Existential decidability in power series rings over finite fields

Tysger Boelens

Master's Thesis
MSc Mathematical Sciences
Utrecht University

supervised by Prof Gunther Cornelissen

July 17th, 2020

Utrecht University

This is the Master's Thesis of Tysger (T.Y.M.) Boelens, student number 6665314, Utrecht University, submitted in order to receive the Master's degree in Mathematical Sciences.
The work on this thesis was supervised by Prof Gunther Cornelissen at Utrecht University in the period October 2019 – July 2020. The second reading of the thesis was done by Dr Marta Pieropan.

Voor Daphne

Abstract

In this Master's Thesis we study two ways of answering the following question: is there an algorithm that decides the truth of existential statements about the power series ring over a finite field?

The first approach to the problem uses tools from algebraic geometry and is described in the article *On the decidability of the existential theory of* $\mathbf{F}_p[[t]]$ by Jan Denef and Hans Schoutens (1999, [9]). It is shown that the truth of an existential statement in a ring R corresponds to the existence of a rational point on a scheme over the spectrum of R. We study a form of Artin approximation that allows to related decidability in power series rings to decidability in the finite residue field. Finally, we look at the dependency of the results of Denef and Schoutens on the Resolutions of Singularities conjecture.

The other approach is the one described by Arno Fehm and Sylvy Anscombe in the article *The existential theory of equicharacteristic henselian valued fields* (2016, [1]). Here the problem is studied in the context of the model theory of valued fields. Using results by Franz-Viktor Kuhlmann on a special class of henselian valued fields, it can be shown that the truth of existential statements transfers for a larger class of henselian valued fields with finite residue field, of which the power series ring over a finite field is an example.

Besides trying to understand the details of the proofs in the two articles mentioned above, a short introduction to the relevant fields of mathematics is given.

Preface

I would like to use this preface to thank some people whose help was a necessary condition for finishing this thesis: first of all my supportive supervisor, Gunther Cornelissen, who has drawn me out of my mathematical comfort zone. I also am grateful to Marta Pieropan, for finding the time to be the second reader of the thesis and her helpful comments at the final stage of this thesis. Furthermore, I would like to thank Hans Schoutens for answering some questions about his paper.

This thesis could also not have been written without the support of my family and friends. Most of all, I am thankful for the love and enthusiasm of Daphne.

Groningen,
July 17th, 2020.

Contents

Chapter 1

Introduction

In this introduction, we will give a quick and informal introduction to the question that is studied in this thesis. This question is:

Is the power series field over a finite field existentially decidable?

Now, what does it mean? Roughly speaking, we are interested in whether there exists an 'mechanical' way of determining the veracity of a special type of statement about an algebraic object. We will first introduce this object.

Let $\mathbf{F}_q$ be the finite field with q elements, where q is a prime power. The object we are studying consists of all power series with coefficients in $\mathbf{F}_q$, i.e. all expressions of the form

$$a_0 t^0 + a_1 t^1 + a_2 t^2 + \cdots$$

with $a_i \in \mathbf{F}_q$ and n an integer, with possibly an infinite number of terms. By adding and multiplying the power series just as we do with polynomials we make this object into a ring. We call this ring the *power series ring over* $\mathbf{F}_q$ and we write $\mathbf{F}_q[[t]]$.

We can formulate statements about this ring using the 'ring language' that consists of the equality symbol $=$, the functions $+$, $-$, $\cdot$ and the constants 0 and 1. An *existential statement* in this language is a sentence of the form 'there exist power series $f_1, \ldots, f_k$ such that $\ldots$' followed by a expression in the ring language and the variables $f_1, \ldots, f_k$. An example is the statement

$$\text{There exists a power series } f \text{ such that } f \cdot f \cdot f = 1 - f.$$

We could also formulate statements in a richer language by adding the constant t to the language, so that we can write expressions as $f \cdot f = t^2 - 3 \cdot t$.

We have a class of statements about a certain ring: these statements are either true of false. Naturally, we would like to be able to determine which of these two

is the case, for a given existential statement. Our research question above can be rephrased to 'is there an algorithm that can decide whether an existential statement is true or not?'

In this thesis, we will study two articles on this matter that differ considerably in a number of aspects. However, in both cases the answer to our question is a yes, be it conditional in one of the papers. We now give a quick overview of the way in which these articles try to answer our question. In the last chapter we will study differences and similarities between the articles in more detail.

Two approaches

The first article we study is written by Jan Denef and Hans Schoutens ([9]). In it we try to solve the problem with a algebro-geometric toolkit. It is worth noting that they consider statement formulated in the larger language that includes the constant t.

We translate the problem in geometric terms by noting that an existential statement about $\mathbf{F}_q[[t]]$ can always be written as a system of equations such that a solution of this system corresponds to the existence of a $\mathbf{F}_q[[t]]$-rational point on an open set W of a closed subscheme X of affine space over $\mathbf{F}_q[[t]]$.

We show that – given that the generic fibre of X is non-singular – the existence of such a $\mathbf{F}_q[[t]]$-rational point on W implies the existence of such a point on X. Using a form of Artin approximation, we can check whether X has a $\mathbf{F}_q[[t]]$-rational point by checking if a finite number of equations over $\mathbf{F}_q$ holds, which implies that the problem is decidable.

However, we cannot always ensure that the singularities of the generic fibre of X can be resolved by a blow-up, as the Resolution of Singularities conjecture is not yet proven in positive characteristic, so the result of Denef and Schoutens is conditional.

In the second article ([1]), by Arno Fehm and Sylvy Anscombe, we look at the problem from the point of view of the model theory of valued fields. To be able to do so, we move our attention from the ring $\mathbf{F}_q[[t]]$ to its fraction field $\mathbf{F}_q((t))$ (the field of Laurent series over $\mathbf{F}_q$ with a finite number of negative terms). This field has a natural valued field structure.

As we are working in a valued field, we use the valued field language that is an extended version of the ring language, but that is weaker than the language Denef and Schoutens use.

To answer the question of existential decidability in $\mathbf{F}_q((t))$, we study some deeper results by Franz-Viktor Kuhlmann about the class of tame valued fields, even though $\mathbf{F}_q((t))$ itself is not a member of this class. Looking at a larger class (called $\mathbf{H}$) of valued fields, these results of Kuhlmann allow us to infer

that certain statements are true in all models in **H** if they hold in one of these models.

Ignoring a lot of details, we now have a form of completeness: if the negation of an existential statement does not hold, there should be a model in which the statement is true. The result above implies that the statement holds in all models. So either the statement holds or its negation holds. From this form of completeness it follows that we have existential decidability, as we can write an algorithm that derives all logical consequences of the axioms of **H**: this algorithm will eventually derive the statement or its negation.

Structure of the thesis

The thesis is divided in three parts: in the first we develop the algebraic and logical tools we need, including the theory of valued fields. The second part is devoted to geometry. Starting with commutative algebra, we give a short overview of algebraic geometry using the language of schemes. A separate chapter covers a proof Artin approximation that uses non-standard analysis. The last part of the thesis covers in detail the reasoning in the two articles discussed above, and ends with a comparison between the two approaches.

In Chapter 2, we define (ordered) groups, rings, modules and the like. Following [20], we derive some basic results about separable extensions. The chapter concludes with a bit of Galois theory which is needed for a structure result about field extensions of $\mathbf{F}_q((t))$.

All logical machinery is introduced in Chapter 3. Most of the chapter is spent on model theory, especially the concept of (logical) completeness. Besides, we introduce ultrapowers as they are used in the proof of Artin approximation later on.

In Chapter 4, we give a short overview of the theory of valued fields based on [13]. As they are the focus of the article of Anscombe and Fehm, a lot of attention is given to henselian fields and power series fields. We end the chapter with a axiomatization of the theory of valued fields.

Building on the concepts already defined, we develop the necessary commutative algebra in Chapter 5. Again we return to henselianity and also the stronger notion of (algebraic) completeness. In the chapter we also prove some algebraic lemmas that are used in the article of Denef and Schoutens.

The basic notions of modern algebraic geometry are discussed in Chapter 6. After we have defined sheaves and schemes, we cover rational points in detail and study proper morphisms.

In Chapter 7, we prove a form of Artin approximation for excellent equicharacteristic henselian local rings, reducing this to the case of a power series ring in a finite number of variables over a field and then applying non-standard analysis.

The algebro-geometric approach by Denef and Schoutens is studied in Chapter 8. We give some background information on the Resolution of Singularities conjecture assumed in their proof. A great deal of attention is given to the implicit technical details in the proof of Denef and Schoutens.

Chapter 9 – on the model-theoretic appraoch of Fehm and Anscombe – starts with a description of the model theory of tame valued fields. After that, we give a set of axioms of which $\mathbf{F}_q((t))$ is a model and define the class $\mathbf{H}$ mentioned above, and derive the existential decidability from a completeness result.

Conventions

We will assume the Axiom of Choice holds, which is equivalent to Zorn's Lemma. If we need this in a proof, it will be mentioned.

Unless indicated otherwise, we will operate under the following assumptions regarding notation and terminology in this thesis.

The word 'iff' will be used as a shorthand for 'if and only if'.

We write $A \subseteq B$ to indicate that A is either a proper subset of B or that $A = B$. We write $A \subset B$ for '$A \subseteq B$ and $A \neq B$'.

By the natural numbers $\mathbf{N}$ we mean $\{0, 1, 2, \ldots\}$.
By the integers $\mathbf{Z}$ we mean $\{\ldots, -1, 0, 1, 2, \ldots\}$.
The rational numbers $\mathbf{Q}$ consist of all fractions a/b with $a \in \mathbf{Z}$ and $b \in \mathbf{N} \backslash \{0\}$.

Throughout, p will stand for a fixed prime number and q for a fixed power of p.

A group is always a commutative group, and a ring is always a commutative ring with a unit element denoted by 1. In a ring it can be true that $0 = 1$, although this only holds for the one-element ring.

We follow the usual terminology in algebraic geometry and call a topological space quasi-compact if every open cover of it has a finite subcover. A compact space is a quasi-compact space that has the Hausdorff property.

Occasionally, we will refer to a finite tuple of variables by $\bar{x}$. The length of this tuple will be indicated where it is not clear from the context.

Part I

Algebraic and logical preliminaries

Chapter 2

Rings, fields and groups

In this chapter we will define the algebraic objects that we will need later on, such as (ordered) groups, rings and fields.

2.1 Groups and orders

DEFINITION 2.1.1. An (abelian or commutative) *group* is a set G together with a binary function $+ : G \times G \to G$, a unary function $- : G \to G$ and a constant $0 \in G$, satisfying for all $g, h, k \in G$:

- $g + h = h + g$;
- $g + 0 = g$;
- $g + (-g) = 0$;
- $g + (h + k) = (g + h) + k$.

As mentioned, we will only consider commutative groups, so we omit the adjective 'commutative' from now on.

DEFINITION 2.1.2. A *subgroup* of a group G is a subset H of G such that

- $0 \in H$;
- if $h \in H$, then $-h \in H$;
- if $h, h' \in H$, then $h + h' \in H$.

EXAMPLE 2.1.3. The integers $\mathbf{Z}$ with their usual addition are a group. Its subgroups are $n\mathbf{Z} = \{na : a \in \mathbf{Z}\}$ for $n \in \mathbf{N}$.
The group with one element which is 0 is denoted 0.

DEFINITION 2.1.4. Let G be a group and H a subgroup. The *quotient group* G/H of G by H is the set G modulo the following equivalence relation: $g \sim g'$ if $g - g' \in H$. The operation $[g] + [g'] = [g + g']$ is well-defined and makes the set of equivalence classes into a group.
We write $[G : H]$ for the number of equivalence classes in G/H. It can be infinite.

EXAMPLE 2.1.5. The factor group of the integers by the subgroup $n\mathbf{Z}$ is the group $\mathbf{Z}/n\mathbf{Z}$ of n elements.

DEFINITION 2.1.6. Let G_1 and G_2 be groups. The *product group* $G_1 \times G_2$ is the cartesian product of the sets G_1 and G_2, equipped with the following group operation:

$$(g_1, g_2) + (g_1', g_2') = (g_1 + g_1', g_2 + g_2').$$

DEFINITION 2.1.7. A *homomorphism* or *morphism of groups* is a map f from a group G to another group H such that for all $g, g' \in G$ we have:

$$f(g + g') = f(g) + f(g')$$

in the group H.
An injective homomorphism is called an *embedding*. If an embedding $G \to H$ exists, we say G *embeds* in H.
A bijective homomorphism is called an *isomorphism*. If a isomorphism exists between two groups, they are said to be *isomorphic*.

EXAMPLE 2.1.8. The map $\mathbf{Z} \to \mathbf{Z} : a \mapsto a + a$ is a homomorphism from $\mathbf{Z}$ to itself.
For all groups G and all subgroups H the map $G \to G/H : g \mapsto g + H$ is a homomorphism that is surjective.
The group of integers embeds in the additive group of real numbers via the inclusion map.

REMARK 2.1.9. In a group G with an element a and $n \in \mathbf{N}\backslash\{0\}$, we write $n \cdot a$ for the sum

$$\overbrace{a + a + \cdots + a}^{n \text{ terms}}$$

We define $0 \cdot a$ to be 0.

DEFINITION 2.1.10. An element g of a group G is said to be a *torsion element* if $n \cdot g = 0$ for some $n \in \mathbf{N}\backslash\{0\}$.
A group is *torsion-free* if the only torsion element is 0.

EXAMPLE 2.1.11. $\mathbf{Z}$ is torsion-free. On the other hand, all elements in a finite group are torsion elements, so all non-trivial quotient groups of $\mathbf{Z}$ consist solely of torsion elements.

DEFINITION 2.1.12. Let G be a group. We say G is *divisible* if for every natural number n and every element $g \in G$ there is an $h \in G$ such that $n \cdot h = g$.
We say a group is *p-divisible* if the above holds just for $n = p$.

EXAMPLE 2.1.13. The rationals $\mathbf{Q}$ form a divisible group under addition.
The group $\mathbf{Q}/\mathbf{Z}$ is a divisible group as well.
A finite non-trivial group cannot be divisible, but it can be p-divisible for some primes p. For instance, $\mathbf{Z}/2\mathbf{Z}$ is 3-divisble.

We shall return to divisible groups after we have defined the tensor product.

For the definition of a valued field, we will generalize two properties of the real numbers: that they are an additive group, and that they are ordered. We recall the definition of an order.

DEFINITION 2.1.14. Let X be a set. A *partial order* on X is a binary relation $\leq$ on X such that for all $x, y, z \in X$ holds:

- $x \leq x$;
- if $x \leq y$ and $y \leq x$, then $x = y$;
- if $x \leq y$ and $y \leq z$, then $x \leq z$.

A *total order* on X is a partial order such that for all x and y in X holds that $x \leq y$ or $y \leq x$.

DEFINITION 2.1.15. An *ordered group* $(G, \leq)$ is a group that is totally ordered by $\leq$, and in which for all x, y and z in G holds that $x \leq y$ implies $x+z \leq y+z$.

EXAMPLE 2.1.16. The groups of the integers, the rationals and the reals are ordered groups under addition and their usual ordering.
If $G_1, \ldots, G_n$ are ordered groups, then so is the group $G_1 \times \cdots \times G_n$, using the dictionary ordering in which $(a_1, \ldots, a_n) \leq (b_1, \ldots, b_n)$ iff there is an i between 1 and n such that $a_1 = b_1$, $a_2 = b_2$, $\ldots$, $a_{i-1} = b_{i-1}$ and $a_i \leq b_i$.

Note that an ordered group is necessarily torsion-free: suppose x is a non-zero torsion element, say $n \cdot x = 0$ for some integer $n > 0$. By if needed switching to the negative of x, we have $0 < x$. By the order property, for all k, $k \cdot x = 0 + k \cdot x < x + k \cdot x = (k+1) \cdot x$ and by induction we see $0 < n \cdot x = 0$ which is a contradiction.

