had a *diophantine model* of $\mathbb{Z}$ in $\mathbb{Q}$ we could also deduce H10/$\mathbb{Q}$ is undecidable.

Definition 5.1.2. A *diophantine model* of the ring $\mathbb{Z}$ in $\mathbb{Q}$ is a diophantine set $S \subseteq X(\mathbb{Q})$ for some algebraic set X over $\mathbb{Q}$, equipped with a bijection $\phi : \mathbb{Z} \to S$ such that the graphs of addition and multiplication - subsets of $\mathbb{Z}^3$ - correspond to diophantine subsets of $S^3 \subseteq X^3(\mathbb{Q})$.

Remark 5.1.3. Using terminology from model theory, a *diophantine model* of $\mathbb{Z}$ in $\mathbb{Q}$ is equivalent to $\mathbb{Z}$ being *existentially definably interpretable* in $\mathbb{Q}$ [Mar02, §1.3]. □

Unfortunately, Mazur's conjecture still blocks our path.

Theorem 5.1.4. ([CZ00]). *If there exists a diophantine model of $\mathbb{Z}$ in $\mathbb{Q}$, then Mazur's Conjecture is false.* ■

Remarkably, however, the same problem is *not* encountered in function fields.

5.2 Function Fields

In [Maz98, II §2] Mazur devised a conjecture of the same type as before which applies to any completion of a number field (not just an archimedian completion like $\mathbb{R}$). This conjecture can be transferred to function fields, as Cornelissen & Zahidi do:

Conjecture (Function Field Mazur Conjecture). [CZ00, §4][1]. *Let V be a variety over a global field K, v a valuation on K, and K_v the completion of K w.r.t. v. For every point $x \in V(K_v)$, let $W(x)$ be the Zariski closure of $\bigcap_U (V(K) \cap U)$, where U ranges over all v-open neighbourhoods of x in $V(K_v)$.*

Is the set $\{W(x) : x \in V(K_v)\}$ finite? ■

Cornelissen & Zahidi then immediately show the answer to this question is negative in positive characteristic global fields:

Theorem 5.2.1. *Let $K = \mathbb{F}_q(t)$ and v be the valuation at infinity. There is a variety V for which the Function Field Mazur Conjecture does not hold.*

Proof. In [Phe91] and [Vid94] it was proven that, for any prime p, the set $D_p = \{t^{p^s} : s \in \mathbb{Z}_{\geq 0}\}$ is diophantine over $\mathbb{F}_q(t)$. For the prime p such that $q = p^n$, let V be the variety whose projection to the first coordinate is D_p.

The sets $W(x)$ for $x \in V(K)$ are disjoint, since their first coordinates are separated in the topology; $v(t^{p^r} - t^{p^s}) > 1$ for $r \neq s$. Therefore $\{W(x) : x \in V(K_v)\}$ is infinite, in contradiction to the Function Field Mazur Conjecture. ■

[1] There is a typo in [CZ00, Question 4.1] that is corrected here to fit Mazur's original statement [Maz98, II §2].

Finally, Cornelissen & Zahidi demonstrate that, not only does Mazur's conjecture not hold in function fields, there is indeed a diophantine model of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$. Similar to the approach of [Dem07], in [CZ00, Theorem 4.3] it is shown that the polynomial ring has a diophantine model in $\mathbb{Z}_{\geq 0}$, and the latter has a diophantine model in the field of rational functions.

Since there is a diophantine model of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$, we now wonder if there is a diophantine *definition* of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$; equivalently if there exists an existential definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$. This question remains open and its answer could have major implications for the decidability of $\mathtt{Th}_\exists(\mathbb{Q})$. As we know from §2.2.4, the Bombieri-Lang conjecture implies there is no existential definition of $\mathbb{Z}$ in $\mathbb{Q}$; one might wonder whether a similar conclusion can be drawn from a formulation of the Bombieri-Lang conjecture over function fields (one such formulation is due to Gillet & Rössler [GR17] for the function field of a variety over an algebraically closed field of constants). Alas this thesis does not offer an answer to this question, and only indicates that one method of answering such a query is to adapt the proofs of *Lemma 2.2.17* and *Theorem 2.2.18* (or [Koe13, Corollary 23]) to the function field setting. It is perhaps too brazen to suggest leaving this as an exercise for the reader.

