A MODEL-THEORETIC APPROACH TO THE ARITHMETIC OF GLOBAL FIELDS

Philip Sebastian Dittmann

Merton College
University of Oxford

A Thesis Submitted for the Degree of Doctor of Philosophy

June 2018

meinen Eltern gewidmet

ACKNOWLEDGEMENTS

Over the past few years, I have become indebted to a large number of people, who—in R. Bringhurst's words—made this a much better thesis and its author a less ignorant human being, in a variety of ways. These include

my supervisor, Jochen Koenigsmann, for his excellent guidance, support and attention to detail during my time at Oxford;

the other senior members of the Oxford research group for mathematical logic, for their inquisitiveness and ever-helpful contributions in seminars, as well as the atmosphere they have fostered;

my collaborators Sylvy Anscombe and Arno Fehm, for their encouragement and numerous mathematical conversations on the subjects of this thesis and others;

the other junior members of the logic group, for all the mathematical and non-mathematical chat, for arguing when it was necessary, for teaching me other languages, and for simply being good company; and

all my friends in Oxford, whether they accompanied me for a small or a big part of the way—it would not have been possible without you.

A special thank-you goes to my proof-readers for their help during the final stage.

Lastly, I gratefully acknowledge the financial support of Merton College and the Clarendon Fund.

ABSTRACT

This thesis assembles some new results in the field arithmetic of various classes of fields, including global fields, models of the common first-order theory of algebraic extensions of global fields, and fields of finite transcendence degree over their prime field. Most of the results stem from a very simple technique for first-order definitions in fields, based on the satisfaction of a first-order sentence in a family of finite extensions of the ground field. In the first two chapters, we develop this technique to associate existentially definable sets to central simple algebras and Pfister forms, respectively.

We then use these tools to obtain results on global fields, their algebraic extensions, fields elementarily equivalent to ultraproducts thereof, and finitely generated fields. We study valuations on such fields, and notably obtain a large class of examples of fields without Self-Embedded Residue, a natural notion that arises in the study of definable valuations.

Subsequently, we focus on the study of a single global field, where we obtain new definability results. Most importantly, we show that non-solubility of a polynomial equation in one variable over the global field is expressible as an existential condition on the coefficients. This also yields consequences in algebraic geometry over the given field.

After a category-theoretic interlude in the model theory of absolute Galois groups, the final chapter investigates p-valuations on fields. We introduce a notion of generalised Stufe in this context, and prove an interpretability result for spaces of p-valuations in situations of interest.

CONTENTS

INTRODUCTION

This thesis assembles some new results regarding definability in and arithmetic of fields, with a particular focus on global fields, i.e. finite extensions of $\mathbb{Q}$ and $\mathbb{F}_p(T)$, and their algebraic extensions.

The study of fields has a long history in mathematical logic, with particular milestones including the decidability of first-order theories of algebraically closed fields, real-closed fields and p-adically closed fields, as well as the undecidability of the theory of $\mathbb{Q}$ (following J. Robinson's definition of $\mathbb{Z}$ in $\mathbb{Q}$).

The general philosophy here is that local fields, at least in characteristic zero, tend to be model-theoretically tame—for instance model complete, decidable, NIP, with some form of elimination of imaginaries—whereas global fields interpret arithmetic and are therefore undecidable and do not have any stability properties.

This means that the study of global fields from the perspective of mathematical logic does not focus on understanding all definable sets—as this is too rich a structure—, but usually aims to produce definitions for "sets of arithmetic interest" of restricted quantifier complexity or with some degree of uniformity across global fields.

An example for results of this kind can be found in [Rum80], in which a *uniform* interpretation of $\mathbb{Z}$ within global fields is given. On the other hand, there are ongoing efforts to produce definitions of $\mathbb{Z}$ within a single global field with lower quantifier complexity, for instance Koenigsmann's universal definition of $\mathbb{Z}$ in $\mathbb{Q}$ in [Koe16], with a view towards Hilbert's Tenth Problem over fields.

With satisfactory uniform definitions in global fields in place, one can then frequently make some statements also about infinite algebraic extensions of global fields. This touches on some questions of interest in *field arithmetic*, where such fields form a class of considerable interest.

The main technical tool in use throughout this thesis is a specific method for definitions in fields introduced in the second and the third chapter. The key property here is that these are both of low quantifier complexity, namely existential, and have readily understood meaning in different global or finitely generated fields. This tight coupling of an existentially definable set with a property of arithmetic interest across a class of fields—in our cases, the behaviour of a central simple algebra or a cohomology class under the restriction maps arising from inclusions of fields—is key to all our applications. The use of arithmetic features however does mean that we rely on a rather substantial body of preexisting work. As an immediate corollary to our definability results we obtain a $\forall\exists$-definition of the ring of integers in a large class of algebraic extensions of $\mathbb{Q}$, namely all (potentially infinite) Galois extensions of number fields with degree not divisible by some fixed prime number, see Theorem 2.3.7. This substantially generalises results of Videla.

More serious applications of our new definitions are seen in the fourth chapter, in which we mainly discuss the notion of fields with *self-embedded residue*. This property of fields comes from the work [AF17] on existential definability of henselian valuation rings based on the residue field, in which fields with self-embedded residue arose as in some sense dual to the more familiar notion of ample (also known as large or anti-

mordellic) fields. We prove that global fields, and more generally finitely generated fields, at least in characteristic away from 2, do not have self-embedded residue. This is expected, since fields with self-embedded residue should be thought of as "big" fields, but had previously only been shown for the field $\mathbb{Q}$. As a minor result, we can classify valuations on "non-standard number fields" to a certain extent, i.e. on fields which are elementarily equivalent to ultraproducts of number fields. This is driven by the observation that our proofs for global fields are in fact very uniform across the entire class, allowing passage to other models of their common theory.

The fifth chapter focuses on the study of a single global field at a time, and produces new existential definitions within this field. The basic result here is that the set of tuples $a_0, \ldots, a_{n-1}$ such that the polynomial $X^n + a_{n-1}X^{n-1} + \cdots + a_0$ does not have a zero in the global field is existentially definable. This can be seen as a kind of restricted model completeness in that positive formulae with a single existential quantifier are equivalent to universal formulae. We also deduce that for polynomials in an arbitrary number of variables, irreducibility is an existential condition on its coefficients. Furthermore, we develop geometric consequences, giving new diophantine subsets of varieties over global fields.

The sixth chapter departs from the arithmetic side, and develops a new framework for model theory of absolute Galois groups of fields. While there is a standard framework due to Cherlin, Van den Dries and Macintyre, which is satisfactory in practice, we point out some shortcomings of their approach and suggest an alternative. This is mainly

a matter of replacing the absolute Galois group, which intrinsically involves a choice of algebraic closure, by a categorical approach due to Grothendieck. One of the most important advantages of this approach is better behaviour when studying not just a single field, but an entire class of fields, for instance the class of finite extensions of a fixed ground field.

In the seventh chapter, we turn to the study of p-valuations on fields. To some extent, this involves extending some of the existing theory of formally real fields to this situation. The most important new notion here is that of a class of fields of bounded p-Stufe, which is defined in analogy to the theory of formally real fields. We give examples for such classes, notably the class of fields elementarily equivalent to an ultraproduct of number fields, and study the set of all p-valuations on any field in the class in terms of its Galois theory. Some applications to Pop's pseudo classically closed fields are also given.

1.1 technical prerequisites

The corpus of mathematical results that this thesis builds on is quite substantial, though varying between the chapters. In various places, we use model theory, algebraic geometry, Galois cohomology, quadratic form theory, class field theory, category theory, and valuation theory. Due to this breadth of prerequisites, it is not practical to give introductions to all of these; we instead usually refer to the literature.

SPLITTING SENTENCES BY POLYNOMIALS

This chapter introduces a general method for first-order definitions in fields. In its original version, it involves associating to parameters a, b in a field F sets $S_{a,b}$ and $T_{a,b}$, defined by an existential formula with a, b as parameters.

This method originally appeared in [Eis05], and rose to prominence in the articles [Poo09] and [Koe16], the latter of which was then generalised in [Par13] and [EM16]. In all of these instances, the method was used for first-order definitions in global fields. From the first appearance of the method, it was clear that $S_{a,b}$ should be understood in terms of the quaternion algebra (a, b), i.e. the four-dimensional associative unital F-algebra generated by elements x, y subject to the conditions $x^2 = a, y^2 = b, xy = -yx$.

In the author's previous work [Dit18], the method was generalised to arbitrary elements of the Brauer group of a global field.

2.1 THE GENERAL METHOD

Let F be a field and φ an existential sentence in the language of rings, with parameters in F. We are interested in the extension fields E/F which satisfy φ.[1] Typical choices of φ involve the vanishing of a Brauer class, i.e. φ expresses that an element of the Brauer group $\mathrm{Br}(F)$ is sent to zero

[1] One may restate this in a geometric fashion by observing that to every φ one may associate an affine variety V/F such that φ is satisfied in E if and only if V has an E-point. However, we will only occasionally use this viewpoint, for instance in Section 5.4.

by the restriction map $\mathrm{Br}(F) \to \mathrm{Br}(E)$, or more general cohomological vanishing properties.

Specifically, we would like to consider which fields in an "algebraic family" of extension fields of F satisfy φ. But as it is hard to formulate a sensible notion of an algebraic family of fields—families of fields tend to degenerate to rings which are not fields—, we consider polynomials instead. We therefore make the following definition:

Definition 2.1.1. *A monic polynomial $f \in F[X]$* splits *φ if for every irreducible factor $g \mid f$, the quotient field $F[X]/(g)$ satisfies φ.*

The name "splitting" is chosen in analogy to the situation of a central simple algebra which we will consider below.

Proposition 2.1.2. *Let F be a field, φ an existential sentence with parameters in F, and $n > 0$. Then the set of monic polynomials $f \in F[X]$ of degree n which split φ is positively existentially definable, i.e. more formally the* splitting set

$$\{(f_0, \ldots, f_{n-1}) \in F^n \colon X^n + f_{n-1}X^{n-1} + \cdots + f_0 \text{ splits } \varphi\}$$

is a positively existentially definable set.

Proof. By replacing inequalities $p \neq 0$ in φ with equalities $\exists q(pq = 1)$, we may assume that φ is positive existential.

Observe that for any monic $h \in F[X]$ and irreducible factor $g \mid h$, $F[X]/(h) \models \varphi$ implies $F[X]/(g) \models \varphi$ since positive sentences are preserved under homomorphisms.

It follows that f splits φ if and only if there exists $k \leq n$ and non-constant $f_1, \ldots, f_k \in F[X]$ with $f_1 \cdots f_k = f$ and $F[X]/(f_i) \models \varphi$ for all

i. Since $F[X]/(f_i)$ is quantifier-freely interpretable in K in terms of the coefficients of f_i, we can therefore express that f splits φ as an existential first-order statement. Eliminating inequalities as above, it is even positive existential. □

For later use, we establish an improvement on the construction above.

Lemma 2.1.3. *Let F be a perfect field and φ a positive primitive sentence (i.e. positive existential with no disjunctions) with parameters in F. Then f splits φ if and only if $F[X]/(f) \models \varphi$. More generally, for any commutative unital finite-dimensional F-algebra A we have $A \models \varphi$ if and only if $A/\mathfrak{m} \models \varphi$ for every maximal ideal of A.*

We need the following easy result on the structure of finite algebras over fields.

Lemma 2.1.4. *Let A/F be a commutative unital finite-dimensional algebra over a field F.*

- *The algebra A is a finite product of local algebras over F, i.e. $A \cong A_1 \times \cdots \times A_k$ where each A_i has a unique maximal ideal.*
- *Assume that A is local. Let $n = \dim_F A$. Then the residue field E of A is an extension of F of degree $\leq n$. Furthermore, an element $x \in A$ is in the maximal ideal if and only if $x^n = 0$.*

Proof. Since A is finite-dimensional over F, it is an Artinian ring. The first part is now a standard fact from commutative algebra, see e.g. [AM65, Theorem 8.6].

For the second point, let $\mathfrak{m}$ be the maximal ideal. Clearly $[E\colon F] = \dim_F(A/\mathfrak{m}) \leq \dim_F A = n$. For any natural number m, if $\mathfrak{m}^m \neq 0$, then $\mathfrak{m}^{m+1} \subsetneq \mathfrak{m}^m$ by Nakayama's Lemma. Since $n = \dim_F A$, it follows that $\mathfrak{m}^n = 0$. □

Proof of Lemma 2.1.3. The first statement follows from the second by setting $A = F[X]/(f)$, so assume we are in the situation of the second statement.

By Lemma 2.1.4, A is a product of local algebras $A \cong A_1 \times \cdots \times A_k$. Since φ is preserved under homomorphisms and products of structures as a positive primitive sentence, it suffices to see that $A_i \models \varphi$ if and only if $A_i/\mathfrak{m} \models \varphi$ for every A_i, where $\mathfrak{m}$ is the unique maximal ideal of A_i.

The residue field $A_i/\mathfrak{m}$ is a finite separable extension of F and therefore generated by a single separable element. The ideal $\mathfrak{m}$ is nilpotent, and therefore A_i is complete with respect to $\mathfrak{m}$; hence Hensel's Lemma in the version for complete rings, applied to the minimal polynomial of a primitive element of $A_i/\mathfrak{m}$ over F, gives an embedding of $A_i/\mathfrak{m}$ into A_i, so we have maps $A_i/\mathfrak{m} \to A_i \to A_i/\mathfrak{m}$. Since φ is preserved under homomorphisms, this proves that $A_i \models \varphi$ if and only if $A_i/\mathfrak{m} \models \varphi$. □

On the other hand, if F is not perfect, then this simplification does not work: Consider imperfect F of characteristic p and let $t \in F \setminus F^p$. Then one easily verifies that $F[X]/((X^p - t)^2)$ does not satisfy the sentence $\varphi = \exists x(x^p = t)$, even though $F[X]/(X^p - t)$ does.

For us, the usefulness of this method for definability is in situations where we can firstly understand the satisfaction of φ explicitly in a nice

class of fields—usually some henselian valued fields—, and secondly where we have a local-global principle for the sentence φ, which allows us to understand φ in a given field by passing to henselian extensions.

2.2 SPLITTING CENTRAL SIMPLE ALGEBRAS

Fix an arbitrary field F and a natural number l. Let A/F be a central simple algebra of degree l; by definition, this is a (usually non-commutative) associative unital algebra over F such that the base change $A \otimes_F \overline{F}$ to the algebraic closure $\overline{F}$ is isomorphic over $\overline{F}$ to the matrix algebra $M_{l\times l}(\overline{F})$. This is a well-studied class of algebras; our main reference is [GS17].

For a field extension E/F, we may ask whether A *splits* over E; i.e. whether $A \otimes_F E$ is isomorphic over E to the matrix algebra $M_{l\times l}(E)$.

Lemma 2.2.1. *Let $a^1_{1,1}, \dots, a^{l^2}_{l^2,l^2}$ be structure constants of A/F, i.e. there exists a F-vector space basis $X_1, \dots, X_{l^2}$ of A such that $X_i \cdot X_j = \sum_k a^k_{ij} X_k$.*

There is a positive primitive formula $\varphi(x^1_{1,1}, \dots, x^{l^2}_{l^2,l^2})$ in the language of rings such that for any field extension E/F, $E \models \varphi(a^1_{1,1}, \dots, a^{l^2}_{l^2,l^2})$ if and only if A splits over E.

Proof. The $a^k_{i,j}$ are also structure constants of $A \otimes_F E/E$. This central simple algebra is isomorphic to $M_{l\times l}(E)$ if and only if there exists a base change matrix $P \in \mathrm{GL}_{l^2}(E)$ under which the structure constants become those of the standard basis of $M_{l\times l}$. This is a positive primitive statement. □

Hence the following definition is an instance of the general situation considered above.

Definition 2.2.2. *Let $f \in F[X]$ be monic of degree l. We say that f splits A if for every irreducible factor $g \mid f$, the field $F[X]/(g)$ splits A.*

Now write f as $X^l + a_{l-1}X^{l-1} + \cdots + a_0$. We define

$$S(A/F) = \{a \in K\colon \text{there exists } f \text{ of degree } l \text{ splitting } A \text{ with } a_{l-1} = -a \text{ and } a_0 = (-1)^l\}.$$

Our definition of $S(A/F)$ does *not* agree with the one in [Dit18] or in the previous literature (which only covers the case $l = 2$); however, the change is a rather simple one. The definition given in [Dit18] is

$$S'(A/F) = \{\mathrm{Trd}_{A/F}(x)\colon x \in A, \mathrm{Nrd}_{A/F}(x) = 1\},$$

where Trd and Nrd are the reduced trace and norm, respectively: That is, Trd and Nrd are induced from trace and determinant on $A \otimes_F \overline{F} \cong M_{l\times l}$, see [GS17, Section 2.6].

Proposition 2.2.3. *Assume l is prime. Then*

$$S'(A/F) = S(A/F) \cup \{l\zeta_l\colon \zeta_l^l = 1\}.$$

The proof uses several results from the theory of central simple algebras; since we do not use S' in further constructions, it may be skipped by the reader.

Lemma 2.2.4 ([Jac09, Theorem 4.12])**.** *Let D be a central division algebra of degree n over a field F, and let F' be a field of degree n over F. Then F' splits D if and only if F' can be embedded into D over F, i.e. if and only if there is a subalgebra of D isomorphic to F' over F.*

Lemma 2.2.5 ([GS17, Proposition 2.6.3]). *Let A/F be a central simple algebra of degree n and $x \in A$. If $F' \subseteq A$ is commutative subalgebra which contains x and is a degree n field extension of F, then $\mathrm{Nrd}_{A/F}(x) = \mathrm{N}_{F'/F}(x)$ and $\mathrm{Trd}_{A/F}(x) = \mathrm{Tr}_{F'/F}(x)$., where $\mathrm{N}_{F'/F}$ and $\mathrm{Tr}_{F'/F}$ denote field norm and trace, respectively.*

Proof of Proposition 2.2.3. Since l is prime, A is either a division algebra or isomorphic to the matrix algebra $M_{l\times l}(F)$ by Wedderburn's Theorem. If A is a matrix algebra, then $S(A/F) = F$ by definition and $S'(A/F) = F$ since there are matrices with arbitrary given determinant and trace, so there is nothing to show. Hence assume that A is a division algebra.

To show the inclusion $\subseteq$, let $a \in S'(A/F)$, so there is $x \in A$ with $\mathrm{Nrd}_{A/F}(x) = 1$, $\mathrm{Trd}_{A/F}(x) = a$. If x is in the centre F of A, then $1 = \mathrm{Nrd}_{A/F}(x) = x^l$ and $a = \mathrm{Trd}_{A/F}(x) = lx$, so a is an l-fold multiple of an l-th root of unity.

Otherwise consider the subalgebra $F[x]$ of A generated by x and F; it is a commutative division algebra, i.e. a field. Since $l^2 = \dim_F A = \dim_F(F[x]) \cdot \dim_{F[x]} A$, where we consider A as an $F[x]$-vector space via left multiplication, we must have $\dim_F F[x] = l$ since l is prime. Now the field $F[x]$ splits A by Lemma 2.2.4, and $F[x]$ is naturally isomorphic to $F[X]/(f)$ where $f \in F[X]$ is the minimal polynomial of x. But $\mathrm{N}_{F[x]/F}(x) = 1$ and $\mathrm{Tr}_{F[x]/F}(x) = a$ by Lemma 2.2.5, determining the X^{l-1}-coefficient and the constant coefficient of f, proving that $a \in S(A/F)$.

For the inclusion $\supseteq$, let first $\zeta_l \in F$ be an l-th root of unity. Then the element $\zeta_l \cdot 1 \in A$ has reduced norm $\zeta_l^l = 1$ and reduced trace $l\zeta_l$,

proving $l\zeta_l \in S'(A/F)$. It remains to show $S(A/F) \subseteq S'(A/F)$, so let $f = X^l + a_{l-1}X^{l-1} + \cdots a_0 \in F[X]$ be a monic polynomial of degree l which splits A, with $a_0 = (-1)^l$. We have to show $-a_{l-1} \in S'(A/F)$. Since a field extension E/F splitting A must be of degree a multiple of l by [GS17, second part of Corollary 4.5.4], f must be irreducible. Now the field $F[X]/(f)$ embeds into A by Lemma 2.2.5; fix such an embedding. Write $x \in A$ for the image of X under the composite map $F[X] \to F[X]/(f) \hookrightarrow A$. By Lemma 2.2.5, we have $\mathrm{Nrd}_{A/F}(x) = (-1)^l a_0 = 1$ and $\mathrm{Trd}_{A/F}(x) = -a_{l-1}$. Hence $-a_{l-1} \in S'(A/K)$, which was the claim. □

In what is to follow, the possible difference between S and S' will never matter for the statements of results; however, S is more amenable to generalisations and makes some proofs simpler. (For instance, S is always topologically open when F is a local field, while this is not the case for S'.)

Lemma 2.2.6. *Assume that A/F is non-split of prime degree l. Then any monic $f \in F[X]$ of degree l which splits A must be irreducible.*

Proof. Since A is non-split of prime degree, it must be a division algebra by Wedderburn's Theorem. Any finite field extension E/F which splits A must be of degree a multiple of l. Since f splits A, it must have precisely one irreducible factor, namely itself. □

2.2.1 *Over local fields*

Let F be a non-archimedean local field throughout this subsection, i.e. a complete valued field with finite residue field and value group $\mathbb{Z}$. (In

fact, all results remain true if we replace the assumption of completeness by henselianity.) Here we characterise $S(A/F)$.

Lemma 2.2.7. *Let E be an henselian field and $f \in E[X]$ be a monic irreducible polynomial. If the constant coefficient of f is in the valuation ring of E, then so are all others.*

Proof. This is the Hensel–Kürschák Lemma, one of the equivalent conditions for henselianity. □

For a finite field $\mathbb{F}$, define

$$U_l(\mathbb{F}) = \{a \in \mathbb{F} : \text{there exists irreducible } f = X^l + a_{l-1}X^{l-1} + \cdots + a_0 \text{ with } a_0 = (-1)^l, a_{l-1} = -a\}.$$

Lemma 2.2.8. *Let A/F be a central simple algebra of prime degree l.*

1. *If A is split, then $S(A/F) = F$.*
2. *Every irreducible monic polynomial $f = X^l + a_{l-1}X^{l-1} + \cdots + a_0$ splits A; in particular, if f is irreducible with constant coefficient $a_0 = (-1)^l$ we have $-a_{l-1} \in S(A/F)$.*
3. *$S(A/F)$ is topologically open.*
4. *If A is a division algebra, then*

$$\mathcal{O} \supseteq S'(A/F) \supseteq S(A/F) \supseteq \mathrm{res}^{-1}(U_l(\mathbb{F})),$$

where $\mathcal{O}$ is the valuation ring, $\mathbb{F}$ is the residue field, and $\mathrm{res}\colon \mathcal{O} \to \mathbb{F}$ is the residue map.

Proof. The first point is clear, since every extension field of F splits A.

The second point is the statement that every field extension $F[X]/(f)$ of degree l splits A. This is a fact from the theory of central simple algebras over local fields, see e.g. [NSW08, Corollary 7.1.4].

For the third point, we only have to consider the situation where A is non-split over F. Then the monic polynomials f of degree l which split A are precisely the irreducible ones, by the previous point and Lemma 2.2.6. If such f has constant coefficient $(-1)^l$, then f must be separable. But then any small perturbation of the coefficients of f still yields an irreducible separable polynomial by Krasner's Lemma. This means that $S(A/F)$ must be open.

For the fourth point, recall that any lift of an irreducible polynomial in $\mathbb{F}[X]$ to a monic polynomial in $\mathcal{O}[X]$ is itself irreducible by Gauß' Lemma. This proves $\mathrm{res}^{-1}(U_l(\mathbb{F})) \subseteq S(A/F)$ by the previous point. The statement $S(A/F) \subseteq \mathcal{O}$ follows from Lemma 2.2.6 and the fact that any irreducible monic polynomial in $F[X]$ with constant coefficient ± 1 must be in $\mathcal{O}[X]$ by Lemma 2.2.7. Since $S'(A/F) \setminus S(A/F)$ consists of elements integral over the prime ring by Proposition 2.2.3, this proves the claim. □

We can now determine $S(A/F)$ to a sufficient extent.

Proposition 2.2.9. *Let A/F be a central division algebra of prime degree l.*

1. *If $l > 2$, then $S(A/F)$ is equal to the valuation ring $\mathcal{O}$ of F.*
2. *If $l = 2$, then we have $S(A/F) - S(A/F) = \mathcal{O}$, i.e. every element of the valuation ring is the difference of two elements in $S(A/F)$.*

For the proof of the first point it suffices to prove the following lemma:

Lemma 2.2.10. *For $l > 2$ and an arbitrary finite field $\mathbb{F}$, we have $U_l(\mathbb{F}) = \mathbb{F}$.*

Proof. We have to show that for any given $a \in \mathbb{F}$ there exists a monic irreducible polynomial $f \in \mathbb{F}[X]$ of degree l with X^{l-1}-coefficient $-a$ and constant coefficient -1. Let us write q for the cardinality of $\mathbb{F}$. If $l > 5$, or $l = 5$ and $q > 9$, the result follows from Theorem 2.2.11 below. The remaining cases for $l = 5$ one may check by hand.

It remains to consider the case $l = 3$. If a polynomial $f_b = X^3 - aX^2 + bX - 1$ is not irreducible, it must be divisible by $X - c$ for some $c \in \mathbb{F}^\times$. However, for each c there exists exactly one f_b divisible by $X - c$. By counting, there exists an f_b which is not divisible by any $X - c$ and hence irreducible. □

Theorem 2.2.11. *Let $\mathbb{F}$ be a finite field of cardinality q and $n > 0$.*

1. *If $n \geq 5$ and $q > \left(\frac{n+1}{2}\right)^2$, there exists a monic irreducible polynomial of degree n over $\mathbb{F}$ with any given non-zero constant coefficient and given X^{n-1}-coefficient.*

2. *If $n \geq 6$, the same is true without assumption on q.*

Proof. These results follow from Corollaries 2.2 and 2.3 of [Coh05]. □

Proof of Proposition 2.2.9. For $l > 2$, the claim follows from the fourth part of Lemma 2.2.8 and Lemma 2.2.10, so let us consider $l = 2$. Write $\mathbb{F}$ for the residue field of F and pick a uniformiser π.

The polynomial $f = X^2 - (2 + \pi)X + 1$ is irreducible, since $f(X + 1) = X^2 - \pi X - \pi$ is irreducible by Eisenstein's criterion, and likewise

$f(-X) = X^2 + (2+\pi)X + 1$ is irreducible. Hence, by the second point of Lemma 2.2.8, we have $2+\pi, -2-\pi \in S(A/F)$. Furthermore, we also have $S(A/F) \supseteq \mathrm{res}^{-1}(U_2(\mathbb{F}))$ by Lemma 2.2.8.

We want to argue that $(U_2(\mathbb{F}) \cup \{2,-2\}) - U_2(\mathbb{F}) = \mathbb{F}$. To see this, observe first that every element of $\mathbb{F}^\times$ is a zero of precisely one polynomial of the form $X^2 - aX + 1$. This gives a surjective mapping from $\mathbb{F}^\times$ to reducible polynomials of this form, which is two-to-one apart from the inseparable polynomials $X^2 \pm 2X + 1$, which coincide in characteristic 2. Hence we have $\left\lfloor \frac{|\mathbb{F}|+1}{2} \right\rfloor$ reducible polynomials of this form, leaving $\left\lfloor \frac{|\mathbb{F}|}{2} \right\rfloor$ irreducible ones. Thus $|U_2(\mathbb{F})| = \left\lfloor \frac{|\mathbb{F}|}{2} \right\rfloor$.

Now $(U_2(\mathbb{F}) \cup \{2,-2\}) - U_2(\mathbb{F}) = \mathbb{F}$ is clear, since for any $x \in \mathbb{F}$ the intersection of $U_2(\mathbb{F}) \cup \{2,-2\}$ and $U_2(\mathbb{F}) + x$ cannot be empty for cardinality reasons.[2]

Hence any element in $\mathcal{O}$ can be written as the difference of an element of $\mathrm{res}^{-1}(U_2(\mathbb{F})) \cup \{2+\pi, -2-\pi\}$ and an element of $\mathrm{res}^{-1}(U_2(\mathbb{F}))$, so $\mathcal{O}$ is contained in $S(A/F) - S(A/F)$. Since $S(A/F) \subseteq \mathcal{O}$, we have equality. □

This proof is adapted from the proof of Proposition 2.3 in [Par13], but replacing the element 2 used there by $2+\pi$. (The use of 2 in [Par13] is an error, since 2 is in $S'(A/F)$ but not in the interior thereof, which interferes with the use of approximation theorems in the same proposition.)

[2] I would like to thank Nicolas Daans for pointing out this combinatorial argument to me, using the explicit calculation of the cardinality of $U_2(\mathbb{F})$. This differs from the previously published version in [Dit18, Proposition 2.6], where a more complicated algebro-geometric argument from [Poo09] was used, together with an exhaustive search for small fields.

We also state a result for the local field $\mathbb{R}$. (Since all central simple algebras over $\mathbb{C}$ are split, there is nothing to do for that case.)

Proposition 2.2.12. *Let $A/\mathbb{R}$ be a central simple algebra of prime degree l. If A is non-split, then $l = 2$ and $S(A/\mathbb{R}) =]-2, 2[$. Otherwise $S(A/\mathbb{R}) = \mathbb{R}$. In particular, $S(A/\mathbb{R})$ is always topologically open.*

Proof. If $l > 2$, then A must be split; otherwise, it would have to be a division algebra by Wedderburn's Theorem, but then any element of A not in $\mathbb{R}$ would generate a subalgebra of A which would have to be a field extension of $\mathbb{R}$ of degree l, which is impossible.

Therefore $l = 2$ in the non-split case. (In fact, A is necessarily isomorphic to Hamilton's quaternions.)

A polynomial $X^2 - aX + 1 \in \mathbb{R}[X]$ is irreducible if and only if $a \in]-2, 2[$, and precisely in this case does it generate the extension field $\mathbb{C}/\mathbb{R}$ and therefore split A. □

2.2.2 *Over global fields*

Now let K be a global field, i.e. either a number field (a finite extension of $\mathbb{Q}$) or a global function field (a finite extension of $\mathbb{F}_p(T)$ for some prime number p). Let A/K be a central simple algebra of prime degree l. Recall that a *place* v of K is an equivalence class of absolute values $K \to \mathbb{R}$. We write K_v for the completion of K with respect to v, which is a local field. (This notation follows standard practice in number theory, but unfortunately clashes with our later use of K_v to denote the henselisation of K with respect to a valuation v. However, because in our situation the

differences between henselian and complete fields are minor—explained in characteristic 0 by Ax–Kochen–Ershov principles—, this is unlikely to cause problems.)

Proposition 2.2.13.

$$S(A/K) = \bigcap_v (S(A \otimes_K K_v / K_v) \cap K),$$

where the intersection is over all places v of K.

For the proof we need the following fact: A central simple algebra over a global field splits over all but finitely many completions, and if it splits over all completions then it is already split. This will be restated below in a different language, with references, as Theorem 2.3.2.

Proof. Since S is defined by an existential formula, the inclusion $\subseteq$ is automatic.

To show the other inclusion, we may assume that A/K is non-split, since otherwise both sides of the equation are equal to K. List the finitely many places $v_1, \ldots, v_n$ of K such that A is not split by the corresponding completion. Let $a \in S(A \otimes_K K_{v_i}/K_{v_i})$ for all i. Then there exist irreducible polynomials $f_i \in K_{v_i}[X]$, monic and of degree l, with constant coefficient $(-1)^l$ and the coefficient of X^{l-1} equal to $-a$, which split $A \otimes_K K_{v_i}$. By weak approximation, we find $f \in K[X]$, monic of degree l, again with constant coefficient $(-1)^l$ and X^{l-1}-coefficient $-a$, which is v_i-adically arbitrarily close to f_i, for all i simultaneously. By approximating closely enough, we obtain $K_{v_i}[X]/(f) \cong K_{v_i}[X]/(f_i)$ by Krasner's Lemma, in particular f is irreducible over K, and $K[X]/(f)$ splits A since all its completions split A. This proves $a \in S(A/K)$. □

Definition 2.2.14. *For a field F and a central simple algebra A/F of prime degree l, we define $T(A/F) = S(A/F)$ if $l > 2$, and $T(A/F) = S(A/F) - S(A/F)$ if $l = 2$, i.e. the set of pairwise differences of elements of $S(A/F)$.*

Since $S(A/F)$ is positively existentially definable in terms of structure constants of A, the same holds for $T(A/F)$.

For notational simplicity, if A is a central simple algebra defined over a subfield $F_0 \subseteq F$, we will occasionally write $T(A/F)$ for $T(A \otimes_{F_0} F/F)$.

We return to the situation of a global field K.

Theorem 2.2.15. *Write $\Delta(A/K)$ for the finite set of places of K such that A does not split over the corresponding completion. Then*

$$T(A/K) = \bigcap_{v \in \Delta(A/K)} (\mathcal{O}_v \cap K),$$

where for a real place $v \in \Delta(A/K)$ we set $\mathcal{O}_v = \{x \in K_v \colon -4 < x < 4\}$, $<$ being the unique field ordering on $K_v \cong \mathbb{R}$.