2.2 Rings and ideals

DEFINITION 2.2.1. A *ring* is a set R together with binary functions $+ : R \times T \to R$ and $\cdot : R \times R \to R$, an unary function $- : R \to R$ and two constants 1 and 0 in R, such that for all $a, b, c \in R$ holds:

- R is a group operation with the functions $+$ and $-$ and the constant 0;

- $a \cdot b = b \cdot a$;
- $a \cdot 1 = a$;
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
- $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$;

EXAMPLE 2.2.2. The integers $\mathbf{Z}$ with the usual addition and multiplication are an example of a ring, as well as the rationals $\mathbf{Q}$ and the complex numbers $\mathbf{C}$.
The integers modulo n ($\mathbf{Z}/n\mathbf{Z}$) are a ring as well, for all integers $n \geq 1$.
The ring with one element (which is both 0 and 1) is denoted with 0.

REMARK 2.2.3. Let A and B be subsets of a ring or group. From now on, we will write $A + B$ for the subset $\{a + b : a \in A, b \in B\}$, and similarly $A \cdot B$ for the set of all elements of the form $a \cdot b$.

DEFINITION 2.2.4. A *ring homomorphism* or *ring map* between rings R and S is a set function $f : R \to S$ such that $f(1) = 1$, $f(a + b) = f(a) + f(b)$ and $f(a \cdot b) = f(a) \cdot f(b)$ for all elements a, b in R.

EXAMPLE 2.2.5. For every ring R there exists a unique map $f : \mathbf{Z} \to R$ that sends $n \geq 0$ to the sum of n terms $f(1)$, and $n \leq 0$ to the sum of $-n$ terms $-f(1)$.
For every ring R there is a unique map $R \to 0$ that sends all elements to the only element of the ring 0.
The inclusion map $\mathbf{Z} \to \mathbf{Q}$ is a ring map.

DEFINITION 2.2.6. An element a of a ring is *invertible* if there exists a b in that ring such that $a \cdot b = 1$. We write $R^\times$ for the set of invertible elements in R.
A *field* is a ring in which $0 \neq 1$ and every element except 0 is invertible.

DEFINITION 2.2.7. An *ideal* I of a ring R is a subset such that $I + I \subseteq I$, $R \cdot I \subseteq I$ and $0 \in I$.
For every $a \in R$ the set $(a) = \{ar : r \in R\}$ is an ideal. An ideal of this form is called a *principal ideal*.

EXAMPLE 2.2.8. In every ring R the set $(0) = \{0\}$ is an ideal. The ring R itself is also an ideal which is called the *unit ideal*, which is (1) in the notation above.
If $a \in R$ is invertible, then the only ideal I containing a is the unit ideal, since for all $x \in R$ we have

$$x = (xa^{-1}) \cdot a \in R \cdot I \subseteq I.$$

DEFINITION 2.2.9. Let R be a ring, and $S \subseteq R$ be a subset of R. The *ideal generated by* S is the smallest ideal of R containing all elements of S. (This is well-defined, since the intersection of two ideals is also an ideal.) If $S = \{a_1, \ldots, a_n\}$ we write $(a_1, \ldots, a_n)$ for this ideal. We call such an ideal *finitely generated*.

The notation introduced agrees with the notation for a principal ideal.

DEFINITION 2.2.10. A *noetherian ring* is a ring in which every ideal is finitely generated.

Note that every ideal is a subgroup of R considered as an abelian group with respect to addition.

PROPOSITION 2.2.11. *If R is a ring and I an ideal of R, we can give the quotient group R/I a ring structure by defining $(a+I)(b+I) = ab+I$.*

Proof. This is shown on page 89 of [20]. □

DEFINITION 2.2.12. Let R be a ring and I an ideal, not equal to the unit ideal. We call I a *prime ideal* if for all $a, b \in R$ holds that $ab \in I$ implies that $a \in I$ or $b \in I$.
We call I a *maximal ideal* if there is no ideal J such that $I \subset J \subset R$.

EXAMPLE 2.2.13. In the ring $\mathbf{Z}$, the prime ideals are (p) for prime numbers p, and the ideal (0). All prime ideals except (0) are maximal ideals.

PROPOSITION 2.2.14. *every non-invertible element of a ring is contained in a maximal ideal.*

Proof. This is Corollary 1.5 in [2]. The proof uses the Axiom of Choice. □

DEFINITION 2.2.15. An *integral domain* is a ring where (0) is a prime ideal.

Equivalently, in an integral domain there are no $a, b \neq 0$ such that $ab = 0$.

PROPOSITION 2.2.16. *Let R be a ring and I an ideal.*
The ring R/I is an integral domain iff I is a prime ideal of R.
The ring R/I is a field iff I is a maximal ideal of R.

Proof. This is shown on page 93 of [20]. □

EXAMPLE 2.2.17. It follows that the ring $\mathbf{Z}/p\mathbf{Z}$ for p prime is in fact a field. We also write $\mathbf{F}_p$ for it.

DEFINITION 2.2.18. The *characteristic* of a ring R is the smallest positive $n \in \mathbf{N}$ such that

$$\overbrace{1+1+\cdots+1}^{n \text{ terms}} = 0,$$

in R if such an n exists and 0 otherwise. We write $\operatorname{char} R$ for this number.

EXAMPLE 2.2.19. An integral domain R has 0 or a prime number as characteristic: suppose $\operatorname{char} R = n = ab$ for positive integers $a, b < n$. Then

$$0 = n \cdot 1 = (ab) \cdot 1 = (a \cdot 1)(b \cdot 1),$$

so either $a \cdot 1 = 0$ or $b \cdot 1 = 0$, contradicting the minimality of n.

In algebraic geometry we will often study the (pre)image of ideals under ring maps. Note that the image of an ideal is not necessarily an ideal:

EXAMPLE 2.2.20. Consider $\mathbf{Z}$ and $\mathbf{Q}$, and the inclusion map $i : \mathbf{Z} \to \mathbf{Q}$. Now (2) is an ideal of $\mathbf{Z}$, but the set $\{2n : n \in \mathbf{Z}\}$ is not an ideal of $\mathbf{Q}$.

PROPOSITION 2.2.21. *Let $f : R \to S$ be a ring map and I an ideal of S. Then $f^{-1}(I)$ is an ideal of R. If I is prime, then $f^{-1}(I)$ is prime.*

Proof. Let I be an ideal. As $f(0) = 0$, $0 \in f^{-1}(I)$. Let $a, b \in f^{-1}(I)$. As $f(a + b) = f(a) + f(b) \in I$, we see $a + b \in f^{-1}(I)$. Suppose $a \in f^{-1}(I)$ and $r \in R$. Then $f(ar) = f(a)f(r) \in S \cdot I \subseteq I$. We see that $f^{-1}(I)$ is an ideal.
Suppose I is prime. Then let $ab \in f^{-1}(I)$ for some $a, b \in R$. As $f(a)f(b) = f(ab) \in I$, we see $f(a) \in I$ or $f(b) \in I$, so $a \in f^{-1}(I)$ or $b \in f^{-1}(I)$. □

DEFINITION 2.2.22. Let $f : R \to S$ be a ring map. The *kernel* of f is denoted $\ker(f)$ and is defined as the preimage of 0 under f. As it is the preimage of the ideal (0), it is an ideal of R.

We note that the kernel of a ring map is (0) precisely if the map is injective.

In Chapter 5 we will continue our study of prime ideals and related concepts.

2.3 Modules, algebras and tensor products

For our study of rational points, we need to define the fibre product of two schemes, which corresponds to the tensor product of rings in the special case of affine schemes. It turns out that modules, a generalization of several ring-related concepts, are a good setting to define the tensor product.

DEFINITION 2.3.1. Let R be a ring. An *R-module* is a group M together with a map $f : R \times M \to M$, such that for all $r, r' \in R$ and $m, m' \in M$ holds:

- $f(1, m) = m$;
- $f(r + r', m) = f(r, m) + f(r', m)$;
- $f(r, m + m') = f(r, m) + f(r, m')$;
- $f(r \cdot r', m) = f(r, f(r', m))$;

EXAMPLE 2.3.2. The ring R is itself an R-module, via the map $f(r, r') = r \cdot r'$.
Every ideal I of R is an R-module, again via the map $f(r, r') = r \cdot r'$, now restricted to $R \times I$.
Every abelian group G is a $\mathbf{Z}$-module via the map $f(n, g) = n \cdot g$, where $n \cdot g = (-n) \cdot (-g)$ if $n < 0$, in the notation of Remark 2.1.9

Every map $\phi : R \to S$ of rings gives a natural R-module structure on S, by setting $f(r, s) = \phi(r)s$ as the associated map $R \times S \to S$. This follows immediately from the associative properties of a ring and the fact that ring maps respect the ring operations.

DEFINITION 2.3.3. Let R be a ring and M an R-module by $f : R \times M \to M$. We say $r \in R$ is a *zero divisor* in M if there exists a $m \in M \backslash \{0\}$ such that $f(r, m) = 0$.

DEFINITION 2.3.4. A *map of R-modules* $M \to M'$ is a map $\phi : M \to M'$ that is a group homomorphism, and that satisfies:

$$\phi(f(r, m)) = g(r, \phi(m))$$

where f and g are the maps corresponding to the module structure of M and M'.

DEFINITION 2.3.5. Let us consider an R-module M with associated map $f : R \times M \to M$.
An *R-submodule* of M is a subgroup N of M such that $f(r, n) \in N$ for all $r \in R$ and $n \in N$.
We write $R \cdot m$ for the submodule consisting of all elements of M of the form $f(r, m)$ for $r \in R$.
Given submodules M_1, M_2 of M, we write $M_1 + M_2$ for the submodule of M consisting of elements of the form $m_1 + m_2$ for $m_1 \in M_1$ and $m_2 \in M_2$.
An R-module M is *finitely generated* if there exist elements $m_1, \ldots, m_n \in M$ such that

$$M = Rm_1 + \cdots + Rm_n.$$

EXAMPLE 2.3.6. All ideals of R are R-modules, and an ideal is finitely generated as a module if it is so as an ideal.

DEFINITION 2.3.7. Let M be an R-module with associated map f and N a submodule. The *quotient module* M/N is the quotient group M/N with the following associated map $\bar{f}$:

$$\bar{f}(r, m + N) = f(r, m) + N.$$

EXAMPLE 2.3.8. As every ideal I of a ring R is an R-submodule of R itself, we see that this gives the quotient ring R/I also an R-module structure.

DEFINITION 2.3.9. Let R be a ring. An *R-algebra* is a ring S together with a fixed ring map $R \to S$.
A *homomorphism of R-algebras* is a ring map such that the triangle of this map with the two fixed maps from R commutes.

We can view an R-algebra as a R-module with a multiplication defined on it that respects the module structure: in the notation of Definition 2.3.1 we require $f(r, m \cdot m') = f(r, m) \cdot m'$. This implies that $f(r, m) = f(r)m$, so the structure is completely determined by the image of the map f.

We now define an important example of an R-algebra.

DEFINITION 2.3.10. Let R be a ring. The *ring of polynomials* in the variable X with coefficients in R is

$$R[X] = \{a_0 + a_1X + \cdots + a_nX^n : a_i \in R, n \in \mathbf{N}\}.$$

The addition is done term-wise, multplication is defined in the following way:

$$\left(\sum_{i=0}^{n} a_iX^i\right)\left(\sum_{i=0}^{m} b_iX^i\right) = \sum_{i=0}^{m+n}\left(\sum_{j=0}^{i} a_jb_{i-j}\right)X^i.$$

This is an R-algebra via the map that sends an element r of R to the polynomial $r \cdot X^0$. Another example of an R-algebra is that of the power series ring.

DEFINITION 2.3.11. Let R be a ring. The *ring of power series* in the variable X with coefficients in R is

$$R[[X]] = \{a_0 + a_1X + \cdots : a_i \in R\}.$$

Addition and multiplication proceeds as in $R[X]$.

Note that $R[X]$ embeds in $R[[X]]$.

PROPOSITION 2.3.12. *A morphism ϕ of R-algebras from $R[X]$ to an R-algebra S is completely determined by the choice of $\phi(X) \in S$. On the other hand, for all $s \in S$ there exists a R-algebra morphism $\phi_s : R[X] \to S$ such that $\phi(X) = s$.*

Proof. This follows directly from the properties an R-algebra morphism has to satisfy: for polynomials in $R[X]$ we have

$$\phi(\sum_{i=0}^{n} a_iX^i) = \sum_{i=0}^{n} \phi(a_i)\phi(X)^i$$

as ϕ is a ring map, and since ϕ is an R-algebra morphism, $\phi(r) = r$ for all elements of R, so

$$\phi(\sum_{i=0}^{n} a_iX^i) = \sum_{i=0}^{n} a_i\phi(X)^i,$$

which is determined by $\phi(X)$.

For the second claim, it can easily be checked that given $s \in S$ the map

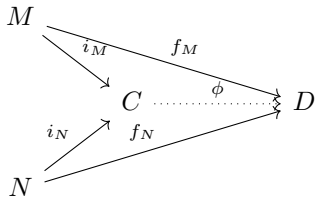
$$\phi : R[X] \to S : \sum_{i=0}^{n} a_iX^i \mapsto \sum_{i=0}^{n} a_is^i$$

is an R-algebra morphism. □

DEFINITION 2.3.13. We let $\mathbf{Z}[\frac{1}{p}]$ be the image of $\mathbf{Z}[X]$ in $\mathbf{Q}$ under the $\mathbf{Z}$-algebra map that sends X to $1/p$.

We will only state the universal property of the tensor product and omit the details of the actual construction of this object. In categorical terms, we define the tensor product to be the coproduct in the category of R-algebras for some ring R.

DEFINITION 2.3.14. Let M and N be R-modules. A *tensor product* of M and N is an R-module C together with R-module homomorphisms $i_M : M \to C$ and $i_N : N \to C$ such that for all pairs of R-module homomorphisms $f_M : M \to D$ and $f_N : N \to D$ there exists a unique map $\phi : C \to D$ of R-modules that makes the diagram below commute.



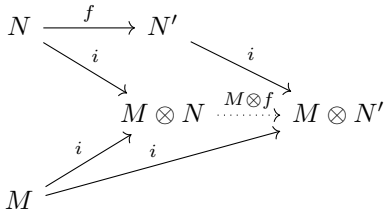
PROPOSITION 2.3.15. *For all R-modules A and B a tensor product of A and B exists, and this object is unique up to isomorphism. We write $A \otimes_R B$ for this R-module.*

Proof. This is shown in detail in §1 of Chapter XVI in [20]. □

REMARK 2.3.16. Unless indicated otherwise, when we speak about the tensor product of groups, we mean their tensor products as $\mathbf{Z}$-modules.

EXAMPLE 2.3.17. The tensor product $S \otimes_R R[X]$ is isomorphic to $S[X]$.
The tensor product of the groups $\mathbf{Z}/m\mathbf{Z}$ and $\mathbf{Z}/n\mathbf{Z}$ is the trivial group if m and n are relatively prime.

Via this universal property, we see that all maps $f : N \to N'$ of R-modules can be 'tensored' by another R-module M. In the diagram below, every map labeled i is the standard map from a factor to the tensor product. The existence of the dotted map $M \otimes N \to M \otimes N'$ is obtained by applying the universal property to $i \circ f : N \to M \otimes N'$ and $i : M \to M \otimes N'$.



DEFINITION 2.3.18. We call an R-module M *flat* if for all short exact sequences

$$0 \to N' \to N \to N'' \to 0$$

holds that

$$0 \to M \otimes N' \to M \otimes N \to M \otimes N'' \to 0$$

is a short exact sequence as well.

The proof of the following statement depends on localization, a concept defined in section 5.1. We will not use this proposition in that section, so no circularity occurs.

PROPOSITION 2.3.19. $\mathbf{Q}$ *is a flat group (i.e.* $\mathbf{Z}$*-module).*

Proof. By Corollary 3.6 in [2], every localization of a ring R is a flat R-module. As $\mathbf{Q}$ is the fraction field of $\mathbf{Z}$, i.e. the localization at (0), it follows that $\mathbf{Q}$ is a flat $\mathbf{Z}$-module. □

It can be shown that the tensor product of two R-algebras (interpreted as R-modules) can be given the structure of an R-algebra as well. This is described on page 30 of [2].