To summarise, this thesis explored the definability of certain rings in certain fields. We began in *Chapter 1* with a discussion of the decidability of the existential theories of certain rings and certain fields and how answering definability questions can in turn answer decidability questions. In *Chapter 2* we turned our attention to $\mathbb{Z}$ and $\mathbb{Q}$ and explored results due to Poonen, Daans and a trio of results from Koenigsmann about the definability of $\mathbb{Z}$ in $\mathbb{Q}$: its universal definition, its $\forall\exists$-definition, and its existential definition. The universal definition was generalised in *Chapter 3* to number fields after introducing the required class field theory. We began exploring function fields in *Chapter 4* to mirror the previous progress made in number fields. This chapter highlighted a universal definition of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$ (amongst other things) due to Eisenträger & Morrison, Daans, and the author and concluded with Shlapentokh's $\forall\exists$-definition. Finally in *Chapter 5* we briefly discussed obstructions to the existential definition of $\mathbb{Z}$ in $\mathbb{Q}$ and how they may appear (or disappear) for defining $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$.

Ongoing work includes adapting *Section 4.4* to cater to function fields $\mathbb{F}_q(t)$ with $\mathrm{char}(\mathbb{F}_q) = 2$ (as Daans has adapted his own definition [Daa18, §4.5]), and answering the question of the existential definability of $\mathbb{F}_q[t]$ in $\mathbb{F}_q(t)$. It is the hope of the author that one day soon Hilbert's Tenth Problem over $\mathbb{Q}$ will be solved; until then we will make efforts in its direction.

Appendix A

Background Definitions

A.1 There is a Prime and a Place for everything

In this section we will present an overview of the theory of primes for global fields. This material can be found in most introductory texts to valuation theory, however the author found [vdD14], [Daa18], [O'M00] and [Mil17] most helpful.

Let K be a field.

Definition A.1.1. A *norm* on K is a map $|\cdot| : K \to \mathbb{R}^{\geq 0}$ such that the following 3 conditions hold:

(1) For all $x \in K$, $|x| = 0 \Leftrightarrow x = 0$.

(2) For all $x, y \in K$, $|x \cdot y| = |x| \cdot |y|$.

(3) For all $x, y \in K$, $|x + y| \leq |x| + |y|$.

If in addition the norm satisfies the stronger property

(3') For all $x, y \in K$, $|x + y| \leq \max\{|x|, |y|\}$,

then the norm is known as *nonarchimedian*. Otherwise it is *archimedian*. Finally, one calls a norm *trivial* if $|x| = 1$ for all $x \in K$.

There is a canonical metric arising from each norm ($d(x, y) = |x - y|$) which is commonly used to turn K into a topological field.

Definition A.1.2. A *local field* is a field K with a nontrivial norm $|\cdot|$ such that the induced topology is locally compact.

Examples of local fields are $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}_p$ for any prime $p \in \mathbb{N}$. In fact, it is possible to give a complete classification of local fields [Mil17, Remark 7.49].

Definition A.1.3. We call two norms $|\cdot|_1$ and $|\cdot|_2$ on K *equivalent* if there exists $\alpha \in \mathbb{R}^{>0}$ such that $|\cdot|_1 = |\cdot|_2^{\alpha}$. An equivalence class of nontrivial norms on K is known as a *place* of K.

Note a nonarchimedian norm and an archimedian norm can never be equivalent.

On the other side of the algebraic coin lie *valuations*.

Definition A.1.4. Let $v : K \to \Gamma \cup \{\infty\}$ where Γ is a totally ordered abelian group (commonly $\mathbb{Z}$ in this thesis) and $\infty \notin \Gamma$. This map is a *valuation* if

(1) $v(x) = \infty$ if and only if $x = 0$.

(2) For all $x, y \in K$, $v(x \cdot y) = v(x) + v(y)$.

(3) For all $x, y \in K$, $v(x + y) \geq \min\{v(x), v(y)\}$.