Proof. This is a combination of the local-global principle in Proposition 2.2.13 and the local computation in Propositions 2.2.9 and 2.2.12. For $l > 2$ the statement is immediately implied by the propositions since $T(A/K) = S(A/K)$. For $l = 2$, we additionally recall that $S(A \otimes K_v/K_v)$ is v-adically open for all places v, and equal to K_v for all $v \notin \Delta(A/K)$. Hence weak approximation implies that

$$S(A/K) - S(A/K) = \bigcap_v \big(S(A \otimes_K K_v/K_v) - S(A \otimes_K K_v/K_v)\big),$$

which gives the result. □

If $\Delta(A/K)$ does not contain any real places, we see that we obtain the same set for $T(A/K)$ if we use $S'(A/K)$ in the definition instead of $S(A/K)$. (If we do consider real places, we get a genuine difference—for $A/\mathbb{R}$ non-split, we have $S(A/\mathbb{R}) =]-2,2[$ and $S'(A/\mathbb{R}) = [-2,2]$—, but this situation has previously always been avoided in the literature.)

Theorem 2.2.15 can be strengthened to the situation of infinite algebraic extensions of global fields.

Theorem 2.2.16. *Let K be an algebraic extension of a global field, i.e. either a field algebraic over $\mathbb{Q}$ or a field of transcendence degree 1 over a finite field.*

Then we still have

$$T(A/K) = \bigcap_{v \in \Delta(A/K)} (\mathcal{O}_v \cap K).$$

Here $\mathcal{O}_v$, in the non-archimedean case, is the valuation ring of K_v, which according with standard practice in algebraic number theory we take to be the direct limit of the completions $K'_{v'}$, where K' runs over the global fields contained in K and v' is the place of K' below v. This means that K_v is not usually complete, merely henselian.

No such issue arises for real places, where K embeds into the completion $\mathbb{Q}_{\leq} = \mathbb{R}$ and we may simply take $K_v = \mathbb{R}$.

Proof. Let $K_0 \subseteq K$ be a global field over which A is defined, i.e. such that there exists a central simple algebra A_0/K_0 such that $A \cong A_0 \otimes_{K_0} K$. (Such K_0 exists because the structure constants of A with respect to any basis lie in a finitely generated subfield of K.)

The inclusion of the left-hand side in the right-hand side is clear, since for any $x \in T(A/K)$ there exists a global field $L \subseteq K$ containing x and

K_0 such that $x \in T(A_0/L)$ (because T is existentially definable), and

$$T(A_0/L) \subseteq \bigcap_{v \in \Delta(A_0/L)} (\mathcal{O}_v \cap L) \subseteq \bigcap_{v \in \Delta(A/K)} (\mathcal{O}_v \cap L).$$

For the other inclusion, let $x \in K$ be contained in the right-hand side. For every global field $L \subseteq K$ containing x and K_0, write Δ'_L for the set of places v of L contained in $\Delta(A/L)$ such that $x \notin \mathcal{O}_v$. For $L' \supseteq L$ we have a restriction map $\Delta'_{L'} \to \Delta'_L$, assigning to a place of L' its restriction to L.

Write K as the union of a chain $K_0 = L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots$, so we obtain maps

$$\cdots \to \Delta'_{L_2} \to \Delta'_{L_1} \to \Delta'_{L_0}.$$

Now a sequence of places $(v_i)_{i \in \mathbb{N}}$, where $v_i \in \Delta'_{L_i}$ and v_i is the restriction of v_{i+1}, induces a place v of K such that $x \notin \mathcal{O}_v$ and A does not split over K_v.

By assumption, such a place of K does not exist; this means that some Δ'_{L_n} must be empty, since due to finiteness of each Δ'_{L_i} we could otherwise pick an infinite compatible sequence by Kőnig's Lemma.

Δ'_{L_n} being empty means precisely that

$$x \in \bigcap_{v \in \Delta(A/L_n)} (\mathcal{O}_v \cap L_n) = T(A/L_n) \subseteq T(A/L),$$

which finishes the proof. □

2.3 THE BRAUER GROUP

It is helpful to collect all central simple algebras over a given field in one structure; this is accomplished by the Brauer group.

Definition 2.3.1. *Let F be a field. Two central simple algebras $A, B/F$ are* Brauer equivalent *if $A \otimes_F M_{n\times n}(F) \cong B \otimes_F M_{m\times m}(F)$ for some positive integers n and m.*

Write $Br(F)$ for the collection of all Brauer equivalence classes of central simple algebras over F. This is a group—the Brauer group*—under the operation induced on the equivalence classes by the tensor product of central simple algebras.*

If F'/F is any field extension, then mapping a central simple algebra A/F to $A \otimes_F F'/F$ induces a group homomorphism $\mathrm{Br}(F) \to \mathrm{Br}(F')$, known as the restriction.

We turn our attention to the Brauer group of global fields. We have previously used the Hasse–Brauer–Noether Theorem, which states that a central simple algebra over a global field is split if and only if it is split over all completions. This statement is refined by the following.

Theorem 2.3.2 ([NSW08, Theorem 8.1.17], [GS17, Corollary 6.5.3])**.** *Let K be a global field. There is an exact sequence*

$$0 \to \mathrm{Br}(K) \to \oplus_v \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0,$$

where the direct sum is over all places of K, the left-hand map is given by the sum of the restriction maps $\mathrm{Br}(K) \to \mathrm{Br}(K_v)$, and the right-hand map is given by the sum of injective local Hasse invariant *maps $\mathrm{inv}_v \colon K_v \to \mathbb{Q}/\mathbb{Z}$, which are bijective for finite places v, have image $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ for real places v, and zero image for complex v.*

This also may be used to prove the following remarkable fact.

Theorem 2.3.3. *Let K be a global field. Any Brauer class of order n in* $\mathrm{Br}(K)$ *is represented by a central simple algebra of degree n.*

Proof. We may even arrange for the central simple algebra to be cyclic in the sense of the next subsection: this is a consequence of the local–global principle derived by Hasse, Brauer and Noether. See [GS17, Remarks 6.5.4, 6.5.5] (without proofs) or [Roq05] (for a detailed historical account). □

This allows us to deduce the following lemmas to be used later.

Lemma 2.3.4. *Let l be a prime number and Δ a set of places of a global field K. Then there exists a central simple algebra A/K of degree l with $\Delta(A/K) = \Delta$ if and only if the following conditions are satisfied:*

1. *Δ is finite;*
2. *Δ is either empty or contains at least two elements;*
3. *Δ contains no complex places;*
4. *Δ contains no real places if l is odd;*
5. *if $l = 2$, then the number of elements of Δ is even.*

Proof. This follows without difficulty from the preceding theorems. □

Lemma 2.3.5. *Let L be an algebraic extension of a global field and l a prime number. Then any l-torsion element of* $\mathrm{Br}(L)$ *is represented by a non-split central simple algebra over L of degree l.*

Proof. Any l-torsion element of $\mathrm{Br}(L)$ is by definition represented by a non-split central simple algebra A/L such that $A^{\otimes l}$ splits; we need to show that A is Brauer equivalent to a central simple algebra of degree l.

Let $K \subseteq L$ be a global field over which A is defined, i.e. such that there exists a central simple algebra A_0/K with $A_0 \otimes_K L \cong A$. Enlarging K if necessary, we may ensure that $A_0^{\otimes l}$ splits over K. By Theorem 2.3.3, there exists a central simple algebra B_0/K of degree l which is Brauer equivalent to A_0. Then $B := B_0 \otimes_K L$ is a central simple algebra over L as desired. □

We recover existential definability of valuation rings in K, known since [Shl94, Theorem 4.4].

Corollary 2.3.6. *For any finite place $\mathfrak{p}$ of a global field K, the ring $\mathcal{O}_\mathfrak{p} \cap K$ is positively existentially definable with parameters in K.*

Proof. Take a prime number l, e.g. $l = 2$, and pick two central simple algebras $A, A'/K$ of degree l splitting at all real places of K and such that $\Delta_{A/K} \cap \Delta_{A'/K} = \{\mathfrak{p}\}$; this is possible by Lemma 2.3.4. Then $T(A/K) + T(A'/K) = \mathcal{O}_\mathfrak{p} \cap K$, and this is positively existentially definable in K with parameters. □

This proof is essentially given in [Poo09, Remark 2.6].

We also obtain a uniform definition of rings of integers in a large class of algebraic extensions of global fields, in the style of the definition given in [Poo09].

Theorem 2.3.7. *Let l be a prime number, K a number field and L/K a Galois extension such l that does not divide the supernatural number $[L\colon K]$. If $l = 2$, assume that L has no field orderings. Then we have*

$$\mathcal{O}_L = \bigcap_A T(A/L),$$

where the left-hand side is the integral closure of $\mathbb{Z}$ inside L and the intersection on the right-hand side is over all central simple algebras of degree l over L.

In particular, $\mathcal{O}_L$ is uniformly $\forall\exists$-$\emptyset$-definable in such fields L.

This is a generalisation of the main definability result of [Vid00]—which was obtained using Rumely's method for defining rings of integers of number fields—with improved quantifier complexity.

Proof. By Theorem 2.2.16, it suffices to show that for every place w of L there exists a central simple algebra A/L of degree l which is not split over L_w. Write v for the place of K below w. Then $[L_w\colon K_v]$ divides $[L\colon K]$ and is hence not a multiple of l. Therefore any non-split central simple algebra A/K_v of degree l remains non-split over L_w by [GS17, Corollary 4.5.4].

To prove that this gives a uniform $\forall\exists$-$\emptyset$-definition, it suffices to see that the set of tuples $(a_{ij}^k)_{1\leq i,j,k\leq k}$ which are structure constants of some central simple algebra over L is quantifier-freely definable. This follows from the definition of central simple algebras and quantifier elimination over algebraically closed fields. □

2.3.1 Cyclic algebras

We have so far not given a way of explicitly constructing central simple algebras of arbitrary degree.

Definition 2.3.8. *Let F be a field, M/F a cyclic extension of degree n and σ a generator of* $\mathrm{Gal}(M/F)$. *Then for $b \in F^\times$ the* cyclic algebra (M, σ, b) *is the associative F-algebra generated by M and an element y subject to the relations $y^n = b$, $xy = y\sigma(x)$ for all $x \in M$.*

The algebra (M, σ, b) is a central simple algebra of degree n. (See [GS17, Proposition 2.5.2])

We can determine whether a cyclic algebra splits by the following basic result.

Proposition 2.3.9 ([GS17, Corollary 4.7.5])**.** *The algebra (M, σ, b) is split if and only if b is a norm from the extension M/F.*

Observation 2.3.10. Given a K-basis $x_0, \ldots, x_{n-1}$ of M, a K-basis for the cyclic algebra (M, σ, b) is given by the elements $y^i x_j$, where y is the distinguished generator for (M, σ, b) and $0 \leq i, j < l$.

We verify that we may write structure constants of (M, σ, b) with respect to this basis as polynomial expressions in b. In any extension field L/K, these structure constants become those of the algebra $(M, \sigma, b) \otimes_K L$.

In particular, there is a positive existential formula with parameters in K and free variable b which in any L/K defines the set $T((M, \sigma, b) \otimes_K L)$.

COHOMOLOGICAL SPLITTING SETS

3.1 COHOMOLOGY AND MILNOR K-THEORY

In this chapter, we assume that the reader is familiar with the basic definitions of Galois cohomology, as given e.g. in [NSW08] or [GS17, Chapter 3].

There is a well-known interpretation of the Brauer group through Galois cohomology. Namely, if F is a field and n a natural number coprime to the characteristic of F, then $\mathrm{Br}(F)[n]$ is canonically isomorphic to $H^2(F, \mu_n)$, and this isomorphism is compatible with restriction maps for overfields E/F, i.e. the maps $\mathrm{Br}(F)[n] \to \mathrm{Br}(E)[n] \to H^2(E, \mu_n)$ and $\mathrm{Br}(F)[n] \to H^2(E, \mu_n) \to H^2(E, \mu_n)$ are the same.

One could now make a general definition of splitting sets for arbitrary cohomology classes, by defining that a monic polynomial $f \in F[X]$ splits an arbitrary cohomology class $\alpha \in H^n(F, A)$, where A is a (finite) Galois-module, if and only if the restriction of α vanishes in all residue fields of $F[X]/(f)$. This is attractive because of the well-developed theory around Galois cohomology in many cases, including results on henselian valued fields as well as local–global principles.

However, one has to deal with the following issues.

- To make resulting splitting sets reflect first-order properties of the field, one needs to find a way to make "interesting" cohomology class visible in a first-order way. (E.g. we represented classes in the Brauer group, i.e. in $H^2(F, \mu_n)$, by structure constants for central simple algebras.)

- Once cohomology classes are represented by members of a definable set in F, it is necessary to find a first-order definition of the splitting condition, so that the condition $\mathrm{res}_{E/F}(\alpha) = 0$, where res is the cohomological restriction map, is defined by a first-order formula.

- Additional challenges arise over fields of positive characteristic. For instance, the p-torsion of the Brauer group of a field of characteristic $p > 0$ is not easily represented as Galois cohomology over a torsion Galois module, and further problems arise for restriction maps in inseparable extensions E/F.

In some useful cases, these difficulties are surmountable. Notably, we obtain first-order definable splitting sets for $H^n(F, \mathbb{Z}/2)$, where $n > 1$, $\operatorname{char} F \neq 2$; these will be used in Chapter 4 in the context of finitely generated fields, when the results from the previous chapter based on central simple algebras are not applicable due to failure of the relevant local–global principle.

Likewise, we will also indicate how the method applies to $H^3(F, \mathbb{Z}/n)$, where n is square-free and coprime to $\operatorname{char} F$ with F containing all n-th roots of unity, although we have no immediate application in mind.

The relevant background theory for both cases is Milnor K-theory, which we now describe; we roughly follow the exposition in [GS17, Section 4.6 and Chapter 7].

Definition 3.1.1. *Let F be a field and $n \geq 2$. The* n-th Milnor K-group *of F, denoted $K_n^M(F)$ and written additively, is the quotient of the n-fold tensor product of abelian groups $F^\times \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} F^\times$ by the subgroup generated by*

elements $a_1 \otimes \cdots \otimes a_n$ *with* $a_i + a_j = 1$ *for some* $i \neq j$. *We put* $K_0^M(F) = \mathbb{Z}$ *and* $K_1^M(F) = F^\times$. *We write* $\{a_1, \ldots, a_n\}$ *for the image of* $a_1 \otimes \cdots \otimes a_n$ *in* $K_n^M(F)$. *An element of the form* $\{a_1, \ldots, a_n\}$, *i.e. one induced by an elementary tensor, is called* pure symbol *or* symbol of length one.

The $K_n^M(F)$ naturally fit together in a graded ring $K^M(F)$, where multiplication is induced by the tensor product. Multiplication is written as $(\alpha, \beta) \mapsto \{\alpha, \beta\}$. If $E \supseteq F$ is an overfield, we have a natural map $K_n^M(F) \to K_n^M(E)$ induced by the inclusion, which is called *restriction*.

The crucial result connecting Milnor K-theory and cohomology is the following *Norm Residue Isomorphism Theorem*.

Theorem 3.1.2 ([Voe11]). *Let* F *be any field,* $n > 0$, *and* $m > 0$ *coprime to the characteristic of* F. *Then there is an isomorphism* $K_n^M(F)/m \to H^n(F, \mu_m^{\otimes n})$, *the* Galois symbol map, *determined by*

$$\{a_1, \ldots, a_n\} \mapsto (a_1) \cup \cdots \cup (a_n),$$

where (a_i) *is the element* $a_i {F^\times}^m \in F^\times / {F^\times}^m \cong H^1(F, \mu_m)$.

We do not need the full power of this theorem. Firstly, as mentioned above, our main application is with $m = 2$, in which case the theorem had been conjectured my Milnor and proven by Voevodsky in [Voe03]. Secondly, we will only require injectivity of the Galois symbol map on pure symbols; i.e. we need that $(a_1) \cup \cdots \cup (a_n) \in H^n(F, \mu_m^{\otimes n})$ vanishes if and only if $\{a_1, \ldots, a_n\}$ vanishes in $K_n^M(F)/m$.

3.2 splitting pfister forms

As mentioned before, the method developed in the last chapter was originally applied to quaternion algebras. One generalisation that we have seen in a previous section has been to Brauer group elements of different order, i.e. replacing $\mathrm{Br}(F)[2]$ by $\mathrm{Br}(F)[l]$ for a different prime number l. On the other hand, the norm forms of quaternion algebras are a kind of quadratic form—the quaternion algebra (a, b) has norm form $X^2 - aY^2 - bZ^2 + abW^2$, and the algebra splits if and only if the norm form has a non-trivial zero—and one can generalise to more general quadratic forms, namely Pfister forms. It turns out that the splitting of Pfister forms is related to the symbols of Milnor K-theory discussed in the previous section.

Throughout this section, F is a field of characteristic not 2. We follow the exposition given in [Pfi95]. Recall that a *quadratic form* or *quadratic map* on a finite-dimensional F-vector space V is a map $q\colon V \to F$ given by $q(v) = b(v, v)$, where $b\colon V \times V \to F$ is a bilinear form. Given elements $a_1, \ldots, a_n \in F$, there is a quadratic form $\langle a_1, \ldots, a_n \rangle\colon F^n \to F$ given by $(x_1, \ldots, x_n) \mapsto \sum_i a_i x_i^2$. Given two vector spaces V_1, V_2 with respective quadratic forms q_1 and q_2, the direct sum and tensor product $V_1 \oplus V_2$ and $V_1 \otimes V_2$ are naturally endowed with quadratic forms $q_1 \oplus q_2$ and $q_1 \otimes q_2$.

Definition 3.2.1. *Let $a_1, \ldots, a_n \in F^\times$. The* Pfister form $\langle\langle a_1, \ldots, a_n \rangle\rangle$ *is the 2^n-dimensional quadratic form*

$$\langle 1, -a_1 \rangle \otimes \cdots \otimes \langle 1, -a_n \rangle.$$

There are two different sign conventions in the literature; the alternative to ours replaces $\langle 1, -a_i \rangle$ by $\langle 1, a_i \rangle$.

Theorem 3.2.2. *Let $a_1, \ldots, a_n \in F^\times$ and write $q = \langle\langle a_1, \ldots, a_n \rangle\rangle$. The following are equivalent:*

- *q has a non-trivial zero over F;*
- *q is isomorphic to the form $\langle 1, -1 \rangle^{\otimes n}$ over F;*
- *the pure symbol $\{a_1, \ldots, a_n\}$ vanishes in $K_n^M(F)/2$;*
- *the cohomology class $(a_1) \cup \cdots \cup (a_n) \in H^n(F, \mathbb{Z}/2)$ vanishes.*

In this situation we will say that q, respectively the associated pure symbol mod 2, respectively the associated cohomology class, *split* in F.

Note that the second condition is expressible by a parameter-free positive primitive formula in the language of rings $\varphi(a_1, \ldots, a_n)$, as it asserts the existence of a base change matrix in $\mathrm{GL}_{2^n}(F)$ under which the matrix of q with respect to the standard basis of F^{2^n} transforms to the matrix of $\langle 1, -1 \rangle^{\otimes n}$.

Proof. The equivalence of the last two conditions follows from the Norm Residue Isomorphism Theorem; more specifically, it is one of the Milnor Conjectures from [Mil70], proved in [Voe03].

The equivalence of the third and the second condition was also conjectured in [Mil70], and proven in [OVV07].

The equivalence of the first two conditions is a classical result in the theory of Pfister forms, going back to [Pfi65, Theorem 2]. □

We can now make the following definition.

Definition 3.2.3. *Let $\gamma \in K_n^M(F)/2$ for some $n > 0$. A monic polynomial $f \in F[X]$* splits *γ if and only if for every irreducible $g \mid f$, the restriction of γ in $K_n^M(F[X]/(g))/2$ is zero.*

For $c \in F$, we define

$$S_c(\gamma) = \{t \in F \colon X^2 - tX + c \text{ splits } \gamma\}.$$

For a Pfister form $q = \langle\langle a_1, \ldots, a_n \rangle\rangle$, we let $S_c(q) = S_c(\gamma)$, where $\gamma = \{a_1, \ldots, a_n\} \in K_n^M(F)/2$ is the pure symbol corresponding to q.

One can show that the isomorphism class of a Pfister form q uniquely determines the element $\gamma \in K_n^M(F)/2$, irrespective of the coefficients a_i chosen to represent q, but we will not use this fact. The definition of $S_c(q)$ is related to the splitting sets from Proposition 2.1.2. The set $S_c(\langle\langle a_1, \ldots, a_n \rangle\rangle)$ is therefore existentially definable in terms of c and the a_i.

The use of Pfister forms here is exclusively a device to obtain first-order definability, and we will work with cohomology and Milnor K-groups in the remainder of this chapter. This is similar to the use of Pfister forms in [Pop02].

Another situation in which we have first-order definability concerns the group $K_3^M(F)/n$, where n is a square-free natural number with $\mu_n \subset F$. In this situation, given a pure symbol $\{a, b, c\}$ with $a, b, c \in F^\times$, we can consider the element $(a) \cup (b) \in H^2(F, \mathbb{Z}/n) \cong H^2(F, \mu_n) \cong \mathrm{Br}(F)[n]$. (Here one needs to choose an isomorphism $\mathbb{Z}/n \cong \mu_n$, but this shall not

concern us further.) This element of the Brauer group is in fact given by a cyclic central simple algebra A of degree n over F. By [GS17, Theorem 8.9.1], the element $\{a, b, c\}$ of $K_3^M(F)/n$ vanishes if and only if c is a reduced norm of the algebra A—an existentially definable condition. Hence Proposition 2.1.2 is available for associating an existentially definable set to a pure symbol.

We will not discuss this variant of the general method further due to lack of an application.

3.2.1 *Over henselian discretely valued fields*

In this section, we give some results on S_c for henselian discretely valued fields with value group of rank one.

Theorem 3.2.4. *Let (F, v) be henselian valued with value group $vF \cong \mathbb{Z}$, and $n > 0$. Then there is a* residue map $\partial = \partial_v \colon K_n^M(F) \to K_{n-1}^M(Fv)$, *where Fv is the residue field, satisfying the following properties:*

- *The map ∂ is the unique group homomorphism satisfying*

$$\partial(\{\pi, u_2, \dots, u_n\}) = \{\overline{u_2}, \dots, \overline{u_n}\}$$

  for all uniformisers $\pi \in F$ and units $u_2, \dots, u_n \in \mathcal{O}_v^\times$.

- *We have compatibility with field extensions in the following sense: Let F'/F be a finite extension and denote the unique extension of v to F' also by v. Then the following diagram commutes:*

$$\begin{array}{ccc} K_n^M(F) & \xrightarrow{\partial} & K_{n-1}^M(Fv) \\ \downarrow & & \downarrow e\cdot \\ K_n^M(F') & \xrightarrow{\partial} & K_{n-1}^M(F'v) \end{array}$$

Here the left vertical map is restriction, and the right vertical map is restriction followed by multiplication by the ramification index e of F'/F.

- *If $m > 0$ is coprime to $\mathrm{char}(Fv)$ or $\mathrm{char}(Fv) = 0$, i.e. if m is invertible in Fv, then the kernel of the induced map $K_n^M(F)/m \to K_{n-1}^M(Fv)/m$ is canonically isomorphic to $K_n^M(Fv)/m$.*

- *Let E be a field embedded into the valuation ring $\mathcal{O}_v$, so we have inclusions $E \subseteq F$ and $E \hookrightarrow Fv$. If p, q are positive natural numbers, then the following diagram commutes:*

$$\begin{array}{ccc} K_p^M(F) \otimes K_q^M(E) & \longrightarrow & K_{p+q}^M(F) \\ \downarrow & & \downarrow \\ K_{p-1}^M(Fv) \otimes K_q^M(E) & \longrightarrow & K_{p+q-1}^M(Fv) \end{array}$$

Here the vertical maps are given by ∂ (in different degrees) and the horizontal ones by the product in $K_\bullet^M$.

Proof. All of these points are standard. See [GS17, Proposition 7.1.4] for existence and uniqueness of ∂ satisfying the first point. Compatibility with finite field extensions is Remark 7.1.6.2 ibid. Isomorphism of the kernel of $K_n^M(F)/m \to K_{n-1}^M(Fv)/m$ to $K_n^M(Fv)/m$ follows from Corollary 7.1.10 ibid. (there stated only for complete valued fields (F, v), but inspection of the proof shows that only henselianity is needed).

Commutativity of the diagram in the last point is clear on pure symbols by the defining property of ∂ and then extends. □

The residue map is also known as the *tame symbol*. By the Norm Residue Isomorphism Theorem, it induces a map

$$\partial\colon H^n(F, \mu_m^{\otimes n}) \to H^{n-1}(Fv, \mu_m^{\otimes(n-1)})$$

when $m > 0$ is invertible in Fv. There is also a purely cohomological definition of this induced map ∂, see [GS17, Construction 6.8.5, Proposition 7.5.1].

From this construction we may also easily derive a tame symbol map $\partial_v \colon K_n^M(F) \to K_{n-1}^M(Fv)$ when (F, v) is a not necessarily henselian discretely valued field, by first using the restriction map $K_n^M(F) \to K_n^M(F_v)$, where F_v is the henselisation.

We will now take a closer look at the tame symbol map modulo 2, $\partial_v \colon K_n^M(F)/2 \to K_{n-1}^M(Fv)/2$. Above, its kernel was identified with the group $K_n^M(Fv)/2$, which is isomorphic to $H^n(Fv, \mathbb{Z}/2)$. In situations of interest, this kernel is often trivial since we can bound the 2-cohomological dimension of Fv by $n-1$: Recall that we write $\mathrm{cd}_2(Fv) < n$, where cd stands for *cohomological dimension*, if $H^m(Fv, A) = 0$ for all $m \geq n$ and all 2-torsion Galois modules A over Fv.

Proposition 3.2.5. *Let (F, v) be henselian with $vF \cong \mathbb{Z}$, $\operatorname{char} Fv \neq 2$ and $\mathrm{cd}_2 Fv < n$, and $c \in \mathcal{O}_v$. Let $a_1, \ldots, a_n \in F^\times$, $q = \langle\langle a_1, \ldots, a_n \rangle\rangle$ the corresponding Pfister form and $\gamma = (a_1) \cup \cdots \cup (a_n) \in H^n(F, \mathbb{Z}/2)$ the corresponding cohomology class. Then*

$$S_c(q) = S_c(\gamma) \supseteq \mathrm{res}^{-1}(S_{\bar{c}}(\partial\gamma).$$

If $\gamma \neq 0$, then $S_c(q) = S_c(\gamma) \subseteq \mathcal{O}_v$.

Proof. Under the assumption on the cohomological dimension of Fv, we have $K_n^M(Fv)/2 \cong H^n(Fv, \mu_2) = 0$ by the Norm Residue Isomorphism Theorem. Hence $\partial \colon K_n^M(F)/2 \to K_{n-1}^M(Fv)/2$ is injective by the third point of Theorem 3.2.4.

If $\gamma = 0$, then $S_c(\gamma) = F$ and $S_{\overline{c}}(\partial\gamma) = Fv$, so there is nothing to show; therefore assume $\gamma \neq 0$ and thus $\partial\gamma \neq 0$. Let $t \in \mathcal{O}_v$ such that $\overline{t} \in S_{\overline{c}}(\partial\gamma)$. Write $f = X^2 - tX + c \in F[X]$. Then the reduction $\overline{f} = X^2 - \overline{t}X + \overline{c} \in Fv[X]$ must split $\partial\gamma$ and is in particular irreducible. Therefore f is also irreducible and in the unramified extension $F' = F[X]/(f)$ the residue field $Fv[X]/(\overline{f})$ splits $\partial\gamma$, so by the compatibility of ∂ with field extensions as in the second point of Theorem 3.2.4 and injectivity of ∂, the restriction of γ to $H^n(F', \mathbb{Z}/2)$ vanishes as required.

Furthermore, if $t \in S_c(\gamma)$, then $f = X^2 - tX + c$ splits γ, so f is in particular irreducible with $v(c) \geq 0$, which forces $v(t) \geq 0$ by Lemma 2.2.7. □

3.2.2 *The local–global principle*

Recall that the *Kronecker dimension* of a field of positive characteristic is its transcendence degree over its prime field, while the Kronecker dimension of a field of characteristic zero is its transcendence degree over $\mathbb{Q}$ plus 1. It is easy to see that the Kronecker dimension of a field K is the maximal (archimedean) rank of (the value group of) any valuation on K.

The Kronecker dimension of a finitely generated field of positive characteristic is one less than its p-cohomological dimension for any prime number p not equal to the characteristic, and this is also true in characteristic zero as long as $p \neq 2$ or the field is not formally real. (This follows from [NSW08, Theorem 6.5.14].) In particular, if K has Kronecker dimension d, then $H^{d+2}(K, \mathbb{Z}/2) = 0$ unless K is a formally real field.

We will use the following cohomological local–global principle, which is a generalisation of the Hasse–Brauer–Noether Theorem to fields of Kronecker dimension greater than 1.

Theorem 3.2.6. *Let K be finitely generated of Kronecker dimension d. Let*

$$\tilde{H}^{d+1}(K, \mathbb{Z}/2) \subseteq H^{d+1}(K, \mathbb{Z}/2)$$

be the subset of elements splitting in all overfields of K embedding a real-closed field or a field with a henselian valuation of residue characteristic 2. Then the product of restriction maps

$$\tilde{H}^{d+1}(K, \mathbb{Z}/2) \to \prod_v H^{d+1}(K_v, \mathbb{Z}/2)$$

is injective, where the product is over all valuations of K with value group $\mathbb{Z}$ and residue characteristic not 2, and K_v is the henselisation of K with respect to v.

The proof is by reduction to the situation where K has a regular proper model over $\mathbb{Z}[\frac{1}{2}]$ or a finite field, in which case the theorem follows from a cohomological Hasse principle proven by Kerz and Saito. The reduction uses Gabber's variant of *alterations*, originally due to de Jong. This necessitates some use of the language of scheme-theoretic algebraic geometry.

We treat the cases of positive characteristic and characteristic zero separately, although the argument is very similar.

Theorem 3.2.7. *Let X be a proper smooth integral variety of dimension d over a finite field k of characteristic $\neq 2$. Then*

$$H^{d+1}(k(X), \mathbb{Z}/2) \to \bigoplus_{x \in X_{(d-1)}} H^d(x, \mathbb{Z}/2)$$

is injective, where $X_{(d-1)}$ is the set of generic points of codimension-1 subvarieties, and $H^d(x, \mathbb{Z}/2)$ is the cohomology of the residue field of x. Here the map is a direct sum of restriction maps $H^{d+1}(k(X), \mathbb{Z}/2) \to H^{d+1}(k(X)_x, \mathbb{Z}/2) \to H^d(x, \mathbb{Z}/2)$, where $k(X)_x$ is the henselisation of $k(X)$ along the discrete valuation associated to the divisor induced by x, and the maps are cohomological restriction and tame symbol, respectively.

Proof. After resolving notation, this follows from [KS12, Theorem 0.4]. □

For a prime number l, a morphism of noetherian schemes $X' \to X$ is an *l'-alteration* if it is proper, surjective, generically finite, sends generic points of irreducible components of X' to generic points of irreducible components of X (i.e. is *maximally dominating*), and the degree of the function field of an irreducible component of X' over the function field of the corresponding irreducible component of X is prime to l. (This definition can be found in [IT14, Section 2].)

Theorem 3.2.8 ([IT14, Theorem 2.1])**.** *Let k be a field, $l \neq \operatorname{char} k$ a prime number and X a separated and finite type k-scheme. Then there exists a finite extension k' of k, of degree prime to l, and a projective l'-alteration $\tilde{X} \to X$ above $\operatorname{Spec}(k') \to \operatorname{Spec}(k)$, with $\tilde{X}$ smooth and quasi-projective over k'.*

Proof of Theorem 3.2.6 in positive characteristic. Let $p = \operatorname{char} K > 0$. If $p = 2$ there is nothing to show, as K carries the trivial henselian valuation and hence $\tilde{H}^{d+1}(K, \mathbb{Z}/2) = 0$. Therefore assume $p \neq 2$.

The field K has a proper model over $\mathbb{F}_p$, i.e. a scheme X proper, integral and of finite type over $\mathbb{F}_p$ such that $K = \mathbb{F}_p(X)$; it is easy to construct

such X as a branched covering of $\mathbb{P}^d$, where d is the transcendence degree of K.

Find an alteration $\tilde{X} \to X$ of degree prime to 2 as in Theorem 3.2.8. The scheme $\tilde{X}$ is proper over X and therefore over $\mathbb{F}_p$, and smooth over $\mathbb{F}_p$ since it is smooth over a finite extension of $\mathbb{F}_p$ and $\mathbb{F}_p$ is perfect; in particular $\tilde{X}$ is reduced. By replacing $\tilde{X}$ with one of its connected components, we may assume $\tilde{X}$ is irreducible and hence integral. By construction, $\mathbb{F}_p(\tilde{X})$ is a finite extension of $\mathbb{F}_p(X)$ of degree prime to 2, hence $H^{d+1}(\mathbb{F}_p(X), \mathbb{Z}/2) \to H^{d+1}(\mathbb{F}_p(\tilde{X}), \mathbb{Z}/2)$ is injective by basic Galois cohomology. (Note that the field extension $\mathbb{F}_p(\tilde{X})/\mathbb{F}_p(X)$ may well fail to be separable, but this does not cause any issues.)

Now we can apply Theorem 3.2.7 to $\tilde{X}$ to obtain the result. □

Theorem 3.2.9. *Consider a regular integral scheme X proper and flat over* $\mathrm{Spec}(\mathbb{Z}[\frac{1}{2}])$ *with function field K, and write d for the absolute transcendence degree of K. Then*

$$H^{d+2}(K, \mathbb{Z}/2) \to \bigoplus_{x \in X_d} H^{d+1}(x, \mathbb{Z}/2) \oplus \bigoplus_{x \in (X_{\mathbb{R}})_d} H^{d+2}(x, \mathbb{Z}/2) \oplus \bigoplus_{x \in (X_{\mathbb{Q}_2})_d} H^{d+2}(x, \mathbb{Z}/2))$$

is injective. Here X_d denotes the set of generic points of subvarieties of dimension d as before, and the map is given as a direct sum of maps $H^{d+2}(K, \mathbb{Z}/2) \to H^{d+1}(x, \mathbb{Z}/2)$ induced by the tame symbol for $x \in X_d$, and cohomological restriction maps $H^{d+2}(K, \mathbb{Z}/2) \to H^{d+2}(x, \mathbb{Z}/2)$ for $x \in (X_{\mathbb{R}})_d$ and $x \in (X_{\mathbb{Q}_2})_d$.