DEFINITION 2.3.20. We call a map of rings $\phi : R \to S$ *flat* if S is flat as an R-module, where the module structure is given by the map ϕ

2.4 The divisible hull

DEFINITION 2.4.1. Let G be a group. The *divisible hull* G_{div} of G is the group $G \otimes_{\mathbf{Z}} \mathbf{Q}$.
The *p-divisible hull* $\frac{1}{p^\infty}G$ is the $\mathbf{Z}$-module $G \otimes_{\mathbf{Z}} \mathbf{Z}[\frac{1}{p}]$.

EXAMPLE 2.4.2. The divisible hull of $\mathbf{Z}^n$ is $\mathbf{Q}^n$ for all natural numbers n.
The divisible hull of a finite group is the trivial group.

PROPOSITION 2.4.3. *Let G be a group. Then its divisible hull is a divisible group, in which we can embed $\mathbf{Q}$ if G is not a torsion group. If G is torsion-free, we can embed G in G_{div}.*
Similarly, the p-divisible hull of a group is a p-divisible group.

Proof. This follows from Proposition 1.2.2(a) and 1.2.4(a) in [10]. □

PROPOSITION 2.4.4. *Let G be a group, and G_{div} its divisible hull. Then there is no torsion-free group $H \supset G_{\text{div}}$ such that $[H : G_{\text{div}}] < \infty$.*

Proof. The $\mathbf{Z}$-module $\mathbf{Q}$ is flat by Proposition 2.3.19. This means that tensoring with $\mathbf{Q}$ sends exact rows to exact rows. The exact row

$$0 \to H \to G_{\text{div}} \to G/H_{\text{div}} \to 0$$

becomes the exact row

$$0 \to H_{\text{div}} \to G_{\text{div}} \to 0 \to 0,$$

since $G \otimes \mathbf{Q} \otimes \mathbf{Q} = G \otimes \mathbf{Q}$, and the tensor product of a torsion group with $\mathbf{Q}$ is the trival group. We see that $H_{\text{div}} = G_{\text{div}}$, and since H is torsion-free $H \subseteq G_{\text{div}}$. So $H = G_{\text{div}}$ which is impossible. □

PROPOSITION 2.4.5. *If $(G, \leq)$ is an ordered group, then the divisible hull of G can be made into an ordered group $(G_{\text{div}}, \leq_{\text{div}})$ such that there exists a morphism of ordered groups $G \to G_{\text{div}}$ in a unique way.*

Proof. This is Proposition 2.1.2 in [10]. □

COROLLARY 2.4.6. *Let $(G, \leq)$ be an ordered group. Then $(G_{\text{div}}, \leq_{\text{div}})$ is an divisible ordered group in which G and $\mathbf{Q}$ embed.*

Proof. This follows from the fact that G is torsion-free since it is ordered. □

2.5 Basic field theory

We recall that in a field all elements except 0 are invertible. As no non-trivial ideal can contain invertible elements, we see that in all fields k only (0) and (1) are ideals. It follows that for all ring maps between fields $f : k \to K$ we have $\ker(f) = (0)$ or $\ker(f) = k$: we see that every map between fields is either an embedding or the zero map. We will therefore assume that the smaller field is a subring of the larger field, and speak of field extensions.

We recall that in an integral domain the characteristic is always 0 or a prime number. As every non-zero map between fields is an embedding, field maps only exist between fields of equal characteristic.

EXAMPLE 2.5.1. We already encountered the finite fields $\mathbf{F}_p$ for prime numbers p. These fields are of characteristic p. The rational numbers form a field too (clearly a/b has inverse b/a if a and b are non-zero), which is of characteristic 0.

PROPOSITION 2.5.2. *Let k be a field of characteristic p. Then the map*

$$F : k \to k : x \mapsto x^p$$

is a field map from k to itself. We call this map the Frobenius map.

Proof. It is clear that $1^p = 1$ and $(xy)^p = x^p y^p$ for all $x, y \in k$. For the addition, we use that p divides $\binom{p}{k}$ for $1 \leq k \leq p-1$, so that in the binomial expansion we have:

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = x^p + y^p$$

as all the terms that are of the form $p \cdot x$ for some $x \in k$ vanish due to $p \cdot 1 = 0$. □

DEFINITION 2.5.3. Let k be a field, and let $k \subseteq K$ be a field extension. A polynomial $f(X) \in k[X]$ is said to have a *root* $\alpha \in K$ if it holds that $f(\alpha) = 0$.

PROPOSITION 2.5.4. *Let k be a field, and $f(X)$ an monic irreducible polynomial over k. Then $k[X]/(f(X))$ is a field which contains k. In this field the polynomial $f(X)$ has a root.*

Proof. This is shown on page 223 and 224 of [20]. □

DEFINITION 2.5.5. A field extension $k \subseteq K$ is *algebraic* if all elements of K are roots of a polynomial over k.

EXAMPLE 2.5.6. Consider the field extension $\mathbf{Q} \subseteq \mathbf{R}$. The polynomial $X^2 - 2$ has no root in $\mathbf{Q}$, as $\sqrt{2}$ is not a rational number. However, it has a root in $\mathbf{R}$.

PROPOSITION 2.5.7. *Let $f(X)$ be a polynomial over k. Then $\alpha \in k$ is a root of $f(X)$ in k if and only if $f(X)$ can be written as $(X - \alpha)h(X)$ for some polynomial $h(X) \in k[X]$*

Proof. This is Theorem IV.1.4 in [20]. □

DEFINITION 2.5.8. The *multiplicity* of a root α of a polynomial $f(X)$ in $k[X]$ is the largest $m \geq 1$ such that $f(X) = (X - \alpha)^m h(X)$ for some polynomial $h(X)$. A *simple root* is a root of multiplicity 1.

DEFINITION 2.5.9. A field k is *algebraically closed* if every polynomial $f(X)$ over k can be written as the product of linear factors in k.

PROPOSITION 2.5.10. *Every field k has an algebraic extension $\bar{k}$ that is algebraically closed. All such fields are isomorphic, and we call such a field an* algebraic closure *of k.*

Proof. This is Corollary V.2.6 in [20]. Note that this proof depends on the Axiom of Choice. □

2.6 Separable field extensions

DEFINITION 2.6.1. Let K be a field, and L_1 and L_2 be field extensions of K contained in a field Ω. The *compositum* L_1L_2 is the smallest subfield of Ω that contains both L_1 and L_2. (Note that the compositum depends on the way L_1 and L_2 are embedded in Ω.)

DEFINITION 2.6.2. A field of characteristic p is *perfect* if every element can be written as the p-th power of an element. We call all fields of characteristic 0 perfect as well.

EXAMPLE 2.6.3. Every finite field is perfect, since the Frobenius map is injective, and an injective map between two finite sets of equal size is bijective. So we can take the inverse of this map to find a p-th root of any given element.
The field $\mathbf{F}_p(t)$ is not perfect, since there exists no p-th root of t in it.

DEFINITION 2.6.4. A *separable polynomial* over K is a polynomial in K with no multiple roots in the algebraic closure of K (i.e. the polynomial has as many distinct roots there as its degree).

Following the form of the analytical derivative of polynomials, we define the following.

DEFINITION 2.6.5. Let K be a field and $f = \sum_{i=0}^{n} a_i X^i$ be a polynomial over K. The *formal derivative* of f is the polynomial $f' = \sum_{i=1}^{n} i a_i X^{i-1}$.

The use of this is a root α of a polynomial f is a multiple root precisely if it is a root of both f and f'. We can see this by checking that the product rule $(fg)' = f'g + fg'$ also holds for the formal derivative, which implies that for $f = (X - \alpha)^2 g$ we have

$$f' = 2(X - \alpha)g + (X - \alpha)^2 g,$$

so $f'(\alpha) = 0$. On the other hand, if α is a root of f and f', then $f = (X - \alpha)h$ for some polynomial h, so

$$f' = (X - \alpha)h' + h.$$

As α is a root of f', it is also a root of h, so $X - \alpha$ divides h, and hence $(X - \alpha)^2$ divides f.

We can use this to detect separable polynomials.

EXAMPLE 2.6.6. Every irreducible polynomial f is separable in characteristic 0: the g.c.d. of f and f' must be 1 by irreducibility.
In positive characteristic p, one can prove that every inseparable polynomial in X can be written as a polynomial in X^p as well. In $\mathbf{F}_p$ for instance, we see that $X^p - 1$ is inseparable, since $x^p = x$ for every element x and hence 1 can be the only root.

For general field extensions, we define the following. For a discussion of transcendental (i.e. non-algebraic) field extensions and transcendence bases the reader is referred to Chapter VIII in [20].

DEFINITION 2.6.7. A *separably algebraic* field extension $K \subseteq L$ is an algebraic field extension in which the minimal polynomial over K of any given element of L is separable.
A *separably generated* field extension $K \subseteq L$ is a field extension for which there exists a transcendence base $t = (t_1, \ldots, t_n)$ such that $K(t) \subseteq L$ is separably algebraic.
A field extension that is either separably algebraic or separably generated is called *separable*.

PROPOSITION 2.6.8. *Let K be a field of characteristic p. The following two conditions are equivalent:*

- *the field K is perfect;*
- *every algebraic extension of K is separable.*

Proof. We show first that every algebraic extension of a perfect field is separable. Suppose $K \subseteq L$ is an algebraic extension of characteristic p fields, and suppose K is perfect. Let α be a element of L, and $f(X)$ its minimal polynomial over K. Suppose it was not separable. Then we can write $f(X) = g(X^p)$, say with $g(X^p) = \sum_{i=0}^{k} a_i X^{pi}$ with $a_i \in K$. Since K is perfect, we can find b_i such that $b_i^p = a_i$, and hence

$$f(X) = g(X^p) = \sum_{i=0}^{k} a_i X^{pi} = \sum_{i=0}^{k} b_i^p X^{pi} = \left(\sum_{i=0}^{k} b_i X^i \right)^p = h(X)^p.$$

But we assumed that f was a minimal polynomial and hence irreducible. Contradiction, so the extension is separable.

Now we show the other way around. Let K be a field that is not perfect, say $x \in K$ is not a p-th power. We will show that the algebraic field extension $K \subseteq K[Y]/(Y^p - x)$ is not separable. As $Y^p - x$ is an irreducible polynomial, $(Y^p - x)$ is a maximal ideal of $K[Y]$, so $K[Y]/(Y^p - X)$ is a field.

However, this polynomial (which is the minimal polynomial of y) has multiple roots: its formal derivative is $p \cdot y^{p-1} = 0$ (since K has characteristic p). So the field extension is not separable. □

DEFINITION 2.6.9. An element x of an algebraic extension L over a field K of characteristic p is *purely inseparable* if there exists an integer $n \geq 0$ such that $x^{p^n} \in K$.
An algebraic extension L of a field K is *purely inseparable* if every element of L is purely inseparable over K.

PROPOSITION 2.6.10. *Let L be an algebraic extension of K. Then there exists a field M such that $K \subseteq M \subseteq L$, M is separable over K and L is purely inseparable over M.*

Proof. This is Proposition V.6.6 in [20] □

EXAMPLE 2.6.11. The extension $K \subseteq K[Y]/(Y^p - x)$ discussed in the proof of Proposition 2.6.8 is purely inseparable.

DEFINITION 2.6.12. The *perfect hull* K^{perf} of a field K of characteristic $p > 0$ is the field K adjoined with all the p^n-th roots of its elements, for all integers $n \geq 1$

EXAMPLE 2.6.13. The perfect hull of $\mathbf{F}_p(t)$ is the field

$$\mathbf{F}_p(t, t^{1/p}, t^{1/p^2}, \ldots)$$

DEFINITION 2.6.14. Two extensions L and L' of a field K are *linearly disjoint* if every finite set of elements of L that is linearly independent over K is linearly independent over L' as well.

PROPOSITION 2.6.15. *Let $K \subseteq K'$ be a field extension with K algebraically closed in K'. Let α be an element in an extension of K' that is algebraic over K. Then $K(\alpha)$ and K' are linearly disjoint,*

$$[K(\alpha) : K] = [K'(\alpha) : K']$$

and $K(\alpha)$ is algebraically closed in $K'(\alpha)$.

Proof. Consider the minimal polynomial of α over K. This polynomial is irreducible over K' as well: if it factored over K', the coefficients of the factors would be algebraic over K so they would be elements of K. This means that the basis $1, \alpha, \ldots, \alpha^{n-1}$ (where $n = [K(\alpha) : K]$) is both a K-basis of $K(\alpha)$ and a K'-basis of $K'(\alpha)$. □

Chapter 3

Logic

This chapter is based on [27] and section 2 of [6].

3.1 Languages and models

Definition 3.1.1. A *language* L consists of a set of constants, a set of function symbols, each with a specified finite arity which is a positive integer, and a set of relation symbols, each with a specified finite arity which is also a positive integer. We say 'n-ary' as a shorthand for 'with arity n', and also 'unary' and 'binary' as synonyms for '1-ary' and '2-ary'.

Example 3.1.2. We can talk about (for instance) rings in the *ring language* L_{ring} which contains two constants, 0 and 1, and three functions. Two of those functions are binary ($+$ and $\cdot$), and one is unary ($-$).

We assume we have some set of countably many variables, which we usually denote with x, y, z, ...

Definition 3.1.3. The set of *terms* in a language L (or L-terms) is the smallest set containing:

- all constants;
- all variables;
- the expression $f(t_1, \ldots, t_n)$ whenever f is a n-ary function symbol and t_1, ..., t_n are terms.

Definition 3.1.4. The set of *formulas* in a language L (or L-formulas) is the smallest set containing:

- the expression $s = t$ whenever s and t are terms;
- the expression $R(t_1, \ldots, t_n)$ whenever f is a n-ary relation symbol and t_1, $\ldots$, t_n are terms.
- the expressions $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \to \psi$ and $\neg\phi$ whenever ϕ and ψ are formulas;
- the expressions $\exists x\phi$ and $\forall x\phi$ whenever x is a variable and ϕ a formula. ($\exists$ and $\forall$ are known as *quantifiers*).

REMARK 3.1.5. We will not formally introduce brackets in the context of formulas. They will be used wherever necessary to prevent ambiguity, for instance in expressions like $\phi \wedge \psi \to \chi$.

DEFINITION 3.1.6. A variable x that occurs in a formula is *free* if it is not in the scope of a quantifier $\forall x$ or $\exists x$.
A *L-sentence* is a L-formula that does not contain free variables.
A *L-theory* is a set of L-sentences.

EXAMPLE 3.1.7. In the ring language, $\forall y(x + 0 = y)$ is a formula with free variable x. The formula $\exists x \forall y(x + 0 = y)$ is a sentence.

We often omit the predicate L- if this is clear from the context. We will use the notation $\phi(x_1, \ldots, x_n)$ for a formula ϕ to indicate that its free variables are contained in the set $\{x_1, \ldots, x_n\}$.

DEFINITION 3.1.8. A *model* (or *structure*) in a language L consists of:

- a non-empty set M, called the domain or universe;
- an interpretation of the symbols in L:
  - for every constant c in L an element $c^M \in M$;
  - for every n-ary function f in L a function $f^M : M^n \to M$;
  - for every n-ary relation R in L a subset R^M of M^n.

We usually denote the model by the name of its domain.

We extend the notation $\cdot^M$ to all terms of L, by setting $f(t_1, \ldots, t_n)^M = f^M(t_1^M, \ldots, t_n^M)$. In general, we write t^M for the interpretation in M of a term t.

DEFINITION 3.1.9. Inductively, we evaluate the symbol $\models$ relating L-models and L-sentences in the following way:

- $M \models s = t$ iff $s^M = t^M$;
- $M \models R(t_1, \ldots t_n)$ iff $(t_1^M, \ldots, t_n^M) \in R^M$;

- $M \models \phi \wedge \psi$ iff $M \models \phi$ and $M \models \psi$;
- $M \models \phi \vee \psi$ iff $M \models \phi$ or $M \models \psi$;
- $M \models \phi \to \psi$ iff $M \not\models \phi$ or $M \models \psi$;
- $M \models \neg\phi$ iff $M \not\models \phi$;
- $M \models \exists x \phi(x)$ if there is a $m \in M$ such that $M \models \phi(m)$;
- $M \models \forall x \phi(x)$ if for all $m \in M$ we have $M \models \phi(m)$.