Given a valuation v on a field K we also define

(1) $\mathcal{O}_v := \{x \in K : v(x) \geq 0\}$, the *valuation ring (of v)*.

(2) $\mathfrak{m}_v := \{x \in K : v(x) > 0\}$, the *maximal ideal (of $\mathcal{O}_v$)*.

(3) $k_v := \mathcal{O}_v/\mathfrak{m}_v$, the *residue field (of K)*.

(4) $\mathrm{red}_v : \mathcal{O}_v \to k_v$ (the canonical map).

Valuations and norms are connection by the following proposition:

Proposition A.1.5. *There is a 1-1 correspondence between nonarchimedian norms and $\mathbb{R}$-valued valuations on K. For a nonarchimedian norm $|\cdot|$ on K,*

$$v : K \to \mathbb{R} \cup \{-\ln(0)\} \quad : \quad x \mapsto -\ln|x|,$$

is a real valued valuation on K. Conversely if v is an $\mathbb{R}$-valued valuation then

$$|\cdot| : K \to \mathbb{R}^{\geq 0} \quad : \quad x \mapsto e^{-v(x)},$$

is a nonarchimedian norm on K, with the convention $e^{-\infty} = 0$.

Proof. See [Daa18, Prop. 1.1.5] ■

The terminology introduced in *Definition A.1.3* also applies to valuations. Throughout the thesis, when the author speaks of *places* we shall understand this to mean an equivalence class of valuations, instead of norms.

Now let K be a number field (a finite extension of $\mathbb{Q}$).

Definition A.1.6. By a *prime* of K we mean a place of K. Primes can be separated into two flavours: *finite* (the nonarchimedian places), which can be identified with prime ideals of $\mathcal{O}_K$, and *infinite* (the archimedian places).

If K is a number field then either K embeds into $\mathbb{R}$ or K cannot embed into $\mathbb{R}$ but can embed into $\mathbb{C}$. The former embedding is known as *real* and the latter as *complex*.

We can further separate the infinite primes into two classes:

Definition A.1.7.

(1) A *real infinite prime* is the equivalence class of the norm $|\cdot| := |\sigma(\cdot)|$ where $\sigma : K \hookrightarrow \mathbb{R}$.

(2) A *complex infinite prime* is the equivalence class of the norm $|\cdot| := |\sigma(\cdot)|$ where $\sigma : K \hookrightarrow \mathbb{C}$.

Example A.1.8. Let $K = \mathbb{Q}(\sqrt{-5})$. Then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. The finite primes of K are primes ideals of $\mathbb{Z}[\sqrt{-5}]$ and there is one (complex) infinite prime corresponding to the equivalence class of $\sigma : \mathbb{Q}(\sqrt{-5}) \hookrightarrow \mathbb{C}$. In this setting the conjugate pair of embeddings

$$\sigma_1 : \sqrt{-5} \mapsto \sqrt{-5}, \qquad \sigma_2 : \sqrt{-5} \mapsto -\sqrt{-5},$$

are equivalent so determine the same place of $\mathbb{Q}(\sqrt{-5})$. □

If K is an algebraic function field (i.e. a finite extension of $\mathbb{F}_q(t)$), much of the same is true: primes of K are places of K. There is one difference to *Definition A.1.6;* all primes of K are nonarchimedian, including the infinite primes. So we instead introduce the following terminology:

Definition A.1.9. Let K be an algebraic function field and $\mathcal{O}_K$ be the integral closure of $\mathbb{F}_q[t]$ in K. Let v be a prime (i.e. a place) of K.

(1) If v corresponds to a prime of $\mathcal{O}_K$ (if the set $\{x \in K : v(x) > 0\}$ is a prime ideal of the ring $\mathcal{O}_K$) then v is known as *finite*. Otherwise v is known as *infinite*.

(2) In the special case of $K = \mathbb{F}_q(t)$, $\mathcal{O}_K = \mathbb{F}_q[t]$, there is one infinite prime known as *the prime at infinity* and denoted ∞ or v_∞ as a valuation. For $f \in \mathbb{F}_q(t)$, $v_\infty = -\deg(f)$. In general ∞ may decompose in the extension $K/\mathbb{F}_q(t)$ to many infinite primes.