Note that X has dimension $d+1$, but $X_{\mathbb{R}}$ and $X_{\mathbb{Q}_2}$ have dimension d, so points in X_d have closure of codimension 1 while $(X_{\mathbb{R}})_d$ and $(X_{\mathbb{Q}_2})_d$ consist of the generic points of irreducible components of full dimension.

Proof. This follows from [KS12, Theorem 0.5] after resolving notation. □

Theorem 3.2.10 ([IT14, Theorem 2.4])**.** *Let D be a Dedekind domain of characteristic 0, X a scheme separated, flat and of finite type over $\mathrm{Spec}(D)$, and l a prime number invertible in D. Then there exists a projective l'-alteration $\tilde{X} \to X$ with $\tilde{X}$ regular.*

Proof of Theorem 3.2.6 in characteristic zero. The field K has a proper model over $\mathbb{Z}[\frac{1}{2}]$, i.e. a scheme X proper, integral, flat and of finite type over $\mathbb{Z}[\frac{1}{2}]$ such that K is the residue field of the generic point of X. Find an alteration $\tilde{X} \to X$ of degree prime to 2 as in Theorem 3.2.10. The scheme $\tilde{X}$ is proper over X and therefore over $\mathbb{Z}[\frac{1}{2}]$. By replacing $\tilde{X}$ with one of its connected components, we may assume $\tilde{X}$ is irreducible and hence integral. The map $\tilde{X} \to \mathrm{Spec}(\mathbb{Z}[\frac{1}{2}])$ is flat because any dominant morphism from an integral scheme to a Dedekind scheme is flat.

The restriction in $\mathbb{Z}/2$-cohomology induced by $\tilde{X} \to X$ is injective for degree reasons, so the claim follows by applying Theorem 3.2.9 to $\tilde{X}$. □

We can now use this local–global principle in the following way.

Proposition 3.2.11. *Let K be finitely generated of Kronecker dimension d and α a non-zero element of $H^{d+1}(K, \mathbb{Z}/2)$.*

- *Assume $\mathrm{char}(K) \neq 2, 0$. Then the image of α in*

$$\prod_v H^{d+1}(K_v, \mathbb{Z}/2)$$

is not zero, where the product is over all valuations v on K of archimedean rank d.

- *Assume that* $\mathrm{char}(K) = 0$ *and* $\alpha = q \cup \beta$*, where* $q \in \mathrm{Br}(\mathbb{Q})[2]$ *is a quaternion algebra over* $\mathbb{Q}$ *splitting over* $\mathbb{R}$ *and* $\mathbb{Q}_2$*, which induces a quaternion algebra in* $H^2(K, \mathbb{Z}/2)$*, and* $\beta \in H^{d-1}(K, \mathbb{Z}/2)$*. Then the conclusion of the first point holds.*

Proof. We prove the first point by induction on d. The case $d = 0$ is clear, as we can take the trivial valuation for v. Now let $d > 0$ and assume the statement is true for $d - 1$. Let $\alpha \in H^{d+1}(K, \mathbb{Z}/2)$. By Theorem 3.2.6, there exists a discrete valuation v on K such that the restriction α to K_v does not vanish. The field Kv has Kronecker dimension at most $d - 1$ and is of the same characteristic as K. In particular, it has cohomological dimension at most d and hence $\partial_v \colon H^{d+1}(K_v, \mathbb{Z}/2) \to H^d(Kv, \mathbb{Z}/2)$ has trivial kernel by Theorem 3.2.4. Therefore $\partial_v \alpha \in H^d(Kv, \mathbb{Z}/2)$ is non-zero, so in particular Kv has Kronecker dimension exactly $d - 1$. By induction hypothesis, there exists a valuation w on Kv of rank $d - 1$ such that the restriction of $\partial_v \alpha$ to $H^d((Kv)_w, \mathbb{Z}/2)$ does not vanish. Write $w \circ v$ for the refinement of v by w. Then α does not vanish in $K_{w \circ v}$, as $K_{w \circ v}$ is the unramified extension of K_v with residue field $(Kv)_w$, and the following diagram commutes by Theorem 3.2.4:

$$\begin{array}{ccc} H^{d+1}(K_v, \mathbb{Z}/2) & \xrightarrow{\partial_v} & H^d(Kv, \mathbb{Z}/2) \\ \downarrow & & \downarrow \\ H^{d+1}(K_{w \circ v}, \mathbb{Z}/2) & \xrightarrow{\partial_v} & H^d((Kv)_w, \mathbb{Z}/2) \end{array}$$

Since $w \circ v$ has rank d, this proves the claim.

For the second point we work in the same fashion, observing that α satisfies the requirements of Theorem 3.2.6 since q splits over all real-closed fields and all henselian fields of mixed characteristic $(0, 2)$, and additionally noting that if v is a discrete valuation on K of residue characteristic 0, then $\partial(\alpha) = q \cup \partial(\beta)$ (again by Theorem 3.2.4) so we can proceed inductively. □

Proposition 3.2.12. *Let K be finitely generated of Kronecker dimension d, $c \in K$, and $\alpha \in H^{d+1}(K, \mathbb{Z}/2)$. If $\operatorname{char} K = 0$, assume furthermore that α is of the form given in the second point of Proposition 3.2.11. Then*

$$S_c(\alpha) = \bigcap_v S_c(\alpha/K_v) \cap K,$$

where the intersection is over all valuations v of archimedean rank d, and hence

$$\bigcap_v \mathcal{O}_v \supseteq S_c(\alpha) \supseteq \bigcap_v \operatorname{res}_v^{-1}(S_{\bar{c}}(\partial_v^d \alpha / Kv)),$$

where the intersection is over all valuations v of rank d such that α does not split over K_v.

Here we write ∂_v^d for the d-fold composition of tame symbol maps, which is justified since v necessarily has value group isomorphic to a lexicographic product $\mathbb{Z}^d$.

Proof. The inclusion $S_c(\alpha) \subseteq \bigcap_v S_c(\alpha/K_v)$ follows from existential definability of S_c. For the other inclusion, let $a \in K$ be an element of the right-hand side and consider $f = X^2 - aX + c \in K[X]$. For any root $x \in \overline{K}$ of f and any rank-d valuation v on K, α splits in $K_v[x]$; therefore α splits in $K[x]_w$ for any rank-d valuation w on $K[x]$. Hence α splits in $K[x]$ by Proposition 3.2.11, thus $a \in S_c(\alpha)$.

The last statement is true since $\mathcal{O}_v \supseteq S_c(\alpha/K_v) \supseteq \mathrm{res}_v^{-1}(S_{\bar{c}}(\partial_{\bar{v}}^d \alpha/Kv))$ by iterated application of Proposition 3.2.5, and $S_c(\alpha/K_v) = K_v$ if α splits over K_v. □

FIELDS WITHOUT SELF-EMBEDDED RESIDUE

The notion of embedded residue was introduced in the paper [AF17] by Anscombe and Fehm and used to give a statement on existential definability of henselian valuation rings. We focus on a special case of their definition, cf. [AF17, Lemma 3.7]:

Definition 4.0.1. *A field F has* self-embedded residue *if there exists an elementary extension $F^* \succ F$ and a non-trivial valuation v on F^*, trivial on F, with an embedding $F^*v \hookrightarrow F^*$ over F.*

The utility of the notion of self-embedded residue lies in the following theorem.

Theorem 4.0.2 (Special case of [AF17, Theorems 3.11, 5.1])**.** *The following are equivalent for a field F.*

- *F does not have self-embedded residue;*
- *in the class of equicharacteristic henselian valued fields (E, v) with a fixed embedding $F \hookrightarrow \mathcal{O}_v$ such that the composite map $F \hookrightarrow \mathcal{O}_v \twoheadrightarrow Ev$ is an elementary embedding, the valuation ring $\mathcal{O}_v$ is uniformly existentially definable in E with parameters in (the image of) F.*

If F is perfect, both conditions are equivalent to $F[[t]]$ being existentially definable in $F((t))$ with parameters from F.

In the work of Anscombe and Fehm, the notion of fields with self-embedded residue is in a precise sense dual to the well-known notion of *ample* fields, also known as large fields—specifically, ample fields

are precisely those for which $F[[t]]$ is not universally definable with parameters from F in $F((t))$, see [AF17, Corollary 6.12].

4.1 fields of kronecker dimension 1

In this section we give a strong example of a class of fields without self-embedded residue. Recall that a field has Kronecker dimension 1 if it is an algebraic extension of a global field. Equivalently, it is either algebraic over $\mathbb{Q}$ or of transcendence degree 1 over a finite field.

Write $\mathrm{Th}_{\mathrm{K-dim=1}}$ for the first-order theory of fields of Kronecker dimension 1. This theory was previously investigated in [Cha90], where it was shown that all of its models are fields of virtual cohomological dimension at most 2.

Theorem 4.1.1. *Let $K \models \mathrm{Th}_{\mathrm{K-dim=1}}$ and assume that the Brauer group of K is non-trivial. Then K has self-embedded residue if and only if it is either real-closed or henselian.*

Note that this theorem is a considerable strengthening of the statement that no global field has self-embedded residue. However, the restriction on Brauer groups is essential; in particular, results about the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ seem out of reach with the present method.

The proof technique is built on combining the existentially definable sets associated to central simple algebras in Chapter 2 with the following first-order version of Hensel's Lemma.

Lemma 4.1.2 (Hensel's Urlemma)**.** *Let K be a global field and $\mathcal{O} \subseteq K$ a valuation ring. Let $f = X^n + X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0 \in \mathcal{O}[X]$ with all*

a_i in the maximal ideal of $\mathcal{O}$. Then f has an approximate zero in K of arbitrarily high order, i.e. for all $b \in K^\times$ there exists $x \in \mathcal{O}$ such that $f(x) \in b \cdot \mathcal{O}$.

The name "Hensel's Urlemma" seems justified as the statement is equivalent to the usual statement of Hensel's Lemma over global fields for polynomials f of the given form (i.e. that f has a zero in the completion of K with respect to $\mathcal{O}$), but on the other hand was already known to Gauß; see [Fre07, Sections 3.6 and 2.2.4] for a historical discussion.

Corollary 4.1.3. *If $K \models \mathrm{Th}_{\mathrm{K-dim=1}}$ and $\mathcal{O}$ is a definable valuation ring, then the conclusion of Lemma 4.1.2 holds.*

Proof. First observe that if K is of Kronecker dimension 1 and $\mathcal{O}$ is any valuation ring of K, then the statement is true since we can reduce to a global subfield of K. Then the claim follows from first-order transfer. □

An analogous result for orderings is the following.

Lemma 4.1.4. *Let $K \models \mathrm{Th}_{\mathrm{K-dim=1}}$, $P \subseteq K$ a definable set which is the positive cone of a field ordering, and $b \in K^\times$.*

1. *For every polynomial $f \in K[X]$ of odd degree, there exists $x \in K$ such that $b^2 - f(x) \in P$ and $b^2 + f(x) \in P$;*

2. *for every $c \in P$ there exists $x \in K$ such that $b^2 + c - x^2 \in P$ and $b^2 - (c - x^2) \in P$.*

Writing $\leq$ for the ordering induced by P, we can read the conditions in the lemma as $-b^2 \leq f(x) \leq b^2$ and $-b^2 \leq c - x^2 \leq b^2$, so the statement is that polynomials of odd degree have approximate zeroes

and non-negative elements have approximate square roots to arbitrary order.

Proof. First observe that the result is true if K is a number field, because K is dense in its completion with respect to P, and in this completion polynomials of odd degree have zeroes and non-negative elements have square roots.

Therefore the result is true if K is an algebraic extension of $\mathbb{Q}$, since for any given polynomial $f \in K[X]$ or element $c \in K$ we may restrict to a number field containing the coefficients of f or c.

Since the result is vacuous if K has positive characteristic due to the absence of positive cones, this means that any field of Kronecker dimension 1 satisfies the statement. As the assertion is first-order, this completes the proof. □

Proposition 4.1.5. *Let (F, v) be an equicharacteristically valued field and F_0 a subfield of the valuation ring $\mathcal{O}_v$, so F_0 is compatibly embedded into F and Fv. Let A/F_0 be a central simple algebra of prime degree l. If A does not split over Fv, then it does not split over F, and furthermore $T(A/F)$ is contained in the valuation ring $\mathcal{O}_v$. If A splits over F, then $T(A/F) = F$.*

Proof. We may replace (F, v) by its henselisation.

Assume first that A is not split over Fv. If A splits in F, then its norm form has a non-trivial zero in F, but since the norm form is a homogeneous polynomial defined over F_0, it will also have a non-trivial zero in Fv, which is not the case.

To see that $T(A/F)$ is contained in the valuation ring $\mathcal{O}_v$, observe first that any polynomial of degree l which splits A is necessarily irreducible by Lemma 2.2.6. Therefore, if it has constant coefficient ± 1, then all its coefficients are in $\mathcal{O}_v$ by Lemma 2.2.7. This proves $T(A/F) \subseteq \mathcal{O}_v$ by the definitions of $S(A/F)$ and $T(A/F)$.

If A splits over F, then clearly $T(A/F) = F$ since $S(A/F) = F$. □

Let $K \models \mathrm{Th}_{\mathrm{K-dim=1}}$ for the rest of this section.

Lemma 4.1.6. *If there exist central simple algebra $A, B/K$ of prime degree such that $T(A/K) + T(B/K) = K$, but $T(A/K) \neq K \neq T(B/K)$, then K does not have embedded residue.*

Proof. Let $K^* \succ K$ and u a valuation on K^* with a fixed embedding $K^*u \hookrightarrow K^*$ over K. Then A, B do not split over K and hence not over K^* and K^*u. Thus $T(A/K)$ and $T(B/K)$ are both contained in $\mathcal{O}_u$ by Proposition 4.1.5, but this forces u to be trivial. □

Lemma 4.1.7. *If there exists a central simple algebra A/K of prime degree such that $\mathcal{O} = T(A/K)$ is a non-trivial valuation ring, and if furthermore K has self-embedded residue, then $\mathcal{O}$ is henselian.*

Proof. By one of the equivalent characterisations of henselianity, it suffices to show that every polynomial $f = X^n + X^{n-1} + a_{n-2}X^{n-2} + \cdots + a_0 \in \mathcal{O}[X]$ with all a_i in the maximal ideal has a zero in K. Let $K^* \succ K$ with a non-trivial valuation u such that K^*u embeds into K^* over K. We deduce $\mathcal{O}^* \subseteq \mathcal{O}_u$ by Proposition 4.1.5.

Pick $b \in K^*$ with $ub > 0$. Since $f(-1)$ is zero in the residue field of $\mathcal{O}^*$, f has an approximate zero $x \in \mathcal{O}^*$ with $f(x) \in b \cdot \mathcal{O}^*$ by Corollary 4.1.3. Hence f has an exact zero in K^*u. This zero is algebraic over K. Since K^*u embeds over K into K^*—which is regular over K—, this implies that the zero is already in K. □

Lemma 4.1.8. *If there exists a central simple algebra A/K of prime degree and a field ordering $\leq$ on K such that $T(A/K) = \{x \in K\colon -4 < x < 4\}$, and if furthermore K has self-embedded residue, then $(K, \leq)$ is real closed.*

Proof. Let $K^* \succ K$ with a non-trivial valuation u such that K^*u embeds into K^* over K. By Proposition 4.1.5 we have $T(A \otimes K^*/K^*) \subseteq \mathcal{O}_u$. Pick $b \in K^*$ with $ub > 0$.

The definable set $P = \{x \in K\colon x = 0 \vee x - 4 \in T(A/K) \vee \frac{1}{x} - 4 \in T(A/K)\}$ is the positive cone associated to $\leq$; in particular, the ordering $\leq$ extends in a canonical way to K^*, and the valuation ring of u is convex with respect to this ordering.

Now we apply Lemma 4.1.4. For any polynomial $f \in K[X]$ of odd degree, we can find $x \in K^*$ such that $-b^2 \leq f(x) \leq b^2$, so in the residue field K^*u we have $f(\overline{x}) = 0$. Since K^*u embeds into K^* over K and K^* is regular over K, f has a zero in K.

For any $c \in K$ with $0 \leq c$ we can find $x \in K^*$ with $-b^2 \leq c - x^2 \leq b^2$, so c has a square root in K^*u and therefore in K.

This finishes the proof that $(K, \leq)$ is real closed. □

We can now give the main result for the proof of Theorem 4.1.1.

Lemma 4.1.9. *If there exists a non-trivial central simple algebra C/K of prime degree l, then either $T(C/K)$ is a valuation ring, or $T(C/K) = \{x \in K\colon -4 < x < 4\}$ for some field ordering $<$ of K, or we can find $A, B/K$, also of degree l, such that $T(A/K) + T(B/K) = K$, but $T(A/K) \neq K \neq T(B/K)$.*

In particular, if K has self-embedded residue, then K is henselian or real closed.

Proof. The last statement follows from the first statement as a consequence of the preceding lemmas.

The first statement is first-order, since $T(C/K)$ being a valuation ring or an interval $]-4,4[_v$ with respect to some ordering v are definable conditions. Hence it suffices to consider the case where K has Kronecker dimension 1. The set $T(C/K) \neq K$ is an intersection of valuation rings of K and intervals $]-4,4[_v$ with respect to orderings v of K by Theorem 2.2.16. If $T(C/K)$ is a valuation ring, or if $T(C/K) =]-4,4[_v$ with respect to some field ordering v, then we are done.

Otherwise, there exist two places $v \neq w$ of K such that C is non-split over K_v and K_w. Let $K_0 \subseteq K$ be a global field over which C is defined. Say v, w are above the places v_0, w_0 of K_0. We may assume $v_0 \neq w_0$, by enlarging K_0 if necessary. Then in particular $[K_v\colon K_{0,v_0}]$ is prime to l (as a supernatural number) as K_v does not split C, and likewise for w. Find central simple algebras $A, B/K_0$ of degree l such that $\Delta(A/K_0) \cap \Delta(B/K_0) = \emptyset$, $v_0 \in \Delta(A/K_0)$, $w_0 \in \Delta(B/K_0)$; this is possible by Lemma 2.3.4.

Now we have $T(A/L) + T(B/L) = L$ for every finite extension L/K_0 by Theorem 2.2.15, and hence also for $F = K$. Furthermore $T(A/K) \neq$

$K \neq T(B/K)$, as A and B do not split over K_v, K_w respectively. □

This completes the essential part of the proof of Theorem 4.1.1; we merely have to show that we can obtain a central simple algebra of prime degree over K.

Lemma 4.1.10. *If* $\mathrm{Br}(K) \neq 0$, *there exists a prime number* l *and a non-split central simple algebra over* K *of degree* l.

Proof. If the Brauer group is non-trivial, then there is a prime l such that $\mathrm{Br}(K)$ has an l-torsion element, i.e. there is a non-split central simple algebra A/K whose l-th tensor power splits.

If K is of Kronecker dimension 1, then Lemma 2.3.5 implies the existence of a central simple algebra as desired. This fact that existence of a central simple algebra A/K whose l-fold tensor power splits implies existence of a non-split central simple algebra of degree l is a collection of first-order facts and hence also true in any $K \models \mathrm{Th}_{\mathrm{K-dim=1}}$. □

Proof of Theorem 4.1.1. If K is real closed or henselian, then K has self-embedded residue.

Assume conversely that K has self-embedded residue, and that $K \models \mathrm{Th}_{\mathrm{K-dim=1}}$ and $\mathrm{Br}(K) \neq 0$. By the last lemma, there exists a prime number l and a non-split central simple algebra of degree l over K. Hence, by Lemma 4.1.9, K must be henselian or real closed. □

Remark 4.1.11. The condition that $\mathrm{Br}(K) = 0$ can be reinterpreted using Galois cohomology. In particular, in characteristic zero a sufficient condition is that the absolute Galois group be projective, and in fact it is not

hard to show, using fairly basic cohomological techniques as in [NSW08, Corollary 8.1.18], that in the case of models of $\mathrm{Th}_{\mathrm{K-dim=1}}$ this condition is also necessary.

Hence we have now fully understood the condition of having self-embedded residue for all models of $\mathrm{Th}_{\mathrm{K-dim=1}}$ of characteristic 0 with non-projective absolute Galois group.

We can also use the techniques above to analyse valuations on non-standard number fields.

Theorem 4.1.12. *Let K be a model of the theory of number fields, i.e. K is elementarily equivalent to an ultraproduct of number fields. Let v be a valuation on K and write K_v for the corresponding henselisation. If some finite extension of K_v has non-zero Brauer group, then the valuation ring of v either contains the ring of integers of K or is convex with respect to some field ordering of K.*

Note that we can refer to the ring of integers of K since the ring of integers of standard number fields is uniformly definable by Theorem 2.3.7.

Proof. Let us assume that the valuation ring $\mathcal{O}_v$ is not convex with respect to any field ordering of K, so K_v carries no field ordering by [EP05, Lemma 4.3.6]. Assume first that $\mathrm{Br}(K_v)$ is non-zero.

Let l be a prime number such that $\mathrm{Br}(K_v)[l] \neq 0$, so we may pick a central simple algebra A/K_v of order l in $\mathrm{Br}(K_v)$. By adjoining some structure constants for A to K, we can find a finite subextension L of K_v/K such that A is defined over L, i.e. there exists an algebra A_0/L with $A \cong A_0 \otimes_L K_v$. By passing to a further finite subextension if necessary, we

may assume that $A_0^{\otimes l}$ splits over L, and that L has no field orderings. Since every finite extension of a number field is still a number field, and since finite extensions of fields of given degree are uniformly interpretable in the ground field, the field L is still a model of the theory of number fields; hence we may replace A_0 by a Brauer equivalent central simple algebra of degree l by Theorem 2.3.3.

Since A_0 does not split over K_v, the valuation ring of v in L contains $T(A_0/L)$, since any monic polynomial with constant coefficient $(-1)^l$ splitting A/K_v must be irreducible and hence have all coefficients in the valuation ring by Lemma 2.2.7.

Therefore the ring of integers of L is contained in this valuation ring by Theorem 2.3.7. As it is a first-order fact that the ring of integers of L contains the ring of integers of K, this means that the valuation ring of v in K contains the ring of integers of K.

We assumed above that $\mathrm{Br}(K_v)$ was non-zero, so consider now the situation where only some finite extension of K_v has non-zero Brauer group. This finite extension is a henselisation of some finite extension K'/K. Since K' is still a model of the theory of number fields, and the ring of integers of K' contains the ring of integers of K, the previous proof applies. □

Note that we can classify the valuation rings of v that contain the ring of integers of K; since this ring of integers is a Prüfer domain, they are in bijection to the prime ideals of the ring of integers, which can be understood by the results of [Che75]. (There only stated in the situation where K is a finite extension of an elementary extension of $\mathbb{Q}$, but in

fact the results remain true for arbitrary models of the theory of number fields, once a definition of the ring of integers is available.) Likewise, the valuation rings convex with respect to some given field ordering can be classified as the coarsenings of the valuation ring consisting of elements of K that are finite with respect to this ordering.

4.2 VALUATION SPACES

In working with finitely generated fields which are not global fields, it is sometimes necessary to work with infinitely many valuations at a time. In these situations we use topological methods on sets of valuations.

Throughout this section, let K be an arbitrary field and write V for the set of valuation rings on K; as usual, we identify valuation rings and equivalence classes of valuations. We endow V with the *constructible topology*, meaning a subbasis of open sets is given by sets of the form $\{v\colon v(a) \geq 0\}$ and $\{v\colon v(a) > 0\}$ for $a \in K$. (See [HK94] for this and other topologies on spaces of valuations.) By seeing valuation rings as subsets of K, we can embed V into the powerset $\mathcal{P}(K)$. Identifying the powerset of K with the compact space $\{0,1\}^K$, we find that the constructible topology is exactly the subspace topology induced on V by the topology on $\mathcal{P}(K)$.

Lemma 4.2.1. *Let K be a field and $\mathcal{L}_R(K)$ the language of rings with an additional unary predicate and constants for elements of K. Let Φ be a collection of universal $\mathcal{L}_R(K)$-sentences. Then*

$$\{U \subseteq K\colon (K,U) \models \Phi\} \subseteq \mathcal{P}(K)$$

with the subspace topology is a Stone space, i.e. a compact totally disconnected Hausdorff space.

Proof. Since $\mathcal{P}(K)$ is a Stone space, it suffices to show that the given set is closed. For every quantifier-free $\mathcal{L}_R(K)$-sentence χ, the set of U such that $(K, U) \models \chi$ is clopen by definition of the topology on $\mathcal{P}(K)$, and any universal $\mathcal{L}_R(K)$-sentence φ may be replaced by the set of quantifier-free sentences obtained by substituting all possible field elements for its quantified variables. This proves the claim. □

Since the condition of being a valuation ring is defined by a universal sentence, this means that V with the constructible topology is a Stone space.

With the topology on V in place, we can now state and prove a general approximation lemma.

Lemma 4.2.2. *Let K be a field and $S_1, \ldots, S_n$ be sets of valuations of K satisfying the following conditions:*

- *Each S_i is compact in the constructible topology.*
- *If $v \in S_i$, $w \in S_j$ for any $i \neq j$, then v and w are independent, i.e. have no non-trivial common coarsening. (In particular, the S_i are disjoint except possibly for the trivial valuation.)*
- *There is a monic polynomial $f \in K[X]$ of degree greater than zero such that for any $v \in S_i$, f is in $\mathcal{O}_v[X]$ and the reduction $\bar{f} \in Kv[X]$ has no zero in Kv.*

Let $x_1, \ldots, x_n \in K$ and $z_1, \ldots, z_n \in K^\times$ be given. Then there exists an $x \in K$ such that for any i and $v \in S_i$, $v(x - x_i) \geq v(z_i)$.

This may be understood as a generalisation of weak approximation—weak approximation is obtained when each S_i contains only one valuation. The statement of the lemma, in a less general version, and its proof are originally due to Arno Fehm.

Proof. Let $d = \deg(f)$, $g = X^d f(Y/X) \in K[X,Y]$ be the homogenisation of f and write $h = 1/g(1/X, 1/Y) \in K(X,Y)$. Then for each $x, y \in K$ and v in any S_i the following properties hold:

- $v(g(x,y)) = d \min(vx, vy)$
- $v(h(x,y)) = d \max(vx, vy)$

Fix $z \in K^\times$ such that $v(z) \geq 0$ and $v(z) \geq v(z_j) - v(x_k)$ for any j,k and v in any S_i; this is possible by combining the terms 1, z_1/x_1, $z_2/x_1, \ldots, z_n/x_n$ by iterated application of h (terms z_j/x_k where $x_k = 0$ may be ignored).

We now claim that for each i there exists a b_i such that $v(b_i) \geq v(z)$ for all $v \in S_i$ and $w(b_i) \leq 0$ for $w \in S_j$, $j \neq i$. To prove this, we may choose for each $v \in S_i$, $w \in S_j$ an element $a_{v,w} \in K$ such that $v(a_{v,w}) \geq v(z)$, $w(a_{v,w}) \leq 0$; this is possible by weak approximation. Since the condition $v(a_{v,w}) \geq v(z)$ is an open condition on v, we can in fact by compactness find finitely many $a_w^{(1)}, \ldots, a_w^{(m)}$ such that $w(a_w^{(k)}) \leq 0$ for all k, and for each v there exists k such that $v(a_w^{(k)}) \geq v(z)$. Using the function h, we may combine all these to one element a_w such that $w(a_w) \leq 0$ and $v(a_w) \geq v(z)$. In this way we proceed for all $w \in \bigcup_{j \neq i} S_j$. But since the condition $w(a_w) \leq 0$ is open, there are in fact finitely many $a^{(1)}, \ldots, a^{(m')}$

such that $v(a^{(k)}) \geq v(z)$ for all k, and for each w there exists a k such that $w(a^{(k)}) \leq 0$. Combining all these $a^{(k)}$ using g yields an element b_i as desired, so the claim is proven.

Now set $c_i = h(1, b_i)$, so $v(c_i) \geq v(z)$ for $v \in S_i$ and $w(c_i) = 0$ for $w \in S_j$, $j \neq i$. Set $d_i = c_i \prod_{j \neq i} c_j^{-1}$; this satisfies $v(d_i) \geq v(z)$, $w(d_i) \leq -w(z)$. Set $e_i = 1/(d_i^d f(1/d_i)) = 1/g(d_i, 1)$; this satisfies $v(e_i - 1) \geq v(d_i) \geq v(z)$ and $w(e_i) = -dw(d_i) \geq w(z)$. Then $x = \sum_i x_i e_i$ is as desired. □

4.3 finitely generated fields

Let L be a finitely generated field of Kronecker dimension $d > 0$ of characteristic not 2. We shall show that L does not have self-embedded residue. (Finitely generated fields of Kronecker dimension 0, i.e. finite fields, do not have self-embedded residue, as is immediately apparent from the definition.)

The technical tool for the task at hand is the splitting of Pfister forms developed in Chapter 2. This approach, based on the local–global principle for higher cohomology, is reminiscent of Pop's work on his eponymous conjecture, see [Pop17].

Let $\alpha, \beta \in K^M_{d+1}(L)/2$ be pure symbols and $c, C \in L$ such that the following conditions are satisfied:

1. Both α and β are non-zero.
2. For any valuation v on L of residue characteristic 2, both α and β split over the henselisation L_v.

3. For any non-trivial valuation v on L, at least one of α and β split over L_v.

4. If v is a valuation on L with value group of archimedean rank d such that one of α and β is non-split over L_v, then we have $v(C) > 0$, $v(c) \geq 0$ and $X^2 + c$ reduces to an irreducible polynomial in the residue field Lv.

Existence of α, β, c and C will be justified in Section 4.3.1. Let V be the space of all valuations of L with the constructible topology, and let $V_\alpha, V_\beta \subseteq V$ be the space of valuations $v \in V$ such that α (respectively, β) does not split in L_v.

Lemma 4.3.1. *The sets V_α and V_β are both compact. Any $v \in V_\alpha, v' \in V_\beta$ are independent.*

Proof. For compactness it suffices to show that the sets are both closed. We give the argument for V_α. For any $v \in V \setminus V_\alpha$, α restricts to zero in K_v, meaning that either the residue characteristic of v is two, which is an open condition, or the residue characteristic is not two and the associated Pfister form has a zero. By Hensel's Lemma, the latter is an open condition on v.

If $v \in V_\alpha, v' \in V_\beta$ have a common coarsening w, then neither α nor β split in L_w, hence w is the trivial valuation. Thus v and v' are independent. □

We now make use of the sets S_c from Definition 3.2.3.

Lemma 4.3.2.

$$\bigcap_v \mathfrak{m}_v \subseteq S_c(\alpha) \subseteq \bigcap_v \mathcal{O}_v,$$

where the intersection is over all valuations v of rank d such that α does not split over L_v, and analogously for $S_c(\beta)$.

Proof. By Proposition 3.2.12, $S_c(\alpha)$ contains the intersection of all the sets $\mathrm{res}_v^{-1}(S_{\bar{c}}(\partial_v^d \alpha / Lv))$ for valuations v of rank d such that α does not split over L_v. By construction, in the residue field Lv of such valuations the polynomial $X^2 + \bar{c}$ is irreducible and hence splits $\partial^d \alpha$ (since its splitting field is the unique quadratic extension of the finite field Lv), so $0 \in S_{\bar{c}}(\partial_v^d \alpha)$. The proof for β is identical. □

Lemma 4.3.3.

$$L = S_c(\alpha) \cdot S_c(\beta)$$

Proof. Let $y \in L^\times$ be given. We apply Lemma 4.2.2 with $S_1 = V_\alpha$, $S_2 = V_\beta$; observe that the preconditions are satisfied. Choose $x_1 = \frac{y}{C}$, $x_2 = C$, $z_1 = x_1 C$, $z_2 = x_2 C$, so the lemma gives $x \in L$ with $v(x - x_1) \geq v(z_1)$ for all $v \in V_\alpha$ and $v'(x - x_2) \geq v'(z_2)$ for all $v' \in V_\beta$. In particular, if v and v' are of rank d and thus $v(C), v'(C) > 0$, then $v(z_1) > v(x_1)$ and hence $v(x) = v(x_1) < v(y)$, and likewise $v'(z_2) > v'(x_2)$, therefore $v'(x) = v'(x_2) > 0$.

This proves $x \in S_c(\beta)$ and $y/x \in S_c(\alpha)$ by the preceding lemma, so $y \in S_c(\alpha) \cdot S_c(\beta)$ as desired. □

Theorem 4.3.4. *The field L does not have L-embedded residue.*

Proof. Let $L^* \succ L$ and v a valuation on L^* such that L^*v embeds into L^* over L. In the light of Lemma 4.3.3 it suffices to show that the valuation ring of v contains both $S_c(\alpha)$ and $S_c(\beta)$, since then v must be trivial. This is achieved by the following lemma. □

Lemma 4.3.5. *Let (L, v) be a valued field,* $\mathrm{char}(Lv) \neq 2$, *$c \in \mathcal{O}_v$, and M a field embedded into the valuation ring of v. If $\gamma \in H^n(M, \mathbb{Z}/2)$, represented by a Pfister form, does not become zero in $H^n(Lv, \mathbb{Z}/2)$, then the valuation ring of v contains $S_c(\gamma/L)$.*

Proof. This is similar to the proof of Proposition 4.1.5. Splitting of γ is equivalent to the associated Pfister form having a non-trivial zero. If $X^2 + aX + c$ with $va < 0$ splits γ, then γ already vanishes over L since the polynomial is reducible by Lemma 2.2.7. This means the Pfister form has a non-trivial zero over L, and therefore also in Lv by scaling the zero appropriately and reducing. □

4.3.1 Constructing special symbols

We still need to prove that there are α, β, C and c satisfying our assumptions.