We say a formula ϕ *holds* or *is true* in a model M if $M \models \phi$.

Definition 3.1.10. We call a formula without quantifiers *quantifier-free*.
A formula is in *prenex form* if it starts with a number of quantifiers followed by a quantifier-free part.

Example 3.1.11. In the ring language, the formula

$$(\exists x(x = x \cdot x)) \to \neg\forall y(y = 0))$$

is logically equivalent to the prenex form formula

$$\forall x \exists y(x = x \cdot x \to \neg y = 0).$$

It can be shown that every formula is logically equivalent to a formula in prenex form, i.e. in all models both formulas either both hold or are both false.

We can now rephrase Definition 2.2.1 more formally.

Example 3.1.12. A *ring* is a model M in the ring language L_{ring} that satisfies the theory consisting of the following L-sentences:

$$\begin{aligned}
\forall x\, x + 0 &= x \\
\forall x\, x + (-x) &= 0 \\
\forall x \forall y\, x + y &= y + x \\
\forall x \forall y \forall z\, (x + y) + z &= x + (y + z) \\
\forall x\, x \cdot 1 &= x \\
\forall x \forall y\, x \cdot y &= y \cdot x \\
\forall x \forall y \forall z\, (x \cdot y) \cdot z &= x \cdot (y \cdot z) \\
\forall x \forall y \forall z\, x \cdot (y + z) &= x \cdot y + x \cdot z
\end{aligned}$$

Example 3.1.13. A *field* is a model M in the language L_{ring} that satisfies the theory consisting of the following L-sentences:

- all the axioms of a commutative ring in Example 3.1.12;

- $\neg(0 = 1)$;
- $\forall x \exists y\, x = 0 \vee x \cdot y = 1$

In Definition 2.1.15, we defined ordered groups. Anticipating the definition of valued fields in Chapter 4, we will consider ordered groups to which an extra element ∞ is added that is larger than all other elements.

There is a bijection between ordered groups as defined in the previous chapter and ordered groups with infinity, obtained by adding an extra element. That this is a bijection follows from the fact that this extra element satisfies unique properties such as $a + \infty = \infty$ for all a. A technicality that arises is that we cannot sensibly define $-\infty$, so that in the language of ordered groups with infinity we cannot have a unary function $-$. However, as $x = -y$ iff $x + y = 0$ in a group, this poses no restriction.

EXAMPLE 3.1.14. The *language of ordered groups with infinity* consists of two constants, 0 and ∞, a binary function symbol $+$ and a binary relation symbol $<$.

An *ordered group with infinity* is a model M in the language of ordered groups with infinity satisfying the following sentences:

$$\begin{aligned}
\forall x\, x + 0 &= x \\
\forall x \forall y \forall z\, x + (y + z) &= (x + y) + z \\
\forall x \exists y\, x &= \infty \vee x + y = 0 \\
\forall x \forall y\, x + y &= y + x \\
\forall x\, x + \infty &= \infty \\
\forall x\, \neg(x < x) & \\
\forall x \forall y\, x < y \vee x &= y \vee y < x \\
\forall x \forall y \forall z\, x < y \wedge y < z &\to x < z \\
\forall x \forall y \forall z\, x < y &\to x + z < y + z \\
\forall x\, x &= \infty \vee x < \infty
\end{aligned}$$

DEFINITION 3.1.15. If M is a model in a language L, we write $\mathrm{Th}(M)$ for the collection of all L-sentences that are true in M.
If M and N are L-models, we say they are *elementary equivalent* if $\mathrm{Th}(M) = \mathrm{Th}(N)$, and we write $M \equiv N$.

DEFINITION 3.1.16. A L-theory T is *complete* if for every L-sentence ϕ we either have $\phi \in T$ or $\neg\phi \in T$.

EXAMPLE 3.1.17. For every L-model M the L-theory $\mathrm{Th}(M)$ is complete, since every L-sentence ϕ is either true or false in M, which means $\phi \in \mathrm{Th}(M)$ or $\neg\phi \in \mathrm{Th}(M)$.

A concept we will often encounter is that of adding constants to a language. Let us consider a L-model M. We expand the language L by adding a family of constants c_m where the index m runs through M. If we call this new language L_M, we can make M into a L_M-model by assigning m to the constant c_m for all $m \in M$. Often we write m for c_m, which is not ambiguous since c_m will never be assigned an other value than m.

In the language L_M we are able to refer to specific elements of M, which might not be possible in L.

Of course, sometimes we want to add only a part of the elements of M as constants. We will denote this by $L(S)$, if we add only the elements of $S \subseteq M$ as constants. In this context, we refer to the elements of S as *parameters*.

3.2 Maps between models

DEFINITION 3.2.1. An *L-embedding* of a L-model M in a L-model N is a function h between the domains such that

- the map h is injective;
- for every constant c in L we have $h(c^M) = c^N$;
- for every n-ary function symbol f in L and all elements $m_1, \ldots, m_n \in M$ we have
$$h(f^M(m_1, \ldots, m_n)) = f^N(h(m_1), \ldots, h(m_n)).$$
- for every n-ary relation symbol R in L and all elements $m_1, \ldots, m_n \in M$ we have
$$(m_1, \ldots, m_n) \in R^M \text{ iff } (h(m_1), \ldots, h(m_n)) \in R^N$$

PROPOSITION 3.2.2. *If $h : M \to N$ is an embedding of models, then for every quantifier-free formula $\phi(x_1, \ldots, x_n)$ and elements $m_1, \ldots, m_n$ in M we have $M \models \phi(m_1, \ldots, m_n)$ iff $N \models \phi(h(m_1), \ldots, h(m_n))$.*

Proof. This is shown on page 70 of [27] as a consequence of Theorem 2.2.1. □

DEFINITION 3.2.3. If M and N are L-models and the inclusion $M \subseteq N$ is an L-embedding, we say M is a *substructure* of N and N is an *extension* of M.

DEFINITION 3.2.4. An L-embedding $h : M \to N$ is *elementary* if for all m_1, $\ldots$, $m_n \in M$ and all formulas $\phi(x_1, \ldots, x_n)$ it holds that

$$M \models \phi(m_1, \ldots, m_n) \text{ iff } N \models \phi(h(m_1), \ldots, h(m_n)).$$

If there exists an elementary embedding between M and N we write $M \preccurlyeq N$.

EXAMPLE 3.2.5. The inclusion map of $\mathbf{Z}$ in $\mathbf{Q}$ as rings is an embedding, but not an elementary embedding, as the sentence $\exists x(2 \cdot x = 1)$ is false in $\mathbf{Z}$ but true in $\mathbf{Q}$.

We return to the prenex forms defined in Definition 3.1.10.

DEFINITION 3.2.6. We say that an L-formula is an $\exists$-*formula* if it has a prenex form without the quantifier $\forall$.
If M is a substructure of N, and every $\exists$-$L(M)$-formula that holds in N also holds in M, we say that M is *existentially closed* in N, and we write $M \preccurlyeq_\exists N$.

3.3 Multi-sorted languages

In the next section we will describe valued fields in model-theoretic terms. It turns out to be natural to formulate the axioms for valued fields in a multi-sorted language, i.e. a language where we have different functions, relations and constants for the various parts of the model. We will first define this and then discuss how this relates to the language defined above.

DEFINITION 3.3.1. Let S be a finite set indexing the *sorts*. A S-*sorted language* consists of

- constants, each of which has as sort an element of S;
- n-ary function symbols, where each of the n inputs has as sort an element of S and the output has also a sort.
- n-ary relation symbol, where each of n inputs has a sort.

DEFINITION 3.3.2. For a S-sorted language L, an L-model (or structure) consists of the following data:

- for every sort $s \in S$ a domain M_s (the domains are assumed to be pairwise disjoint);
- an interpretation of every symbol in L:
  - for every constant c of sort s an element $c^M \in M_s$;
  - for every n-ary function symbol f with input sorts $(s_1, \ldots, s_n)$ and output sort s_0 a function
$$f^M : M_{s_1} \times \cdots \times M_{s_n} \to M_{s_0};$$
  - for every n-ary relation symbol R with input sorts $(s_1, \ldots, s_n)$ a subset
$$R^M \subseteq M_{s_1} \times \cdots \times M_{s_n}.$$

We will denote the sorts associated to a symbol in the following way: $c : s$, $f : s_1 \times \cdots \times s_n \to s_0$ and $R : s_1 \times \cdots \times s_n$, where we use the notation as in the definition.

Terms are built in the same way as before, respecting the input sorts of the functions. The only difference is that every variable has an associated sort as well, so that quantifiers range over only the elements of one domain M_s, not over all M_s's.

EXAMPLE 3.3.3. An example of a sorted language is the language L_{vect} in which we can talk about vector spaces. We use two sorts: one for the vector space itself and one for the scalar field. We call the sorts V and F. The language L_{vect} then consists of the following symbols:

- the constants $0^F : F$ and $1^F : F$;
- the binary functions $+^F : F \times F \to F$ and $\cdot^F : F \times F \to F$;
- the unary function $- : F \to F$;
- the constant $0^V : V$;
- the binary function $+^V : V \times V \to V$;
- the unary function $-^V : V \to V$.
- scalar multiplication $\cdot^s : F \times V \to V$.

A k-vector space W is now a L_{vect}-model (k, W) satisfying the usual axioms, as for instance

$$\forall a \in k \forall b \in k \forall x \in W \, (a +^F b) \cdot^s x = a \cdot^s x +^V b \cdot^s x.$$

It is not hard to show that multi-sorted languages have the same expression power as one-sorted languages. A one-sorted language is an instance of a multi-sorted language, so we shall only discuss how to translate a theory in a multi-sorted language to a theory in a one-sorted language.

Suppose we have the sorts $s_1, \ldots, s_n$. Then we add to our language unary relations $S_1, \ldots, S_n$ which are supposed to mean 'is of sort i', and always assume the axioms

$$\forall x S_1(x) \vee \cdots \vee S_n(x)$$

and

$$\forall x S_i(x) \to \neg(S_1(x) \vee S_{i-1}(x) \vee S_{i+1}(x) \vee \cdots \vee S_n(x))$$

for all $1 \leq i \leq n$.

Now if we have a function $f : s_i \times s_j \to s_k$ in the multi-sorted language, we define a new relation F which holds of (x, y, z) precisely if

$$S_i(x) \wedge S_j(y) \wedge S_k(z) \wedge (f(x, y) = z).$$

We then define a function f' by setting $f'(x, y) = z$ iff $F(x, y, z)$. In a similar way we can deal with constants and relations.

We see that if we have a model $(M_1, \ldots, M_n)$ in a multi-sorted language satisfying certain axioms, we can translate to a model with as domain the disjoint union of the M_i's satisfying essentially the same axioms, and the other way around as well.

3.4 Completeness and model completeness

Recall that we denote the existence of a elementary embedding from a model A to a model B by $A \preccurlyeq B$.

DEFINITION 3.4.1. Let A be a model in a language L. The collection of all quantifier-free sentences in the language $L(A)$ that are true in A is the *diagram* of A. We write $\mathrm{Diag}(A)$ for this set.

EXAMPLE 3.4.2. Consider the model $A = (\mathbf{Z}, 0, 1, +, \cdot, -)$ in the ring language. Typical members of the diagram of A are $3+0 = 3$ and $((-1)\cdot(-2) = 2) \vee \neg(1 = 0)$.

We have already defined what it means for a theory to be complete. A weaker property of a theory is model completeness.

DEFINITION 3.4.3. An L-theory Σ is *model complete* if for every model A of Σ, the set of $L(A)$-sentences $\Sigma \cup \mathrm{Diag}(A)$ is complete.

PROPOSITION 3.4.4. *An L-theory Σ is model complete iff for all two models A and B of Σ such that $A \subseteq B$ we have $A \preccurlyeq B$.*

Proof. This is Lemma 3.3.1 in [27]. □

EXAMPLE 3.4.5. The theory of algebraically closed fields is model complete (Theorem 3.3.4 in [27]), but not complete: the following sentence (where p is a prime) is only true in fields of characteristic p:

$$\overbrace{1 + 1 + \cdots + 1}^{p \text{ terms}} = 0.$$

EXAMPLE 3.4.6. The theory of fields is not model complete: for instance, $\mathbf{F}_p$ and an algebraic closure of it. Clearly we can embed the former in the latter, but the sentence that states that a model has no more than p elements is false in the (infinite) algebraic closure.

THEOREM 3.4.7. *The theory of ordered divisible groups is model complete.*

Proof. This is Theorem 4.1.1 in [27]. □

3.5 Types and saturated models

DEFINITION 3.5.1. Let L be a language, and $(x_1, \ldots, x_n)$ a sequence of variables. A *type* is a collection of L-formula whose free variables are among $x_1, \ldots, x_n$.

Let A be an L-model. We say the A-tuple $(a_1, \ldots, a_n)$ *realizes* the type p if every formula in p is true when we substitute a_i for x_i. If such a tuple exists, we say p is realized in A.

A type p is *finitely satisfiable* in an L-model if every finite subset of p is realized in A.

EXAMPLE 3.5.2. We return once more to Example 3.1.14: consider the ordered group $\mathbf{Q}$, and let x be a variable. The type

$$p(x) = \{x > 1, x > 1 + 1, x > 1 + 1 + 1, \ldots\}$$

is finitely satisfiable but not satisfiable as there is no rational number that is larger than all integers.

Using the Compactness Theorem (that can be found as in Theorem 1.5.6 in [21]), it can be shown that every finitely satisfiable type in a model can be realized in an elementary extension of it. However, we are interested in elementary extensions in which *every* finitely satisfiable type can be realized. It turns out that these exist, given some restrictions on the size of the language.

DEFINITION 3.5.3. Let κ be an infinite cardinal. We say that an L-model A is *κ-saturated* if for every subset $X \subseteq A$ with $|X| < \kappa$, every type p that is finitely satisfiable in A with parameters in X (i.e. in the language $L(X)$) can be realized in A with parameters in X.

EXAMPLE 3.5.4. We see that the ordered group $\mathbf{Q}$ from the previous example is not $\aleph_0$-saturated, as there is a type that is finitely satisfiable that cannot be realized in $\mathbf{Q}$.

EXAMPLE 3.5.5. However, if we consider $\mathbf{Q}$ as a totally ordered set (so without the group structure, and only the relation $<$), it is an $\aleph_0$-saturated model. In [21] this model is discussed more thoroughly (as an instance of a dense linear order) in section 4.1 and Example 4.3.9.

We write κ^+ for the successor cardinal of κ.

THEOREM 3.5.6. *Let L be a language, and κ a cardinal such that $\kappa \geq |L|$. If A is an infinite L-model of cardinality $\leq 2^\kappa$, then there exists an κ^+-saturated elementary extension A^* of cardinality $\leq 2^\kappa$.*

Proof. This is Theorem 2.5.2 in [27].

Roughly speaking, under the conditions in the theorem, we can construct a chain of models A_α of length κ^+, with $A_0 = A$. Given a model A_α in this chain, we index all finitely satisfiable types in it and let $A_{\alpha+1}$ be the union of all elementary extensions of A_α in which these types are (individually) realized. For limit ordinals, we let A_λ be the union of A_α for $\alpha < \lambda$. The size conditions of the theorem make that we can bound the number of types from above, and ensure that the union of all A_α's has cardinality $\leq 2^\kappa$. □

3.6 Ultraproducts

Like [3], we will only consider (ultra)filters of the set $\mathbf{N}$.

Definition 3.6.1. A *filter* on the set $\mathbf{N}$ is a non-empty family $\mathcal{F}$ of subsets of $\mathbf{N}$, such that $\emptyset \notin \mathcal{F}$, and $\mathcal{F}$ is closed under finite intersection and taking supersets (i.e. if $A \in \mathcal{F}$ and $A \subseteq B \subseteq \mathcal{P}(\mathbf{N})$, then $B \in \mathcal{F}$).

Example 3.6.2. Let A be a non-empty subset of $\mathbf{N}$. Then

$$\mathcal{F}_A = \{B \subseteq \mathbf{N} : A \subseteq B\}$$

is a filter. We call a filter of this form *principal*.