Remark A.1.10. Note that although we make a distinction between finite and infinite primes of global function fields in the above definition, in other works such a distinction is not usually made. In [EM18] and [Daa18] the finite primes of a global field are the non-archimedian ones; thus, every prime of a global function field is *finite* from this viewpoint. This frame of reference is in fact necessary to obtain important results on diophantine definability, so is one perspective we shall take in this thesis. □

For convenience when we speak about (finite) primes we are usually referring to the corresponding ideal, and occasionally the corresponding valuation, though this distinction should be clear from context. We will close this section with the following diagram relating (finite) *prime ideals, norms*, and *valuations* for global fields:

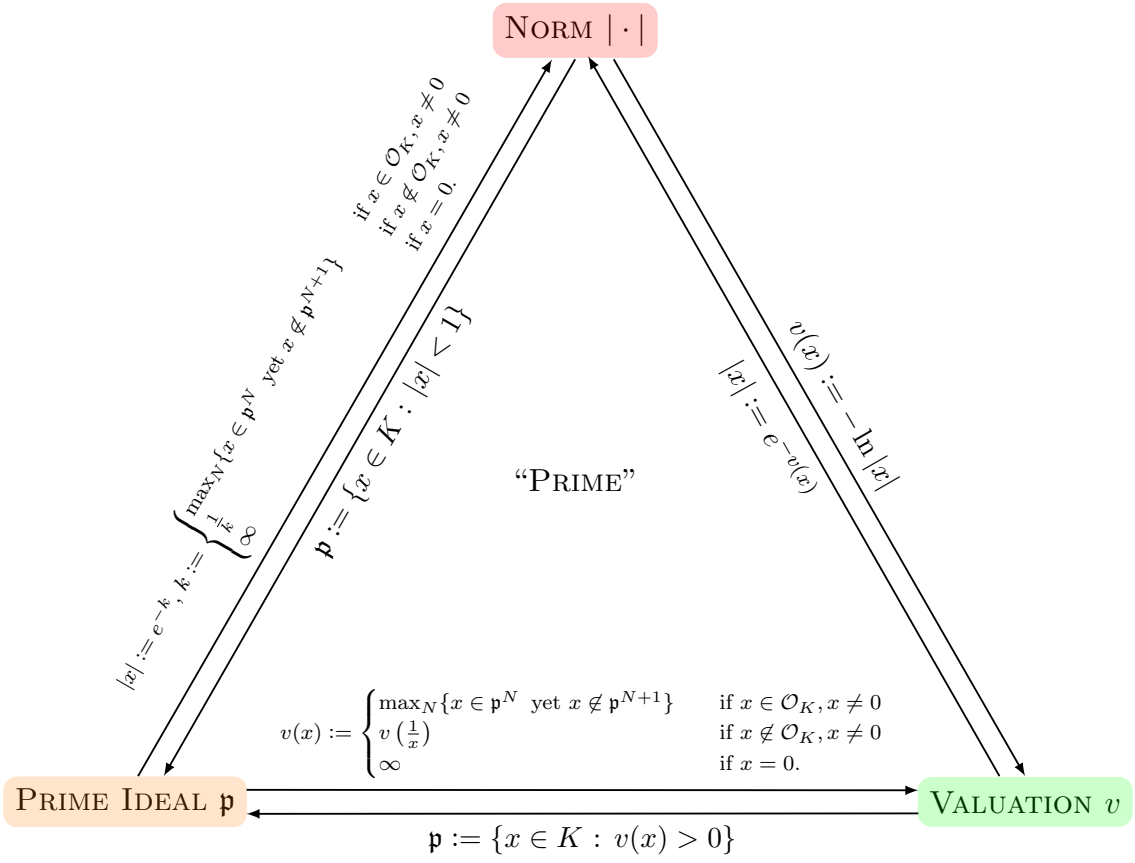

Figure A.1: Relationship between (finite) prime ideals, norms, and valuations for global fields. An arrow from A to B indicates how one might take object A and turn it into object B.