In characteristic zero, choose a transcendence basis $t_1, \ldots, t_{d-1}$ of $L/\mathbb{Q}$, so that L is a finite extension of $L_1 = \mathbb{Q}(t_1, \ldots, t_{d-1})$. Write $L_i = \mathbb{Q}(t_i, \ldots, t_{d-1})$ for $1 \leq i < d$, $L_d = \mathbb{Q}$. In characteristic $p > 0$, we may choose a *separating* transcendence basis $t_1, \ldots, t_d$ of $L/\mathbb{F}_p$ since $\mathbb{F}_p$ is perfect, so L is a finite separable extension of $L_1 = \mathbb{F}_p(t_1, \ldots, t_d)$. Write $L_i = \mathbb{F}_p(t_i, \ldots, t_d)$ for $1 \leq i \leq d$.

Write $L^{(1)} = L$. We shall inductively construct finite separable extensions $L^{(i)}/L_i$ in the following way. Assume that $L^{(i)}$ has been constructed for some $i < d$. Consider all non-trivial valuations of $L_i = L_{i+1}(t_i)$ trivial on L_{i+1}. By basic valuation theory, there is one such for each irreducible polynomials in $L_{i+1}[t_i]$ and one additional valuation, the degree valuation. Since $L^{(i)}/L_i$ is separable, all but finitely many of these valuations do not ramify in $L^{(i)}/L_i$; we may therefore choose distinct elements $n_i, m_i \in L_d$ such that the $(t_i - n_i)$-adic and the $(t_i - m_i)$-adic valuation on L_i do not ramify in $L^{(i)}$. We may additionally enforce that the four elements $n_i, n_i - 1, m_i, m_i - 1$ of L_d are all distinct.

Pick extensions v_i and w_i of the $(t_i - n_i)$-adic and the $(t_i - m_i)$-adic valuations to L_i, respectively; then $v_i(t_i - n_i)$ and $w_i(t_i - m_i)$ are minimal positive in the respective value groups.

The residue fields of v_i and w_i are finite separable extensions of L_{i+1}; let $L^{(i+1)}/L_{i+1}$ be a finite separable extension into which both embed. In this way, we may continue inductively until we have constructing a finite separable extension $L^{(d)}/L_d$, so $L^{(d)}$ is a global field. In characteristic zero, choose distinct odd prime numbers p_1, p_2, q_1, q_2 such that the corresponding prime ideals split completely in $L^{(d)}/L_d$. In positive characteristic, choose distinct irreducible polynomials $p_1, p_2, q_1, q_2 \in \mathbb{F}_p[t_d]$ such that the corresponding prime ideals split completely in $L^{(d)}/L_{(d)}$.

Choose quaternion algebras $a, b \in \mathrm{Br}(L_d)[2]$ such that a is non-split at precisely the places corresponding to p_1 and p_2, and b is non-split at precisely the places corresponding to q_1 and q_2.

Let

$$\alpha = \{\frac{t_1 - n_1}{t_1 - n_1 - 1}, \dots, \frac{t_{d-1} - n_{d-1}}{t_{d-1} - n_{d-1} - 1}, a\}$$
$$\beta = \{\frac{t_1 - m_1}{t_1 - m_1 - 1}, \dots, \frac{t_{d-1} - m_{d-1}}{t_{d-1} - m_{d-1} - 1}, b\}$$
$$C = p_1 p_2 q_1 q_2.$$

In characteristic zero, choose $c \in \mathbb{Z}$ such that $X^2 + c$ reduces to an irreducible polynomial in the finite fields $\mathbb{F}_{p_1}$, $\mathbb{F}_{p_2}$, $\mathbb{F}_{q_1}$ and $\mathbb{F}_{q_2}$. In positive characteristic, choose $c \in \mathbb{F}_p[t_d]$ such that $X^2 + c$ reduces to an irreducible polynomial modulo p_1, p_2, q_1 and q_2. We claim that these satisfy our conditions.

Let first v be a valuation on L, non-trivial on L_d, such that a or b are non-split in the henselisation L_v; write v' for the restriction of v to L_d. Since L_v contains the henselisation $(L_d)_{v'}$, by construction of a and b the valuation v' must be induced by one of p_1, p_2, q_1 and q_2, in particular $v(C) > 0$. In characteristic zero we furthermore conclude that v does not have residue characteristic 2, and in positive characteristic we deduce that $v(t_d) \geq 0$ and therefore $v(c) \geq 0$. The residue field Lv cannot contain the unique degree-2 extension of the finite field $L_d v'$—if it did, then L_v would contain the unique unramified degree 2-extension of the henselisation $(L_d)_{v'}$, and thus a and b would split in L_v. This means that the polynomial $X^2 + c$ reduces to an irreducible polynomial over Lv.

Let us now argue that α and β are not split over L; we give the argument for α. Note that a is not split over $L^{(d)}$, therefore $\{\frac{t_{d-1} - n_{d-1}}{t_{d-1} - n_{d-1} - 1}, a\}$ is not split over $L^{(d-1)}$ since $v_{d-1}(\frac{t_{d-1} - n_{d-1}}{t_{d-1} - n_{d-1} - 1})$ is minimal positive in the value group of v_{d-1} by construction and thus $\partial_{v_{d-1}}(\{\frac{t_{d-1} - n_{d-1}}{t_{d-1} - n_{d-1} - 1}, a\}) =$

$a \neq 0$. Inductively, we deduce that $\{\frac{t_i-n_i}{t_i-n_i-1}, \ldots, \frac{t_{d-1}-n_{d-1}}{t_{d-1}-n_{d-1}-1}, a\}$ is not split over $L^{(i)}$ and therefore α is not split over $L^{(1)} = L$, as desired.

It remains to show that if v is a non-trivial valuation on L, then at least one of α and β splits in L_v. If v is non-trivial on L_d, then by construction at least one of a and b splits in the henselisation, and hence so does one of α and β.

Now assume that v is trivial on L_d, and α does not split in L_v. We cannot have $v(\frac{t_j-n_j}{t_j-n_j-1}) = 0$ for all j: If this is the case, we obtain an element $\{\overline{\frac{t_1-n_1}{t_1-n_1-1}}, \ldots, \overline{\frac{t_d-n_d}{t_d-n_d-1}}, a\} \in K^M_{d+1}(Lv)/2$, but this group is trivial for reasons of cohomological dimension; hence the corresponding Pfister form over Lv has a zero, which means that the Pfister form corresponding to α has a non-trivial zero in L_v by Hensel's Lemma, so α splits in L_v in contradiction to our assumption.

Therefore we must have $v(\frac{t_j-n_j}{t_j-n_j-1}) \neq 0$ for some j, so $v(t_j - n_j) > 0$ or $v(t_j - n_j - 1) > 0$. This means that $v(t_j - m_j) = v(t_j - m_j - 1) = 0$, and in fact there is an element $r \in L_d^\times$, given as either $\frac{n_j-m_j}{n_j-m_j-1}$ or $\frac{n_j-m_j+1}{n_j-m_j}$, such that $v(\frac{t_j-m_j}{t_j-m_j-1} - r) > 0$. Hence $\frac{t_j-m_j}{t_j-m_j-1}$ and r induce the same square class in L_v, so $\{\frac{t_j-m_j}{t_j-m_j-1}, b\} = \{r, b\} \in K^M_3(L)/2$. But the element $\{r, b\}$ is zero in $K^M_3(L_d)/2$ since $K^M_3(L_d)/2 = 0$ for reasons of cohomological dimensions, so in fact β splits over L_v.

NEW EXISTENTIAL PREDICATES OVER GLOBAL FIELDS

In this chapter, we apply the tools developed in Chapter 2 to give new existential definitions in global fields. One of the central results is that irreducibility of a polynomial is an *existential* statement about its coefficients.

Most of the results of this chapter have appeared in the author's paper [Dit18]. The techniques used here have since been applied in [Mor17] to obtain even more existential definitions in global fields.

5.1 PRELIMINARIES FROM CLASS FIELD THEORY

Fix a global field K and $n > 1$. Also fix a prime $l \mid n$ for this section. Our strategy for developing new existential definitions over K is based on distinguishing K from its finite extensions of degree n using first-order sentences. This involves investigating the splitting behaviour of central simple algebras of degree l over K, as developed in Chapter 2, across an infinite collection of such algebras. This depends on class field theory to construct cyclic central simple algebras. See [Lan70] and [Ros02] for general references for class field theory.

The entirety of this section is rather technical; we set up the necessary machinery—notably describing certain ideal groups $I_{\mathfrak{m}}$ and H, as well as field extensions M_i/K—which is needed for our main proofs in the next section, in particular the central Proposition 5.2.5.

Let us fix some notation. Write Σ for the set of places of K. If K is a number field, write $\Sigma_\infty \subset \Sigma$ for the set of archimedean places. If K is a

global function field, arbitrarily fix Σ_∞ to be any finite non-empty subset of Σ. In either case, we call Σ_∞ the set of *places at infinity*.

Let $\mathcal{O}_K$ be the ring of elements of K integral at each place in $\Sigma \setminus \Sigma_\infty$; this is a Dedekind domain, and the prime ideals of $\mathcal{O}_K$ are in bijection to places in $\Sigma \setminus \Sigma_\infty$. This ring is the usual ring of integers in the number field case. In the case of function fields, $\mathcal{O}_K$ depends on the choice of Σ_∞.

Write $I_{\mathcal{O}_K}$ for the group of fractional ideals of $\mathcal{O}_K$, $P_{\mathcal{O}_K}$ for the subgroup of principal fractional ideals, and $\mathrm{Cl}(\mathcal{O}_K) = I_{\mathcal{O}_K}/P_{\mathcal{O}_K}$. In the number field case, this is the usual ideal class group and well-known to be finite. In the function field case, this is not the usual divisor class group, since we are ignoring the places at infinity, but rather the Σ_∞-class group in the sense of [Ros02, Chapter 14]—essentially the divisor class group modulo the classes of prime divisors at infinity. It is finite by Corollary 2 to Proposition 14.1 ibid.

We now fix some field extensions of K for later use. Choose a natural number k such that $l^k > |\mathrm{Cl}(\mathcal{O}_K)| \cdot n!$. Find an abelian extension M/K with Galois group $\mathrm{Gal}(M/K) \cong (\mathbb{Z}/l\mathbb{Z})^k$ and such that M/K is completely split at all infinite places.

Lemma 5.1.1. *For any choice of k we can find such M.*

Proof. This follows from general existence theorems for abelian extensions in class field theory, e.g. the version of the Grunwald-Wang Theorem in [NSW08, Theorem 9.2.8]. (Note that we are never in what is called the "special case" there, since we are looking for an abelian extension whose Galois group has prime exponent.)

It is not hard to give an explicit argument in the present situation, using (the totally real part of) cyclotomic extensions in the number field case, and the analogous Carlitz module construction (see [Ros02, Chapter 12]) over a suitable subfield $\mathbb{F}_p(T) \subseteq K$ in the function field case. □

Remark 5.1.2. This choice of a distinguished abelian extension of K is already present in previous papers, in the special case $l = k = 2$; most notably in subsection 3.3 of [Par13], a field extension $K(\sqrt{a}, \sqrt{b})/K$ is chosen. Likewise, the modulus 8 which appears throughout [Koe16] can be retrospectively explained by an implicit choice of field extension $\mathbb{Q}(\sqrt{2}, \sqrt{-1})/\mathbb{Q}$. The paper [EM16], independently from the work of the present author, transfers some of the ideas of [Par13] to the setting of global function fields. Note however that in our situation the analogy between function fields and number fields is more direct: We do not have to impose the condition that M be linearly disjoint from the Hilbert class field of K as in (the proof of) [Par13, Lemma 3.19]—a condition that [EM16] changes in the function field situation.

Let us write $I_{\mathfrak{m}} \leq I_{\mathcal{O}_K}$ for the set of fractional ideals of $\mathcal{O}_K$ in which none of the prime ideals ramified in M/K occur in numerator or denominator. Then we obtain the well-known *Artin map*

$$I_{\mathfrak{m}} \to \mathrm{Gal}(M/K)$$

as the unique homomorphism sending an unramified prime ideal to its Frobenius element. (In the function field case, note that since all infinite places are completely split in M/K, this map is induced by the Artin map on divisors.) Write $H < I_{\mathfrak{m}}$ for the kernel of this map.

By the Chebotarev Density Theorem, the set of prime ideals (excluding those at infinity and ramified ones) mapping to a given element of $\mathrm{Gal}(M/K)$—put otherwise, in a given coset in $I_\mathfrak{m}/H$—has density

$$\frac{1}{|\mathrm{Gal}(M/K)|} = \frac{1}{|I_\mathfrak{m}/H|} = l^{-k}.$$

(Throughout, it does not matter whether we choose natural or Dirichlet density.)

By class field theory—see e.g. [Lan70, X, §2] for number fields and [Ros02, Theorem 9.23] for function fields—there exists a modulus or cycle $\mathfrak{m} = \sum_\mathfrak{p} n_\mathfrak{p}\mathfrak{p}$, a formal sum of places of K ramified in M with $n_\mathfrak{p} \geq 0$, such that H contains the subgroup $P_\mathfrak{m} = \{(a) \colon a \in U_\mathfrak{m}\}$, where

$$U_\mathfrak{m} = \{a \in K^\times \colon v_\mathfrak{p}(a-1) \geq n_\mathfrak{p} \text{ for all ramified } \mathfrak{p}\}$$

and (a) denotes the principal fractional ideal generated by a. The quotient group $I_\mathfrak{m}/P_\mathfrak{m}$, a *generalised ideal class group*, is finite.

Now choose subextensions $M_1, \ldots, M_k$ which generate M as their compositum and which have $\mathrm{Gal}(M_i/K) \cong \mathbb{Z}/l\mathbb{Z}$. Furthermore, fix a generator σ_i of $\mathrm{Gal}(M_i/K)$ for each i.

In the next section, we will work with cyclic central simple algebras (M_i, σ_i, b) for suitable $b \in K$, see Section 2.3.1.

We conclude this section with two technical lemmas needed in the proof of Proposition 5.2.5.

Lemma 5.1.3. *Let $a \in K^\times$ such that $(a) \in I_\mathfrak{m}$ and $(a) \notin H$. Then there exist a place $\mathfrak{p} \notin \Sigma_\infty$ and an M_i such that the algebra (M_i, σ_i, a) is not split at $\mathfrak{p}$, and $a \notin \mathcal{O}_\mathfrak{p}^\times$.*

Proof. The fractional ideal (a) of $\mathcal{O}_K$ factors as a product of prime ideals of K unramified in M and not in Σ_∞. The group $I_\mathfrak{m}/H \cong \mathrm{Gal}(M/K) \cong (\mathbb{Z}/l\mathbb{Z})^k$ has exponent l, hence there exists a prime ideal $\mathfrak{p} \notin H$ that occurs in (a) with multiplicity not divisible by l since $(a) \notin H$.

The prime $\mathfrak{p}$ is not completely split in M since $\mathfrak{p} \notin H$, so there exists some M_i in which $\mathfrak{p}$ is inert, i.e. the local extension $M_iK_\mathfrak{p}/K_\mathfrak{p}$ is unramified of degree l. Therefore the group of local norms

$$\mathrm{N}_{M_iK_\mathfrak{p}/K_\mathfrak{p}}((M_iK_\mathfrak{p})^\times) \subseteq K_\mathfrak{p}^\times$$

consists only of elements of l-divisible valuation, since the norm of an element of $M_iK_\mathfrak{p}$ is the product of its Galois conjugates; thus a is not a local norm and therefore (M_i, σ_i, a) is not split at $\mathfrak{p}$ by Proposition 2.3.9. □

Lemma 5.1.4. *Let $P \subset \Sigma \setminus \Sigma_\infty$ be a set of places of density at least $\frac{1}{n!}$. Then there exists $a \in K^\times$ such that $(a) \in I_\mathfrak{m}$, $(a) \notin H$ and all places $\mathfrak{p} \in \Sigma \setminus \Sigma_\infty$ with $a \notin \mathcal{O}_\mathfrak{p}^\times$ are in P.*

Proof. We may remove the finitely many places ramified in M/K from P without affecting the hypotheses.

The set P has density at least $\frac{1}{n!} > |\mathrm{Cl}(\mathcal{O}_K)|/|I_\mathfrak{m}/H|$. Since the set of prime ideals in each coset in $I_\mathfrak{m}/H$ has density $1/|I_\mathfrak{m}/H|$ as noted above, P contains prime ideals from at least $|\mathrm{Cl}(\mathcal{O}_K)| + 1$ different cosets; thus we may pick $\mathfrak{p}, \mathfrak{p}' \in P$ in different classes in $I_\mathfrak{m}/H$ and in the same class in $\mathrm{Cl}(\mathcal{O}_K)$.

Now $\mathfrak{p}\mathfrak{p}'^{-1}$ is a principal fractional ideal of $\mathcal{O}_K$; pick a generator a. By construction, this generator satisfies all of the requirements. □

5.2 detecting extensions of global fields

In this section we find an existential sentence that distinguishes the fixed global field K from its finite extensions of degree n, see Theorem 5.2.11.

Definition 5.2.1. *Let L/K be an extension of degree n and $l \mid n$ a prime number. A prime ideal $\mathfrak{p}$ of K is* l-good *(for L) if it is unramified in L and for all prime ideals $\mathfrak{q}$ of L above $\mathfrak{p}$ the inertia degree $[\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$ is divisible by l.*

The prime number $l \mid n$ is admissible *(for L) if either*

- *L/K is separable and the set of l-good prime ideals of K has density at least $\frac{1}{n!}$, or*
- *L/K is inseparable and $l = \operatorname{char} K$.*

Lemma 5.2.2. *For every L/K of degree n there exists an admissible $l \mid n$.*

Proof. If L/K is inseparable, then by basic field theory $\operatorname{char} K \mid n$, so $l = \operatorname{char} K$ is admissible. Let us now assume that L/K is separable.

Let L'/K be the Galois hull of L/K, $G = \operatorname{Gal}(L'/K)$, $H = \operatorname{Gal}(L'/L) \lneq G$. Then $|G| \leq n!$. Let $g \in G$ of prime power order l^r with $l \mid n$ such that no conjugate of g is in H. Existence of such g is assured by Theorem 5.2.3 below: An element g has no conjugate in H if and only if g has no fixed point in the left multiplication action of G on $\Omega = G/H$. If $\mathfrak{q}$ is a prime ideal of L' above an unramified ideal $\mathfrak{p}$ of K such that $\operatorname{Frob}(\mathfrak{q}/\mathfrak{p})$ is conjugate to g, then the inertia degree $f(\mathfrak{q}/\mathfrak{p})$ is equal to $\operatorname{ord}(g) = l^r$, so for $\mathfrak{q}' = \mathfrak{q} \cap L$ we have $f(\mathfrak{q}'/\mathfrak{p}) \neq 1$ since $\operatorname{Frob}(\mathfrak{q}/\mathfrak{p}) \notin H$, and $f(\mathfrak{q}'/\mathfrak{p}) \mid l^r$, hence $l \mid f(\mathfrak{q}'/\mathfrak{p})$. The set of such prime ideals $\mathfrak{p}$ has density at least $\frac{1}{n!}$ by the Chebotarev Density Theorem. □

Theorem 5.2.3 (Fein-Kantor-Schacher)**.** *Let G be a finite group acting transitively on a set Ω with $|\Omega| > 1$. Then there exists an element $g \in G$ of prime power order l^r, with $l \mid |\Omega|$, acting without fixed points on Ω.*

Remark 5.2.4. The paper [FKS81], in which this theorem was first proved, used it for a similar purpose as we do: classifying relative Brauer groups $\mathrm{Br}(L/K)$ of global fields. There appears to be no known proof of this theorem that does not use the classification of finite simple groups.

The following is the central technical result of this section. It uses the existentially definable sets T from Definition 2.2.14. We also use the extension M/K and its subextensions M_i chosen in the last section, depending on l.

Proposition 5.2.5. *For a global field L/K consider the following statement, which we call $(\dagger)^l_{L/K}$:*

> *There exists an element $a \in K^\times$ such that $(a) \in I_\mathfrak{m}$, $(a) \notin H$ and for all i both a and $\frac{1}{a}$ are in $T((M_i, \sigma_i, a) \otimes_K L/L)$.*

Then this statement is false for $L = K$, and it is true if L/K is an extension of degree n with l admissible.

For the case of inseparable extensions, we need the following lemma:

Lemma 5.2.6. *Assume K is global field of characteristic $p > 0$ and L/K is a finite inseparable extension. Then any central simple algebra A/K of degree p is split by L.*

Proof. By replacing K with the maximal separable subextension of L/K, we may assume that L/K is a purely inseparable proper extension. Since $[K^{1/p}\colon K] = p$, we now necessarily have $L \supseteq K^{1/p}$. Hence the result follows from Lemma 5.2.7 below. □

Lemma 5.2.7 ([GS17, Lemma 9.1.7])**.** *Let F be a field of characteristic $p > 0$ and A/F be a central simple algebra of degree p. Then A is split by the field $F^{1/p}$.*

Proof of Proposition 5.2.5. Let us first consider the case $L = K$, and assume there were a as in the statement. By Lemma 5.1.3 there exist an M_i and a place $\mathfrak{p} \notin \Sigma_\infty$ such that the algebra (M_i, σ_i, a) is not split at $\mathfrak{p}$ and $a \notin \mathcal{O}_\mathfrak{p}^\times$. Hence $a \notin T((M_i, \sigma_i, a))^\times$ by Theorem 2.2.15 in contradiction to our assumption on a.

Now consider the case of a proper extension L/K of degree n with l admissible. If L/K is inseparable and $l = \operatorname{char} K$, then Lemma 5.2.6 implies that all algebras (M_i, σ_i, a) are split over L, so any choice of a will do as long as $(a) \in I_\mathfrak{m}$, $(a) \notin H$. Such a is afforded by Lemma 5.1.4.

If L/K is separable, let $P \subseteq \Sigma \setminus \Sigma_\infty$ be the set of l-good primes; it has density at least $\frac{1}{n!}$. Therefore Lemma 5.1.4 is applicable, so we obtain $a \in K^\times$ such that $(a) \in I_\mathfrak{m}$, $(a) \notin H$ and all places $\mathfrak{p} \in \Sigma \setminus \Sigma_\infty$ such that $a \notin \mathcal{O}_\mathfrak{p}^\times$ are in P. We claim that a is as desired, so we must show that

$$a, \frac{1}{a} \in T((M_i, \sigma_i, a) \otimes_K L/L)$$

for all i. The algebras $(M_i, \sigma_i, a) \otimes_K L$ split at all infinite places of L by construction of the M_i, so by Theorem 2.2.15 it suffices to show that they

split at all primes $\mathfrak{q}$ of L above primes $\mathfrak{p} \in \Sigma \setminus \Sigma_\infty$ with $a \notin \mathcal{O}_\mathfrak{p}^\times$. But all those $\mathfrak{p}$ are l-good, so $l \mid [L_\mathfrak{q} \colon K_\mathfrak{p}]$ and hence $L_\mathfrak{q}$ does split all (M_i, σ_i, a) by the theory of central simple algebras over local fields. □

Remark 5.2.8. The element a in the statement $(\dagger)^l_{L/K}$ can be multiplied by an arbitrary element of $\mathcal{O}_K^\times$, i.e. the statement is really one about the principal ideal (a). To see this, observe that T is invariant under multiplication by $\mathcal{O}_K^\times$, and the local splitting behaviour of (M_i, σ_i, a) at a prime $\mathfrak{p}$ unramified in M/K only depends on the valuation $v_\mathfrak{p}(a)$, since the local norm group contains the local unit group for unramified extensions.

For each class of ideals in the set $(I_\mathfrak{m}/P_\mathfrak{m}) \setminus (H/P_\mathfrak{m})$ that contains a principal (fractional) ideal, fix a representative principal ideal (a_j) and a generator $a_j \in K^\times$ thereof. This is a finite list since $I_\mathfrak{m}/P_\mathfrak{m}$ is finite. Thus every principal ideal in $I_\mathfrak{m} \setminus H$ has the form $(a_j b)$ for some $b \in U_\mathfrak{m}$ and one of the a_j. Therefore, by Remark 5.2.8, we may rephrase the statement $(\dagger)^l_{L/K}$ as follows:

> For some a_j, there exists a $b \in U_\mathfrak{m}$ such that for all i we have $a_j b, \frac{1}{a_j b} \in T((M_i, \sigma_i, a_j b) \otimes_K L/L)$.

This statement is of a very specific form, namely positive existential in a certain first-order language of pairs of rings. In a more elementary fashion, this means that is equivalent to a certain system of polynomial equations $G_r(x_1, \ldots, x_s, y_1, \ldots, y_t) = 0$ having a solution in $K^s \times L^t$.

Definition 5.2.9. *The* language of pairs of rings *is the two-sorted first-order language where both sorts have symbols* $+, \cdot, 0, 1$*, with an additional unary*

function symbol from the second to the first sort. The intended interpretation is as two rings S, R with a ring homomorphism $f\colon R \to S$. We write (S, R, f) for the associated structure, or simply (S, R) when $S \supseteq R$ and f is the inclusion map.

This differs from the language used in [Dit18, Lemma 4.7], where the ring language with an additional unary predicate for a distinguished subring was used. Both languages are equivalent for modelling pairs of rings as long as the ring homomorphism $f\colon R \to S$ is injective; however, we will later make use of the case where S is the zero ring in Section 5.4 and hence adjust the language.

Lemma 5.2.10. *There exists a positive existential sentence $\psi_{K,n,l}$ in the language of pairs of rings such that the condition $(\dagger)^l_{L/K}$ from Proposition 5.2.5 is expressed precisely by $(L, K) \models \psi_{K,n,l}$. Here $\psi_{K,n,l}$ may involve parameters from K.*

Proof. We use the equivalent form of $(\dagger)^l_{L/K}$ introduced above. This statement is straightforwardly written as

$$\bigvee_j \exists b \in K \Big(b \in U_{\mathfrak{m}} \wedge \bigwedge_i a_j b, \frac{1}{a_j b} \in T((M_i, \sigma_i, a_j b) \otimes_K L) \Big).$$

Here $b \in U_{\mathfrak{m}}$ can be phrased as a positive existential statement since $U_{\mathfrak{m}}$ is a positively existentially definable subset of K by Corollary 2.3.6, and $a_j b \in T((M_i, \sigma_i, a_j b) \otimes_K L)$ can likewise be expressed as a positive existential condition in L by Observation 2.3.10. Hence we can write this as a positive existential sentence in the language of pairs of rings. □

Theorem 5.2.11. *There exists a positive existential sentence $\psi_{K,n}$ in the language of pairs of rings, with parameters from the global field K, such that $(K,K) \models \neg\psi_{K,n}$, but $(L,K) \models \psi_{K,n}$ for all extensions L/K of degree n.*

Proof. Let $\psi_{K,n} = \bigvee_{l|n} \psi_{K,n,l}$. Now the statement is an immediate consequence of Proposition 5.2.5, Lemma 5.2.10 and Lemma 5.2.2. □

5.3 PROOF OF THE MAIN DEFINABILITY RESULTS

We can strengthen Theorem 5.2.11 to the following result.

Theorem 5.3.1. *There exists a positive existential sentence $\varphi_{K,n}$ in the language of pairs of rings, with parameters from the global field K, such that for any commutative unital K-algebra A/K with $\dim_K A \leq n$ we have $(A,K) \models \varphi_{K,n}$ if and only if there is no K-homomorphism $A \to K$.*

The proof is a variant of the proof of Proposition 2.1.2.

Proof. Let $\psi = \bigwedge_{1<m\leq n} \psi_{K,m}$, where $\psi_{K,n}$ is the sentence from Theorem 5.2.11; this is positive existential.

Let us first find a positive existential sentence ψ' with the desired property restricted to local algebras A/K of dimension less or equal to n. Since a homomorphism $A \to K$ factors through the residue field of A, and the residue field is positively existentially interpretable in A by the second point of Lemma 2.1.4, this is easily achieved by constructing $(A,K) \models \psi'$ to be equivalent to $(A/\mathfrak{m},K) \models \psi$. (For the same reasons as in the proof of Lemma 2.1.3, we may actually choose $\psi' = \psi$ in case K is perfect, i.e. a number field.)

Now let A be not necessarily local. We claim that there is no K-homomorphism $A \to K$ if and only if there exist elements $e_1, \dots, e_n \in A$ with the following properties:

- The e_i are idempotents, i.e. $e_i^2 = e_i$;
- the e_i are pairwise orthogonal, i.e. $e_i e_j = 0$ for $i \neq j$;
- $e_1 + \cdots + e_n = 1$;
- for each i, $(A/(1-e_i)A, K) \models \psi'$.

From this claim, the existence of a suitable sentence follows, since existence of such e_i is expressed by an existential statement, as $(A/(1-e_i)A, K)$ is positively existentially interpretable in (A, K).

Let us now prove the claim. Assume first that there are elements e_i as required, and also (for contradiction) that there is a K-homomorphism $f\colon A \to K$. Since f maps idempotents to idempotents, but the only idempotents in K are 0 and 1, there exists some e_i such that $f(e_i) = 1$. Then f factors through $A/(1-e_i)A$, hence (K, K) is a quotient of $(A/(1-e_i)A, K)$. Since the formula ψ' is preserved under homomorphisms, this implies $(K, K) \models \psi'$, but this contradicts the construction of ψ'.

For the other direction, assume that there is no K-homomorphism $A \to K$. As a finite K-algebra, A factors as a product of local K-algebras, so we may assume $A = A_1 \times \cdots \times A_k$, where each A_i is a local K-algebra of dimension $\leq n$ and $k \leq n$. Set $e_1 = (1, 0, \dots, 0)$, $e_2 = (0, 1, 0, \dots, 0)$, $\dots$, $e_k = (0, \dots, 0, 1)$, $e_{k+1}, \dots, e_n = 0$. Then clearly the e_i are pairwise orthogonal idempotents summing up to 1. For the last condition, observe

that for $i \leq k$, there is no K-homomorphism $A_i \to K$, and so $(A_i, K) \models \psi'$. Since $(A_i, K) \cong (A/(1-e_i)A, K)$, this proves the claim. □

As a special case, we may deduce existential definability of the condition that a polynomial in one variable has no root.

Theorem 5.3.2. *There exists an existential first-order formula $\varphi_{K,n}$ with n free variables, in the language of rings with parameters from the global field K, such that $K \models \varphi_{K,n}(a_0, \ldots, a_{n-1})$ if and only if the polynomial $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ has no root in K.*

Proof. The polynomial f has a root in K if and only if it has a linear factor, which is the case if and only if there exists a K-homomorphism from $K[X]/(f)$ to K. Since $K[X]/(f)$ is quantifier-freely interpretable and of dimension n over K, Theorem 5.3.1 proves the claim. □

As an immediate corollary we obtain:

Corollary 5.3.3. *For every global field K and $n > 0$, the set of non-n-th powers in K is existentially definable.*

This was previously proven in [CTG15] in the case of a number field.

Corollary 5.3.4. *Let $K^{**} \supseteq K^*$ be any two fields which are both elementary extensions of the global field K. Then K^* is relatively algebraically closed in K^{**}.*

Proof. Theorem 5.3.2 is also true in K^* and K^{**}—with the same formulae $\varphi_{K,n}$—by first-order transfer. Let $f = X^n + a_{n-1}X^{n-1} + \cdots a_0 \in K^*[X]$ be a polynomial without a root in K^*. Then $K^* \models \varphi_{K,n}(\mathbf{a})$, therefore $K^{**} \models \varphi_{K,n}(\mathbf{a})$ (since $\varphi_{K,n}$ is an existential formula), whence f does not have a root in K^{**} either. □

This answers Question 25 in [Koe16].

Corollary 5.3.5. *There exists a diophantine criterion for a polynomial over the global field K in an arbitrary number of variables to be irreducible. More formally, fix $r, d \geq 0$. Then the set*

$$\{(a_{i_1,\ldots,i_r})_{0\leq i_1,\ldots,i_r\leq d} \in K^{(d+1)^r} : \sum_{0\leq i_1,\ldots,i_r\leq d} a_{i_1,\ldots,i_r} X_1^{i_1}\cdots X_r^{i_r} \in K[X_1,\ldots,X_r] \text{ is irreducible}\}$$

is existentially definable with parameters in K.

Proof. Irreducibility can be expressed by a universal first-order formula, since f being irreducible means that for all pairs of polynomials of strictly smaller total degree f is not equal to their product. By the Łoś-Tarski Preservation Theorem of model theory ([Hod97, Corollary 5.4.5]), this property is expressible by an existential first-order formula with parameters if and only if for every $K^{**} \supseteq K^*$ with $K^{**}, K^* \succeq K$ every irreducible polynomial over K^* remains irreducible over K^{**}.

This condition is a simple consequence of relative algebraic closedness: Consider an irreducible polynomial $f \in K^*[\mathbf{X}]$, and assume without loss of generality (after affine change of coordinates and rescaling) that f has constant coefficient 1. Then f factors into irreducible factors $f_1, \ldots, f_n \in \overline{K^*}[\mathbf{X}]$, each with constant coefficient 1, and these factors remain irreducible in $\overline{K^{**}}[\mathbf{X}]$. If f factors non-trivially as $g \cdot h$ in $K^{**}[\mathbf{X}]$, we may assume after rescaling that both g and h have constant coefficient 1, so g, h can be factored into products of the f_i in $\overline{K^{**}}[\mathbf{X}]$ since this is a unique factorisation domain. But then the coefficients of g and h are both in $\overline{K^*}$ and in K^{**}, so they are in K^*, contradicting f being irreducible. □

Remark 5.3.6. We stated Theorems 5.2.11, 5.3.1, 5.3.2 and Corollary 5.3.5 for the global field K fixed at the very beginning of this chapter. However, inspection of the proofs shows that we have used no more facts about global fields than Theorem 5.2.11 in the proof of the subsequent results.