Example 3.6.3. The *Fréchet filter* is defined as

$$\mathcal{F}_0 = \{B \subseteq \mathbf{N} : \mathbf{N} \backslash B \text{ is finite }\}.$$

We see it is a filter, as the subset of a finite set and the union of two finite sets are both finite.

Proposition 3.6.4. *Let $(\mathcal{F}_i)_{i\in I}$ be a family of filters, where I is a linearly ordered set and $F_i \subseteq F_j$ if $i \leq j$. Then $\bigcup_{i\in I} \mathcal{F}_i$ is a filter too.*

Proof. We write $\mathcal{F} = \bigcup_{i\in I} \mathcal{F}_i$. As every $\mathcal{F}_i$ is non-empty so is their union, and as $\emptyset$ is not a member of $\mathcal{F}_i$ for all $i \in I$, it is also not contained in the union $\mathcal{F}$.

Let $A, B \in \mathcal{F}$, and let $i, j \in I$ be such that $A \in \mathcal{F}_i$ and $B \in \mathcal{F}_j$. Without loss of generality, we assume $i \leq j$. Since $F_i \subseteq F_j$ we have $A \in \mathcal{F}_j$, so $A \cap B \in \mathcal{F}_j \subseteq \mathcal{F}$.

Lastly, if $A \in \mathcal{F}$, then $A \in \mathcal{F}_i$ for some $i \in I$, so every superset of A is also contained in $\mathcal{F}_i$ and hence in $\mathcal{F}$. We see $\mathcal{F}$ is indeed a filter. □

Definition 3.6.5. An *ultrafilter* on the set $\mathbf{N}$ is a maximal filter, with respect to the inclusion ordering.

Proposition 3.6.6. *A filter $\mathcal{F}$ on $\mathbf{N}$ is an ultrafilter iff for every set $A \subseteq \mathbf{N}$ either $A \in \mathcal{F}$ or $\mathbf{N}\backslash A \in \mathcal{F}$.*

Proof. Let $\mathcal{F}$ be a filter on $\mathbf{N}$, and suppose that for every set $A \subseteq \mathbf{N}$ either $A \in \mathcal{F}$ or $\mathbf{N}\backslash A \in \mathcal{F}$. We will show that $\mathcal{F}$ is indeed maximal. Let $\mathcal{G}$ be a filter that strictly contains $\mathcal{F}$, and let $C \in \mathcal{G}\backslash\mathcal{F}$. Since either C or its complement is a member of $\mathcal{F}$, we see that $\mathbf{N}\backslash C \in \mathcal{F}$ must hold. So this set is also a member of the larger filter $\mathcal{G}$. As every filter is closed under finite intersections we see

$$\emptyset = C \cap (\mathbf{N}\backslash C) \in \mathcal{G},$$

which contradicts that $\mathcal{G}$ is a filter. We see that $\mathcal{F}$ must be maximal, which proves one direction of the equivalence we wanted to show.

For the other direction we argue as follows. Let $\mathcal{F}$ be a filter on $\mathbf{N}$, and suppose that there is a set $A \subseteq \mathbf{N}$ such that $A \notin \mathcal{F}$ and $\mathbf{N}\backslash A \notin \mathcal{F}$. We will show that

$$\mathcal{F}' = \{C \subseteq \mathbf{N} : \text{ there is a } B \in \mathcal{F} \text{ such that } C \supseteq B \cap A\}$$

is a filter that strictly contains $\mathcal{F}$, which implies that $\mathcal{F}$ is not an ultrafilter.

Suppose $B \in \mathcal{F}$. As $B \supseteq B \cap A$, we see $\mathcal{F} \subseteq \mathcal{F}'$. As a consequence $\mathcal{F}'$ is not empty. Besides, $A \in \mathcal{F}'$ by definition and $A \notin \mathcal{F}$ so the inclusion is strict.

We will now show $\mathcal{F}'$ is indeed a filter. We have already seen it is not empty.

Suppose $\emptyset \in \mathcal{F}'$. Then there exist a $B_\emptyset \in \mathcal{F}$ such that $\emptyset = B_\emptyset \cap A$, which means $B_\emptyset \subseteq \mathbf{N}\backslash A$. However, since $\mathbf{N}\backslash A \notin \mathcal{F}$ by assumption, this is impossible. So $\emptyset \notin \mathcal{F}'$.

Pick $C \in \mathcal{F}'$. Now there is a $B_C \in \mathcal{F}$ so that $C \supseteq B_C \cap A$, so every superset of C also contains $B_C \cap A$, hence must be a member of $\mathcal{F}'$ as well.

Let $C, C' \in \mathcal{F}'$, and let $B_C, B_{C'} \in \mathcal{F}$ be such that $C \supseteq B_C \cap A$ and $C' \supseteq B_{C'} \cap A$. Then $C \cap C' \supseteq (B_C \cap B_{C'}) \cap A$. As $\mathcal{F}$ is closed under finite intersections, we see $C \cap C' \in \mathcal{F}'$.

Having checked the properties listed in the definition, we see $\mathcal{F}'$ is a filter. □

Example 3.6.7. From the previous proposition, we see that the principal filter $\mathcal{F}_A$ is an ultrafilter iff $|A| = 1$.

In our applications we are interested in non-principal ultrafilters. While the existence of principal ultrafilters is trivial, it turns out that we need a form of the Axiom of Choice to show non-principal ultrafilters exist.

Proposition 3.6.8. *There exist non-principal ultrafilters on* $\mathbf{N}$.

Proof. We can see this with an application of Zorn's Lemma (which is discussed extensively in Chapter 5 of [17]), which states that in a partially ordered non-empty set where every linearly ordered subset has an upper bound there exist maximal elements.

Note that the non-principal ultrafilters are precisely the ultrafilters that contain the Fréchet filter. Clearly every principal ultrafilter contains a singleton (and therefore not its cofinite complement), while on the other hand a non-principal ultrafilter cannot contain a finite set. We can see this as follows.

Let $\mathcal{U}$ be an ultrafilter, and suppose $\{a_1, \ldots, a_n\} \in \mathcal{U}$ is an element of $\mathcal{U}$ of smallest cardinality. Then either $\{a_1\} \in \mathcal{U}$ (which would mean $\mathcal{U}$ is the principal filter on $\{a_i\}$) or $\mathbf{N} \backslash \{a_1\} \in \mathcal{U}$, but then its intersection with $\{a_1, \ldots, a_n\}$ is a member of $\mathcal{U}$ with cardinality smaller than n which is a contradiction.

Now consider the collection C of all filters on $\mathbf{N}$ that contain the Fréchet filter $\mathcal{F}_0$. It can be partially ordered by inclusion, and as it contains the Fréchet filter itself it is non-empty. We note that every linearly ordered subset $(\mathcal{F}_i)_{i \in I}$ has an upper bound since the union of a family of filters that is linearly ordered by inclusion is also a filter by Proposition 3.6.4.

We see that by Zorn's Lemma, the collection C has maximal elements. Since there can be no filters outside C that contain filters in C by its definition, we see that these maximal elements are non-principal ultrafilters on $\mathbf{N}$. □

Now that we have defined ultrafilters, we look at their applications in model theory. Ultrafilters can be used to define a equivalence relation on the Cartesian product of a family of models. In Section 4.1 of [5] it is shown that the following definition makes sense.

DEFINITION 3.6.9. Let L be a language, and $(A_i)_{i \in \mathbf{N}}$ a family of L-structures. Now let $\mathcal{U}$ be an ultrafilter on $\mathbf{N}$. Then the *ultraproduct* $\prod_{\mathcal{U}} A_i$ of (A_i) is the L-structure with underlying set $\prod_i A_i / \sim$, where $\sim$ is the equivalence relation defined by $(a_i) \sim (a_i')$ iff

$$\{i \in \mathbf{N} : a_i = a_i'\} \in \mathcal{U},$$

and all the relations, functions and constants defined coordinate-wise.
If all A_i are the same, the ultraproduct is called an *ultrapower*.

We write $[(a_i)_i)]$ for the equivalence class of $(a_i)_i$ in the ultraproduct.

The following result is due to Łos:

THEOREM 3.6.10. *Let L be a language, $\mathcal{U}$ be an ultrafilter on $\mathbf{N}$, and $(A_i)_{i \in \mathbf{N}}$ a family of L-structures. Then for every L-formula $\phi(x)$ and every element $(a_i)_i \in \prod_{i \in \mathbf{N}} A_i$ holds that*

$$\prod_{\mathcal{U}} A_i \models \phi([(a_i)_i]) \text{ iff } \{i \in \mathbf{N} : A_i \models \phi(a_i)\} \in \mathcal{U}.$$

Proof. This is Theorem 4.1.9 in [5]. □

Note that for all L-structures A we have a canonical map A to its ultrapower by sending an element a to the element $[(a)_i]$ (i.e. the class of the constant sequence with value a). From Theorem 3.6.10 it follows that this map is an elementary embedding.

For the remainder of this section we fix a non-principal ultrafilter and assume that all ultraproducts use this ultrafilter without further mention.

EXAMPLE 3.6.11. Let L be the ring language, and let k be a field. Then the ultrapower of k is also a field. For instance, we can determine give an inverse $(b_i)_i$ for any element $[(a_i)_i] \neq 0$ by setting

$$b_i = \begin{cases} a_i^{-1} & \text{if } a_i \neq 0; \\ 0 & \text{if } a_i = 0, \end{cases}$$

since

$$\{i \in I : a_i \cdot b_i = 1\} = \{i \in I : a_i \neq 0\} \in \mathcal{U}.$$

3.7 Decidability and completeness

Informally speaking, a set of L-sentences T is decidable if there exists an algorithm that can decide in a finite amount of time if a sentence belongs to T or not. To make this statement precise, we need to define 'algorithm'. As it turns out, all sensible definitions are equivalent to each other so we stick to the standard definition of a Turing machine.

A *Turing machine* is a very simple idealization of a computer program. It manipulates an countable infinite tape of cells (indexed by $\mathbf{Z}$) that can contain symbols from a countable alphabet, by reading and writing symbols and moving up and down the tape, while it follows a finite program. This means that it can only be in a finite number of states, and in every state it is described how it responds (i.e. moving to another cell, changing state or writing a symbol) to reading a certain symbol in the cell it is reading at that moment. A precise definition can be found in Chapter 3 of [4].

A set of L-sentences T is *decidable* if there is a Turing machine with alphabet $L \cup S \cup \{Y, N\}$ (we let S be the set of logical symbols we need to write sentences ($\wedge$, $\forall$, x, ...) and assume that Y and N are outside of $L \cup S$), which when given as input a L-sentence ϕ prints after a finite number of steps either Y (if $\phi \in T$) or N (if $\phi \notin T$) in a cell.

A set of L-sentences T is *effectively enumerable* if there is a Turing machine with alphabet L that starts with an empty tape and prints all L-sentences in T (and no others) on the tape separated by empty cells, and that will print any given sentence in T within a finite number of steps.

We will not define precisely what it means for a L-sentence to be *provable* from a set of L-sentences, and refer instead to Chapter 14 of [4]. The only property we will need is that if a sentence is provable from an effectively enumerable set of sentences, then a Turing machine can confirm this in a finite number of steps.

THEOREM 3.7.1. *Let L be a language, and T an L-theory. Suppose there is a effectively enumerable set A of sentences in T such that every sentence in T is provable from A (i.e. T is axiomatizable). If T is a complete theory, then T is decidable.*

Proof. This follows from Church' thesis and Corollary 15.7 in [4]. □

Chapter 4

Valued fields

4.1 Definitions

Fields can be equiped with an absolute value $|\cdot| : K \to \mathbf{R}$ that respects multiplication, satisfies the triangle inequality $|x + y| \leq |x| + |y|$ and is positive anywhere except at 0, whose absolute value is defined as 0. Absolute values that satisfy the stronger ultrametric inequality $|x+y| \leq \max(|x|, |y|)$ are known as non-archimedean absolute values.

EXAMPLE 4.1.1. On the field $\mathbf{Q}$ we can define the following *p-adic absolute value* $|\cdot|_p$ for every prime number p:

$$\left|\frac{a}{b}p^k\right|_p = p^{-k} \quad (a, b \in \mathbf{Z}, p \nmid a, b, k \in \mathbf{Z}).$$

This absolute value is non-archimedean. Besides, we have the absolute value we know from undergraduate analysis: this is an archimedean absolute value. (In fact, Ostrowski's Theorem states that up to exponentiation by a constant, these are the only possible absolute values on the rationals.)

For convenience, we usually look at the negative logarithm of an non-archimedean absolute value, usually denoted by $v(\cdot)$. The defining properties of the absolute value translate to

$$v(xy) = v(x) + v(y) \text{ and } v(x + y) \leq \min(v(x), v(y)).$$

We have to deal with the fact that $\log 0$ is not defined: we do so by adding an extra symbol ∞ that is larger than all real numbers and we define its behavior with respect to $+$ and $\cdot$ accordingly. A function $v : K \to \mathbf{R} \cup \{\infty\}$ with this properties will be called a valuation.

EXAMPLE 4.1.2. On the field $\mathbf{Q}$ we define the following valuation which corresponds to the previous example. Let p be a prime. Then for $a, b \in \mathbf{Z}$ not divisible by p and all $k \in \mathbf{Z}$ we let

$$v_p\left(\frac{a}{b}p^k\right) = k.$$

We are almost ready to give the formal definition of a valuation. The only missing ingredient is that of ordered fields: we want to be able to define valuations other than the real valuations (i.e. with codomain $\mathbf{R}$) mentioned above. The desired properties of a valuation forces the codomain of the valution to have two things: addition and an ordering. For this reason, we will look at abelian groups endowed with an ordering, which we defined in Section 2.1. Now we are able to define a valuation:

DEFINITION 4.1.3. A valuation on a field K is a surjective map $v : K \to \Gamma \cup \{\infty\}$ where Γ is an ordered group and ∞ a symbol outside Γ, satisfying

- $v(xy) = v(x) + v(y)$;
- $v(x + y) \leq \min(v(x), v(y))$;
- $v(x) = \infty$ iff $x = 0$,

where we define ∞ to be larger than all of Γ and furthermore we set for all $\gamma \in \Gamma$:

$$\gamma + \infty = \infty + \gamma = \infty + \infty = \infty$$

Given a valuation v on K, we call (K, v) a valued field. We call Γ the value group of (K, v), which often is denoted by vK.

The following concept occurs often in the theory:

DEFINITION 4.1.4. A *convex subgroup* Δ of an ordered group $(\Gamma, \leq)$ is a subgroup such that $0 \leq \gamma \leq \delta$ and $\delta \in \Delta$ implies $\gamma \in \Delta$ for every $\gamma \in \Gamma$.

DEFINITION 4.1.5. The *rank* of an ordered group is the number of its proper convex subgroups. (It can be infinite.)
The *rank* of a valuation is the rank of its image.

One can show that the convex subgroups of an ordered group are linearly ordered by inclusion, so its rank is the length of the longest chain of convex subgroups.

EXAMPLE 4.1.6. The group $\mathbf{Z}^n$ with the product group structure and the dictionary order on it is an ordered group of rank n for every natural number n.

We will now define a number of essential concepts in the theory of valued fields.

DEFINITION 4.1.7. Let (K, v) be a valued field.
The *valuation ring* $\mathcal{O}_v$ of v is the following subring of K:

$$\{x \in K : v(x) \geq 0\}.$$

The *maximal ideal* $\mathcal{M}_v$ of v is the unique maximal ideal of $\mathcal{O}_v$:

$$\mathcal{M}_v = \mathcal{O}_v \backslash \mathcal{O}_v^\times = \{x \in K : v(x) > 0\}.$$

The *residue field* of (K, v) is

$$\overline{K}_v = Kv = \mathcal{O}_v/\mathcal{M}_v.$$

Since Γ is totally ordered, we have that $\gamma \leq 0$ or $0 \leq \gamma$ for all $\gamma \in \Gamma$. This means $x \in \mathcal{O}_v$ or $x^{-1} \in \mathcal{O}_v$ for all x. We will see that every subring of a field with this property corresponds to a valuation.

DEFINITION 4.1.8. Let K be a field. A *valuation ring* of K is a subring R such that for every $x \in K^\times$ we have either $x \in R$ or $x^{-1} \in R$.