A.2 Function Fields

Some basic definitions from [Ros02] are presented below. The author also found [Che51] to be a helpful reference.

Definition A.2.1. Let F be a field.

a) An *(algebraic) function field* of m variables over a field k is a finitely generated field extension K of the field of rational functions in m variables over k, $k(x_1, \ldots, x_m)$.

b) For the function fields we shall consider, $k = \mathbb{F}_q$, a finite field of characteristic p and $q = p^n$ elements, and $m = 1$. The variable x_1 is usually denoted t. In this case, K is known as a *global function field*.

We will follow the same definitions as noted by [Shl15] for a global function field K:

c) The *order of* $f \in K$ *at* (a prime) $\mathfrak{p}$ is defined as:

$$\operatorname{ord}_{\mathfrak{p}} f = \begin{cases} \max_{N \in \mathbb{Z}} \{f \in \mathfrak{p}^N \text{ and } f \notin \mathfrak{p}^{N+1}\}, & \text{if } f \in \mathcal{O}_v \text{ and } f \neq 0, \\ -\operatorname{ord}_{\mathfrak{p}_v} \frac{1}{x}, & \text{if } f \notin \mathcal{O}_v \text{ and } f \neq 0, \\ \infty & \text{if } f = 0. \end{cases}$$

Furthermore we say f *has a zero at* $\mathfrak{p}$ if $\operatorname{ord}_{\mathfrak{p}} f > 0$ and f *has a pole at* $\mathfrak{p}$ if $\operatorname{ord}_{\mathfrak{p}} f < 0$. In the terminology of *Appendix A.1*, $\operatorname{ord}_{\mathfrak{p}}$ is a valuation on K.

d) If S_K is the set of all primes of a function field K, and $S \subseteq S_K$, then define $\mathcal{O}_{K,S}$ to be the subring of K consisting of those elements without any poles outside of S; i.e.

$$\mathcal{O}_{K,S} := \{x \in K : \forall \text{ primes } \mathfrak{p} \notin S, \operatorname{ord}_{\mathfrak{p}} x \geq 0\}.$$

If S is finite, then $\mathcal{O}_{K,S}$ is known as the *ring of S-integers*. Frequently this is written simply as $\mathcal{O}_S$.

e) Finally, for any prime $\mathfrak{p}$, we set $K_{\mathfrak{p}}$ to be the completion of K under the $\mathfrak{p}$-adic topology (much like $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ under the p-adic topology).

We adopt the following piece of notation: if $\mathfrak{p} = (f(t))$ is a prime of $\mathbb{F}_q(t)$ (where $f(t)$ is a monic and irreducible polynomial) then the residue field of $\mathbb{F}_q(t)_{\mathfrak{p}} = \mathbb{F}_q(t)_{f(t)}$ is denoted $\mathbb{F}_{f(t)}$ and is isomorphic to the set of

polynomials of $\mathbb{F}_q[t]$ of degree strictly less than $\deg(f)$, which is isomorphic to $\mathbb{F}_{q^{\deg(f)}}$. The residue map $\mathbb{F}_q[t]_{f(t)} \to \mathbb{F}_{f(t)}$ is denoted $\mathrm{red}_{f(t)}$.

The final collection of definitions concerns *divisors*, which are the function field analogue of the fractional ideals of a number field according to [Poo06, §2.6].

Definition A.2.2.

a) Let $\mathcal{D}_K$ be the free abelian group consisting of formal sums, generated by the primes of a function field K; this is known as the *group of divisors of* K. If $D \in \mathcal{D}_K$ is of the form $D = \sum_P a_P P$ then the *degree of* D,
$$\deg(D) := \sum_P a_P \deg(P).$$
(The degree of a finite prime ideal is the degree of the polynomial to which it corresponds, while the degree of the prime at infinity is 1.)

b) Let $a \in K^*$. The *divisor* of a, denoted (a), is defined to be $\sum_P \mathrm{ord}_P(a)P$. Note that $\mathrm{ord}_P(a)$ is zero for all but finitely many P.