On the other hand, if over some given arbitrary field K irreducibility of polynomials in one variable is existentially definable (as in Corollary 5.3.5), then automatically absence of roots is existentially definable (as in Theorem 5.3.2), since a polynomial in one variable has no root if and only if there exists a factorisation into non-linear irreducibles. Furthermore, this definability in turn implies that there exists a sentence as in Theorem 5.2.11, since given a proper field extension L/K of degree $\leq n$ there exists a monic polynomial of degree $\leq n$ in $K[X]$ with a root in L but no root in K, which is now an existentially definable condition.

This shows, that for an arbitrary field K, the statements from Theorems 5.2.11, 5.3.1, 5.3.2 and Corollary 5.3.5 are all equivalent.

One may ask for which other fields our theorems are true. This is obviously the case in any model-complete field, in particular all local fields of characteristic zero. We also have the following non-example.

Example 5.3.7 (After a suggestion of Sylvy Anscombe). Consider a field $K = K_0(t_1, t_2, \dots)$ obtained by adjoining countably many transcendental elements to an arbitrary base field K_0. For any n we have the field $K^{(n)} = K(\sqrt{t_n})$, which is isomorphic to K via $f_n \colon K \to K^{(n)}$, fixing K_0, sending t_n to $\sqrt{t_n}$ and t_m to t_m for $m \neq n$. Assume that $\varphi(x)$ is an existential formula with parameters in a finite set A such that $K \models \varphi(a)$ if and only if a is not a square in K. For any sufficiently large n, f_n will fix

A. However, then $K \models \varphi(t_n)$ implies $K^{(n)} \models \varphi(t_n)$ by existential transfer, hence $K \models \varphi(f_n^{-1}(t_n))$ by pulling back via the isomorphism f_n, but this means $K \models \varphi(t_n^2)$. This contradicts the defining property of φ. Hence Corollary 5.3.3 is not true in K.

5.4 geometric consequences

In this section, we prove the following geometric version of the results of the last section.

Theorem 5.4.1. *Let K be a global field and $f\colon W \to V$ be a quasifinite morphism of K-varieties. Then the set $V(K) \setminus f(W(K))$ is diophantine, i.e. there is a K-variety W' and a morphism $g\colon W' \to V$ such that $V(K)$ is the disjoint union of $f(W(K))$ and $g(W'(K))$.*

I would like to thank Laurent Moret-Bailly, who originally communicated to me a derivation of the theorem from the results of the previous section; the more general results here are in some ways inspired by that proof.

For the remainder of this section, let F be an arbitrary field and φ a positive existential sentence in the language of pairs of rings, with parameters from F. We assume that the reader has some familiarity with basic scheme-theoretic algebraic geometry.

Theorem 5.4.1 will follow from Theorem 5.3.1 using the following general result.

Theorem 5.4.2. *Let $f\colon W \to V$ be a quasifinite morphism of F-varieties, so for every $x \in V(F)$, the scheme-theoretic preimage $f^{-1}(x)$ is an affine F-scheme,*

say $f^{-1}(x) = \operatorname{Spec}(P_x)$. *The set of* $x \in V(F)$ *such that* $(P_x, F) \models \varphi$ *is diophantine.*

Recall here that the scheme-theoretic preimage is defined by the condition that $f^{-1}(x) \to W$ is the pullback of $x\colon \operatorname{Spec} F \to V$ along $f\colon W \to V$. Note that it may well happen that $f^{-1}(x)$ is empty, i.e. $P_x = 0$. This necessitates using the two-sorted language for pairs of rings.

The proof strategy is to reduce to the case of affine schemes V and W with a finite free morphism between them, i.e. $V = \operatorname{Spec} R$, $W = \operatorname{Spec} S$ with a morphism $f\colon W \to V$ corresponding to a homomorphism of rings $R \to S$ that makes S isomorphic as an R-module to R^n for some n.

In this section, we use geometric language as far as possible, and hence begin by interpreting φ geometrically.

Lemma 5.4.3. *There exists a morphism* $A \to B$ *of affine finite type* F*-schemes with the following property. For every affine* F*-scheme* $C = \operatorname{Spec} R$, $(R, F) \models \varphi$ *if and only if there exist* F*-morphisms* $C \to A$, $\operatorname{Spec} F \to B$ *making the following diagram commute.*

$$\begin{array}{ccc} C & \longrightarrow & A \\ \downarrow & & \downarrow \\ \operatorname{Spec} F & \longrightarrow & B \end{array} \tag{5.1}$$

Proof. As φ is equivalent to a sentence in disjunctive normal form, we may assume that φ is a disjunction of positive primitive sentences. However, if $\varphi = \varphi_1 \vee \varphi_2$, then schemes A, B for φ can be built as a disjoint union of appropriate schemes for the φ_i. Hence assume that φ is positive primitive, i.e. $(S, R, f) \models \varphi$ expresses $\exists x_1, \ldots, x_n \in S \exists y_1, \ldots, y_m \in$

$R\Big(\bigwedge_i p_i(\overline{x}, f(\overline{y})) = 0 \wedge \bigwedge_j q_j(\overline{y}) = 0\Big)$ for some polynomials p_i, q_j with coefficients in F.

Let

$$A = \operatorname{Spec}(F[X_1, \ldots, X_n, Y_1, \ldots, Y_m]/\mathfrak{p}),$$
$$B = \operatorname{Spec}(F[Y_1, \ldots, Y_m]/\mathfrak{q}),$$

where $\mathfrak{q}$ is the ideal generated by the q_j, and $\mathfrak{p}$ is the ideal generated by the p_i and $\mathfrak{q}$, and consider the map $A \to B$ corresponding to the natural map of rings in the opposite direction.

Now compatible maps $C \to A$, $\operatorname{Spec} F \to B$ correspond to a choice $y_1, \ldots, y_m \in F$, $x_1, \ldots, x_n \in R$ such that $p_i(\overline{x}, \overline{y}) = 0$ and $q_j(\overline{y}) = 0$ for all i and j, as desired. □

We will now work in the situation of a given morphism $f\colon W \to V$. A point $x \in V(F)$—i.e. a morphism $x\colon \operatorname{Spec} F \to V$—turns $\operatorname{Spec} F$ into a V-scheme, so we can speak about morphisms of V-schemes.

Lemma 5.4.4. *Let $f\colon W \to V$ be as in Theorem 5.4.2. Then an F-point $x\colon \operatorname{Spec} F \to V$ satisfies the condition $(P_x, F) \models \varphi$ from the theorem if and only if there exists a morphism $y\colon \operatorname{Spec} F \to B \times_F V$ of V-schemes and a morphism $z\colon \operatorname{Spec} F \times_V W \to A \times_F W$ of W-schemes such that the map*

$$\operatorname{Spec} F \times_V W \to A \times_F W \to B \times_F W$$

agrees with the base change $y_W\colon \operatorname{Spec} F \times_V W \to B \times_F W$.

Proof. This is merely a restatement of Lemma 5.4.3.

A V-morphism $y\colon \operatorname{Spec} F \to B \times_F V$ is given by the data of an F-morphism $y'\colon \operatorname{Spec} F \to B$, and likewise a W-morphism $z\colon \operatorname{Spec} F \times_V W \to A \times_F W$ is given by the data of an F-morphism $z\colon \operatorname{Spec} F \times_V W \to A$. The base change $y_W\colon \operatorname{Spec} F \times_V W \to B \times_F W$ is then given by y' on the first component and the identity on the second component, so we verify that commutativity of diagram (5.1) with horizontal morphisms z' and y' is equivalent to y_W factoring as z followed by the map $A \times_F W \to B \times_F W$ induced by $A \to B$. This proves the claim. □

We can now prove the theorem in the finite free affine situation. While one could present this proof in very explicit algebraic way, we work in terms of the *Weil restriction*, as presented in for instance [BLR90, Section 7.6].

Definition 5.4.5. *Let $f\colon W \to V$ be a morphism of schemes and X a W-scheme. Consider the contravariant functor $\operatorname{Hom}_W(\cdot \times_V W, X)$ sending a V-scheme S to the set of W-morphisms $S \times_V W \to X$. This is called the* Weil restriction functor.

If this functor is represented by a V-scheme $\mathcal{R}(X)$, i.e. $\operatorname{Hom}_W(\cdot \times_V W, X)$ is naturally isomorphic to $\operatorname{Hom}_V(\cdot, \mathcal{R}(X))$, then we call $\mathcal{R}(X)$ the Weil restriction of X along f*; in particular, we say that the Weil restriction exists.*

In the situation of the definition, the V-points of $\mathcal{R}(X)$ are in bijection to the W-points of X; in this way, the Weil restriction generalises the standard construction of seeing a complex variety of dimension n as a real variety of dimension $2n$.

Proposition 5.4.6. *The Weil restriction $\mathcal{R}(X)$ exists when f is a finite free morphism of affine schemes and X is affine of finite type over W.*

Proof. This is easily proved by hand, by copying the usual technique of restriction of scalars from $\mathbb{C}$ to $\mathbb{R}$ mentioned above. However, it also follows from the far more general existence result for the Weil restriction in [BLR90, Theorem 7.6/4]. □

If $X \to Y$ is a morphism of W-schemes and the Weil restrictions $\mathcal{R}(X)$ and $\mathcal{R}(Y)$ exist, then we obtain in a natural way a morphism $\mathcal{R}(X) \to \mathcal{R}(Y)$ of V-schemes: It is uniquely determined (by the Yoneda Lemma) by the condition that for every V-scheme S the map $X(S \times_V W) \cong \mathcal{R}(X)(S) \to \mathcal{R}(Y)(S) \cong Y(S \times_V W)$ agrees with the one induced by the given morphism $X \to Y$.

Lemma 5.4.7. *Theorem 5.4.2 is true in the situation where f is a finite free morphism of affine schemes.*

With the stronger existence results for the Weil restriction cited above, we could weaken the hypotheses to f being finite and locally free.

Proof. Let A'/V be the Weil restriction of $A \times_F W$ along $f\colon W \to V$, and B'/V the Weil restriction of $B \times_F W$ along f. The F-morphism $A \to B$ induces a W-morphism $A \times_F W \to B \times_F W$ and hence a V-morphism $A' \to B'$. There is a morphism $B \times_F V \to B'$ over V corresponding to the identity $B \times_F W \to B \times_F W$. We construct our variety W' as $A' \times_{B'} (B \times_F V)$, endowed with the morphism $W' \to V$ coming from $B' \to V$.

Fix a point $x\colon \operatorname{Spec} F \to V$, and write $f^{-1}(x) \cong \operatorname{Spec} P_x$ as usual. We have to prove that $(P_x, F) \models \varphi$ if and only if there exists a point $x'\colon \operatorname{Spec} F \to W'$ mapping to x.

By the definition of W', such a point x' corresponds to a pair of morphisms $z\colon \operatorname{Spec} F \to A'$ and $y\colon \operatorname{Spec} F \to B \times_F V$ inducing the same morphism $\operatorname{Spec} F \to B'$, which furthermore has to map to x.

Under the universal property of the Weil restriction, z corresponds to some W-morphism $\bar{z}\colon \operatorname{Spec} F \times_V W \to A \times_F W$, and commutativity of

$$\begin{array}{ccc} \operatorname{Spec} F & \xrightarrow{z} & A' \\ \downarrow{\scriptstyle y} & & \downarrow \\ B \times_F V & \longrightarrow & B' \end{array}$$

is equivalent, by applying the defining property of the Weil restriction to the two morphisms $\operatorname{Spec} F \to A' \to B'$ and $\operatorname{Spec} F \to B \times_F V \to B'$, to commutativity of the following diagram, where y_W is the base change of y via $W \to V$:

$$\begin{array}{ccc} \operatorname{Spec} F \times_V W & \xrightarrow{\bar{z}} & A \times_F W \\ \downarrow{\scriptstyle y_W} & & \downarrow \\ B \times_F W & \xrightarrow{=} & B \times_F W \end{array}$$

(This is because the morphism $\operatorname{Spec} F \to A' \to B'$ corresponds to the morphism

$$\operatorname{Spec} F \times_V W \to A \times_F W \to B \times_F W$$

by the defining property of $A' \to B'$, and $\operatorname{Spec} F \xrightarrow{y} B \times_F V \to B'$ corresponds to

$$\operatorname{Spec} F \times_V W \xrightarrow{y_W} B \times_F W = B \times_F W$$

by the definition of $B \times_F V \to B'$ and naturality of the Weil restriction isomorphism $\mathrm{Hom}_V(\cdot, B') \cong \mathrm{Hom}_W(\cdot \times_V W, B \times_F W)$.)

But existence of such y and $\bar{z}$ is precisely the condition for $(P_x, F) \models \varphi$ given in Lemma 5.4.4. □

Lemma 5.4.8. *Let $f\colon W \to V$ be a quasifinite morphism of F-varieties. Then there exists a non-empty open subvariety $V_0 \subseteq V$ such that the pullback (restriction) $f\colon f^{-1}(V_0) \to V_0$ is a finite free morphism of affine varieties.*

Proof. One can find a dense open $U \subseteq V$ such that the pulled back morphism $f\colon f^{-1}(U) \to U$ is finite ([Sta18, Tag 03I1]).

By Generic Freeness, there exists a dense open subvariety $U' \subseteq U$ such that the pullback $f\colon f^{-1}(U') \to U'$ is a free morphism. (For a reference, see for instance [Sta18, Tag 052B] for obtaining a dense open subvariety over which the morphism is flat ("Generic Flatness"), and then Tag 02KB loc. cit. for the fact that finite flat morphisms of varieties are locally free, so we can obtain a free morphism after choosing a further open subset.)

Now let V_0 be a non-empty affine open subvariety of U'. Since free morphisms are affine, the preimage $f^{-1}(V_0)$ will be an affine subvariety of W. □

We can now easily finish the proof of Theorem 5.4.2.

Proof of Theorem 5.4.2. By Lemma 5.4.8 we can obtain an open subscheme $V_0 \subseteq V$ such that for the restriction $f\colon f^{-1}(V_0) \to V_0$ the theorem holds by Lemma 5.4.7, so we obtain an F-variety W_0' and a morphism $W_0' \to V_0$ such that the image of $W_0'(F)$ in $V_0(F)$ consists of precisely those points

whose f-fibre satisfies φ. Write V_0' for the closed subvariety of V which is the complement of V_0. By continuing inductively with the restriction $f\colon f^{-1}(V_0') \to V_0'$, we obtain a sequence of disjoint open subschemes $V_0, \dots, V_k \subseteq V$ and morphisms $W_0' \to V_0, \dots, W_k' \to V_k$; since V is a noetherian topological space and therefore all decreasing chains of closed subschemes stabilise, this process terminates after finitely many steps k, so the set $V(F)$ is the disjoint union of the $V_i(F)$.

Now we let W' be the disjoint union of the varieties W_i', endowed with the morphism $W' \to V$ given by gluing the $W_i' \to V_i$. This is as desired. □

Proof of Theorem 5.4.1. By Lemma 5.4.8 we can find a dense open affine subvariety V_0 of V such that $f|_{f^{-1}(V_0)}$ is finite free, say $V_0 = \operatorname{Spec} R$, $f^{-1}(V_0) = \operatorname{Spec} S$, with $S \cong R^n$ as R-modules. This implies in particular that for every $x \in V_0(F)$ the K-algebra P_x with $f^{-1}(x) = \operatorname{Spec}(P_x)$ is of K-dimension at most n.

Now the theorem follows for $f|_{f^{-1}(V_0)}$ by Theorem 5.4.2 and Theorem 5.3.1, since a point $x \in V_0(K)$ has a K-rational preimage in W if and only if P_x has a K-homomorphism to K. We can extend to all of f by the same inductive argument as in the proof of Theorem 5.4.2. □

THE MODEL THEORY OF ABSOLUTE GALOIS GROUPS

In the model theory of fields, the task naturally arises to find a suitable first-order setting for the study of absolute Galois groups. In particular, this is important in the investigation of properties of pseudo-algebraically closed (PAC) fields.

In this chapter, which does not depend on any of the previous chapters, we give a new framework for studying the model theory of absolute Galois groups, to be used in Chapter 7.

From Section 6.2 onwards, we will assume that the reader is familiar with basic notions from category theory, notably limits and colimits, functors preserving these, natural isomorphism of functors, and equivalence of categories.

6.1 THE CHERLIN–VAN DEN DRIES–MACINTYRE FORMALISM

The following formalism for profinite groups was first suggested in the unpublished article [CvdDM82], but underwent several minor modifications later. We follow the exposition in [Cha02, Appendix 1]. For the convenience of the reader, we give the full definitions.

To a profinite group G one assigns a multi-sorted structure $S(G)$, the *complete inverse system associated to* G. Its sorts are indexed by positive integers, and the elements of sort n are precisely the cosets $gN \in G/N$, where $N \lhd G$ is an open normal subgroup of index $\leq n$. Observe that the sorts are not disjoint, but nested; one could alternatively work with disjoint sorts and introduce function symbols identifying elements of distinct sorts, but we shall not do so here.

The language consists of two binary relations $\leq$ and C, as well as a ternary relation P; more precisely, each of these symbols stands for a family of relations across all sorts, but no confusion is likely to arise by suppressing this in the notation. In $S(G)$ these relations are interpreted in the following way.

- $gN \leq hM$ if and only if $N \subseteq M$;
- $C(gN, hM)$ if and only if $N \subseteq M$ and $gM = hM$, i.e. there is a projection $G/N \to G/M$ and it sends gN to hM;
- $P(g_1N_1, g_2N_2, g_3N_3)$ if and only if $N_1 = N_2 = N_3$ and $g_1g_2N_1 = g_3N_1$, i.e. P encodes the group structure on all the quotient groups.

It is not hard to see that the class of structures in this multi-sorted language—called the *language of inverse systems*—which arise as $S(G)$ for some profinite group G is first-order axiomatisable; an axiomatisation is given in loc. cit. For structures $S(G)$ arising in this way, the profinite group G can be recovered as the projective limit of the finite groups assembled in $S(G)$. This correspondence between profinite groups and multi-sorted structures respects morphisms in the following way: Epimorphisms of profinite groups $G \to H$ correspond bijectively to embeddings $S(H) \to S(G)$. Hence the assignment $G \mapsto S(G)$ is an equivalence of suitable categories.

Furthermore, given an epimorphism $G \to H$ we may expand $S(G)$ by constants for the embedded substructure $S(H)$. Given a second epimorphism $G' \to H$, it then makes sense to ask for $S(G)$ and $S(G')$ to

be elementarily equivalent *over* $S(H)$, i.e. in the language expanded by constants. Note, however, that there is no correspondence between arbitrary morphisms $G \to H$ and (not necessarily injective) homomorphisms $S(H) \to S(G)$.

Once this formalism for profinite groups is established, one can apply it to the study of absolute Galois groups of a field K, i.e. the profinite group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ where K^{sep} is a separable closure.

Theorem 6.1.1 (Cherlin–Van den Dries–Macintyre)**.** *Let K be a field.*

1. *If K is κ-saturated, then so is $S(\mathrm{G}_K)$.*
2. *Let L be a second field and E a common subfield of K and L such that K/E is regular, i.e. E is relatively algebraically closed in K and K/E is separable. If K is elementarily equivalent to L over E, then $S(\mathrm{G}_K)$ is elementarily equivalent to $S(\mathrm{G}_L)$ over $S(\mathrm{G}_E)$.*
3. *For every sentence φ in the language of inverse systems there is a sentence φ^* in the language of rings, depending only on φ, such that for any K we have $S(\mathrm{G}_K) \models \varphi$ if and only if $K \models \varphi^*$.*
4. *To a formula $\varphi(\overline{x})$ in the language of inverse systems there is a formula $\varphi^*(\overline{y}, \overline{z})$ in the language of fields such that for a tuple $\overline{a}$ of the right sorts in $S(\mathrm{G}_K)$ we have $S(\mathrm{G}_K), \overline{a} \models \varphi$ if and only if $K, \overline{b}, \overline{c} \models \varphi^*$, where $\overline{b}, \overline{c}$ are tuples in K coding the elements $\overline{a}$ of $S(\mathrm{G}_K)$ in a suitable way.*

We omit the details of the coding in the last point of the theorem; the essential point is that an element σ of a finite Galois group $\mathrm{Gal}(L/K)$ may be described by firstly giving an irreducible monic polynomial with

a root generating L/K, and secondly describing the action of σ on such a generator.

Proof. These were all proved in [CvdDM82]. All the points except for saturation are stated in [Cha02, Theorem 5.9], while saturation is a consequence of Proposition 5.5 and Theorem 5.8 ibid. □

Two observations are in order here. Firstly, observe that in the second point of the theorem, the assumption that K/E (and therefore L/E) be regular is necessary to even make the statement: We need the assumption of regularity (or rather relative algebraic closedness) for the restriction map $\mathrm{G}_K \to \mathrm{G}_E$ to be an epimorphism and therefore $S(\mathrm{G}_K)$ to be endowed with constants for elements of $S(\mathrm{G}_E)$. However, this assumption of regularity does not have any meaningful consequence for the content of the statement: Even without regularity the assumption that $K \equiv_E L$ implies that we may assume by amalgamation that K and L are both elementary subfields of a common overfield, so it follows that $K \equiv_{\mathrm{acl}(E)} L$, where $\mathrm{acl}(E)$ is the model-theoretic algebraic closure of E within the common overfield. It is now a standard fact that K and L are both regular over the field $\mathrm{acl}(E)$—see [Cha99, Subsection 1.17] (the only minor difficulty is showing separability in the situation where E is not perfect)—, so the original theorem applies.

This requirement of regularity is a hindrance when one wishes to study absolute Galois groups of an entire class of fields, say the class of finite extensions of the ground field K, together with the restriction morphisms to G_K.

Secondly, suppose for the moment that $S(\mathrm{G}_K)$ were interpretable in K, uniformly across fields, i.e. the sorts of $S(\mathrm{G}_K)$ were given by definable sets in the field language modulo definable equivalence relations, with the relations in the language of inverse systems induced from relations definable in the field language, and furthermore that this interpretation was compatible with the coding mentioned in the fourth point of the theorem. This interpretability would at once imply the entirety of the theorem, assuming for the second point some mild assumption on the compatibility of the interpretation with regular field extensions. Hence the theorem can be seen as a "weak interpretability" result of absolute Galois groups within fields.

However, we can show that we do in fact not have interpretability in the standard sense.

Let $K/\mathbb{Q}$ be a Galois extension with Galois group isomorphic to $\mathbb{Z}/3$, and let further L/K be a finite Galois extension such that $L/\mathbb{Q}$ is not a Galois extension. (One can achieve this situation by first realising a group G as a Galois group of $\mathbb{Q}$ which has a normal subgroup H of index 3 such that H in turn has a normal subgroup H' with H' not normal in G. An example for this situation is $G = (\mathbb{Z}/2)^3 \rtimes \mathbb{Z}/3$, where $\mathbb{Z}/3$ acts on $(\mathbb{Z}/2)^3$ by permuting coordinates cyclically; in other words, G is a wreath product of $\mathbb{Z}/2$ and $\mathbb{Z}/3$. Then $(\mathbb{Z}/2)^3$ is a normal subgroup of G with quotient $\mathbb{Z}/3$, and it has $(\mathbb{Z}/2)^2 \times 0$ as a normal subgroup which is not normal in G. The group G is realised as a Galois group over $\mathbb{Q}$ since it is solvable.)

We shall now argue that there is no natural parameter-free interpreta-

tion of $S(\mathrm{G}_K)$ in K; note that there are "unnatural" interpretations, since $\mathbb{Z}$ is parameter-freely definable in K by Rumely's results and hence any computable structure (as opposed to a structure with decidable theory) is parameter-freely interpretable in K. (It is not hard to see that $S(\mathrm{G}_K)$ is computable since there are computable realisations of the algebraic closure $\overline{K}$ by [FJ10, Section 19.4].)

Theorem 6.1.2. *Let $K/\mathbb{Q}$ be a finite Galois extension. For every automorphism $\sigma\colon \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Gal}(K^{\mathrm{sep}}/K)$ there exists a unique $\alpha\colon K^{\mathrm{sep}} \to K^{\mathrm{sep}}$, i.e. $\alpha \in \mathrm{Gal}(K^{\mathrm{sep}}/\mathbb{Q})$, such that σ is given by conjugation by α. In other words, the map $\mathrm{Gal}(K^{\mathrm{sep}}/\mathbb{Q}) \to \mathrm{Aut}(\mathrm{Gal}(K^{\mathrm{sep}}/K))$ given by the conjugation action is an isomorphism.*

Proof. This is the Neukirch–Uchida Theorem [NSW08, Theorem 12.2.1]. □

The automorphisms of the profinite group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$, where K is the $\mathbb{Z}/3$-extension of $\mathbb{Q}$ from above, are in bijection to the automorphisms of the multi-sorted structure $S(\mathrm{G}_K)$ by functoriality for epimorphisms of the S construction. In particular, we see that the only finite subgroups of $\mathrm{Aut}(S(\mathrm{G}_K))$ are of order 1 or 2, since finite subgroups of $\mathrm{G}_{\mathbb{Q}}$ can only have these orders by the results of Artin and Schreier on finite absolute Galois groups.

Therefore, for any parameter-free interpretation of $S(\mathrm{G}_K)$ in K the induced homomorphism $\mathrm{Aut}(K) \to \mathrm{Aut}(S(\mathrm{G}_K))$ must be trivial since $\mathrm{Aut}(K)$ is of order 3. Let $f \in K[X]$ be a monic irreducible polynomial such that $K[X]/(f)$ is isomorphic to L over K. Since L is not Galois

over $\mathbb{Q}$ by assumption, there exists an automorphism σ of K such that $K[X]/(\sigma f)$ is not isomorphic to L over K. This means that there cannot be a parameter-free interpretation of $S(\mathrm{G}_K)$ in K with a way of associating to every irreducible polynomial g a subgroup of G_K corresponding to the field $K[X]/(g)$, since we observed above that $S(\mathrm{G}_K)$ is not affected by any automorphism σ of K. This means that for a parameter-free interpretation the last point of Theorem 6.1.1 could not be recovered.

6.2 Galois theory through categories

Let K be a field. As recalled above, the absolute Galois group of K is defined to be the Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$, where K^{sep} is a separable closure of K. A different choice of separable closure $K^{\mathrm{sep}\prime}$ is always isomorphic to K^{sep} and hence yields an isomorphic group $\mathrm{Gal}(K^{\mathrm{sep}\prime}/K)$; however, there is no *canonical* isomorphism $K^{\mathrm{sep}} \to K^{\mathrm{sep}\prime}$, and hence the isomorphism between $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ and $\mathrm{Gal}(K^{\mathrm{sep}\prime}/K)$ is only determined up to conjugation. This is occasionally referred to as the absolute Galois group only being "determined up to inner automorphism".

This phenomenon is akin to the familiar situation in fundamental groups of (path-connected) topological spaces, where a different choice of base-point yields non-canonically isomorphic fundamental groups.

We have seen in the last section that the presence of automorphisms in a field and its absolute Galois group is an obstacle to interpretability. The new formalism to which we are led comes from Grothendieck's reinterpretation of Galois theory, which avoids fixing an algebraic closure. We follow the exposition in Exposé V of [SGA71].

Definition 6.2.1. *A* Galois category *is a category $\mathcal{C}$ such that there exists a profinite group G and an equivalence between $\mathcal{C}$ and the category $G-$*FinSet *of finite sets with a continuous action of G.*

Note that we do not fix a specific equivalence of categories. Some other sources define a Galois category to be a category together with a functor from $\mathcal{C}$ to FinSet satisfying certain conditions, but we avoid this as it often turns out to be tantamount to fixing a separable closure in the situation of Galois theory.

As we wish to replace (or augment) the study of profinite groups by the study of Galois categories, it is necessary to investigate what morphisms of profinite groups correspond to on the categorical side.

Proposition 6.2.2. *Let G and H be profinite groups. Then a morphism $f\colon G \to H$ of profinite groups gives any H-set the structure of a G-set. This defines an exact functor $P_f\colon H-$*FinSet$\to G-$*FinSet, i.e. a functor preserving finite limits and colimits.*

*This induces an equivalence of the category of exact functors $H-$*FinSet$\to G-$*FinSet and natural transformations with the category whose objects are morphisms $G \to H$ of profinite groups and whose arrows $f \to f'$ are elements $h \in H$ such that $hf(x)h^{-1} = f'(x)$ for all $x \in G$, i.e. precisely the* conjugations *from f to f'.*

The second statement, spelt out, means that every exact functor from $H-$FinSet to $G-$FinSet is naturally isomorphic to a functor induced by a morphism $G \to H$, and that the group of natural isomorphisms $P_f \Rightarrow P_{f'}$ is in functorial bijection to the set of conjugations $f \Rightarrow f'$.

Proof. Exactness of the functor P_f is stated in [SGA71, Corollaire V.6.2], as is the fact that any exact functor is naturally isomorphic to one of this form.

The second part is Corollaire V.6.3 loc. cit., there stated as an equivalence of the category of exact functors $H - \text{FinSet} \to G - \text{FinSet}$ with the category of functors from the fundamental groupoid of $G - \text{FinSet}$ to the fundamental groupoid of $H - \text{FinSet}$ respecting the topology, but these groupoids are equivalent to the profinite groups in question by Corollaire V.5.7 loc. cit. □

The correspondence between profinite groups and Galois categories is neatly stated in the language of 2-categories. However, as the category $G - \text{FinSet}$ is not a *small* category—the collection of its objects is a proper class—, foundational issues arise. They are easily corrected by fixing an infinite set U and replacing $G - \text{FinSet}$ by $G - \text{FinSet}(U)$, the full subcategory whose objects are the finite subsets of U with a continuous G-action. This is clearly a small category which is equivalent to $G - \text{FinSet}$, as every finite set is in bijection to a subset of U.

Theorem 6.2.3. *Assigning to a profinite group G the Galois category $G - \text{FinSet}(U)$ extends to a functor, contravariant in* 1*-morphisms, between the following* 2*-categories:*

1. *The category of profinite groups with* 1*-morphisms being morphisms in the standard sense, and the collection of* 2*-morphisms between $f, f' \colon G \to H$ given by the collection of $h \in H$ such that $f'(x) = hf(x)h^{-1}$ for all $x \in G$.*

2. *The category of small Galois categories with* 1*-morphisms being exact functors, and* 2*-morphisms between* $F, F' : \mathcal{C} \to \mathcal{C}'$ *given by natural isomorphisms between* F *and* F'*.*

This functor is a contravariant equivalence of 2*-categories.*

Proof. Noting that every Galois category is equivalent to a category $G - \mathrm{FinSet}(U)$ by definition, this is a restatement of the preceding proposition, observing that the correspondence between morphisms respects composition. □

Corollary 6.2.4. *For each Galois category* $\mathcal{C}$*, there is precisely one profinite group* G *such that* $\mathcal{C}$ *is equivalent to* $G - \mathrm{FinSet}$*.*

Proof. Two non-isomorphic profinite groups are never equivalent in the profinite group category. □

Corollary 6.2.5. *All exact functors from a Galois category to* $\mathrm{FinSet}(U)$ *are naturally isomorphic. Hence any object* c *in a Galois category has a well-defined* degree*, the cardinality of the finite set assigned to* c *under any exact functor into* FinSet*.*

Proof. Morphisms into $\mathrm{FinSet}(U)$ correspond to morphisms of profinite groups from the trivial profinite group, which is an initial object. □

Corollary 6.2.6. *Exact functors* $\mathcal{C} \to \mathcal{C}'$ *up to natural isomorphism correspond bijectively to profinite group morphisms up to conjugation between the associated profinite groups.*

Proof. This is an instance of *decategorification*, or passing to homotopy categories: Since the category of exact functors $\mathcal{C} \to \mathcal{C}'$ with natural isomorphisms is equivalent to the category of morphisms between the associated profinite groups with conjugations, there is a bijection between isomorphism classes in the first category and those in the second category. This is exactly the claim. □

In a sense, this is the core of the categorical approach to Galois theory: The problematic distinction between morphisms of profinite groups that differ only by inner automorphism is eliminated.

6.3 Galois categories as structures

We consider small Galois categories as structures in the sense of logic in the following way. We use a multi-sorted language with sorts Obj_n and $\mathrm{Mor}_{n \leftarrow m}$, where n, m, k are non-negative integers, function symbols

$$\begin{aligned} \mathrm{dom}_{n \leftarrow m} &: \mathrm{Mor}_{n \leftarrow m} \to \mathrm{Obj}_m, \\ \mathrm{cod}_{n \leftarrow m} &: \mathrm{Mor}_{n \leftarrow m} \to \mathrm{Obj}_n, \\ \mathrm{Id}_n &: \mathrm{Obj}_n \to \mathrm{Mor}_{n \leftarrow n} \end{aligned}$$

and relation symbols

$$\begin{aligned} \circ_{n \leftarrow m \leftarrow k} &\subseteq \mathrm{Mor}_{n \leftarrow m} \times \mathrm{Mor}_{m \leftarrow k} \times \mathrm{Mor}_{n \leftarrow k}, \\ \mathrm{pb}_{n,m,k,l}, \mathrm{po}_{n,m,k,l} &\subseteq \mathrm{Mor}_{l \leftarrow n} \times \mathrm{Mor}_{l \leftarrow m} \times \mathrm{Mor}_{n \leftarrow k} \times \mathrm{Mor}_{m \leftarrow k}. \end{aligned}$$

We suppress mention of the sort indices n as far as possible and speak of dom, cod, Id, $\circ$, pb, po.