We have the theorem below that allows us to identify valuations on a field and valuation rings. In the remainder we will therefore use the notation (K, v) and $(K, \mathcal{O})$ interchangebly. Unless indicated otherwise, the latter will imply that $\mathcal{O}$ is a valuation ring in the sense of Definition 4.1.8.

DEFINITION 4.1.9. An *order-preservering isomorphism* between two valuations $v_1 : K \to \Gamma \cup \{\infty\}$ and $v_2 : K \to \Delta \cup \{\infty\}$ is a map $\rho : \Gamma \to \Delta$ that is a group isomorphism respecting the ordering, such that $\rho \circ v_1$ and v_2 agree on $K^\times$.

THEOREM 4.1.10. *Let K be a field. Then we have the following bijection:*

$$\{\textit{valuations on } K\}/\{\textit{order-preserving isomorphisms}\} \xrightarrow{\sim} \{\textit{valuation rings in } K\}$$

that sends the equivalence class of v to $\mathcal{O}_v$.

Proof. This follows from Proposition 2.1.2 and 2.1.3 in [13]. □

We end the section with some examples of (constructions of) valuations.

EXAMPLE 4.1.11. Let $\mathbf{F}_p$ be the finite field with p elements, for a prime number p. We write $\mathbf{F}_p((t))$ for the field of formal power series $\sum_{i \geq N}^{\infty} a_i X^i$ with $a_i \in \mathbf{F}_p$. We have the following valuation on it:

$$v(a_r X^r + a_{r+1} X^{r+1} + \cdots) = r \quad (a_r \neq 0)$$

EXAMPLE 4.1.12. Let $v : K \to \Gamma \cup \{\infty\}$ be a valuation of K. Let $K(X)$ be the field of rational functions in the indeterminate X over K. There is exactly one valuation w of $K(X)$ that sends X to 0 and agrees with v on K for which the image of X is transcendental over the residue class field of (K, v). In this case $\overline{K(X)} = \overline{K}(\overline{X})$ and w maps onto Γ. This valuation is called the *Gauss valuation*.

4.2 Extensions of valuations

DEFINITION 4.2.1. We say that two valuation rings $\mathcal{O}_1$ and $\mathcal{O}_2$ on a field K are *dependent* if their compositum (the smallest subring of K containing both rings) is strictly smaller than K itself.

We can show that dependence is a equivalence relation: we write $[\mathcal{O}]$ for the dependence class of $\mathcal{O}$. (From every valuation of a field K a topology on K arises in a rather natural way: these topologies coincide iff valuations are dependent.)

From the definition of a valuation ring it is clear that every proper subring of a field that contains a valuation ring must be a valuation ring itself. Of course, these two valuation rings are dependent. In fact, it is the case that the dependence classes of a field are linearly ordered by inclusion.

Let $\mathcal{O} \subseteq \mathcal{O}'$ be two proper valuation rings in K, and let $\mathcal{M}$ and $\mathcal{M}'$ be its associated maximal ideals. Since every unit in $\mathcal{O}$ is also a unit in $\mathcal{O}'$, the set of units becomes larger and therefore the maximal ideal (i.e. the non-units) becomes smaller: $\mathcal{M}' \subseteq \mathcal{M}$. The ideal $\mathcal{M}'$ is prime in $\mathcal{O}'$ and therefore also prime in the smaller ring $\mathcal{O}$. On the other hand, if we have a prime ideal $\mathfrak{p}$ of $\mathcal{O}$, we get a valuation ring containing $\mathcal{O}$ if we localize $\mathcal{O}$ at $\mathfrak{p}$.

In this manner, we obtain a correspondence between prime ideals of $\mathcal{O}$ and valuation rings containing $\mathcal{O}$.

THEOREM 4.2.2. *Let $\mathcal{O}$ be a valuation ring in K, and let $v : K \to \Gamma \cup \{\infty\}$ be the associated valuation (note that this is determined up to order isomorphism). There exists a correspondence*

$$\{\textit{prime ideals in } \mathcal{O}\} \xrightarrow{\sim} \{\textit{proper convex subgroups of } \Gamma\}$$

and a correspondence

$$\{\textit{prime ideals in } \mathcal{O}\} \xrightarrow{\sim} \{\textit{valuation rings containing } \mathcal{O}\}$$

Proof. This is Lemma 2.3.1 in [13]. □

In the remainder of this section we will discuss extensions of valuations.

DEFINITION 4.2.3. Given a field extension $K \subseteq L$, we say that a valuation w of L is an *extension* or *prolongation* of a valuation v on K if $w|_K = v$. In terms of valuation rings, we say $(L, \mathcal{O}')$ is an extension of $(K, \mathcal{O})$ if $\mathcal{O}' \cap K = \mathcal{O}$.

THEOREM 4.2.4 (Chevalley's Extension Theorem). *Let R be a subring of a field K, and let P be a prime ideal of R. Then there exists a valuation ring $\mathcal{O}$ of K containing R such that its maximal ideal $\mathcal{M}$ satisfies $\mathcal{M} \cap R = P$.*

Proof. This is Theorem 3.1.1 in [13]. □

As a consequence we have:

THEOREM 4.2.5. *Let $K \subseteq L$ be a field extension, and let $\mathcal{O}$ be a valuation ring in K. Then there exists a valuation ring $\mathcal{O}'$ in L that extends $(K, \mathcal{O})$.*

Proof. This is Theorem 3.1.2 in [13]. □

Now we know the set of prolongations over a field extension $L \supseteq K$ of a given valued field (K, v) is not empty. Below we will see that its size is bounded by $[L : K]$ and we will look at a connection with the Galois group of L over K, if $L \supseteq K$ is a normal field extension.

First we introduce some notation. Let $(K, \mathcal{O}) \subseteq (L, \mathcal{O}')$ be an extension of valued fields. Let $v : K \to \Gamma \cup \{\infty\}$ and $w : L \to \Delta \cup \{\infty\}$ be valuations corresponding to these valuation rings, such that $w|_K = v$. By restriction, we obtain surjective maps $K^\times \to \Gamma$ and $L^\times \to \Delta$. By the isomorphism theorem we have

$$K^\times/\mathcal{O}^\times \cong \Gamma, \quad L^\times/\mathcal{O}'^\times \cong \Delta$$

The map

$$K^\times \hookrightarrow L^\times \twoheadrightarrow L^\times/\mathcal{O}'^\times \cong \Delta$$

has kernel $\mathcal{O}' \cap K = \mathcal{O}$, so the isomorphism theorem implies that

$$\Gamma \cong K^\times/\mathcal{O} \hookrightarrow \Delta$$

so Γ is a subgroup of Δ. So we can define:

DEFINITION 4.2.6. With the above notation, we define the *ramification degree* to be $[\Delta : \Gamma]$ and we denote this by $e(\mathcal{O}'/\mathcal{O})$. Note that this number may be infinite, in which case we will write ∞ for it.

In a rather similar fashion, we note that the composed map

$$\mathcal{O} \hookrightarrow \mathcal{O}' \twoheadrightarrow \mathcal{O}'/\mathcal{M}' \cong \overline{L}$$

has kernel $\mathcal{M}' \cap \mathcal{O} = \mathcal{M}$, so we get an injection of fields

$$\overline{K} \cong \mathcal{O}/\mathcal{M} \hookrightarrow \overline{L},$$

which allows us to define

DEFINITION 4.2.7. With the above notation, we define the *residue degree* to be $[\overline{L} : \overline{K}]$ and we denote this by $f(\mathcal{O}'/\mathcal{O})$. Note that this number may be infinite, in which case we will write ∞ for it.

DEFINITION 4.2.8. An extension of valued fields $(K, \mathcal{O}) \subseteq (L, \mathcal{O}')$ is *immediate* if $e(\mathcal{O}'/\mathcal{O}) = f(\mathcal{O}'/\mathcal{O}) = 1$.

For finite extensions, we have the following bound:

THEOREM 4.2.9. *Let $(K, \mathcal{O}) \subseteq (L, \mathcal{O}')$ be a extensions of valued fields. Then*

$$e(\mathcal{O}'/\mathcal{O}) \cdot f(\mathcal{O}'/\mathcal{O}) \leq [L : K].$$

Proof. This is Corollary 3.2.3 in [13]. □

More general the following lemma holds:

LEMMA 4.2.10. *Let $K \subseteq L$ be an algebraic field extension, and $\mathcal{O}$ a valuation ring of K. Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be extensions of $\mathcal{O}$ in L. Then $\mathcal{O}_1 \not\subseteq \mathcal{O}_2$ and $\mathcal{O}_2 \not\subseteq \mathcal{O}_1$.*

Proof. This is Lemma 3.2.8 in [13]. □

As we will see in the next section, separability plays an important part in determining how many extensions a valuation ring has over a field extension. In fact, over a purely inseparable extension, every valuation ring has precisely one extension. First we fix a bit of terminology.

DEFINITION 4.2.11. Let K be a field. We say a polynomial over K is *separable* if it has no multiple roots in a splitting field.
Now let $L \supseteq K$ be a algebraic field extension. We say an element of L is *separable* over K if its minimal polynomial over K is separable.
An element is *inseparable* if it is not separable.
An algebraic field extension $L \supseteq K$ is *separable* if every element of L is separable over K. A field extension is *inseparable* if it is not separable. A field extension $L \supseteq K$ is *purely inseparable* if the only elements of L that are separable over K are the elements of K itself.

LEMMA 4.2.12. *Let $K \subseteq L$ be an algebraic extension. Then there is a unique field M between K and L such that $K \subseteq M$ is a separable field extension and $M \subseteq L$ is a purely inseparable extension.*

Proof. This is Proposition V.6.6 in [20]. □

DEFINITION 4.2.13. Let $K \subseteq L$ be an algebraic extension. The field M from Lemma 4.2.12 is called the *separable closure* of K in L.
The *degree of separability* $[K : L]_s$ of this extension is $[M : K]$ where M is the separable closure of K in L. The *degree of inseparability* of this extension is $[L : M]$.

THEOREM 4.2.14. *Let $K \subseteq L$ be an algebraic extension, and $\mathcal{O}$ be a valuation ring in K. The number of prolongations of $\mathcal{O}$ in L is at most $[K : L]_s$.*

Proof. This is Theorem 3.2.9 in [13]. □

Now we look at normal extensions, so that we can use Galois theory.

THEOREM 4.2.15 (Conjugation Theorem). *Let $L \supseteq K$ be a normal extension, with Galois group G. Let $\mathcal{O}$ be a valuation ring in K, and $\mathcal{O}'$ and $\mathcal{O}''$ be extensions of $\mathcal{O}$ in L. Then there is a $\sigma \in G$ such that $\sigma\mathcal{O}' = \mathcal{O}''$.*

Proof. This is Theorem 3.2.15 in [13]. □

THEOREM 4.2.16. *Let $K \subseteq N$ be a normal extension, with Galois group G. If $(K, \mathcal{O}) \subseteq (N, \mathcal{O}')$ is a extension of valued fields, then there exists a field K' which is the fixed field of $H = \{\sigma \in G : \sigma\mathcal{O}' = \mathcal{O}'\}$, so that $K \subseteq K' \subseteq L$ such that $(K, \mathcal{O}) \subseteq (K', \mathcal{O}' \cap K')$ is an immediate extension and $\mathcal{O}$ is the unique extension of $(K', \mathcal{O}' \cap K')$ in K.*

Proof. This is Lemma 3.3.1 in [13]. □

4.3 Henselian fields

We briefly return to valuations that map to (a subgroup of) $\mathbf{R}$. Consider a field K that is complete with respect to such a valuation: this means that every Cauchy sequence in K with respect to the valuation has a limit in K. Then the following statement holds:

THEOREM 4.3.1 (Hensel's Lemma). *Let K be a field complete with respect to a valuation v with a valuation group that can be embedded in $\mathbf{R}$. Let f be a polynomial with coefficients in $\mathcal{O}_v$, and suppose that we have an $a_0 \in \mathcal{O}_v$ such that $v(f(a_0)) > 2v(f'(a_0))$, where f' is the formal derivative of f. Then there exists an $a \in \mathcal{O}_v$ that is a root of f, and for which $v(a_0 - a) > v(f'(a_0))$.*

Proof. This is Theorem 1.3.1 in [13]. □

This has the following consequence:

COROLLARY 4.3.2. *Let K be a field complete with respect to a valuation v with a valuation group that can be embedded in $\mathbf{R}$. Suppose f is a polynomial with coefficients in $\mathcal{O}_v$ such that the image of this polynomial in $\overline{K}_v$ has a simple root $\overline{a_0}$. Then f has a zero $a \in \mathcal{O}_v$ with $\overline{a} = \overline{a_0}$.*

Proof. This is Corollary 1.3.2 in [13]. □

We move back to the general case. It turns out that valued fields where a version of Hensel's Lemma holds are precisely those fields with a special property, namely that their valuation extends uniquely to *every* algebraic extension. This is the reason we define

DEFINITION 4.3.3. A valued field $(K, \mathcal{O})$ is *henselian* if $\mathcal{O}$ extends uniquely to every algebraic extension L of K.

We know that extensions are unique over purely inseparable field extensions: this gives us the alternative characterization below:

DEFINITION 4.3.4. Let K be a field, and Ω an algebraic closure of K. We then define the *separable closure* of K to be

$$K^s = \{x \in \Omega : x \text{ is separable over } K\}.$$

LEMMA 4.3.5. *A valued field $(K, \mathcal{O})$ is henselian iff $\mathcal{O}$ extends uniquely to K^s.*

Proof. One direction is obvious.
Suppose $\mathcal{O}$ extends uniquely to K^s. Now take a algebraic field extension $K \subseteq L$. First we extend $\mathcal{O}$ from K to $\mathcal{O}'$ in $L \cap K^s$. By assumption, this extension is unique. Since $L \cap K^s \subseteq L$ is purely inseparable, there is exactly one extension of $\mathcal{O}'$ to L. □

We are now able to prove the claim above

THEOREM 4.3.6. *A valued field $(K, \mathcal{O})$ is henselian iff it satisfies Hensel's Lemma iff it satisfies Corollary 4.3.2.*

Proof. This is Theorem 4.1.3 (1), (4) and (5) in [13].

□

Now suppose $(K, \mathcal{O})$ has no proper immediate extensions. Then, by Theorem 4.2.16, over the extension $K \subseteq K^s$ the valuation ring $\mathcal{O}$ extends uniquely (since $H = K$, in the notation of the theorem). So then K is henselian.

For some cases, we can also show this in the other direction.

DEFINITION 4.3.7. A valued field $(K, \mathcal{O})$ is *finitely ramified* if either $\operatorname{char} \overline{K} = 0$, or $\operatorname{char} \overline{K} = p$ and there are finitely many elements of the value group between 0 and $v(p)$.
A valued field is *algebraically maximal* if it has no proper separable immediate extensions.

THEOREM 4.3.8. *Let $(K, \mathcal{O})$ be a finitely ramified valued field. Then $(K, \mathcal{O})$ is henselian iff $(K, \mathcal{O})$ is algebraically maximal.*

Proof. This is Theorem 4.1.10 in [13]. □

We end this section with a procedure that embeds every valued field in a henselian field in an universal way. We ignore the technicalities that arise from the fact that we are using infinite Galois groups.

Let $(K, \mathcal{O})$ be a valued field, and let K^s be the separable closure of K in A. We write G for the Galois group of $K^s \supseteq K$. Pick a extension $\mathcal{O}^s$ of $\mathcal{O}$ to K^s. Now we consider the *decomposition group* of $\mathcal{O}^s$:

$$G^h = G^h(\mathcal{O}^s) = \{\sigma \in G : \sigma(\mathcal{O}^s) = \mathcal{O}^s\}.$$

This is a subgroup in G, so we can consider its fixed field. We call this the *decomposition field* of $\mathcal{O}^s$ over K, which we denote with K^h. By Galois theory, we have

$$\mathrm{Gal}(K^s/K^h) = G^h.$$

By the Conjugation Theorem, all extensions of $\mathcal{O}^s \cap K^h$ in K^s are conjugate by G^h, but all elements of G^h send the extension $\mathcal{O}^s$ to itself. So $\mathcal{O}^h = \mathcal{O}^s \cap K^h$ has a unique extension to K^s and we see (K^h, Oh^h) is a henselian valued field which we call a *henselization* of $(K, \mathcal{O})$. One can show that all henselizations are K-conjugate.