c) As in *Definition A.2.1 (c)*, if P is a prime such that $\mathrm{ord}_P(a) = m > 0$, we say P *is a zero of* a *of order* m. Similarly if Q is a prime such that $\mathrm{ord}_Q(a) = -n < 0$, we say Q *is a pole of* a *of order* n.

d) Define the *zero divisor of* a, $(a)_0$, to be
$$(a)_0 := \sum_{\substack{P \\ \mathrm{ord}_P(a)>0}} \mathrm{ord}_P(a)P.$$
Define the *pole divisor of* a, $(a)_\infty$, to be
$$(a)_\infty := -\sum_{\substack{P \\ \mathrm{ord}_P(a)<0}} \mathrm{ord}_P(a)P.$$
Finally, note (a) is simply $(a)_0 - (a)_\infty$.

Appendix B

Squares and Nonsquares in $\mathbb{F}_q(\!(\frac{1}{t})\!)$.

We present here an explicit proof of *Lemma 4.4.1* which gives a direct characterisation of square and nonsquare elements of $\mathbb{F}_q(\!(\frac{1}{t})\!)$.

Lemma B.0.1. *Any nonsquare of $\mathbb{F}_q(\!(\frac{1}{t})\!)$ is of the form $\frac{1}{t}c^2, fc^2$, or $\frac{f}{t}c^2$ where $c \in \mathbb{F}_q(\!(\frac{1}{t})\!)$ and $f \in \mathbb{F}_q$ is a nonsquare.*

Proof. First we have the following characterisation of squares:

$$\sum_{i=N}^{-\infty} c_i t^i \text{ is a square in } \mathbb{F}_q\big(\!\big(\tfrac{1}{t}\big)\!\big)^\times \quad \Leftrightarrow \quad N \text{ is even } \& \ c_N \text{ is a square in } \mathbb{F}_q.$$

The forward direction is obtained by noting

$$\sum_{i=N}^{-\infty} c_i t^i = \left(\sum_{i=K}^{-\infty} a_i t^i\right)^2 = \sum_{i=2K}^{-\infty} \left(\sum_{\substack{j+k=i,\\ j,k\leq K}} a_j a_k\right) t^i,$$

so necessarily $N = 2K$ and $c_N = (a_K)^2$. The reverse direction is obtained by constructing a solution of

$$\sum_{i=N}^{-\infty} c_i t^i = \left(\sum_{i=K}^{-\infty} a_i t^i\right)^2 = \sum_{i=2K}^{-\infty} \left(\sum_{\substack{j+k=i,\\ j,k\leq K}} a_j a_k\right) t^i.$$

For $i = 2K$ it is necessary that $c_N = (a_K)^2$. We have assumed c_N is a square, however, so we can find a_K. Then

$$c_{N-n} = 2a_K a_{K-n} + \sum_{\substack{j+k=2K-n,\\ j,k\leq K}} a_j a_k,$$

so we can solve for a_{K-n} inductively.

From this characterisation there is a useful characterisation of nonsquares (nonsq.) too:

$$\sum_{i=N}^{-\infty} c_i t^i \text{ is a nonsq. in } \mathbb{F}_q(\!(1/t)\!)^\times \Leftrightarrow N \text{ is odd or } c_N \text{ is a nonsq. in } \mathbb{F}_q.$$

Thus any nonsquare of $\mathbb{F}_q(\!(1/t)\!)^\times$ is a square times one of the following elements:

(1) $1/t$.

(2) Some fixed nonsquare $f \in \mathbb{F}_q$.

(3) f/t for f as above.

This concludes the lemma. ■

References

[Cha12] Chan, W. K. Arithmetic of Quaternion Algebras. *Available at* `wkchan.web.wesleyan.edu/quaternion-2012.pdf` (2012).

[Che51] Chevalley, C. *Introduction to the Theory of Algebraic Functions of One Variable*. AMS. Mathematical Surveys and Monographs Volume 6 (1951).

[Cla18] Clark, P. Ray Class Groups and Ray Class Fields: First classically, then adelically. *Available at* `citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.419.4890&rep=rep1&type=pdf` (Accessed 2018).