We call this language the *language of stratified categories*, where *stratified category* is our name for a category with an assignment of a natural number, the degree, to every object. (The only stratified categories we have in mind are Galois categories and their opposite categories, but it is useful for questions of axiomatisability to have the more general notion.)

A small Galois category $\mathcal{C}$ is naturally a structure in this language, by making sort Obj_n consist of all objects of degree n and sort $\mathrm{Mor}_{n \leftarrow m}$ consist of all morphisms from objects of degree m to objects of degree n. (The index $n \leftarrow m$ in the notation reflects this. We write the codomain before the domain because of the usual order of composition of morphisms.)

Then we make dom and cod give the domain and codomain of morphisms, Id give identity morphisms, and let $\circ$ be the composition relation. By the additional relation symbols pb and po we mark pullback and pushout diagrams, i.e. given morphisms

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} \\ C & \xrightarrow{i} & D \end{array} \tag{6.1}$$

we have $\mathrm{pb}(h, i, f, g)$ and $\mathrm{po}(h, i, f, g)$ if and only if this square is a pullback or pushout, respectively.

Lemma 6.3.1. *In structures in this language which correspond to small Galois categories, there is a first-order definition of the relations* pb *and* po *in terms of the other data.*

Proof. Pullbacks and pushouts are defined by universal properties. We also know bounds on degrees of pullbacks and pushouts; specifically,

if we have the square (6.1) where k, n, m, l are the degrees of A, B, C, D respectively, then we must have $k \leq nm$ if the square is a pullback and $l \leq n + m$ if the square is a pushout—this is seen from the way pullbacks and pushouts are constructed in $G - \mathrm{FinSet}$ via the forgetful functor to FinSet.

Hence we see that the square is a pullback if and only if the degree of A is less than nm and for every object E of degree $\leq nm$ with morphisms $E \to B$ and $E \to C$ making the two composites $E \to D$ agree there is a unique $E \to A$ such that the composites $E \to A \to B$ and $E \to A \to C$ agree with the given morphisms. This is a first-order statement. We have the analogous definition for pushouts. □

Notationally, we do not distinguish between categories and the associated multi-sorted structures. We have the following easy observation.

Proposition 6.3.2. *Exact degree-preserving functors between stratified categories $\mathcal{C} \to \mathcal{C}'$ are in bijection to homomorphisms of multi-sorted structures $\mathcal{C} \to \mathcal{C}'$.*

Note that exact functors between Galois categories automatically preserve degree.

Proof. A functor is an assignment of objects to objects and morphisms to morphisms, compatible with domain and codomain assignments, identities and composition. Exact functors turn pullbacks into pullbacks and pushouts into pushouts, so they induce homomorphisms of the multi-sorted structures.

Conversely, any homomorphism of multi-sorted structures induces a functor preserving degrees, in particular preserving terminal and initial objects as these are the unique objects up to isomorphism of degree 1 and 0, respectively, and preserving pullbacks and pushouts, therefore preserving all finite limits and colimits. □

This means that we now have a language of stratified categories *above* a fixed stratified category $\mathcal{C}$, i.e. pairs of a stratified category $\mathcal{D}$ and an exact degree-preserving functor $\mathcal{C} \to \mathcal{D}$, given by expanding the previous language by constants for the images of objects and morphisms in $\mathcal{C}$ under the given functor/homomorphisms.

6.4 the choice of logic

At this point, it is necessary to make a choice of logic with which to study the structures associated to Galois categories in the last section. A natural first choice is simply multi-sorted first-order logic, and this is indeed a viable option. The problem with this choice is that equivalent Galois categories need not be elementarily equivalent in this logic, since for instance first-order logic can formalise assertions about the number of objects in an isomorphism class.

This problem of equivalence in the categorical sense and elementary equivalence in certain languages has been studied in the past by several authors, see e.g. [Bla78] or [Pre85], in which a syntactic characterisation of those first-order formulae is given which are preserved under equivalence of categories. A more general approach to fragments of first-order logic

compatible with a categorical notion of equivalence is developed in [Mak95].

It turns out, however, that in our situation one can almost always get by with full first-order logic. Recall that a category is *skeletal* if no two distinct objects are isomorphic.

Definition 6.4.1. *A Galois category $\mathcal{C}$ is called* anti-skeletal *if*

- *there is precisely one object of degree* 0 *and one of degree* 1 *in the sense of Corollary 6.2.5, and*
- *every object of higher degree has infinitely many objects in its isomorphism class.*

The special conditions for degrees 0 and 1 are arguably unnatural, but mesh well with our later use; we could eliminate them at the expense of a slightly more complicated étale formalism below.

Proposition 6.4.2. *Let $\mathcal{C}$ and $\mathcal{C}'$ be two anti-skeletal Galois categories.*

1. *If $F\colon \mathcal{C} \to \mathcal{C}'$ is part of an equivalence of categories and injective on objects, then it is an elementary embedding.*
2. *If $\mathcal{C}$ and $\mathcal{C}'$ are equivalent as categories, then they are elementarily equivalent.*

Proof. For the first part we use the Tarski-Vaught Test. Take a finite tuple of objects $\bar{o}$ in $\mathcal{C}$ and a finite tuple of morphisms $\bar{m}$ in $\mathcal{C}$. By extending $\bar{o}$ if necessary, we may assume that the domains and codomains of morphisms in $\bar{m}$ are listed in $\bar{o}$, and that furthermore $\bar{o}$ contains

the unique objects of degree 0 and 1. Let $\bar{o}'$ be a tuple of objects of $\mathcal{C}'$ disjoint from the image of $\bar{o}$. Because F is injective and essentially surjective on objects and $\mathcal{C}'$ is anti-skeletal, we may find objects $\bar{o}''$ in $\mathcal{C}'$ which are isomorphic (via some fixed isomorphisms) to the objects $\bar{o}'$, lie in the image of F, and are distinct from the objects in the image of $\bar{o}$. Correspondingly any tuple $\bar{m}'$ of morphisms whose domains and codomains are in $\bar{o}\bar{o}'$ can be moved to morphisms $\bar{m}'$ having domains and codomains in $\bar{o}\bar{o}''$. Now these new objects and morphisms all lie in the image of $\mathcal{C}$ by fullness of F, and for any formula φ such that $\mathcal{C}' \models \varphi(F\bar{o}, \bar{o}', F\bar{m}, \bar{m}')$ we will have $\mathcal{C}' \models \varphi(F\bar{o}, \bar{o}'', F\bar{m}, \bar{m}'')$. By the Tarski-Vaught Test, this proves that F is an elementary embedding.

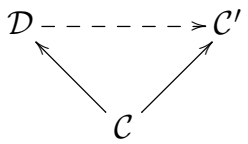
For the second part, one can find isomorphic elementary substructures of $\mathcal{C}$ and $\mathcal{C}'$ using the first part. Alternatively, one may use Ehrenfeucht-Fraïssé games in a standard way; see also [Pre85] for such uses of games in the logic of categories. □

For later use, we state the following.

Lemma 6.4.3. *Let $\mathcal{C}$ and $\mathcal{C}'$ be stratified categories, i.e. categories with an assignment of a natural number, the degree, to every object. Let furthermore an exact degree-preserving functor $\mathcal{C} \to \mathcal{C}'$ be given. Assume that $\mathcal{C}'$ is essentially degreewise finite, meaning that there are only finitely many isomorphism classes of objects of any given degree and only finitely many arrows between any two objects.*

Then there is a set of first-order sentences Φ in the language of stratified categories above $\mathcal{C}$ such that for any $\mathcal{C} \to \mathcal{D}$ we have $\mathcal{D} \models \Phi$ if and only if

there exists an exact functor $\mathcal{D} \to \mathcal{C}'$ making the diagram



commute up to natural isomorphism.

In $\mathcal{D} \models \Phi$, the functor $\mathcal{C} \to \mathcal{D}$, which is part of the structure of $\mathcal{D}$ as a stratified category above $\mathcal{C}$, is suppressed in the notation. Also note that although the lemma is phrased in terms of first-order sentences, the condition expressed is clearly preserved under equivalence of categories, and hence we may also work in a fragment of first-order logic stable under equivalence as in [Bla78, Pre85, Mak95].

The lemma can be seen as a categorical variant on the assertion that for any potentially multi-sorted structure A in a given language with all sorts finite, there exists a set of first-order sentences such that any other structure B satisfies the sentences if and only if there exists a homomorphism $B \to A$. The proofs only differ in notation.

Proof. If $\mathcal{C}' \to \mathcal{C}''$ is part of an equivalence of categories, then the condition of existence of a suitable functor does not change if we replace $\mathcal{C}'$ by $\mathcal{C}''$ and $\mathcal{C} \to \mathcal{C}'$ by the composite $\mathcal{C} \to \mathcal{C}' \to \mathcal{C}''$. Hence we may as well assume that $\mathcal{C}'$ is skeletal, i.e. has only one object in each isomorphism class, since every category is equivalent to such a category. This means that $\mathcal{C}'$ only has finitely many objects of any given degree, and hence also only finitely many morphisms of a given sort $\mathrm{Mor}_{m \leftarrow n}$.

Write $H \colon \mathcal{C} \to \mathcal{D}$ and $H' \colon \mathcal{C} \to \mathcal{C}'$ for the structure functors. We are looking for an exact functor $F \colon \mathcal{D} \to \mathcal{C}'$ with a natural isomorphism η

between the two functors H' and FH. We want to use compactness to argue that a pair F, η exists if and only if it exists whenever we restrict $\mathcal{C}$ and $\mathcal{D}$ to suitable finite subcategories, and that the latter condition is first-order axiomatisable.

The pair F, η is given by the following data:

1. For each object in $\mathcal{D}$ of degree n one of the finitely many objects in $\mathcal{C}'$ of the same degree—this determines F on objects;

2. for each morphism in $\mathcal{D}$ between objects of degree n and m one of the finitely many morphisms in $\mathcal{C}'$ between objects of degree n and m—this determines F on morphisms;

3. for each object in $\mathcal{C}$ of degree n one of the finitely many morphisms in $\mathcal{C}'$ between two objects of degree n—this determines η.

Observe that this collection of data naturally is an element of the compact space

$$K = \prod_n \mathrm{Obj}_n(\mathcal{C}')^{\mathrm{Obj}_n(\mathcal{D})} \times \prod_{n,m} \mathrm{Mor}_{m \leftarrow n}(\mathcal{C}')^{\mathrm{Mor}_{m \leftarrow n}(\mathcal{D})} \times \prod_n \mathrm{Mor}_{n \leftarrow n}(\mathcal{C}')^{\mathrm{Obj}_n(\mathcal{C})}.$$

Compactness is by degreewise finiteness of $\mathcal{C}'$.

For an element of this space to indeed make up a functor and a natural isomorphism, the following conditions need to be satisfied:

1. The collection of assignments (for all n, m) $\mathrm{Obj}_n(\mathcal{D}) \to \mathrm{Obj}_n(\mathcal{C}')$ and $\mathrm{Mor}_{m \leftarrow n}(\mathcal{D}) \to \mathrm{Mor}_{m \leftarrow n}(\mathcal{C}')$ must be compatible in the obvious way with dom and cod, and with Id;

2. the assignment of morphisms must be compatible with the composition relation;

3. for each object o in $\mathcal{C}$ of degree n the morphism η_o must have domain $H'(o)$ and codomain $F(H(o))$;

4. the transformation η must be natural: for every morphism $f : o \to o'$ in $\mathcal{C}$ we need to have the equality of morphisms $\eta_{o'} \circ H'(f) = F(H(f)) \circ \eta_o$ in $\mathcal{C}'$.

Observe that these are topologically closed conditions on the data in K; e.g. the first point above imposes one clopen condition for each morphism of $\mathcal{D}$ (compatibility with dom and cod) and one clopen condition for each object of $\mathcal{D}$ (compatibility with Id).

Hence by compactness an element of K satisfying all these conditions exists if and only if any finite subset of conditions is satisfiable. This is a condition on all finite subcategories of $\mathcal{D}$ above finite subcategories of $\mathcal{C}$ and thereby first-order axiomatisable. □

6.5 THE ÉTALE FORMALISM

We can now use Galois categories to study the Galois theory of fields. We roughly follow the exposition in [Sza09, Section 1.5].

Definition 6.5.1. *Let K be a field. An* étale algebra *of dimension $n \in \mathbb{N}$ is a commutative unital algebra A/K of dimension n such that there exists a field extension L/K satisfying $A \otimes_K L \cong L^n$.*

If there exists a suitable field extension L, one can show without difficulty that the condition is true for any algebraically closed L, and even any separably closed L. One deduces that A/K is étale if and only if it is a finite product of separable finite field extensions of K.

We write Et_K^0 for the category of étale algebras over K with K-algebra homomorphisms. We now have the following result.

Theorem 6.5.2 (Main Theorem of Galois Theory, Grothendieck's Version)**.** *For any field K and any separable closure K^{sep}/K, we have a contravariant equivalence of categories*

$$\mathrm{Et}_K^0 \to \mathrm{Gal}(K^{\mathrm{sep}}/K) - \mathrm{FinSet}$$

given by sending A/K to the finite set $\mathrm{Hom}_K(A, K^{\mathrm{sep}})$ equipped with its natural $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-action. Hence the opposite category of Et_K^0 is a Galois category.

For any field extension L/K there is an exact functor $\mathrm{Et}_K^0 \to \mathrm{Et}_L^0$, given by taking tensor products with L.

This is Grothendieck's "base-point free version" of Galois theory. As Et_K^0 is not a small category, we restrict to a suitable subcategory.

Definition 6.5.3. *The* small étale category *of K is the full subcategory Et_K of Et_K^0 consisting of objects whose underlying K-vector space is K^n for some $n \geq 0$ and whose multiplicative identity is $(1, \ldots, 1)$.*

The categories Et_K and Et_K^0 are equivalent because every K-vector space of finite dimension is isomorphic to some K^n via an isomorphism sending a given distinguished point (the multiplicative identity), non-zero if $n > 0$, to $(1, \ldots, 1)$.

Since we will be working with categories Et_K from now on as opposed to general Galois categories, it is convenient to suppress the passage from Et_K to its opposite category in the notation. We can use the multi-sorted language of stratified categories introduced in Section 6.3 just as well for the opposites of Galois categories.

It is now not hard to show the following.

Proposition 6.5.4. *There is a quantifier-free interpretation of* Et_K *as a multi-sorted structure in K, uniformly in the field K.*

Hence an inclusion of fields $K \hookrightarrow L$ *gives rise to an embedding of multi-sorted structures* $\mathrm{Et}_K \to \mathrm{Et}_L$*. This embedding is associated to the functor* $\mathrm{Et}_K \to \mathrm{Et}_L$ *given by the tensor product with L.*

Proof. An object of degree $n > 0$ in Et_K is a ring structure on K^n compatible with the K-vector space structure, i.e. a bilinear map $K^n \times K^n \to K^n$ which is commutative and associative and for which $(1, \ldots, 1)$ is a multiplicative identity. Such a bilinear map is uniquely determined by its structure constants a_{ij}^k, the constants such that $e_i \cdot e_j = \sum_k a_{ij}^k e_k$, where e_i is the i-th standard basis vector of K^n. The conditions on commutativity, associativity and the multiplicative identity are easily expressed as equations concerning the a_{ij}^k.

A K-homomorphism between algebras $(K^n, \cdot_1)$ and $(K^m, \cdot_2)$ is a K-linear map $K^n \to K^m$ which is compatible with the multiplications and

the multiplicative identities in the obvious way; this compatibility can be expressed as equations concerning the structure constants of $\cdot_1$ and $\cdot_2$ and the matrix representation of the map $K^n \to K^m$. The identity homomorphism is represented by the identity matrix, and composition of homomorphisms is given by matrix multiplication.

There is a unique object of degree 0, the zero ring structure on K^0; there is a unique K-homomorphism from each K-algebra to the zero ring, and no homomorphisms from the zero ring to a non-zero ring, so this poses no problems.

Thus we obtain an interpretation of Et_K in K by representing objects of degree n by structure constants, and morphisms between objects of degrees n and m by triples consisting of structure constants for the two objects in question and nm matrix entries. It is clear that inclusions of fields give rise to functors of étale categories given by tensor products, given that tensor products leave structure constants invariant.

The only thing left to give is the interpretation of the relation symbols for pullbacks and pushouts. According to Lemma 6.3.1, there is a first-order definition in terms of the data already defined. Since a given square is a pullback or pushout if and only if it is so over an algebraically closed overfield of K by exactness of $\mathrm{Et}_K \to \mathrm{Et}_L$, we can use quantifier elimination over algebraically closed fields to make this first-order definition quantifier-free. □

We observe that if the field K is infinite, then the Galois category Et_K is anti-skeletal, so our previous remarks on the logic of Galois categories

apply.[1]

Remark 6.5.5. If one restricts consideration to infinite fields, one can be slightly more economical by restricting instead to the subcategory of Et_K^0 of objects of the form $K[X]/(f)$, where f is a monic separable polynomial, i.e. a monic polynomial coprime to its derivative. One easily proves that every K-algebra of this form is étale and that conversely over an infinite field every étale algebra is isomorphic to one of this form, using that every étale algebra is isomorphic to a product of finite separable field extensions.

A morphism $K[X]/(f) \to K[X]/(g)$ is now given by a polynomial h such that g divides the composite polynomial $f \circ h$, which can be shown to be a quantifier-free condition on the coefficients of h by recourse to quantifier elimination over algebraically closed fields.

This alternative way reduces the number of variables required, since an object of degree n is now represented by the n non-leading coefficients of f as opposed to n^3 structure constants, and similarly for morphisms. Since the resulting categories are equivalent, there are no essential differences to the approach taken above.

We write $\mathrm{Et}_{L/K}$ for Et_L expanded by constants for the image of $\mathrm{Et}_K \to \mathrm{Et}_L$; we call the corresponding language the *étale language over K*. This is familiar from the standard model-theoretic technique of *diagrams*, and just as usual for any L/K we have $\mathrm{Et}_{L/K} \equiv \mathrm{Et}_{K/K}$ if and only if $\mathrm{Et}_L \succ \mathrm{Et}_K$. It follows from the discussion above that $\mathrm{Et}_{L/K}$ is interpretable in the

[1]Note that this is true regardless of whether the absolute Galois group of K is a small profinite group or not.

field L endowed with constants for the elements of K, in a uniform way across field extensions of K.

We make the following observation regarding finite separable field extensions L/K. Every étale algebra A/K with a morphism $L \to A$ is in fact an étale L-algebra via this morphism. Conversely, every étale L-algebra is also trivially an étale K-algebra. Notice that the dimension of algebras changes by a factor of $[L\colon K]$ under this correspondence.

This means that the category Et_L^0 is equivalent to the *coslice category* $L \downarrow \mathrm{Et}_K^0$, consisting of morphisms $A \to L$ in Et_K^0, where A is an arbitrary object, and morphisms $A \to L$ to $B \to L$ being morphisms $A \to B$ making the obvious triangle commute. Thus, if L is an object of Et_K which is a field, then Et_L is equivalent to $L \downarrow \mathrm{Et}_K$. The functor $\mathrm{Et}_K \to \mathrm{Et}_L$ given by tensor product with L is visible as the functor $\mathrm{Et}_K \to L \downarrow \mathrm{Et}_K$, again given by tensor product with L.

Lemma 6.5.6. *Let $n > 0$. Then for any field K, the category Et_K interprets categories equivalent to $\mathrm{Et}_{L/K}$ for any separable field extension L/K of degree n, uniformly in L. This interpretation is uniform in K.*

Proof. This follows from the preceding discussion once we observe that coslice categories are interpretable. This is clear, the degree change being easy to incorporate, and limits and colimits being definable in terms of those of Et_K. □

Note that we can identify the objects in Et_K which are fields as exactly those which are not a product of two non-terminal objects; hence this lemma allows us to quantify over the étale categories of separable field

extensions of K of given degree within Et_K. (In the Galois category $\mathrm{Et}_K^{\mathrm{op}}$, objects which cannot non-trivially be written as a coproduct are known as *connected* objects.)

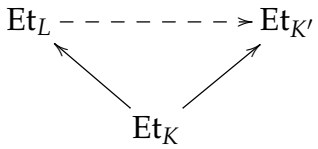
Remark 6.5.7. In fact, this construction is easily seen to work in any Galois category. Given a profinite group G and an open subgroup H, G acts on G/H by left multiplication. One verifies without difficulty that $H - \mathrm{FinSet}$ is equivalent to the slice category $G - \mathrm{FinSet}\,/(G/H)$, via the functor sending an H-set A to the set $(G \times A)/H$ of H-orbits of $G \times A$, where H acts on G by $h.g = gh^{-1}$, and with the obvious morphism $(G \times A)/H \to G/H$, and in the other direction the functor sending a G-equivariant map $B \to G/H$ to the H-subset of B consisting of the preimage of $1H$.

We can now restate Lemma 6.4.3; this reformulation will be used in the next chapter.

Lemma 6.5.8. *Let K be a field and K'/K a separable algebraic field extension. Assume that $\mathrm{Et}_{K'}$ is essentially degreewise finite, which is equivalent to the absolute Galois group $\mathrm{G}_{K'}$ being small. Then there exists a collection of sentences Φ in the language of étale categories above Et_K such that the following is true: For any field L/K, we have $\mathrm{Et}_L \models \Phi$ if and only if there exists an extension L'/L and an embedding $K' \hookrightarrow L'$ such that K' is relatively separably closed in L' and every separable algebraic extension of L' is the composite of L' with a separable algebraic extension of K'.*

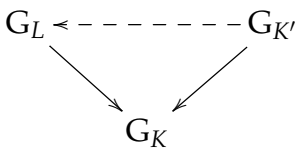
Proof. We claim that the existence of an extension L' and an embedding $K' \hookrightarrow L'$ with the desired properties is equivalent to the existence of an

exact functor $\mathrm{Et}_L \to \mathrm{Et}_{K'}$ making the triangle



commute up to natural isomorphism; then Lemma 6.4.3 proves the claim.

By Theorem 6.2.3, such a triangle of functors is equivalent to a triangle of morphisms of profinite groups



which commutes up to conjugation. If such a morphism $\mathrm{G}_{K'} \to \mathrm{G}_L$ exists, then it is necessarily injective since $\mathrm{G}_{K'} \to \mathrm{G}_K$ is injective, and we can take L'/L to be the fixed field of the image of $\mathrm{G}_{K'}$ in G_L: The intersection of L' with a separable closure of K is isomorphic to K' since the diagram commutes up to conjugation, so we may choose an embedding $K' \hookrightarrow L'$ inducing an isomorphism $\mathrm{G}_{K'} \cong \mathrm{G}_{L'}$.

Assume conversely that we have L' and an embedding $K' \hookrightarrow L'$ as in the statement of the theorem. Then the induced restriction map $\mathrm{G}_{L'} \to \mathrm{G}_{K'}$ is an isomorphism, and the map $\mathrm{G}_{K'} \to \mathrm{G}_{L'} \to \mathrm{G}_L$ makes the triangle commute up to conjugation. □

6.6 An axiomatisation of Galois categories

With a view to proving equivalence of the formalism of Galois categories to the Cherlin–Van den Dries–Macintyre formalism of profinite groups,

it will be necessary to have an axiomatic characterisation of Galois categories. The results of this section are not needed outside this chapter and may hence be omitted by the reader.

Definition 6.6.1. *Let $\mathcal{C}$ be a category in which all finite limits and colimits exist. Then an arrow $f\colon X \to Y$ in $\mathcal{C}$ is a* strict epimorphism *if f is the coequaliser of the diagram $X \times_Y X \rightrightarrows X$.*

There is a more general definition of strict epimorphisms in categories which do not necessarily have all finite limits and colimits, but that more general definition agrees with the one we have given, see [KS06, Proposition 5.1.5]. Note that by definition exact functors map strict epimorphisms to strict epimorphisms.

Definition 6.6.2. *Let $\mathcal{C}$ be a category. An arrow $f\colon X \to Y$ is a* coproduct coprojection *if there exists an arrow $Z \to Y$ such that Y (together with these arrows) is the coproduct of X and Z.*

It is again clear that exact functors map coproduct coprojections to coproduct coprojections. In certain categories, for instance in $G-\mathrm{FinSet}$ for any profinite group G, coproduct coprojections are monomorphisms, although this is not true in general.

The following characterisation of Galois categories can be found in [SGA71, Section V.4].

Theorem 6.6.3. *Let $\mathcal{C}$ be a category. Then $\mathcal{C}$ is a Galois category if and only if there exists a functor $F\colon \mathcal{C} \to \mathrm{FinSet}$ such that the following conditions are satisfied:*

1. *$\mathcal{C}$ has all finite limits and colimits;*

2. *F is exact;*

3. *F is conservative, i.e. any arrow f in $\mathcal{C}$ such that $F(f)$ is an isomorphism is itself an isomorphism;*

4. *every arrow $X \to Y$ in $\mathcal{C}$ factorises as $X \to Y' \to Y$ such that $X \to Y'$ is a strict epimorphism and $Y' \to Y$ is a monomorphism which is a coproduct coprojection.*

Proposition 6.6.4. *Let $\mathcal{C}$ be a small category in which every object is assigned some natural number, its* degree*. Then $\mathcal{C}$ is a Galois category with the given notion of degree agreeing with the one from Corollary 6.2.5 if and only if the following conditions are satisfied:*

1. *Every object of degree 0 in $\mathcal{C}$ is initial and every object of degree 1 is final, and there exist such objects;*

2. *all pullbacks and all pushouts in $\mathcal{C}$ exist;*

3. *all coproduct coprojections in $\mathcal{C}$ are monic;*

4. *every morphism in $\mathcal{C}$ factorises as a strict epimorphism followed by a coproduct coprojection;*

5. *a strict epimorphism $X \to Y$ is an isomorphism if and only if X and Y have the same degree, and likewise for coproduct coprojections;*

6. *there exists an exact functor from $\mathcal{C}$ to the category of finite sets preserving degrees.*

The degree of a finite set in the sense of Galois categories is of course just its cardinality.

Proof. Take a category $\mathcal{C}$ with a functor $F\colon \mathcal{C} \to \mathrm{FinSet}$ satisfying all conditions. Then $\mathcal{C}$ has all finite limits and colimits since it has initial and terminal objects as well as pullbacks and pushouts. The functor F preserves all finite limits and colimits. For any strict epimorphism f in $\mathcal{C}$, if $F(f)$ is an isomorphism then f is an isomorphism, since $F(f)$ must necessarily be a bijection between sets of the same cardinality, so f is a strict epimorphism between objects of the same degree and hence an isomorphism. The same is true for coproduct coprojections. Hence for an arbitrary arrow f with $F(f)$ an isomorphism, f must be an isomorphism by the factorisation condition, so F is conservative.

Therefore $\mathcal{C}$ is a Galois category by Theorem 6.6.3. Since F preserves degrees and the degree of an object in a Galois category is defined via an arbitrary exact functor to FinSet, the given notion of degree on $\mathcal{C}$ agrees with the standard one.

Now assume conversely that $\mathcal{C}$ is a Galois category and the notion of degree is the standard one. Most of the conditions follow from Theorem 6.6.3. A strict epimorphism f in $\mathcal{C}$ is an isomorphism if and only if the strict epimorphism $F(f)$ is an isomorphism in FinSet, which is the case if and only if $F(X)$ and $F(Y)$ have the same cardinality. The same argument applies to coproduct coprojections.

It remains to see that all coproduct coprojections in $\mathcal{C}$ are monic. It suffices to verify this in categories $G - \mathrm{FinSet}$, where this is clear since coproducts are given by disjoint unions of G-sets. □

Proposition 6.6.5. *The class of small Galois categories in the language of stratified categories is first-order axiomatisable.*

Proof. Let $\mathcal{C}$ be a structure in the language of stratified categories. We first need to assert that $\mathcal{C}$ is a category, i.e. satisfies the usual laws for composition of morphisms. This is clearly a first-order condition. Secondly, we can assert in a first-order way that every square marked by the relation pb (respectively po) is a pullback (pushout). By further asserting that any square isomorphic to a pullback square is itself a pullback square and likewise for pushouts, and additionally stipulating that any triangle of morphisms $a \to c \leftarrow b$ can be completed to a square which is marked by pb by adding an object of degree bounded by $\deg(a) \cdot \deg(b)$, and likewise for pushouts (with all arrows reversed, and the degree bound being $\deg(a) + \deg(b)$), we ensure that pb and po mark precisely pullbacks and pushouts.

It remains to axiomatise the conditions from Proposition 6.6.4. It is easy to axiomatise that all coproduct coprojections are monic, since coproducts are definable using the relation for pushouts. The factorisation condition is axiomatisable since strict epimorphisms and coproduct coprojections are definable.

We are left with axiomatising the existence of an exact functor $\mathcal{C} \to$ FinSet. This is a simple version of Lemma 6.4.3, where there is no base category $\mathcal{C}$ to work over (or equivalently, we choose $\mathcal{C}$ to be the empty category).[2] □

[2] In this situation, the proof of the lemma simplifies somewhat because the condition on natural isomorphism of functors trivialises, as there is only one functor from the empty category into any other category.

6.7 COMPARISON WITH THE C-D-M FORMALISM

In this section we show that the two formalisms for profinite groups have the same expressive power in a precise sense. Since none of the results here are used in the remainder of this thesis, the reader may wish to treat this section as an appendix.

Theorem 6.7.1. *Let $\mathcal{C}$ and $\mathcal{C}'$ be two anti-skeletal Galois categories with associated profinite groups G and G'.*

1. *$\mathcal{C} \equiv \mathcal{C}'$ if and only if $S(G) \equiv S(G')$*
2. *An exact functor $F\colon \mathcal{C} \to \mathcal{C}'$ which is injective on objects and fully faithful is an elementary embedding if and only if the associated surjection $G' \to G$ (unique up to conjugation) induces an elementary embedding $S(G) \to S(G')$.*

Since the opposite étale categories of infinite fields are anti-skeletal Galois categories, we immediately deduce the following.

Corollary 6.7.2. *Let K and L be infinite fields.*

1. *$\mathrm{Et}_K \equiv \mathrm{Et}_L$ if and only if $S(\mathrm{G}_K) \equiv S(\mathrm{G}_L)$*
2. *If $L \supseteq K$, then the natural base change map $\mathrm{Et}_K \to \mathrm{Et}_L$ is an elementary embedding if and only if K is relatively algebraically closed in L and the map $S(G_K) \to S(G_L)$ induced by the restriction map $\mathrm{G}_L \to \mathrm{G}_K$ is an elementary embedding.*

We start with the proof that our formalism is no more powerful than the Cherlin–Van den Dries–Macintyre one. At its core there is the following lemma.

Lemma 6.7.3. *Let G be a profinite group and A an infinite set. Then the structure $(S(G), A)$, consisting of all the sorts of $S(G)$ with their operations and the set A with no structure but equality, interprets an anti-skeletal Galois category equivalent to $G - \mathrm{FinSet}$. This interpretation is uniform across pairs of profinite groups and sets.*

Proof. Consider the category $\mathcal{C}$ with two designated objects O_0 and O_1, and other objects given by tuples of $n > 1$ distinct elements $a_1, \ldots, a_n \in A$ together with a morphism $G \to S_n$, thought of as an action $G \curvearrowright \{a_1, \ldots, a_n\}$, and morphisms given by equivariant maps between the finite G-sets, as well as one morphism from O_0 into every object and one morphism into O_1 from every object.

This category is clearly equivalent to $G - \mathrm{FinSet}$. (In fact, it is almost the same as the category $G - \mathrm{FinSet}(A)$ used in Section 6.2, except for collapsing all singleton sets to the object O_1, and using ordered finite subsets of A as opposed to unordered ones.) We also observe that $\mathcal{C}$ is anti-skeletal.

Lastly, observe that $\mathcal{C}$ as a multi-sorted structure is interpretable in $S(G)$: A morphism $G \to S_n$ is given by an open normal subgroup $N \triangleleft G$ of index $\leq n!$ together with a homomorphism of finite groups $G/N \to S_n$, so this gives an interpretation of objects; there is then no difficulty in also interpreting morphisms. This natural interpretation is clearly uniform in G and A. □

Proof of Theorem 6.7.1, backward direction. Take two anti-skeletal small Galois categories $\mathcal{C}$ and $\mathcal{C}'$ with associated groups G and G', and let A be any infinite set bigger than the cardinalities of the structures $\mathcal{C}$ and $\mathcal{C}'$.

Assume that $S(G) \equiv S(G')$. Then the pair structures $(S(G), A)$ and $(S(G'), A)$ are elementarily equivalent, as they have isomorphic ultrapowers. (There are of course more elementary ways to see this.) By the last Lemma, there exists a uniform interpretation of certain Galois categories $\mathcal{D}$ and $\mathcal{D}'$ in $(S(G), A)$ and $(S(G'), A)$, respectively. The elementary equivalence $(S(G), A) \equiv (S(G'), A)$ now implies $\mathcal{D} \equiv \mathcal{D}'$. By Proposition 6.4.2, we therefore have $\mathcal{C} \equiv \mathcal{D} \equiv \mathcal{D}' \equiv \mathcal{C}'$.