THEOREM 4.3.9. *The henselization $(K^h, \mathcal{O}^h)$ of a valued field $(K, \mathcal{O})$ is determined by the following properties:*

- *$(K^h, \mathcal{O}^h)$ is henselian;*
- *if $(K', \mathcal{O}')$ is a henselian extension of $(K, \mathcal{O})$, then there is a unique map $(K^h, \mathcal{O}^h) \to (K', Oh')$ that is the identity on K such that $(K', \mathcal{O}')$ is a prolongation of the image of $(K^h, \mathcal{O}')$ (i.e. a K-embedding).*

Proof. This is Theorem 5.2.2 in [13]. □

THEOREM 4.3.10. *The henselization of a valued field is an immediate extension.*

Proof. This is Theorem 5.2.5 in [13]. □

4.4 Rational function fields

EXAMPLE 4.4.1. Consider the rational function field $\mathbf{F}_q(t)$. On this field we consider the valuation $v_t : \mathbf{F}_q(t) \to \mathbf{Z}$ that sends every polynomial f to the opposite of its degree, $-\deg(f)$, and every quotient of polynomials f/g to $\deg(g) - \deg(f)$.

PROPOSITION 4.4.2. *Let (K, v) be a valued field, and let G be an ordered abelian group containing vK, and $g \in G$ such that $n \cdot g \notin vK$ for all $n \neq 0$. Then there is a unique valuation of $K(t)$ extending v with $v(t) = g$.*

Proof. This is Corollary 2.2.3 in [13] if we take $\Gamma = \Gamma'$ in the statement there. □

DEFINITION 4.4.3. A *henselian field* is a valued field (K, v) such that v extends uniquely to every algebraic field extension $L \supseteq K$.

EXAMPLE 4.4.4. Every valued field with valuation group $\mathbf{Z}$ can be completed with respect to that valuation: this completion is henselian. In the case of $\mathbf{Q}$ and the p-adic valuation on it, this completion is $\mathbf{Q}_p$.
All separably closed valued fields (i.e. fields with no non-trivial separable extensions) are henselian.

The following statement is known as Hensel's Lemma.

PROPOSITION 4.4.5. *Let (K, v) be an henselian valued field, and let $\mathcal{O}$ be its valuation ring. Then the following holds:*

- *For every polynomial f in $\mathcal{O}[X]$ and $a \in \mathcal{O}$ such that $\operatorname{res}(a)$ is a zero of the image of f in $Kv[X]$ but not a zero of the image of the formal derivative f' in Kv there exists an $\alpha \in \mathcal{O}$ such that $\operatorname{res}(\alpha) = \operatorname{res}(a)$ and $f(\alpha) = 0$.*
- *For every polynomial f in $\mathcal{O}[X]$ and $a \in \mathcal{O}$ such that $v(f(a)) > 2v(f'(a))$, there exists an $\alpha \in \mathcal{O}$ such that $f(\alpha) = 0$ and $v(a - \alpha) > v(f'(a))$.*

Proof. This is Theorem 4.1.3 in [13]. □

THEOREM 4.4.6. *Let (K, v) be a valued field. Then there exists an henselian valued field (K^h, v^h) extending (K, v) called the* henselization *with the property that for every other henselian extension (K', v') there exists a unique K-embedding $(K^h, v^h) \to (K', v')$.*
The henselization (K^h, v^h) is an immediate extension of (K, h)

Proof. This is Theorem 5.2.2 en 5.2.5 in [13]. □

EXAMPLE 4.4.7. The henselization of $\mathbf{F}_q(t)$ is the intersection of its algebraic closure and $\mathbf{F}_q((t))$.

DEFINITION 4.4.8. Let (K, v) be a valued field. A *partial section* is a field embedding $f : E \to K$ from a subfield $E \subseteq Kv$ such that $\operatorname{res} \circ f = \operatorname{id}_E$. If $E = Kv$ we call such a map a *section*.

EXAMPLE 4.4.9. Consider the valued field $\mathbf{F}_q(t)$. Its residue field is $\mathbf{F}_q$ and a section is given by mapping the element $a \in \mathbf{F}_q$ to the constant polynomial a in $\mathbf{F}_q(t)$.

In [1] the following is shown for all separable extensions $F \supseteq E$ as well. Since we will only need it for the case $E = \mathbf{F}_p$ and $F = \mathbf{F}_q$, we will prove it for finite extensions only.

THEOREM 4.4.10 (2.3). *Let (K, v) be an henselian valued field with $\operatorname{char} K = \operatorname{char} Kv$. Let $E \subseteq Kv$ be a subfield and let $f : E \to K$ be a partial section. If F is a field such that $E \subseteq F \subseteq Kv$ and F is a finite extension that is separable over E, then we can extend f to a partial section $F \to K$.*

Proof. Consider the subfield $f(E)$ that is isomorphic to E (since f is a section). Let L be the intersection of K and the separable closure of $f(E)$. Since the valuation is trivial on E (since for $x \in K$, $v(x) = 0$ iff $\mathrm{res}(x) \neq 0$), it is also trivial on every element in K algebraic over E, so a fortiori on elements of L. Since the valuation map is trivial on L, the residue map restricted to L must be an embedding: if $a, b \in L$ and $a \neq b$ then $v(a-b) = 0$, so $\mathrm{res}(a-b) \neq 0$, so $\mathrm{res}(a) \neq \mathrm{res}(b)$.

The image of L under the residue map contains F: take an element a of F. It is separable over E (say with minimal polynomial $\bar{g}$), so by Proposition 4.4.5 there is an element α of K that is a root of a polynomial g that is sent by the residue map to $\bar{g}$. Since L is the separable closure of E inside K, α must lie in L.

Let $L' \subseteq L$ be the preimage of F under res. The map $\mathrm{res}|'_L : L' \to F$ is a field isomorphism, so it has an inverse which is the partial section we are looking for. □

Definition 4.4.11. A valued field (K, v) is *defectless* if for all finite extensions of valued fields $(K, v) \subseteq (L, w)$ it holds that

$$[L : K] = [Lw : Kv] \cdot [wL : vK].$$

Example 4.4.12. A non-henselian field (K, v) cannot be defectless, since the henselization (K^h, v^h) has the same value group and the same residue field but $K \neq K^h$.

We recall the following definitions.

Definition 4.4.13. Let $f : \Gamma \to F$ be a map from an ordered abelian group Γ to a field F. We define the *support* of f to be the set

$$\mathrm{Supp}(f) = \{\gamma \in \Gamma : f(\gamma) \neq 0\}.$$

Now we can formulate:

Definition 4.4.14. The formal Laurent series field over F with coefficients in Γ is

$$F((\Gamma)) = \{f : \Gamma \to F : \mathrm{Supp}(f) \text{ is well-ordered } \}$$

Addition of two elements is done pointwise. For multiplication we use convolution: the product of f and g is

$$(f \cdot g)(\gamma) = \sum_{\delta \in \Gamma} f(\gamma - \delta) g(\delta).$$

Unless indicated otherwise, we will assume $F((\Gamma))$ is equipped with the degree valuation v_t with value group Γ that sends $f : \Gamma \to F$ to the minimal γ in the support of f. Note that the residue field is F.

We already encountered the Laurent series field $\mathbf{F}_q(t)$ with the degree valuation. It embeds in $\mathbf{F}_q((\mathbf{Z}))$ via the map

$$\mathbf{F}_q(t) \to \mathbf{F}_q((\mathbf{Z})) : \sum_{n=k}^{\ell} a_n t^n \mapsto (n \mapsto a_n),$$

where $k, \ell \in \mathbf{Z}$. Note that the support of the image of $\sum_{n=k}^{\ell} a_n t^n$ under this map is contained in $\{k, \ldots, \ell\}$, so it must be well-ordered. We will look at some valued fields between $\mathbf{F}_q(t)$ and $\mathbf{F}_q((\mathbf{Q}))$.

DEFINITION 4.4.15. Let Γ be an ordered abelian group. By $\mathbf{F}_q((\Gamma))$ we will mean the valued field from Definition 4.4.14.
We write $\mathbf{F}_q((t))$ for $\mathbf{F}_q((\mathbf{Z}))$.

By $\mathbf{F}_q(t)^h$ we denote the henselization of $\mathbf{F}_q(t)$, which is the intersection of its algebraic closure and $\mathbf{F}_q((t))$.
By $\mathbf{F}_q((t))^{\mathbf{Q}}$ we denote the intersection of the algebraic closure of $\mathbf{F}_q((t))$ and $\mathbf{F}_q((\mathbf{Q}))$.

PROPOSITION 4.4.16. *Let Γ be a p-divisible ordered abelian group. Then $\mathbf{F}_q((\Gamma))$ is a perfect field.*

Proof. We need to show every element is a p-th power. Let $x = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma$ be an element of $\mathbf{F}_q((\Gamma))$. Since $\mathbf{F}_q$ is a perfect field (it is finite), for all $\gamma \in \Gamma$ there exists a b_γ such that $b_\gamma^p = a_\gamma$. Now we use that Γ is p-divisible: for every $\gamma \in \Gamma$, write $f(\gamma)$ for an element in Γ such that $p \cdot f(\gamma) = \gamma$. Now define

$$y = \sum_{\gamma \in \Gamma} b_\gamma t^{f(\gamma)}.$$

This is an element of $\mathbf{F}_q(\Gamma)$, since the support of y is in an order-preserving bijection with the support of x, so both are well-ordered.

We see that, by the properties of the Frobenius map:

$$\begin{aligned} y^p &= \left(\sum_{\gamma \in \Gamma} b_\gamma t^{f(\gamma)} \right)^p \\ &= \sum_{\gamma \in \Gamma} b_\gamma^p t^{p \cdot f(\gamma)} \\ &= \sum_{\gamma \in \Gamma} a_\gamma t^\gamma, \end{aligned}$$

and clearly x is a p-th power. □

PROPOSITION 4.4.17. *Let Γ be a p-divisible ordered group. Then $\bar{\mathbf{F}}_q((\Gamma))$ is an algebraic closure of $\mathbf{F}_q((\Gamma))$.*

Proof. Let $\bar{\mathbf{F}}_q((\Gamma)) \subseteq L$ be an algebraic extension. Then the value group of L is a finite extension of Γ, and as Γ is divisible it must be Γ itself. Similarly, the residue field is a finite field extension of $\bar{\mathbf{F}}_q$, so it must be $\bar{\mathbf{F}}_q$ itself. So $\bar{\mathbf{F}}_q((\Gamma)) \subseteq L$ is an immediate extension. However, by Theorem 18.4.1 of [10], $\bar{\mathbf{F}}_q((\Gamma))$ has no proper immediate extensions, so we must have $\bar{\mathbf{F}}_q((\Gamma)) = L$. □

PROPOSITION 4.4.18. *Let Γ be a p-divisible ordered group. Then the fields between $\mathbf{F}_q((\Gamma))$ and $\bar{\mathbf{F}}_q((\Gamma))$ are precisely the fields $\mathbf{F}_{q^n}((\Gamma))$ for $n \geq 1$.*

Proof. Let K be a field such that $\mathbf{F}_q((\Gamma)) \subseteq K \subseteq \bar{\mathbf{F}}_q((\Gamma))$. We will use Galois theory to show that $K = \mathbf{F}_{q^n}((\Gamma))$ for some $n \geq 1$.

As $\mathbf{F}_q((\Gamma))$ is perfect by Proposition 4.4.16 and $\bar{\mathbf{F}}_q((\Gamma))$ is algebraically closed by Proposition 4.4.17, the extension $\mathbf{F}_q((\Gamma)) \subseteq \bar{\mathbf{F}}_q((\Gamma))$ is separable and normal, and therefore Galois. We will now study the group of automorphisms of $\bar{\mathbf{F}}_q((\Gamma))$ that fixes $\mathbf{F}_q((\Gamma))$, and we will see that these correspond bijectively to the automorphisms of $\bar{\mathbf{F}}_q$ that fix $\mathbf{F}_q$. This bijection is given by the following two operations.

Let ϕ be an automorphism of $\bar{\mathbf{F}}_q$ that fixes $\mathbf{F}_q$. This induces an automorphism $\bar{\phi}$ of $\bar{\mathbf{F}}_q((\Gamma))$ by post-composition: an element of this power series ring is a map $f : \Gamma \to \bar{\mathbf{F}}_q$ with well-ordered support. As $\phi(0) = 0$, the support of $\bar{\phi}(f) = \phi \circ f$ is the same as the support of f. As the subfield $\mathbf{F}_q((\Gamma))$ consists of those maps $\Gamma \to \bar{\mathbf{F}}_q$ with an image contained in $\mathbf{F}_q$, we see that $\bar{\phi}$ is the identity on $\mathbf{F}_q((\Gamma))$.

On the other hand, let ψ be an automorphism of $\bar{\mathbf{F}}_q((\Gamma))$. We now note that we have an field embedding $\bar{\mathbf{F}}_q \subseteq \bar{\mathbf{F}}_q((\Gamma))$ given by $x \mapsto f_x$, where f_x is the map $\Gamma \to \bar{\mathbf{F}}_q$ that assumes the value x at 0, and 0 at all other values of Γ. Now the restriction of ψ to this subfield is an automorphism of $\bar{\mathbf{F}}_q$, which fixes $\mathbf{F}_q$ (as $f_x \in \mathbf{F}_q((\Gamma))$ when $x \in \mathbf{F}_q$).

We now have to show that these two operations are inverses of each other. As $\bar{\phi}(f_x) = f_{\phi(x)}$, it is clear that the first operation followed by the second sends an $\mathbf{F}_q$-automorphism of $\bar{\mathbf{F}}_q$ to itself. It can be shown as well that the second operation is inverse to the other.

We know what the automorphisms of $\bar{\mathbf{F}}_q$ that fix $\mathbf{F}_q$ look like: for every $n \geq 1$, there is precisely one automorphism of $\bar{\mathbf{F}}_q$ that is the fixes $\mathbf{F}_{q^n}$. We see that the corresponding power series field is $\mathbf{F}_{q^n}((\Gamma))$, so we have shown that K is of this form. □

PROPOSITION 4.4.19. *For every ordered group Γ it holds that $(\mathbf{F}_q((\Gamma)), v_t)$ is a henselian valued field.*

Proof. Theorem 18.4.1 in [10] states that every field of this form has no proper immediate extensions. By Theorem 4.3.10, we know that the henselization of every valued field is an immediate extension, so this extension must be trivial, i.e. the valued field is already henselian. □

In the proofs of Theorems 9.1.5 en 9.1.8 we need the following fact.

LEMMA 4.4.20. *Let Γ be a divisible ordered abelian group. Then $(\mathbf{F}_q((\Gamma)), v_t)$ is defectless.*

Proof. For this we need a theorem of Kaplansky that for instance can be found as Theorem 2 in [25]: for every subfield E of $\bar{\mathbf{F}}_q((\Gamma))$ and every finite extension $E \subseteq F$ of valued fields such that the value group of F is contained in Γ and the residue field contained in $\bar{\mathbf{F}}_q$ holds that we can extend the inclusion $E \to \bar{\mathbf{F}}_q((\Gamma))$ to an embedding of valued fields $F \to \bar{\mathbf{F}}_q((\Gamma))$.