[Con18a] Conrad, K. History of class field theory. *Available at* `www.math.uconn.edu/~kconrad/blurbs/gradnumthy/cfthistory.pdf` (Accessed 2018).

[Con18b] Conrad, K. The local-global principle. *Available at* `www.math.uconn.edu/~kconrad/blurbs/gradnumthy/localglobal.pdf` (Accessed 2018).

[Con18c] Conrad, K. Quaternion algebras. *Available at* `www.math.uconn.edu/~kconrad/blurbs/ringtheory/quaternionalg.pdf` (Accessed 2018).

[CZ00] Cornelissen, G. and Zahidi, K. Topology of Diophantine Sets: remarks on Mazur's conjectures. `arXiv:math/0006140` (2000).

[Daa18] Daans, N. Diophantine definability in number fields and their rings of integers. Master's thesis, Universiteit Antwerpen (2018).

[Dem07] Demeyer, J. Diophantine Sets over Polynomial Rings and Hilberts Tenth Problem for Function Fields. Ph.D. thesis, Universiteit Gent (2007).

[Den79] Denef, J. The Diophantine Problem for polynomial rings of positive characteristic. In *Studies in Logic and the Foundations of Mathematics*, Volume 97 (edited by M. Boffa, D. Dalen, and K. Mcaloon), pp. 131–145. Elsevier (1979).

[Eis03a] Eisenträger, K. Hilbert's Tenth Problem and Arithmetic Geometry. Ph.D. thesis, University of California at Berkeley (2003).

[Eis03b] Eisenträger, K. Hilbert's Tenth Problem for algebraic function fields of characteristic 2. *Pacific J. Math.*, **210**(2): pp. 261–281 (2003).

[EM18] Eisenträger, K. and Morrison, T. Universally and existentially definable subsets of global fields. `arXiv:1609.09787v3` (2018).

[Fal91] Faltings, G. Diophantine approximation on abelian varieties. *Ann. of Math.*, **133**: pp. 549–576 (1991).

[Göd31] Gödel, K. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatshefte Math. Phys.*, **38**: pp. 173–198 (1931).

[GR17] Gillet, H. and Rössler, D. Rational points of varieties with ample cotangent bundle over function fields. `arXiv:1312.6008` (2017).

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

[Has30] Hasse, H. Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols. *J. Reine Angew. Math.*, **162**: pp. 134–144 (1930).

[Hil96] Hilbert, D. Ein neuer Beweis des Kroneckerschen Fundamentalsatzes über Abelsche Zahlkörper. *Nachr. Königl. Gesell. Wiss. Göttingen, Mathematisch-Physikalische Klasse*, pp. 29–39 (1896).

[Hil00] Hilbert, D. Mathematische Probleme. *Nachr. Königl. Gesell. Wiss. Göttingen, Mathematisch-Physikalische Klasse*, pp. 253–297 (1900).

[HS00] Hindry, M. and Silverman, J. *Diophantine Geometry: An Introduction.* Springer. Graduate Texts in Mathematics 201 (2000).

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

[Koe13] Koenigsmann, J. Defining $\mathbb{Z}$ in $\mathbb{Q}$. arXiv:1011.3424v2 (2013).

[Koe14] Koenigsmann, J. Undecidability in number theory. In *Model theory in Algebra, Analysis and Arithmetic* (edited by H. D. Macpherson and C. Toffalori), pp. 159–195. Springer-Verlag. *Available at* `arXiv:1309.0441` (2014).

[Koe16] Koenigsmann, J. Defining $\mathbb{Z}$ in $\mathbb{Q}$. *Ann. of Math.*, **183**(1): pp. 73–93 (2016).

[Lam05] Lam, T. *Introduction to Quadratic Forms over Fields.* AMS. Graduate Studies in Mathematics 67 (2005).

[Mar02] Marker, D. *Model Theory: An Introduction.* Springer. Graduate Texts in Mathematics 217 (2002).

[Mat70] Matiyasevich, Y. Enumerable sets are Diophantine. *Soviet Math. Dokl.*, **11**: pp. 354–358 (1970).

[Maz92] Mazur, B. The topology of rational points. *Experiment. Math.*, **1**(1): pp. 35–45 (1992).