Now let $F\colon \mathcal{C} \to \mathcal{C}'$ be a fully faithful functor which is injective on objects, and write $f\colon G' \to G$ for an associated surjection. Assume that f induces an elementary embedding $S(G) \to S(G')$. Then the map $(S(G), A) \to (S(G'), A)$ given by f on the first part and the identity on the second part is elementary. Write $\mathcal{D}$ and $\mathcal{D}'$ for the small Galois categories interpretable in $(S(G), A)$ and $(S(G'), A)$ according to Lemma 6.7.3; the elementary embedding $(S(G), A) \to (S(G'), A)$ induces an elementary embedding $\mathcal{D} \to \mathcal{D}'$. We shall argue that there is a commuting square

$$\begin{array}{ccc} \mathcal{D} & \longrightarrow & \mathcal{D}' \\ \uparrow & & \uparrow \\ \mathcal{C} & \xrightarrow{F} & \mathcal{C}' \end{array}$$

in which all maps but the bottom one are elementary embeddings; then the bottom map F will have to be elementary as well, which is precisely the claim.

Observe that the exact functors of Galois categories $\mathcal{D} \to \mathcal{D}'$ and $F\colon \mathcal{C} \to \mathcal{C}'$ both correspond to the morphism f of profinite groups under

the equivalence of Theorem 6.2.3. Hence there exist equivalence functors $\mathcal{C} \to \mathcal{D}$ and $\mathcal{C}' \to \mathcal{D}'$ making the square commute. Since $\mathcal{D}$ and $\mathcal{D}'$ have sufficiently many objects of each isomorphism class due to choice of A, we can choose these equivalence functors to be injective on objects. Then they are both elementary embeddings of multi-sorted structures by Proposition 6.4.2. This finishes the proof. □

Given the explicit nature of the interpretation of $\mathcal{D}$ in $(S(G), A)$, we can give a very explicit translation of first-order statements about $\mathcal{C}$ into first-order statements about $S(G)$.

The converse direction—the proof that our formalism is no less powerful than the Cherlin–Van den Dries–Macintyre one—is harder, since we have seen in Section 6.1 that we cannot expect a direct interpretation; furthermore, our proof technique will necessarily be "non-categorical" in nature, i.e. involve many non-canonical choices and thereby violate the principle of equivalence from category theory.

Consider the language of Galois categories. For all n, m, add a unary predicate D_n on Obj_n and a unary predicate $D_{m \leftarrow n}$ on $\mathrm{Mor}_{m \leftarrow n}$. Let $\mathcal{C}$ be a Galois category. An object o of $\mathcal{C}$ is called *connected* if it cannot be written as a coproduct of two non-initial objects. A connected object of degree n is called *Galois* if it has precisely n automorphisms. (These notions are standard. In the case of the category $\mathrm{Et}_K^{\mathrm{op}}$ for a field K, an object is connected if and only if it is a field, and Galois if and only if it is a Galois extension of K.) An expansion of a Galois category $\mathcal{C}$ to this language is called *admissible* if the following conditions are satisfied:

1. Each object in Obj_n is connected and Galois;

2. the relation D_0 is empty;

3. for each connected Galois object $o \in \mathrm{Obj}_n$, $n > 0$, there is precisely one object isomorphic to o which is in D_n;

4. for each $f \in D_{m \leftarrow n}$, $\mathrm{dom}\, f \in D_n$ and $\mathrm{cod}\, f \in D_m$;

5. for any two $o \in D_n$, $o' \in D_m$, if there exists a morphism $o \to o'$, then precisely one such morphism is in $D_{m \leftarrow n}$;

6. for each $o \in D_n$, the identity morphism $o \to o$ is in $D_{n \leftarrow n}$;

7. if $f \in D_{m \leftarrow n}$ and $f' \in D_{k \leftarrow m}$, then $f' \circ f \in D_{k \leftarrow n}$.

Note that we may think of the predicates D as distinguishing a subcategory $\mathcal{D}$ of $\mathcal{C}$ satisfying certain admissibility conditions; we will freely use this point of view in the sequel.

Our proof of the backward direction of Theorem 6.7.1 will now proceed by proving that admissible expansions exist and are unique up to isomorphism, and that in an admissibly expanded Galois category the Cherlin–Van den Dries–Macintyre structure is interpretable. This proof technique is already present in [CvdDM82] under the name "implicit interpretation".

Lemma 6.7.4. *Every Galois category $\mathcal{C}$ has an admissible expansion, and any two admissible expansions are isomorphic.*

In the language of [SGA71], this lemma is about the existence and uniqueness of a *fundamental pro-object* of $\mathcal{C}$, and we simply invoke the results of loc. cit. for the proof.

Note, however, that this lemma corresponds very closely to the statement that every field has a separable closure, unique up to isomorphism: A choice of admissible expansion of $(\mathrm{Et}_K^0)^{\mathrm{op}}$ corresponds to choosing one finite Galois field extension of each isomorphism type, together with distinguished morphisms between them. Then the inductive limit of these fields is a separable closure, and every separable closure arises in this way, by simply choosing the distinguished fields to be its finite Galois subfields and the distinguished maps to be the embeddings.

Proof. For existence, take an exact functor $F\colon \mathcal{C} \to \mathrm{FinSet}$. By [SGA71], F is *strictly pro-representable*, i.e. there exists a projective system $(P_i)_{i\in I}$ of objects in $\mathcal{C}$ with I a directed set and all transition morphisms epimorphisms such that the functor F is isomorphic to $\varinjlim_{i\in I} \mathrm{Hom}(P_i, \cdot)$. According to [SGA71, Corollaire V.5.4], the P_i are all connected of non-zero degree, and conversely every such object is isomorphic to some P_i. The Galois objects among the P_i are cofinal within the whole system by Section V.4.(g) loc. cit., so we may remove all non-Galois objects without affecting the limit. By removing isomorphic objects if necessary, we may assume that no two P_i are isomorphic. (One may always remove duplicate objects in this way without affecting inductive and projective limits.) Then the collection of P_i and their transition morphisms gives a distinguished subcategory of $\mathcal{C}$ satisfying all properties for an admissible expansion.

For uniqueness, let $\mathcal{D}$ and $\mathcal{D}'$ be two admissible subcategories of $\mathcal{C}$. Then $\mathcal{D}$, as a collection of objects and morphisms, is a projective system, and since $\mathcal{D}$ contains objects with morphisms to any given connected

object of non-zero degree, $\mathcal{D}$ pro-represents an exact functor $\mathcal{C} \to \mathrm{FinSet}$ (a *fundamental functor*) by [SGA71, Proposition V.5.6]. The same fact holds for $\mathcal{D}'$, and hence the two projective systems are isomorphic, again by [SGA71, Proposition V.5.6], which in the current situation means that we can choose a distinguished set of isomorphisms from all objects of $\mathcal{D}$ to all objects of $\mathcal{D}'$, compatible with morphisms in the natural way.

The admissible expansion $(\mathcal{C}, \mathcal{D})$ is now isomorphic to $(\mathcal{C}, \mathcal{D}')$, by an isomorphism functor swapping each object of $\mathcal{D}$ with the unique isomorphic object of $\mathcal{D}'$ and fixing all other objects, and using the distinguished isomorphisms to suitably map all morphisms with domain and/or codomain in $\mathcal{D}$ or $\mathcal{D}'$. □

Lemma 6.7.5. *Let $F\colon \mathcal{C} \to \mathcal{C}'$ be a functor of small Galois categories which is an elementary embedding. Then there exist admissible expansions of $\mathcal{C}$ and $\mathcal{C}'$ which make this functor an elementary embedding in the expanded language.*

Proof. Choose an admissible expansion of $\mathcal{C}'$. For every distinguished object o in $\mathcal{C}'$, either o is isomorphic to the image of an object in $\mathcal{C}$ or not; for all those distinguished objects which are, pick an object o_0 in $\mathcal{C}$ and an isomorphism $o \to Fo_0$. We can now modify the admissible expansion of $\mathcal{C}'$ by distinguishing Fo_0 instead of o, and adjusting distinguished morphisms according to the chosen isomorphism $o \to Fo_0$. Once this procedure is performed for all o simultaneously, we are left with an admissible expansion of $\mathcal{C}'$ in which every distinguished object is either in the image of F or not even isomorphic to an object in the image of F. This allows us to pull back the distinguished subcategory of $\mathcal{C}'$ to a

subcategory of $\mathcal{C}$, which leads to an admissible expansion of $\mathcal{C}$. (Here we are using that F is elementary; for instance, this is needed so that an object in $\mathcal{C}$ is connected Galois if and only if its image in $\mathcal{C}'$ is.)

Hence we find an admissible expansion of $\mathcal{C}'$ such that F sends the distinguished subcategory of $\mathcal{C}$ into the distinguished subcategory of $\mathcal{C}'$. It is easy to show that F is now automatically an elementary embedding of the expansions by the Tarski-Vaught Test. □

Lemma 6.7.6. *Let $\mathcal{C}$ be a Galois category and G the corresponding profinite group. Then $S(G)$ is interpretable in an admissible expansion of $\mathcal{C}$, uniformly across admissibly expanded Galois categories.*

Proof. The admissibly expanded structure $\mathcal{C}$ induces a structure S in the Cherlin–Van den Dries–Macintyre language in the following way. The objects of sort n in S are pairs (o, m) where o is an object in $\mathcal{C}$ of degree $\leq n$ which is marked by the predicate D and m is any morphism $m\colon o \to o$. We interpret the relations in S as follows: We say $(o, m) \leq (o', m')$ if there exists a morphism $o \to o'$, we say $C((o, m), (o', m'))$ if there exists a morphism $f\colon o \to o'$ which is marked by D and such that $f \circ m = m' \circ f$, and we say $P((o, m), (o', m'), (o'', m''))$ if $o = o' = o''$ and $m \circ m' = m''$.

This structure S is clearly interpretable in $\mathcal{C}$, uniformly in $\mathcal{C}$.

We shall prove that the resulting structure is isomorphic to $S(G)$. Fix an infinite set U which set-theoretically contains all the finite groups G/N, and fix an equivalence of the categories $\mathcal{C}$ and $G - \mathrm{FinSet}(U)$. The marked subcategory $\mathcal{D}$ of $\mathcal{C}$ induces a subcategory of $G - \mathrm{FinSet}(U)$ which is isomorphic to $\mathcal{D}$ (because $\mathcal{D}$ is skeletal), and this gives an

admissible expansion of $G - \mathrm{FinSet}(U)$. It is now easy to verify that the structure S' interpreted in the expansion of $G - \mathrm{FinSet}(U)$ is isomorphic to S, since we have fixed an isomorphism between the D-marked objects in $\mathcal{C}$ and the D-marked objects in $G - \mathrm{FinSet}(U)$.

We may therefore assume that $\mathcal{C} = G - \mathrm{FinSet}(U)$. Since any two admissible expansions of $G - \mathrm{FinSet}(U)$ are isomorphic, we may choose an expansion; we choose the expansion distinguishing as objects the finite sets G/N with the G-action by left multiplication, where N is any open normal subgroup of G, and distinguishing as morphisms the projections $G/N \to G/N'$, where $N \leq N'$.

It is now straightforward to verify that $S(G)$ is indeed isomorphic to the structure S defined above, by sending a coset $gN \in G/N$ to the pair of the object G/N and the equivariant map $G/N \to G/N, hN \to hg^{-1}N$. □

Proof of Theorem 6.7.1, forward direction. Let $\mathcal{C} \equiv \mathcal{C}'$ be small Galois categories, so they have isomorphic ultrapowers. These ultrapowers are still small Galois categories by the first-order axiomatisability, Proposition 6.6.5. Endowing both $\mathcal{C}$ and $\mathcal{C}'$ with an admissible expansion, the expanded ultrapowers are still isomorphic by the uniqueness in Lemma 6.7.4. Therefore the admissible expansions of $\mathcal{C}$ and $\mathcal{C}'$ are elementarily equivalent, and hence so are $S(G)$ and $S(G')$ by Lemma 6.7.6.

If $F\colon \mathcal{C} \to \mathcal{C}'$ is an elementary embedding, then there exist admissible expansions of $\mathcal{C}$ and $\mathcal{C}'$ such that F is an elementary embedding of these by Lemma 6.7.5. Hence F induces an elementary embedding $S(G) \to S(G')$ by Lemma 6.7.6. □

ON THE GENERALISED STUFE

7.1 ON p-VALUATIONS

On a field K of characteristic zero, recall that a p-valuation (for some prime number p) is a valuation v whose residue field is a finite field of characteristic p and in whose value group there are only finitely many elements between 0 and $v(p)$. There is an extensive study of p-valuations in [PR84].

A p-valued field (K, v) is *p-adically closed* if it is henselian and its value group is a $\mathbb{Z}$-group. Every p-valued field (K, v) embeds into a p-adically closed field, and every p-adically closed field containing K contains a minimal p-adically closed field containing K, which is always algebraic over K; such an algebraic extension is called a *p-adic closure of* (K, v). However, p-adic closures are not usually unique up to isomorphism: According to [PR84, Theorem 3.2], we have uniqueness if and only if vK is a $\mathbb{Z}$-group, in which case p-adic closures are just henselisations.

We are interested in investigating how a fixed p-valuation v of K extends to an extension field L/K. Unlike orderings on K, which either extend to an ordering on L or not, a p-valuation on K will always extend to at least one valuation on L, which may or may not be a p-valuation; even if it is, it may have essentially different p-adic closure. It is this notion which we are trying to capture.

Let us write $\mathcal{L}_R$ for the first-order language of rings with an additional unary predicate R; we use this as a language of valued fields, interpreting

R as a valuation ring on a field. Hence for a field L with a valuation v, we may write (L, v) or $(L, \mathcal{O}_v)$ for the associated $\mathcal{L}_R$-structure.

Let us further write $\mathcal{L}_R(K)$ for $\mathcal{L}_R$ expanded by constants for elements of K, and likewise $\mathcal{L}_{\text{ring}}(K)$ for the language of rings expanded by constants for elements of K.

Definition 7.1.1. *A* type τ *over K is a complete $\mathcal{L}_{\text{ring}}(K)$-theory containing the quantifier-free diagram of K and whose $\mathcal{L}_{\text{ring}}$-reduct is exactly the first-order theory of some finite extension of $\mathbb{Q}_p$ for some p.*[1] *In other words, τ is the $\mathcal{L}_{\text{ring}}(K)$-theory of some p-adically closed extension field of K. Since the natural valuation on a finite extension of $\mathbb{Q}_p$ is definable, τ can be expanded canonically to a complete $\mathcal{L}_R(K)$-theory τ'. Models of τ are called* τ-adically closed.

If v is a valuation on K, we say that τ is above v*, or that v is* below τ*, if τ' contains the quantifier-free diagram of the valued field $(K, \mathcal{O}_v)$, i.e. if τ' is the theory of some p-adically closed valued extension field of (K, v). Note that in this situation v is automatically a p-valuation for the prime p determined by τ.*

Let L/K be an extension field and w be a valuation on L. We say that w is of type τ *or* τ-adic *if (L, w) (as a $\mathcal{L}_R(K)$-structure) embeds into a model of τ'. In this case the restriction of w to K is necessarily equal to v.*

The field L is formally τ-adic *if there exists a valuation w on L of type τ; in this case, any τ-adically closed algebraic extension of L is called a* τ-adic closure of L.

One can easily extend this notion to orderings in place of p-valuations by considering $\mathcal{L}_R$-structures in which R is interpreted as the positive

[1] The overloading of the word "type" in this context, which already has a precise meaning in model theory, is unfortunate; however, we will see below that there is precedent for it.

cone of an ordering, and taking τ to be the theory of a real-closed extension field of K; this is however less interesting than in the case of p-valuations, since τ is uniquely determined by the unique ordering on K below it.

For a more algebraic definition of types, we may identify τ with its unique model which is algebraic over K; recall that any relatively algebraically closed subfield of a p-adically closed field is an elementary submodel, so there is indeed such a model, and it is unique due to completeness of τ.[2]

Given an extension $(L, w)/(K, v)$ of p-valued fields for some p, one defines the *relative inertia degree* $f(w/v) = [Lw\colon Kv]$ and the *relative ramification index* $e(w/v) = \frac{|\{\gamma \in wL\colon 0 \leq \gamma < wp\}|}{|\{\gamma \in vK\colon 0 \leq \gamma < vp\}|}$.

Given a type τ over K, we define natural numbers p_τ, q_τ, e_τ, f_τ as follows: Let $(L, w) \models \tau'$ and $v = w|_K$ the unique valuation of K below w, and write p_τ for the residue characteristic of w, q_τ for the cardinality of the residue field Lw, $e_\tau = e(w/v)$ and $f_\tau = f(w/v)$. All these are clearly independent of the model (L, w) chosen.

Remark 7.1.2. In [PR84], an extension $(L, w)/(K, v)$ of p-valued fields is said to be of type (e, f), where e and f are positive integers, if the relative inertia degree divides f and the relative ramification index is at most e. It is not hard to see that this is a strictly coarser notion than what we have defined. Consider for instance the p-valued field $\mathbb{Q}_p$ for any odd prime p: This has three non-isomorphic quadratic extensions, since $\mathbb{Q}_p$

[2] In [Pop88], Pop defines the *Typus* of a p-adically closed field to be the isomorphism type of its absolute part, i.e. the relative algebraic closure of $\mathbb{Q}$ within it. This is now seen to be the special case of our definition where the base field K is $\mathbb{Q}$.

has four square classes, and of these two are ramified and hence have relative inertia degree 1 and relative ramification index 2. However, they have distinct algebraic part and therefore distinct $\mathcal{L}_{\text{ring}}$-theory.

We will now fix K and τ, and write v for the valuation of K below τ, and ask for varying extension fields L/K whether they are formally τ-adic. This is a simultaneous generalisation of the following questions:

- If $K = \mathbb{Q}$ and τ is the type corresponding to $\mathbb{Q}_p$ for some p, then we are asking whether L carries a p-valuation of rank 1 in the sense of [PR84], i.e. a valuation with residue field $\mathbb{F}_p$ and in which p has minimal positive value. This is a standard notion of being formally p-adic.

- If $K = \mathbb{Q}$ and τ corresponds to an unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_{p^f}$, then we are asking whether L has a p-valuation w with $w(p)$ minimal positive and residue field embedding into $\mathbb{F}_{p^f}$.

- If K is arbitrary and τ corresponds to a p-adic closure K_v of K, and (K, v) has the same residue field and value group as K_v, then we are asking whether the p-valuation v on K has an immediate extension to L.

These conditions are well studied; in [PR84], an algebraic theory is developed which answers the question for the coarse invariant (e, f). We summarise some of the known results in the following theorem.

Theorem 7.1.3. *The following are equivalent for an extension L of K.*

1. *L is formally τ-adic;*

2. $L \models \tau_\forall$, *i.e.* L *satisfies the universal part of the theory* τ, *where* L *is considered a structure in the language of rings enriched by constants for elements of* K;

3. *there is a closed subgroup* H *of the absolute Galois group* G_L *such that the restriction map* $\mathrm{G}_L \to \mathrm{G}_K$ *maps* H *isomorphically onto a conjugate of* $\mathrm{G}_{K'} \leq \mathrm{G}_K$, *where* K'/K *is an algebraic extension carrying a valuation* v *with* $(K, v) \models \tau'$.

In fact, one could give an explicit axiomatisation of $\tau_\forall$ in terms of the unique model of τ algebraic over K in the style of [PR84], but we shall not do so here.

Proof. By definition, L is formally τ-adic if and only if L embeds into a model of τ, as any model of τ can be expanded to a model of τ' by first-order definability of valuation rings of p-adically closed fields. This implies the equivalence of the first two points by general model theory.

For the equivalence of the first and the third point, it suffices to show that $L \models \tau$ if and only if the restriction map $\mathrm{G}_L \to \mathrm{G}_K$ is injective with image conjugate to $\mathrm{G}_{K'}$. The former condition implies the latter, since K' embeds elementarily into L and $\mathrm{G}_{K'}$ is a small profinite group by standard results on p-adically closed fields. Conversely, the latter condition implies that K' embeds into L and L is p-adically closed by [Pop88, Theorem (E.12)], so L is in fact an elementary extension of K' by model completeness of p-adically closed fields of given p-rank. □

Remark 7.1.4. One may wish to formulate an "absolute" version of this theorem, where one does not fix a base field K to work over, but the

obvious version of this is false: This is essentially the fact that there are non-isomorphic (and therefore non-elementarily equivalent) finite extensions of $\mathbb{Q}_p$ with isomorphic absolute Galois groups, see for instance [JR79].

7.2 classes of fields of bounded τ-stufe

The last theorem implies in particular that the condition of being formally τ-adic is first-order axiomatisable. For the analogous situation of $K = \mathbb{Q}$ with the unique ordering, one possible axiom system is well-known—it suffices to say that -1 is not equal to a sum of squares $x_1^2 + \cdots + x_n^2$ for any natural number n.

We focus on classes of fields in which being formally τ-adic is *finitely* axiomatisable.

Definition 7.2.1. *Let $\mathcal{K}$ be a class of extension fields of K. We say that $\mathcal{K}$ has* bounded τ-Stufe *if there exists $\varphi \in \tau_\forall$ such that any $L \in \mathcal{K}$ is formally τ-adic if and only if $L \models \varphi$.*

The term τ-Stufe is in analogy to the standard notion of the Stufe of a field—the minimum number n of elements $a_1, \ldots, a_n \in L$ such that $-1 = \sum a_i^2$; we are studying the p-adic analogue of the situation of a class of fields $\mathcal{K}$ in which every field has Stufe ∞ or bounded by some fixed natural number. However, we do not actually define the term of τ-Stufe itself, as no natural definition presents itself.

Note that if $\mathcal{K}$ has bounded τ-Stufe, then so does the class of models of the $\forall\exists$-theory of $\mathcal{K}$, i.e. the minimal elementary class containing $\mathcal{K}$ and closed under unions of chains.

We give some simple equivalent characterisations.

Lemma 7.2.2. *The following are equivalent for a class $\mathcal{K}$ of extension fields of K:*

(i) $\mathcal{K}$ has bounded τ-Stufe;

(ii) there exists a sentence ψ with parameters from K such that for each $L \in \mathcal{K}$, L is formally τ-adic or $L \models \psi$, and no formally τ-adic field M/K satisfies ψ;

(iii) there exists a positive primitive sentence ψ as in (ii).

If $\mathcal{K}$ contains some formally τ-adic field, e.g. if $K \in \mathcal{K}$, and is closed under taking finite extensions, these conditions are furthermore equivalent to the following:

(iv) There exists an existential sentence ψ with parameters from K such that for each $L \in \mathcal{K}$, L is formally τ-adic if and only if $L \models \neg\psi$.

Proof. For the implication from (i) to (iii), let φ be as in the definition of bounded τ-Stufe, and write $\neg\varphi$ in prenex conjunctive normal form; observe that this is almost as required except for the possible presence of negations and disjunctions. We may eliminate negations by rewriting a literal $p(\overline{x}) \neq 0$ as $\exists y(p(\overline{x})y + 1 = 0)$, and then eliminate disjunctions by rewriting $p(\overline{x}) = 0 \vee q(\overline{x}) = 0$ as $p(\overline{x})q(\overline{x}) = 0$.

The implication from (iii) to (ii) is trivial.

For the implication from (ii) to (i), observe that the set of sentences $T_{\text{fields}/K} \cup \{\psi\} \cup \tau_\forall$ is inconsistent, where $T_{\text{fields}/K}$ axiomatises extension fields of K. Hence by compactness there is a finite subset $\Phi \subseteq \tau_\forall$ such

that $T_{\text{fields}/K} \models \psi \to \neg \bigwedge \Phi$. Then $\bigwedge \Phi$ is as required in the definition of bounded τ-Stufe.

Clearly (iii) implies (iv). For the implication from (iv) to (ii), under the stated assumptions on $\mathcal{K}$, let $M \in \mathcal{K}$ carry a τ-adic valuation w. Then a closure M_w is a union of formally τ-adic finite extensions of M, all of which are in $\mathcal{K}$, hence we may deduce $M_w \models \neg\psi$ since ψ is existential. As all formally τ-adic fields embed into a field elementarily equivalent to some M_w over K, this proves that no formally τ-adic field satisfies ψ. □

The τ-Stufe is further connected with definability of the *holomorphy ring*, which we now define.

Definition 7.2.3. *Let L/K be any field extension. The* τ-holomorphy domain of L *is*

$$R_\tau(L) = \bigcap_w \mathcal{O}_w,$$

where the intersection is over all τ-adic valuations w on L.

Note that L/K is formally τ-adic if and only if $\frac{1}{p_\tau} \notin R_\tau(L)$.

Proposition 7.2.4. *Let $\mathcal{K}$ be a class of extension fields of K that contains a formally τ-adic field and is closed under taking finite extensions. Then the following are equivalent:*

- *$\mathcal{K}$ has bounded τ-Stufe;*
- *there exists an existential formula $\varphi(x)$ with parameters in K that defines the τ-holomorphy ring in all fields in $\mathcal{K}$.*

For the proof, we will need the *Kochen operator*. This is the rational function

$$\gamma_\tau^\pi(X) = \frac{1}{\pi}\Big(\frac{X^{q_\tau} - X}{(X^{q_\tau} - X)^2 - 1}\Big)^{e_\tau} \in K(X), \tag{7.1}$$

where $\pi \in K$ is a uniformiser, i.e. of minimal positive valuation. This function is important since—as one easily verifies—for any τ-adic valuation v on an extension field L/K, $\gamma_\tau^\pi(x)$ is in the valuation ring for any $x \in L$, and conversely for every $(L, v) \models \tau'$ every element $y \in L$ in the valuation ring can be written as $y = \gamma_\tau^\pi(x)$ for some $x \in L$ by Hensel's Lemma.

Lemma 7.2.5. *Let $f = ((Y^{q_\tau} - Y)^2 - 1)^{e_\tau} - X^{e_\tau}(Y^{q_\tau} - Y)^{e_\tau} \in K[X, Y]$. Then for any L/K, $x \in L$ and any τ-adic valuation v on L, $vx < 0$ if and only if the algebra $A = L[Y]/(f(x, Y))$ has a residue field with a τ-adic valuation extending v.*

Proof. Fix a uniformiser π of K. The polynomial f is defined such that for any x, y in an extension field of K, $f(x, y) = 0$ if and only if $\gamma_\tau^\pi(y) = \frac{1}{\pi x^{e_\tau}}$.

Let $x \in L$ and $A = L[Y]/(f(x, Y))$ as above. If M is a residue field of A, then the image of Y in M is an element y such that $f(x, y) = 0$, hence $\gamma(y) = \frac{1}{\pi x^{e_\tau}}$. In particular, for any τ-adic valuation w on M, $wx < 0$.

Conversely, if v is a τ-adic valuation on L with $vx < 0$, take any τ-adic closure L_v. Since $v(\frac{1}{\pi x^{e_\tau}}) \geq 0$, by Hensel's Lemma there is an element $y \in L_v$ with $\gamma(y) = \frac{1}{\pi x^{e_\tau}}$. Therefore there is an L-algebra homomorphism $A \to L_v$; its image is a finite ring extension of L which is a domain, and therefore is a field. On this residue field of A, the valuation of L_v restricts to a τ-adic valuation. □

Proof of Proposition 7.2.4. If $\varphi(x)$ defines the τ-holomorphy ring for all fields in $\mathcal{K}$, then $\varphi(\frac{1}{p_\tau})$ is an existential sentence that determines whether a field in $\mathcal{K}$ is not formally v-adic. Hence $\mathcal{K}$ has bounded τ-Stufe by Lemma 7.2.2.

For the converse direction, fix a positive primitive sentence ψ such that for all $M \in \mathcal{K}$, M is formally τ-adic if and only if $M \models \neg\psi$. Consider $L \in \mathcal{K}$ and $x \in L$, and let A be the finite-dimensional L-algebra from Lemma 7.2.5. Then A has a residue field with a τ-adic valuation if and only if L has a τ-adic valuation v with $vx < 0$. Thus $x \in R_\tau(L)$ if and only if no residue field of A is formally τ-adic, i.e. if and only if all residue fields of A satisfy ψ. By Lemma 2.1.3, this is the case if and only if $A \models \psi$. Since A is quantifier-freely interpretable in L, with parameter x and constants in K, we can express $A \models \psi$ as a positive existential formula of the variable x, which gives a definition of the v-holomorphy ring. □

Hence within a class $\mathcal{K}$ of extension fields of K closed under finite extensions, boundedness of τ-Stufe is equivalent to uniform existential definability of the τ-holomorphy ring. Again by analogy with the case of field orderings, one might call the latter property "boundedness of the τ-Pythagoras number". Such a notion of Pythagoras number for p-valuations is explored in forthcoming joint work of the author with S. Anscombe and A. Fehm.

For later use, we record the following standard fact about the Kochen operator.

Lemma 7.2.6. *Let L/K carry a valuation w above v such that $e(w/v) > e_\tau$ or $f(w/v) \nmid f_\tau$. Then there exists $x \in L$ such that $w(\gamma_\tau^\pi(x)) \leq -\frac{1}{e_\tau+1} w(\pi)$.*

Proof. If $f(w/v) \nmid f_\tau$, the residue field Lw does not embed into $\mathbb{F}_{q_\tau}$, so we may pick $x \in L$ whose reduction $\overline{x} \in Lw$ satisfies $\overline{x}^{q_\tau} - \overline{x} \neq 0$, and such that x avoids the finitely many poles of γ_τ^π. Inspecting the definition of the Kochen operator then shows that $w(\gamma_\tau^\pi(x)) \leq -w(\pi)$.

If $e(w/v) > e_\tau$, we may pick $x \in L$ with $0 < w(x) \leq \frac{w(\pi)}{e_\tau+1}$. Then $w(\gamma_\tau^\pi(x)) = ew(x) - w(\pi) \leq -\frac{1}{e_\tau+1} w(\pi)$. □

7.3 Algebraic fields have bounded τ-Stufe

In this section we give an example of a class of fields with bounded τ-Stufe: the class of algebraic fields above a given algebraic extension of $\mathbb{Q}$. The analogue of this result for the situation of orderings is Siegel's theorem that a totally positive element in a number field is a sum of four squares.

Fix $K/\mathbb{Q}$ algebraic and a type τ over K; this determines a p-valuation v on K for some $p = p_\tau$ and a unique (up to isomorphism) finite extension $F/\mathbb{Q}_p$ such that $F \models \tau$.

We can find a subfield $K' \subseteq K$ which is finite over $\mathbb{Q}$ such that (K, v) is an immediate extension of $(K', v|_{K'})$; then we may replace K by K' in the following, so assume that K is a number field. Write $\mathfrak{p}$ for the prime ideal in the ring of integers of K corresponding to the valuation v.

To determine whether an algebraic extension field of K is formally τ-adic, we use the splitting of central simple algebras as developed in Chapter 2 and used in Section 4.1.

Let $l > e_\tau \cdot f_\tau$ be an odd prime number, and fix a uniformiser π of (K, v). Choose central simple algebras $A, B/K$ of degree l satisfying the following properties:

- Neither A nor B split over the completion K_v;
- over every other completion $K_{v'}$, at least one of A and B split.

This is possible by Lemma 2.3.4. Note that F does not split A or B since $[F\colon K_v] = e_\tau \cdot f_\tau < l$.

In a finite extension L/K, write $R(L)$ for $T(A \otimes_K L) + T(B \otimes_K L)$. By Theorem 2.2.15 we have the equality

$$R(L) = \bigcap_w \mathcal{O}_w \cap L,$$

where the intersection is over all valuations w of L above v such that neither A nor B split over L_w; in particular, $R(L)$ is contained in the holomorphy domain $R_\tau(L)$.

The completion K_v has only finitely many extensions of degree $< l$ up to isomorphism; list all of them which are not τ-adic—i.e., do not embed into F—as $F_1, \ldots, F_n$. For each F_i/K_v pick a primitive element x_i; we may choose x_i to have non-negative valuation and to have its minimal polynomial f_i in $K[X]$. Then f_i does not have a zero in F and therefore its value set is bounded by completeness of F, say we have $v(f_i(x)) \leq v(p^{n_i})$ for each $x \in F$.

Proposition 7.3.1. *Let L/K be a finite extension, and let N be a natural number such that $N > \frac{v(p)}{v(\pi)}(e_\tau + 1)(1 + \sum_i n_i)$. Then L is formally τ-adic if and only*

if there exist $x \in L$, $y \in R(L)$, $z_1, \ldots, z_n \in L$ *such that*

$$\frac{1}{\pi} = \gamma_\tau^\pi(x)^N y \prod_{i=1}^{n} \frac{p^{n_i}}{f_i(z_i)}.$$

Proof. If L is formally τ-adic, let $\mathcal{O}$ be the valuation ring of a τ-adic valuation on L. Then there cannot be a solution to this equation, since all terms in the product on the right-hand side are contained in $\mathcal{O}$, but $\frac{1}{\pi}$ is not.

Assume conversely that L is not formally τ-adic, and list all its valuations above v as $w_1, \ldots, w_k$. Then for each w_j, either L_{w_j}/K_v is of degree $\geq l$, or L_{w_j} is isomorphic to some F_i. We wish to find $x \in L$, away from the poles of γ_τ^π, and $z_1, \ldots, z_n \in L$, z_i away from the zeroes of f_i, such that the following conditions are satisfied:

1. For each w_j such that L_{w_j}/K_v is of degree $\geq l$, $w_j(z_i) \geq 0$ for all i, and $w_j(\gamma_\tau^\pi(x)) \leq -\frac{1}{e_\tau+1} w(\pi)$;

2. for each w_j such that L_{w_j} is isomorphic to F_i, $w_j(z_{i'}) \geq 0$ for $i' \neq i$, $w_j(p^{n_i}/f_i(z_i)) \geq N w_j(\pi)$, and $w_j(x - (1+\pi)) > w_j(\pi)$.

Observe that the conditions imposed for each w_j are w_j-adically *open* conditions; hence weak approximation is applicable, so we only need to show for every single j that the conditions are satisfiable.

Let w be one of the w_j such that L_w is isomorphic to F_i, so f_i has a zero in L_w. Then we can find $z_i \in L$ with $w(p^{n_i}/f_i(z_i))$ arbitrarily large.