[Maz98] Mazur, B. Open problems regarding rational points on curves and varieties. In *Galois Representations in Algebraic Arithmetic Geometry, LMS Lecture Note Series*, Volume 254 (edited by A. J. Scholl and R. L. Taylor), pp. 239–265. Cambridge University Press (1998).

[Mil13] Milne, J. S. Class field theory (v4.02). Available at `www.jmilne.org/math/CourseNotes/CFT.pdf` (2013).

[Mil17] Milne, J. S. Algebraic number theory (v3.07). Available at `www.jmilne.org/math/CourseNotes/ANT.pdf` (2017).

[Neu99] Neukirch, J. *Algebraic Number Theory.* Springer (1999).

[O'M00] O'Meara, T. *Introduction to Quadratic Forms.* Springer. Classics in Mathematics (2000).

[Par13] Park, J. A universal first order formula defining the ring of integers in a number field. *Math. Res. Lett.*, **20**(5): pp. 961–980. *Available at* `arXiv:1202.6371` (2013).

[Phe91] Pheidas, T. Hilbert's Tenth Problem for fields of rational functions over finite fields. *Invent. Math.*, **103**(1): pp. 1–8 (1991).

[Poo03] Poonen, B. Hilbert's Tenth Problem over Rings of Number-Theoretic Interest. *Available at* `https://math.mit.edu/∼poonen/papers/aws2003.pdf` (2003).

[Poo06] Poonen, B. Lectures on rational points on curves. *Available at* `www-math.mit.edu/∼poonen/papers/curves.pdf` (2006).

[Poo08] Poonen, B. Undecidability in number theory. *Notices Amer. Math. Soc.*, **55**(3): pp. 344–350 (2008).

[Poo09a] Poonen, B. Characterizing integers amongst rational numbers with a universal-existential formula. *Amer. Jour. Math.*, **131**(3): pp. 675–682. *Available at* `arXiv:math/0703907` (2009).

[Poo09b] Poonen, B. The set of nonsquares in a number field is Diophantine. *Math. Res. Lett*, **16**(1): pp. 165–170. *Available at* `arXiv:0712.1785` (2009).

[Rob49] Robinson, J. Definability and decision problems in arithmetic. *J. Symbolic Logic*, **14**(2): pp. 98–114 (1949).

[Rob59] Robinson, J. The undecidability of algebraic rings and fields. *Proc. Amer. Math. Soc.*, **10**: pp. 950–957 (1959).

[Ros02] Rosen, M. *Number Theory in Function Fields*. Springer-Verlag. Graduate Texts in Mathematics 210 (2002).

[Rum80] Rumely, R. Undecidability and definability for the theory of global fields. *Trans. Amer. Math. Soc.*, **262**(1): pp. 195–217 (1980).

[Ser73] Serre, J.-P. *A Course in Arithmetic*. Springer-Verlag. Graduate Texts in Mathematics 7 (1973).

[Ser79] Serre, J.-P. *Local Fields*. Springer-Verlag. Graduate Texts in Mathematics 67 (1979).

[Shl96] Shlapentokh, A. Diophantine Undecidability over Algebraic Function Fields over Finite Fields of Constants. *J. Number Theory*, **58**(2): pp. 317–342 (1996).

[Shl07] Shlapentokh, A. *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*. Cambridge University Press (2007).

[Shl15] Shlapentokh, A. On definitions of polynomials over function fields of positive characteristic. `arXiv:1502.02714` (2015).

[Tak20] Takagi, T. Über eine Theorie des relativ Abel'schen Zahlkörpers. *Journal of the College of Science, Imperial University of Tokyo*, **41**(9): pp. 1–133 (1920).

[vdD14] van den Dries, L. Lectures on the Model Theory of Valued Fields. In *Model theory in Algebra, Analysis and Arithmetic* (edited by H. D. Macpherson and C. Toffalori), pp. 55–157. Springer-Verlag (2014).

[Vid94] Videla, C. Hilbert's Tenth Problem for rational function fields in characteristic 2. *Proc. Amer. Math. Soc.*, **120**(1): pp. 249–253 (1994).