If L_w/K_v is of degree $\geq l > e \cdot f$, we can find $x \in L$ such that $w(\gamma_\tau^\pi(x)) \leq -\frac{1}{e_\tau+1} w(\pi)$ by Lemma 7.2.6.

Hence the conditions are jointly satisfiable. Rearranging, we find that

$$y = \frac{1}{\pi\gamma_\tau^\pi(x)^N \prod_{i=1}^n \frac{p^{n_i}}{f_i(z_i)}}$$

has non-negative valuation at each w_j, and therefore is contained in $R(L)$. This proves the claim. □

Corollary 7.3.2. *The class of algebraic extensions of K has bounded τ-Stufe.*

Proof. The statement of Proposition 7.3.1 gives an existential first-order sentence φ with parameters from K such that any finite extension field L/K is formally τ-adic if and only if $L \models \neg\varphi$. Hence the class of finite extensions of K has bounded τ-Stufe by the last point of Lemma 7.2.2. Algebraic extensions of K are obtained as unions of chains of finite extensions of K, hence this class also has bounded τ-Stufe. □

7.4 The τ-Stufe, Galois-theoretically

We can use the étale formalism from the last chapter to restate the conditions on being formally τ-adic.

Lemma 7.4.1. *There exists a collection of sentences Φ_τ in the étale language over K, closed under finite conjunction, such that for any field L/K we have $\mathrm{Et}_{L/K} \models \Phi_\tau$ if and only if L is formally τ-adic.*

Proof. This is a simple combination of Theorem 7.1.3 and Lemma 6.5.8; forcing Φ_v to be closed under finite conjunctions is no additional restriction, as we can replace any set of sentences by the set of finite conjunctions of its members. □

Corollary 7.4.2. *An elementary class $\mathcal{K}$ of extension fields of K has bounded τ-Stufe if and only if there exists $\varphi \in \Phi_\tau$ such that $L \in \mathcal{K}$ is formally τ-adic if and only if $\mathrm{Et}_{L/K} \models \varphi$.*

Proof. This is a consequence of first-order compactness in the following way. For every $L \in \mathcal{K}$, we have $L \models \tau_\forall$ if and only if $\mathrm{Et}_{L/K} \models \Phi_\tau$.

By interpretability, to each $\varphi \in \Phi_\tau$ we can associate a sentence φ^* in the field language with parameters in K such that for any field L/K we have $L \models \varphi^*$ if and only if $\mathrm{Et}_{L/K} \models \varphi$.

For all $L \in \mathcal{K}$ we therefore have $L \models \tau_\forall$ if and only if $L \models \Phi_\tau^* := \{\varphi^* \colon \varphi \in \Phi_\tau\}$. Since $\mathcal{K}$ is an elementary class, compactness implies that if either $\tau_\forall$ or Φ_τ^* is equivalent to a finite subset, then so is the other. As $\mathcal{K}$ having finite τ-Stufe means precisely that $\tau_\forall$ is equivalent to a single sentence in $\tau_\forall$, this yields the claim. □

Now fix an elementary class $\mathcal{K}$ of extension fields of K closed under finite extensions with bounded τ-Stufe, e.g. the class of models of the theory of algebraic extensions of $\mathbb{Q}$.

Lemma 7.4.3. *Let $\mathcal{E}_\mathcal{K}$ be the elementary class generated by the étale structures $\mathrm{Et}_{L/K}$, where $L \in \mathcal{K}$. Consider the class of fields $\mathcal{K}' = \{L'/K \colon \mathrm{Et}_{L'/K} \in \mathcal{E}_\mathcal{K}\}$. Then $\mathcal{K}'$ is an elementary class of extension fields of K closed under finite extensions with bounded τ-Stufe, and $\mathcal{K}' \supseteq \mathcal{K}$.*

Hence we may enlarge $\mathcal{K}$ to $\mathcal{K}'$ if we wish.

Proof. Clearly $\mathcal{K}' \supseteq \mathcal{K}$. Since $\mathrm{Et}_{L'/K}$ is interpretable in L' in the ring language with constants for K, $\mathcal{K}'$ is elementary. Since for any $L \in \mathcal{K}$ and

finite L'/L the category $\mathrm{Et}_{L'/K}$ is interpretable in $\mathrm{Et}_{L/K}$ by Lemma 6.5.6, the class $\mathcal{E}_{\mathcal{K}}$ is closed under passing to appropriate coslice categories; this exactly means that $\mathcal{K}'$ is closed under finite extensions. The class $\mathcal{K}'$ has bounded τ-Stufe by Corollary 7.4.2. □

Lemma 7.4.4. *Given $n > 0$ and $\mathcal{K}$ as above, there exists a formula $\varphi(x)$ in the étale language over K, with one free variable in the sort of objects of degree n, such that for any L/K and any étale algebra A/L of degree n we have $\mathrm{Et}_{L/K} \models \varphi(A)$ if and only if A is a formally τ-adic field.*

Proof. An étale algebra is a field if and only if it is not a product of two non-zero étale algebras—a definable condition. If A is a field, then by Lemma 6.5.6 and the preceding discussion, the structure $\mathrm{Et}_{A/K}$ is interpretable (up to elementary equivalence) in $\mathrm{Et}_{L/K}$ with the parameter A. Since the field is formally τ-adic if and only if $\mathrm{Et}_{A/K}$ satisfies a single first-order sentence by Corollary 7.4.2, this proves the claim. □

Given an extension field L/K and an algebraic extension F/L, we call a subextension E/L *maximal formally τ-adic* if E is formally τ-adic, but no proper extension of E within F is. Since every such E embeds into a τ-adic closure of L, by maximality it is necessarily the intersection of F with a τ-adic closure of L.

Proposition 7.4.5. *Let $L \in \mathcal{K}$ be a field such that L has a unique τ-adically closed algebraic extension. Then the same is true for any L' with $\mathrm{Et}_{L'/K} \equiv \mathrm{Et}_{L/K}$; in particular, any such L' has a unique τ-adic valuation.*

We can then deduce from the fact that the class of algebraic fields has bounded τ-Stufe for $\tau = \mathrm{Th}(\mathbb{Q}_p)$ that any field F with $\mathrm{Et}_F \succ \mathrm{Et}_{\mathbb{Q}}$ has a unique p-valuation.

Proof. We may assume that $\mathcal{K} = \mathcal{K}'$ in the notation above; in particular, this implies that L' and all its finite extensions are in $\mathcal{K}$. Since L is formally τ-adic, so is L' by Lemma 7.4.1.

For a finite Galois extension F/L, any two maximal formally τ-adic subextensions E,E' of F are intersections of F with a τ-adic closure L and therefore isomorphic over L by uniqueness of the τ-adic closure.

Note that the maximal formally τ-adic subextensions of a given finite extension F/L are definable on the étale side by Corollary 7.4.2. Therefore, by first-order transfer from $\mathrm{Et}_{L/K}$ to $\mathrm{Et}_{L'/K}$, any two maximal formally τ-adic subextensions of any finite Galois extension F/L' are isomorphic over L'. This implies that L' can have no more than one τ-adic closure up to isomorphism: If L'_1, L'_2 were non-isomorphic τ-adic closures, than a sufficiently large finite subextension of L'_1/L would not embed into L'_2 and vice versa, so we could enlarge to two non-isomorphic maximal formally τ-adic subextensions of some finite Galois extension of L'. □

7.5 THE τ-ADIC SPECTRUM

For an arbitrary field L/K, we define the *τ-adic spectrum* $S_\tau(L)$ to be the set of all τ-adic valuation rings on L. We endow $S_\tau(L)$ with the coarsest topology in which sets of the form $S_\tau(L;a) := \{\mathcal{O} \in S_\tau(L) \colon a \in \mathcal{O}\}$ are clopen, where $a \in L$. Note that this naturally expresses $S_\tau(L)$ as

a subspace of the space of all valuations on L with the constructible topology, defined in Section 4.2.

Lemma 7.5.1. *The space $S_\tau(L)$ is a Stone space, i.e. a totally disconnected compact Hausdorff space.*

Proof. This is an immediate consequence of Lemma 4.2.1, given that the τ-adic valuation rings $\mathcal{O}$ on L are exactly those subsets of L such that $(L, \mathcal{O}) \models \tau'_\forall$. □

Now let $\mathcal{K}$ be a class of extension fields of K which has bounded τ-Stufe and is closed under finite extensions. In the remainder of this section, we will prove the following generalisation of Proposition 7.4.5.

Theorem 7.5.2. *For $L \in \mathcal{K}$ such that each τ-adic valuation has a unique associated τ-adic closure, the boolean algebra of clopen subsets of $S_\tau(L)$ is interpretable in $\mathrm{Et}_{L/K}$. This is uniform along such L.*

Lemma 7.5.3. *Every clopen subset of $S_\tau(L)$ is of the form $S_\tau(L; a)$ for some $a \in L$.*

Proof. First observe that the complement of a clopen set $S_\tau(L; a)$, $a \neq 0$, is again of this form, by taking $b = \frac{1}{p_\tau a^n}$ for $n > e_\tau \cdot v(p_\tau)$ where v is normalised to have minimal positive element 1—this ensures that $w(p_\tau a^n) > 0$ if and only if $w(a) \geq 0$.

Hence the sets $S_\tau(L; a)$ are a subbasis of the topology. Since any clopen subset of $S_\tau(L)$ is compact, it is therefore expressible as a finite union of finite intersections of sets $S_\tau(L; a)$.

It remains to reduce to a single set. This can be done by observing that $S_\tau(L;a) \cap S_\tau(L;a') = S_\tau(a^n + p_\tau a'^n)$ for any $a, a' \in L$ with n as above, and expressing unions as complements of intersections. (Note that this is the same idea as using the functions g and h from the proof of Lemma 4.2.2; this is also available in the literature, see [Feh13, Lemma 7.1].) $\square$

We have previously encountered the condition that a τ-adic valuation on L extend to a τ-adic valuation on some finite extension field L'/L. We can now reinterpret this condition as follows: For any extension field L'/L, restriction of valuations gives a map $S_\tau(L') \to S_\tau(L)$. It follows immediately from the definition of the topology on S_τ that this map is continuous, and in particular has closed image since $S_\tau(L')$ is compact. Now a τ-adic valuation on L extends to a τ-adic valuation on L' if and only if it is in the image of this map.

It is convenient to make the following definition. Here, and for the remainder of this section, all algebras over fields will be implicitly commutative and unital.

Definition 7.5.4. *Let A/L be a finite-dimensional algebra. Write $S_\tau(A/L) \subseteq S_\tau(L)$ for the set of τ-adic valuations on L that extend to some residue field of A.*

We say that A is formally τ-adic *if one of its residue fields is, which is equivalent to $S_\tau(A/L)$ being non-empty.*

We note in passing that A being formally τ-adic is $\mathcal{L}_{\text{ring}}(K)$-definable: Specifically, A is formally τ-adic if and only if it satisfies the negation-normal conjunction-free negative fragment of $\tau_\forall$, i.e. if and only if A

satisfies no positive primitive sentences not in τ. This is easily deduced from Lemma 2.1.3, using that every existential formula is equivalent under the theory of fields to a positive primitive one.

We observe that for any finite-dimensional algebra A/L, the quotient A_{red} of A by its nilradical is a product of finite field extensions of L and therefore an étale algebra as we work in characteristic 0; furthermore, the residue fields of A_{red} and A agree.

Lemma 7.5.5. *For any algebra A/L of dimension $\leq n$ there exists an étale algebra B/L of dimension equal to $n!$ with $S_\tau(A/L) = S_\tau(B/L)$.*

Proof. The algebra A_{red}/L is étale and of degree $\leq n$, hence its degree divides $n!$; therefore we may choose $B = A_{\mathrm{red}}^k$ for suitable k. □

Lemma 7.5.6. *For every clopen subset C of $S_\tau(L)$ there exists an algebra A/L of dimension $2e_\tau q_\tau$ such that $C = S_\tau(A/L)$.*

Proof. The complement of C is of the form $S_\tau(L; a)$ for some $a \in L$, i.e. $v \in C$ if and only if $va < 0$. Lemma 7.2.5 gives a finite L-algebra $A = L[Y]/(f(a, Y))$ such that for any τ-adic valuation v on L, $va < 0$ if and only if v extends to a τ-adic valuation on a residue field of A. By inspection, the L-dimension of A is $2e_\tau q_\tau$. □

Lemma 7.5.7. *Assume that every τ-adic valuation on L has a unique τ-adic closure up to isomorphism. Let $A_1, A_2/L$ be finite-dimensional algebras.*

1. $S_\tau(A_1/L) \cup S_\tau(A_2/L) = S_\tau(A_1 \times A_2)$
2. $S_\tau(A_1/L) \cap S_\tau(A_2/L) = S_\tau(A_1 \otimes_L A_2)$

3. *$S_\tau(A_1/L) = S_\tau(L)$ if and only if there exists no formally τ-adic étale algebra A_3 of dimension $(2e_\tau q_\tau)!$ with $A_3 \otimes_L A_1$ not formally τ-adic.*

Proof. For the first part, observe that every residue field of $A_1 \times A_2$ is also a residue field of A_1 or A_2, and conversely every residue field of A_1 and A_2 occurs. This implies the statement.

For the second part, let $v \in S_\tau(A_1/L) \cap S_\tau(A_2/L)$. Then v extends to some residue field L_1 of A_1 and some residue field L_2 of A_2. This means that both L_1 and L_2 embed into a τ-adic closure of L with respect to v. By assumption, there is a unique such closure L_v. By the universal property of the tensor product, the maps $A_i \to L_i \hookrightarrow L_v$ give rise to a homomorphism $A_1 \otimes_L A_2 \to L_v$, so v extends to some residue field of $A_1 \otimes_L A_2$. This proves $S_\tau(A_1 \otimes_L A_2) \supseteq S_\tau(A_1/L) \cap S_\tau(A_2/L)$. For the converse inclusion, it suffices to note that every residue field of $A_1 \otimes_L A_2$ embeds a residue field of A_1 and a residue field of A_2 through the maps $A_i \to A_1 \otimes_L A_2$.

For the third part, if there exists A_3 with the required properties, then $S_\tau(A_3/L)$ is non-empty and disjoint from $S_\tau(A_1/L)$, hence $S_\tau(A_1/L) \neq S_\tau(L)$. For the converse direction, assume that $S_\tau(A_1/L) \neq S_\tau(L)$. The set $S_\tau(A_1/L)$ is closed: listing the residue fields of A_1 as $L_1, \ldots, L_k$, we see that $S_\tau(A_1/L)$ is the union of the images of the maps $S_\tau(L_i) \to S_\tau(L)$ given by restriction of valuations, and these restriction maps are continuous and therefore have compact image.

Therefore $S_\tau(L) \setminus S_\tau(A_1/L)$ contains a non-empty clopen set, and this clopen set is of the form $S_\tau(A_3/L)$ for some A_3 with the desired properties by Lemmas 7.5.6 and 7.5.5. □

Lemma 7.5.8. *For $n > 0$, the condition that an étale algebra A of dimension n over some $L \in \mathcal{K}$ be formally τ-adic is first-order definable in* $\mathrm{Et}_{L/K}$. *More formally, there exists a formula $\varphi(x)$ in the étale language over K, with a single free variable in the sort of objects of degree n, such that for any $L \in \mathcal{K}$ and A as above we have* $\mathrm{Et}_{L/K} \models \varphi(A)$ *if and only if A is formally τ-adic.*

Proof. The algebra A is formally τ-adic by definition if and only if there exists an L-homomorphism $A \to L'$ into a formally τ-adic field L'. The degree of L'/L may be bounded by n. One can now easily derive a formula as required from the formula in Lemma 7.4.4. □

Proof of Theorem 7.5.2. Let $N = (2e_\tau q_\tau)!$. By Lemmas 7.5.6 and 7.5.5, for every clopen set $C \subseteq S_\tau(L)$ there exist étale algebras $A_1, A_2/L$ of dimension N with $C = S_\tau(A_1/L)$, $S_\tau(L) \setminus C = S_\tau(A_2/L)$. Conversely, the condition that two étale algebras A_1, A_2 of dimension N have $S_\tau(A_1/L)$ and $S_\tau(A_2/L)$ disjoint with union $S_\tau(L)$ is a definable condition in the étale language over K by Lemmas 7.5.7 and 7.5.8.

Given two such pairs (A_1, A_2) and (B_1, B_2), the condition that the sets $S_\tau(A_1/L)$ and $S_\tau(B_1/L)$ be equal is again definable in Et_L; this gives a definable equivalence relation. By construction, the equivalence classes are in bijection to the clopen subsets of $S_\tau(L)$.

The operation of union is definable: Given (A_1, A_2) and (B_1, B_2), there exist (C_1, C_2) of degree N with

$$S_\tau(C_1/L) = S_\tau(A_1 \times B_1/L) = S_\tau(A_1/L) \cup S_\tau(B_1/L)$$

and

$$S_\tau(C_2/L) = S_\tau(A_2 \otimes_L B_2/L) = S_\tau(A_2/L) \cap S_\tau(B_2/L),$$

and this is a definable condition by the same lemmas.

This gives a uniform interpretation of the boolean algebra of clopen subsets of $S_\tau(L)$ in $\mathrm{Et}_{L/K}$ as required, uniformly in L. □

7.6 pseudo-S-closed fields

In this section, we give an example where Theorem 7.5.2 can be applied.

Definition 7.6.1. *Let K be a field and $S = \{\tau_1, \ldots, \tau_n\}$ a finite collection of types over K in the sense of Definition 7.1.1. Assume that any two of the valuations $v_1, \ldots, v_n$ of K below the τ_i are either the same or independent, and assume furthermore that K is dense in its henselisation with respect to v_i for any i. (Both these assumptions are satisfied if all v_i are of rank 1.)*

Then an extension field L/K is called pseudo-S-closed *if every absolutely irreducible L-variety V has an L-point provided it has a smooth L'-point for every L'/L satisfying $L' \models \tau_i$ for some i.*

One can easily extend this definition by allowing S to also contain theories of real-closed extension fields of K, as hinted after Definition 7.1.1.

This notion of being pseudo-S-closed is a slight modification of the fields pseudo-S^τ-closed with respect to classical closures (PS^τCC) studied in [Feh13], the main difference being that loc. cit. works with coarse types (e, f) as opposed to types τ in our sense.

This also ties in with Pop's notion of *pseudo classically closed fields* from [Pop03]: A non-formally real field is PCC if and only if it is pseudo-S-closed for some finite set of types S over $\mathbb{Q}$ by [Feh13, Proposition 4.6].

We will make use of the fact that any finite extension of a PCC field is again PCC by [Pop03, Corollary 2.13].

Fix K and $S = \{\tau_1, \ldots, \tau_n\}$ as above.

Proposition 7.6.2. *There is a class $\mathcal{K}$ of extension fields of K satisfying the following properties:*

1. *Every pseudo-S-closed field is in $\mathcal{K}$;*
2. *any finite extension of a field in $\mathcal{K}$ is in $\mathcal{K}$;*
3. *on any $L \in \mathcal{K}$, any τ_i-adic valuation has a unique τ_i-adic closure for every i;*
4. *the class $\mathcal{K}$ has bounded τ_i-Stufe for every i.*

This means that Theorem 7.5.2 applies, giving a way of uniformly interpreting the τ_i-adic spectrum in the étale categories of pseudo-S-closed fields.[3]

The main challenge in the proof of this proposition is proving boundedness of the τ_i-Stufe.

Lemma 7.6.3. *Let K be a PCC field and A/K a central simple algebra. Then A splits over K if and only if it splits over all henselisations K_v, where v is a p-valuation on K for any p.*

Proof. To A we may associate a *Severi–Brauer variety* V, a smooth absolutely irreducible variety which has an L-point over precisely those fields

[3] It is perhaps worth pointing out that Pop in loc. cit. uses topologies on the space of decomposition groups of valuations inside the absolute Galois group of PCC fields, which is reminiscent of (if not immediately technically related to) our way of recovering the constructible topology on valuations by Galois-theoretic information.

L which split A. (See [GS17, Chapter 5].) Then the claim follows from the local–global principle for absolutely irreducible varieties. □

As above, write v_i for the valuation on K below τ_i; note that the v_i are not necessarily distinct. Choose a large prime l.

Lemma 7.6.4. *There exists a central simple algebra A/K of degree l which does not split over K_{v_1}, but splits over all K_{v_i} with $v_i \neq v_1$.*

Proof. Let K'/K be a cyclic extension of degree l in which every $v_i \neq v_1$ splits completely, but such that $K'K_{v_1}/K_{v_1}$ is unramified of degree l. Such an extension can be obtained from the general Grunwald-Wang style theorems in [LR03].[4]

Take a uniformiser $\pi \in K$ for v_1 and let A/K be a cyclic central simple algebra induced by π and K'. Then A is as desired. □

Write $e = e_{\tau_1}$, $f = f_{\tau_1}$, let $\pi \in K$ be a uniformiser for v_1, and let $\gamma = \gamma^{\pi}_{\tau_1}$ be the Kochen operator as in (7.1).

Lemma 7.6.5. *Let L/K be a PCC field. Then the space of p-valuations of L above v_1 is a compact space of independent valuations in the constructible topology. Furthermore, there exists a monic polynomial $g \in \mathbb{Z}[X]$ whose reduction has no root in any of their residue fields.*

Proof. By [Pop03, Corollary 2.11, Theorem 2.9], all p-valuations of L are pairwise independent. Furthermore, they have only finitely many

[4]This is the only point where we need that K is dense in its henselisations with respect to the v_i. In fact, it seems likely that in the situation of unramified extensions one can dispense with this assumption, by using a specialisation argument as in [Sal82, Theorem 5.9].

distinct types over $\mathbb{Q}$, and hence only finitely many finite fields (up to isomorphism) occur as their residue fields; this easily allows finding a polynomial g as required. Finiteness also allows us to find a type σ over $\mathbb{Q}$ such that any p-valuation of L above v_1 is σ-adic.

Now a valuation on L is a p-valuation above v_1 if and only if its valuation ring contains the valuation ring of v_1, its maximal ideal contains the maximal ideal of v_1, and its valuation ring contains $\gamma_\sigma^p(x)$ for all $x \in L$. All these are constructibly closed conditions, so the space in question is a closed subspace of the compact space of all valuations. □

Lemma 7.6.6. *A PCC field L/K has a valuation w above v_1 with $f(w/v_1) \mid f$ and $e(w/v_1) \leq e$ if and only if for every $x \in L$, $L(\sqrt[l]{1+\pi\gamma(x)^l})$ does not split A.*

Hence there exists a positive primitive sentence φ with parameters from K, independent of L, such that L has such a valuation if and only if $L \models \neg\varphi$.

Proof. If L has a valuation of the desired kind, then there is an extension of it to the field in question satisfying the same conditions on inertia degree and initial ramification, so A does not split.

Conversely, if there are no such valuations, then for every p-valuation v of L above v_1 there exists $x \in L$ such that $v(1+\pi\gamma(x)^l) < 0$ by Lemma 7.2.6; by the Approximation Lemma 4.2.2, find one such x globally. (Applicability of the Approximation Lemma is precisely Lemma 7.6.5.) Then $L(\sqrt[l]{1+\pi\gamma(x)^l})$ is PCC and A splits everywhere locally in it, so it splits globally.

The splitting of A over $L(\sqrt[l]{1+\pi\gamma(x)^l})$ is an existentially definable condition, and we can transform an existential sentence into a positive primitive one in the usual way. □

Lemma 7.6.7. *The class $\mathcal{K}$ of finite extension fields of pseudo-S-closed fields above K has bounded τ_1-Stufe.*

Proof. Let K_i be the minimal p-adically closed subextension of K_{τ_i}/K. For every τ_i, $i \neq 1$, precisely one of the following conditions holds:

1. The valuation v_i of K below τ_i is distinct from v_1;
2. $v_i = v_1$ but the closures K_{τ_1} and K_{τ_i} do not embed into one another over K;
3. $v_i = v_1$ and K_{τ_1} embeds into K_{τ_i} over K;
4. $v_i = v_1$ and K_{τ_i} embeds into K_{τ_1} over K.

Write $n = e_{\tau_1} \cdot f_{\tau_1}$. Take a finite subextension M of K_{τ_1}/K such that, for all i satisfying the second condition, the composite $K_{\tau_i}M$ (for any choice of embedding inside an algebraic closure of K) has degree larger than n over K_i.

Now for any $L \in \mathcal{K}$, L is formally τ_1-adic if and only if LM has a valuation w above v_1 with $e(w/v_1) \leq e_{\tau_1}$ and $f(w/v_1) \mid f_{\tau_1}$ for some way of forming the composite in the algebraic closure.

This is a universally definable condition: Let $f \in K[X]$ be a monic polynomial such that $M \cong K[X]/(f)$. Then L is not formally τ_1-adic if and only if $L[X]/(f) \models \varphi$, where φ is the positive primitive sentence from Lemma 7.6.6. □

Proof of Proposition 7.6.2. Let $\mathcal{K}$ be the class of fields which are finite extensions of pseudo-S-closed fields. All fields in $\mathcal{K}$ are pseudo classically closed. By [Pop03, Theorem 2.9], every pseudo classically closed field is dense in any of its p-adic closures. Hence the value group of every p-valuation is a $\mathbb{Z}$-group, which implies that every τ-adic valuation on any field in $\mathcal{K}$ has a unique τ-adic closure, for any type τ.

Lastly, $\mathcal{K}$ has bounded τ_1-Stufe by the last Lemma, and by symmetry this applies to all other τ_i as well. □

BIBLIOGRAPHY

[AF17] Sylvy Anscombe and Arno Fehm, *Charaterizing diophantine henselian valuation rings and valuation ideals*, Proc. London Math. Soc. **115** (2017), 293–322.

[AM65] Michael Francis Atiyah and Ian Grant Macdonald, *Notes on commutative algebra*, Oxford, Mathematical Institute, 1965.

[Bla78] Georges Blanc, *Équivalence naturelle et formules logiques en théorie des catégories*, Archiv math. Logik **19** (1978), 131–137.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Springer, 1990.

[Cha90] Zoé Chatzidakis, *On the cohomological dimension of non-standard number fields*, J. Pure Appl. Algebra **69** (1990), 121–133.

[Cha99] ———, *Simplicity and independence for pseudo-algebraically closed fields*, Models and Computability, London Mathematical Society Lecture Notes, vol. 259, Cambridge University Press, 1999, pp. 41–61.

[Cha02] ———, *Properties of forking in ω-free pseudo-algebraically closed fields*, J. Symbolic Logic (2002), 957–996.

[Che75] Gregory L. Cherlin, *Ideals of integers in nonstandard number fields*, Model Theory and Algebra: A memorial tribute to Abraham Robinson, Springer, Berlin, 1975, pp. 60–90.

[Coh05] Stephen D. Cohen, *Explicit theorems on generator polynomials*, Finite Fields Appl. (2005), 337–357.

[CTG15] Jean-Louis Colliot-Thélène and Jan Van Geel, *Le complémentaire des puissances n-ièmes dans un corps de nombres est un ensemble diophantien*, Compositio Math. **151** (2015), 1965–1980.

[CvdDM82] Gregory Cherlin, Lou van den Dries, and Angus Macintyre, *The elementary theory of regularly closed fields*, Preprint, 1982.

[Dit18] Philip Dittmann, *Irreducibility of polynomials over global fields is diophantine*, Compositio Math. **154** (2018), no. 4, 761–772.

[Eis05] Kirsten Eisenträger, *Integrality at a prime for global fields and the perfect closure of global fields of characteristic $p > 2$*, J. Number Theory **114** (2005), 170–181.

[EM16] Kirsten Eisenträger and Travis Morrison, *Universally and existentially definable subsets of global fields*, To appear in Math. Res. Lett., available as arXiv:1609.09787 [math.NT], 2016.

[EP05] Antonio J. Engler and Alexander Prestel, *Valued fields*, Springer, 2005.

[Feh13] Arno Fehm, *Elementary geometric local-global principles for fields*, Ann. Pure Appl. Logic (2013), 989–1008.

[FJ10] Michael Fried and Moshe Jarden, *Field arithmetic*, third ed., Springer, 2010.

[FKS81] Burton Fein, William M. Kantor, and Murray Schacher, *Relative Brauer groups II*, J. reine angew. Math. **328** (1981), 39–57.

[Fre07] Günther Frei, *The unpublished section eight: On the way to function fields over a finite field*, The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae (Catherine Goldstein, Norbert Schappacher, and Joachim Schwermer, eds.), Springer, 2007, pp. 159–198.

[GS17] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, second ed., Cambridge University Press, 2017.

[HK94] Roland Huber and Manfred Knebusch, *On valuation spectra*, Contemporary Mathematics **155** (1994), 167–206.

[Hod97] Wilfrid Hodges, *A shorter model theory*, Cambridge University Press, 1997.

[IT14] Luc Illusie and Michael Temkin, *Exposé X. Gabber's modification theorem (log smooth case)*, Travaux de Gabber sur l'uniformisation locale et la cohomologie étale des schémas quasi-excellents (Luc Illusie, Yves Laszlo, and Fabrice Orgogozo, eds.), Astérisque, vol. 363–364, Société Mathématique de France, 2014, pp. 167–212.

[Jac09] Nathan Jacobson, *Basic algebra II*, second ed., Dover, 2009.

[JR79] Moshe Jarden and Jürgen Ritter, *On the characterization of local fields by their absolute galois groups*, J. Number Theory **11** (1979), 1–13.

[Koe16] Jochen Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Ann. Math. **183** (2016), 73–93.

[KS06] Masaki Kashiwara and Pierre Schapira, *Categories and sheaves*, Grundlehren der mathematischen Wissenschaften, vol. 332, Springer, 2006.

[KS12] Moritz Kerz and Shuji Saito, *Cohomological Hasse principle and motivic cohomology for arithmetic schemes*, Publ. Math. IHES **115** (2012), no. 1, 123–183.

[Lan70] Serge Lang, *Algebraic number theory*, Addison-Wesley, 1970.

[LR03] Falko Lorenz and Peter Roquette, *The theorem of Grunwald–Wang in the setting of valuation theory*, Valuation Theory and its Applications Volume II, Fields Institute Communications, American Mathematical Society, 2003, pp. 175–212.

[Mak95] Michael Makkai, *First order logic with dependent sorts, with applications to category theory*, available from the author's website `www.math.mcgill.ca/makkai`, 1995.

[Mil70] John Milnor, *Algebraic K-theory and quadratic forms*, Inventiones math. **9** (1970), 318–344.

[Mor17] Travis Morrison, *Diophantine definability of nonnorms of cyclic extensions of global fields*, unpublished, available as arXiv:1710.07357 [math.NT], 2017.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Springer, 2008.

[OVV07] Dmitri Orlov, Alexander Vishik, and Vladimir Voevodsky, *An exact sequence for $K_*^M/2$ with applications to quadratic forms*, Ann. of Math. **165** (2007), 1–13.

[Par13] Jennifer Park, *A universal first order formula defining the ring of integers in a number field*, Math. Res. Lett. **20** (2013), 961–980.

[Pfi65] Albrecht Pfister, *Multiplikative quadratische Formen*, Arch. Math. **XVI** (1965), 363–370.

[Pfi95] ———, *Quadratic forms with applications to algebraic geometry and topology*, Cambridge University Press, 1995.

[Poo09] Bjorn Poonen, *Characterizing integers among rational numbers with a universal-existential formula*, Amer. J. Math. **131** (2009), no. 3, 675–682.

[Pop88] Florian Pop, *Galoissche Kennzeichnung p-adisch abgeschlossener Körper*, J. reine angew. Math. **392** (1988), 145–175.

[Pop02] ———, *Elementary equivalence versus isomorphism*, Inventiones math. **150** (2002), 385–408.

[Pop03] ———, *Classically projective groups and pseudo classically closed fields*, Valuation Theory and its Applications Volume II, Fields Institute Communications, AMS, 2003, pp. 251–284.

[Pop17] ———, *Elementary equivalence versus isomorphism II*, Algebra & Number Theory **11** (2017), 2091–2111.

[PR84] Alexander Prestel and Peter Roquette, *Formally p-adic fields*, Lecture Notes in Mathematics, no. 1050, Springer, Berlin Heidelberg New York Tokyo, 1984.

[Pre85] Anne Preller, *A language for category theory in which natural equivalence implies elementary equivalence of models*, Zeitschr. f. math. Logik und Grundlagen d. Math. **31** (1985), 227–234.

[Roq05] Peter Roquette, *The Brauer–Hasse–Noether Theorem in historical perspective*, Schriften der Mathematisch-naturwissenschaftlichen Klasse, no. 15, Springer, 2005.

[Ros02] Michael Rosen, *Number theory in function fields*, Springer, 2002.

[Rum80] Robert S. Rumely, *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. **262** (1980), no. 1, 195–217.

[Sal82] David J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982), 250–283.

[SGA71] *Revêtements Étales et groupe fondamental*, Lecture Notes in Mathematics, no. 224, Springer, Berlin Heidelberg New York, 1971, Séminaire de Géométrie Algébrique du Bois Marie 1960/61.

[Shl94] Alexandra Shlapentokh, *Diophantine classes of holomorphy rings of global fields*, J. Algebra **169** (1994), 139–175.

[Sta18] *Stacks project*, `http://stacks.math.columbia.edu`, 2018.

[Sza09] Tamás Szamuely, *Galois groups and fundamental groups*, Cambridge University Press, 2009.

[Vid00] Carlos R. Videla, *Definability of the ring of integers in pro-p Galois extensions of number fields*, Israel J. Math. **118** (2000), 1–14.

[Voe03] Vladimir Voevodsky, *Motivic cohomology with $\mathbb{Z}/2$-coefficients*, Publ. Math. IHES **98** (2003), 59–104.

[Voe11] ———, *On motivic cohomology with $\mathbb{Z}/l$-coefficients*, Ann. of Math. **174** (2011), 401–438.