Let us consider a finite extension $\mathbf{F}_q((\Gamma)) \subseteq K$: by Proposition 2.4.4 the value group of K has to Γ as well. As the residue field of K has to a finite extension of the residue field of $\mathbf{F}_q((\Gamma))$, i.e. $\mathbf{F}_q$, we see that it is an algebraic extension of $\mathbf{F}_q$, so it must be contained in $\bar{\mathbf{F}}_q$. By Kaplansky's theorem, we see that

$$\mathbf{F}_q((\Gamma)) \subseteq K \subseteq \bar{\mathbf{F}}_q((\Gamma)).$$

By Proposition 4.4.18, we know that $K = \mathbf{F}_{q^n}((\Gamma))$ for some $n \geq 1$. So its residue field is $\mathbf{F}_{q^n}$ and its value group is Γ and we see that indeed

$$\begin{aligned}[\mathbf{F}_{q^n}((\Gamma)) : \mathbf{F}_q((\Gamma))] &= n = 1 \cdot n = \\ &= [\Gamma : \Gamma][\mathbf{F}_{q^n} : \mathbf{F}_q] = [v_t\mathbf{F}_{q^n}((\Gamma)) : v_t\mathbf{F}_q((\Gamma))][\mathbf{F}_{q^n}((\Gamma))v_t : \mathbf{F}_q((\Gamma))v_t]\end{aligned}$$

so we see that $\mathbf{F}_q((\Gamma))$ is defectless. □

4.5 Formal axiomatization of valued fields

We are now able to define the language and state the axioms of valued fields. For valued fields we use the following language:

DEFINITION 4.5.1. The *language of valued fields* L_{vf} is a three-sorted language with the sorts K, Γ and k, and the following symbols:

- two binary function symbols $+^K : K \times K \to K$ and $\cdot^K : K \times K \to K$;
- a unary function symbol $-^K : K \to K$;
- two constants $0^K : K$ and $1^K : K$;
- a binary function symbol $+^\Gamma : \Gamma \times \Gamma \to \Gamma$;
- a binary relation symbol $<^\Gamma$: $\Gamma \times \Gamma$;
- two constants $0^\Gamma : \Gamma$ and $\infty^\Gamma : \Gamma$;
- two binary function symbols $+^k : k \times k \to k$ and $\cdot^k : k \times k \to k$;

- a unary function symbol $-^k : k \to k$;
- two constants $0^k : k$ and $1^k : k$;
- a unary function $v : K \to \Gamma$;
- a unary function $\text{res} : K \to k$.

DEFINITION 4.5.2. A valued field is a L_{vf}-model (K, Γ, k) that satisfies the following axioms:

- the field axioms for K and the symbols $+^K, \cdot^K, -^K, 0^K, 1^K$ (as in Example 3.1.13);
- the field axioms for k and the symbols $+^k, \cdot^k, -^k, 0^k, 1^k$ (as in Example 3.1.13);
- the ordered group axioms for Γ and the symbols $+^\Gamma, <_\Gamma, 0^\Gamma, \infty^\Gamma$ (as in Example 3.1.14);
- $\forall x \in \Gamma \exists y \in K\, v(y) = x$;
- $\forall x \in K\, v(x) = \infty^\Gamma \leftrightarrow x = 0^K$;
- $\forall x \in K \forall y \in K\, v(x \cdot^K y) = v(x) +^\Gamma v(y)$;
- $\forall x \in K \forall y \in K\, v(x) < v(x +^K y) \vee v(x) = v(x +^K y)$;
- $\forall x \in K\, v(x) = 0^\Gamma \vee \text{res}(x) = 0^k$;
- $\forall x \in K \forall y \in K\, \text{res}(x \cdot^K y) = \text{res}(x) \cdot^k \text{res}(y)$;
- $\forall x \in k \exists y \in K\, \text{res}(y) = x$;
- $\forall x \in K \forall y \in K\, v(x) < 0 \vee v(y) < 0 \vee (v(x -^K y) = 0 \leftrightarrow \text{res}(x) = \text{res}(y))$.

When we have a valued field (K, v), we get a value group $v(K) = vK$ and a residue field $\overline{K}_v = Kv$ in the usual way, so we then have a model of a valued field, together with the residue map $K \to Kv$, in the sense of the above example.

REMARK 4.5.3. As we discussed in section 3.1, we sometimes want to add constants to our language. In this context, we will always be adding all the elements of a field C, which will always be of the sort K. We will write (K, v, D) for the valued field model (K, v) with added constants from D. We will also write Dv for the image of the constants in D under the residue map.

From [1] we take the following piece of notation.

DEFINITION 4.5.4. We say that a formula in L_{vf} is an $\forall^k\exists$-formula if it is logically equivalent to a formula in prenex form that starts with a number of universal quantifiers *of the residue field sort*, followed by an $\exists$-formula (i.e. a number of existential quantifiers over all three sorts).

The following properties are useful:

PROPOSITION 4.5.5. *Let $(K, v) \subseteq (L, w)$ be an extension of valued fields. We say a L_{vf}-sentence ϕ goes up from K to L if $(K, v) \models \phi$ implies $(L, w) \models \phi$.*
If ϕ is an $\exists$-sentence, then ϕ goes up every extension of valued fields.
If $(K, v) \subseteq (L, w)$ such that $Kv = Lw$, every $\forall^k\exists$-sentence goes up from K to L.

Proof. For the first property, we note that an existential statement

$$\exists x_1 \cdots \exists x_n \phi(x_1, \ldots, x_n)$$

(with ϕ a quantifier-free formula) is true in a valued field iff there exists a tuple $(a_1, \ldots, a_n)$ over that field such that $\phi(a_1, \ldots, a_n)$. If $(K, v) \subseteq (L, w)$ is an extension of valued fields, we see that we can take the image in the larger field of a tuple that satisfies a quantifier-free formula with free variables in the smaller field. For the second property, we use a similar argument. □

Part II

Geometric preliminaries

Chapter 5

Tools for algebraic geometry

5.1 Localization

DEFINITION 5.1.1. Let R be a ring. A *multiplicative subset* S of R is a subset containing 1 such that the product of any two elements of S is again an element of S.

The localization of a ring with respect to a multiplicative subset is obtained by adding inverses of elements of S.

DEFINITION 5.1.2. Let R be a ring and S a multiplicative subset. Then the *localization* $S^{-1}R$ is the set $R \times S$ up to the following equivalence relation $\sim$:

$$(r, s) \sim (r', s') \text{ iff there exists a } t \in S \text{ such that } t(rs' - r's) = 0.$$

We write r/s or $\frac{r}{s}$ for the equivalence class of (r, s). On this set a ring structure is defined as suggested by the fraction notation:

$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}, \quad \frac{r}{s}\frac{r'}{s'} = \frac{rr'}{ss'}.$$

Note that we have a natural ring map $R \to S^{-1}R$ given by $r \mapsto \frac{r}{1}$.

Two instances of localization occur time after time and deserve their own notation:

DEFINITION 5.1.3. Let R be a ring.
Let f be an element of R. Then $S = \{f^n : n \geq 0\}$ is a multiplicative subset, and we write

$$R_f = S^{-1}R = \left\{ \frac{r}{f^n} : r \in R, n \geq 0 \right\}.$$

Let P be a prime ideal of R. For all elements $a, b \in R$, we have that $ab \in P$ implies $a \in P$ or $b \in P$, so $a, b \notin P$ implies $ab \notin P$. Besides, $P \neq R$ so $1 \notin P$. It follows that $S = R \backslash P$ is a multiplicative subset. We write

$$R_P = S^{-1}R = \left\{ \frac{r}{s} : r \in R, s \notin P \right\}.$$

EXAMPLE 5.1.4. We consider the ring $\mathbf{Z}$, and its element 4. Now $\mathbf{Z}_4$ – the localization of $\mathbf{Z}$ at the multiplicative set $\{1, 4, 16, 64, \ldots\}$ – is the following subring of $\mathbf{Q}$:

$$\mathbf{Z}_4 = \left\{ \frac{a}{4^n} : a \in \mathbf{Z}, n \geq 0 \right\}$$

EXAMPLE 5.1.5. Let k be a field. Consider the polynomial ring $k[X]$. As X is an irreducible polynomial, (X) is a prime ideal. The localization of $k[X]$ at the prime ideal (X) – so at the multiplicative set of all polynomials not divisible by X – is the ring

$$k[X]_{(X)} = \left\{ \frac{f(X)}{g(X)} : f(X) \in k[X], g(X) \in k[X], g(0) \neq 0 \right\},$$

since a polynomial is divisible by X precisely if it has a root at 0.

DEFINITION 5.1.6. If R is an integral domain, (0) is a prime ideal. As any non-zero element $\frac{r}{s}$ has the inverse $\frac{s}{r}$, the localization $R_{(0)}$ is a field, called the *fraction field* of R. We write $\mathrm{Frac}(R)$.

DEFINITION 5.1.7. Let R be an integral domain. We define its *function field* $R(X)$ to be the fraction field of the polynomial ring $R[X]$.

EXAMPLE 5.1.8. The fraction field of the integral domain $\mathbf{Z}$ is $\mathbf{Q}$.

DEFINITION 5.1.9. A *local ring* is a ring with exactly one maximal ideal. (Usually this ideal is denoted by $\mathfrak{m}$.)
The *residue field* of a local ring is the quotient field $R/\mathfrak{m}$.

EXAMPLE 5.1.10. Any field has a unique maximal ideal, namely (0). So it is a local ring, and it is equal to its residue field.

PROPOSITION 5.1.11. *A ring R is local iff $R \backslash R^\times$ is an ideal.*

Proof. As we saw in Example 2.2.8, any ideal that contains invertible elements is already the whole ring. So if $R \backslash R^\times$ is an ideal, it must be maximal and all other proper ideals are contained in it, so R is local.

On the other hand, suppose R is local. If its maximal ideal $\mathfrak{m}$ is not equal to $R \backslash R^\times$, it must be smaller by the above reasoning. Let x be a non-invertible element of $R \backslash \mathfrak{m}$. However, by Proposition 2.2.14, this element must be contained in a maximal ideal, so it must be in $\mathfrak{m}$. This is contradiction. □

EXAMPLE 5.1.12. The localization of any ring R with respect to a prime ideal P is a local ring: the maximal ideal is $P \cdot R_P = \{p/s : p \in P, s \notin P\} \subseteq R_P$.

DEFINITION 5.1.13. A ring map from a local ring R to a local ring S is called a *local homomorphism* if the preimage of the maximal ideal is the maximal ideal.

DEFINITION 5.1.14. A local integral domain R with maximal ideal $\mathfrak{m}$ is *equicharacteristic* if $\operatorname{char} R = \operatorname{char} R/\mathfrak{m}$.

EXAMPLE 5.1.15. An example of a equicharacteristic local ring is $k[[X]]$ for a field k, which has maximal ideal (X) and residue field $k[[X]]/(X) \cong k$. As we have a field embedding $k \to k[[X]]$ by sending an element to the constant polynomial with that value, $\operatorname{char} k = \operatorname{char} k[[X]]$.

DEFINITION 5.1.16. A *discrete valuation ring* is an integral domain that is the valuation ring of a valued field with value group $\mathbf{Z}$.

EXAMPLE 5.1.17. For a field k, $k[[X]]$ is the valuation ring of $k((X))$ with value group $\mathbf{Z}$, so it is a discrete valuation ring.

PROPOSITION 5.1.18. *The ideals of a discrete valuation ring are the following:* (0) *and* (π^k) *for* $k \geq 1$ *an integer. For* π *we can take any element of the ring with valuation 1.*

Proof. This is shown on page 94 of [2]. □

5.2 Dimensions and regularity

DEFINITION 5.2.1. Let R be a ring and P a prime ideal of R. The *height* of P is the maximal n such that there exist prime ideals

$$P_0 \subset P_1 \subset \cdots \subset P_n = P.$$

If such an n does not exist we say that the height is infinite.

DEFINITION 5.2.2. The *Krull dimension* of a ring R is the maximal height of any prime ideal in R. If such an n does not exist we say that the Krull dimension is infinite.

EXAMPLE 5.2.3. The Krull dimension of a field is 0, as the only prime ideal is (0). The Krull dimension of $\mathbf{Z}$ is 1, as (0) is contained in all other prime ideals and none of the other prime ideals are contained in one another.

EXAMPLE 5.2.4. The Krull dimension of $k[X_1, \ldots, X_n]$ is n: an example of a chain of length n is

$$(0) \subset (X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, \ldots, X_n).$$

DEFINITION 5.2.5. A *system of parameters* for a noetherian local ring of Krull dimension d and maximal ideal $\mathfrak{m}$ is a set $\{x_1, \ldots, x_d\}$ in that ring such that there exists an integer $N \geq 1$ for which

$$\mathfrak{m}^N \subseteq (x_1, \ldots, x_d).$$

DEFINITION 5.2.6. A *regular local ring* is a noetherian local ring such that the minimal number of generators of the maximal ideal is equal to the Krull dimension.
In line with the previous definition, we call any set of generators of the maximal ideal of minimal size then a *regular system of parameters*.

5.3 Completeness and Hensel's lemma

DEFINITION 5.3.1. An *inverse system* is a sequence of rings R_i indexed by $\mathbf{N}$, and a sequence of ring maps $f_{i+1} : R_{i+1} \to R_i$ for all $i \geq 1$.
The *inverse limit* $\lim_{\leftarrow} R_i$ (with the maps f_i implicit) is the ring that consists of sequences $(r_i)_{i \in \mathbf{N}}$ such that $r_i \in R_i$ and $f_{i+1}(r_{i+1}) = r_i$ for all i. (We call every sequence of this form *coherent*.) Addition and multiplication are defined coordinatewise.

DEFINITION 5.3.2. Let R be a local ring, and $\mathfrak{m}$ the maximal ideal of R. Then the *completion* $\hat{R}$ of R is the inverse limit of the system

$$\cdots \to R/\mathfrak{m}^3 \to R/\mathfrak{m}^2 \to R/\mathfrak{m}$$

where the maps are induced by the quotient map.

DEFINITION 5.3.3. Let R be a local ring, and M an R-module. The *completion* $\hat{M}$ of M is the inverse limit of the system

$$\cdots M/\mathfrak{m}^3 M \to M/\mathfrak{m}^2 M \to M/\mathfrak{m}M$$

where the maps are induced by the quotient map.

PROPOSITION 5.3.4. *Let R be a local ring. Then there is a canonical ring map $\phi : R \to \hat{R}$ given by $\phi(r) = (r + \mathfrak{m}^i)_{i \geq 1}$. Its kernel is the ideal $\bigcap_{n \in \mathbf{N}} \mathfrak{m}^n$, so if this ideal is (0) we see that R embeds in $\hat{R}$.*

Proof. This map is defined on page 102 of [2]. From Theorem 10.17 there it follows that the kernel is the intersection of all $\mathfrak{m}^n$ for $n \geq 1$. The last claim follows from the fact that a ring map is injective iff its kernel is trivial. □

COROLLARY 5.3.5. *If R is a noetherian integral local ring it embeds in its completios.*

Proof. In Corollary 10.18 in [2] it is shown that $\bigcap_{n=1}^{\infty} A^n = (0)$ for every ideal A in R. By Proposition 5.3.4, we see that R embeds in $\hat{R}$. □

DEFINITION 5.3.6. A local ring R is *complete* if it is isomorphic to its completion $\hat{R}$.

EXAMPLE 5.3.7. Let K be a field. Then the completion of the polynomial algebra $K[X_1, \ldots, X_n]$ is the power series ring $K[[X_1, \ldots, X_N]]$.

THEOREM 5.3.8. *If R is a noetherian local ring, then $\hat{R}$ is a noetherian local ring with the same residue field as R.*

Proof. That $\hat{R}$ is local with the same residue field follows from Proposition 10.16 in [2]. From Theorem 10.26 there it follows that $\hat{R}$ is noetherian. □

REMARK 5.3.9. If R is a noetherian local ring, we write $\hat{\mathfrak{m}}$ for the unique maximal ideal of the completion.

COROLLARY 5.3.10. *If R is an equicharacteristic noetherian local ring, then $\hat{R}$ is too.*

Proof. From Theorem 5.3.8 it follows that $\hat{R}$ is a local ring with the same residue field as R, so

$$\operatorname{char} R = \operatorname{char} R/\mathfrak{m} = \operatorname{char} \hat{R}/\hat{\mathfrak{m}}.$$

As there is an injective map $R \to \hat{R}$ by Corollary 5.3.5, $\operatorname{char} R = \operatorname{char} \hat{R}$, so $\operatorname{char} \hat{R} = \operatorname{char} \hat{R}/\hat{\mathfrak{m}}$. □

THEOREM 5.3.11. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and I an ideal of R. Then*

$$\hat{R}/\hat{I} \cong \widehat{R/I},$$

where the completions on the left hand side are with respect to the maximal ideal of R and the completion on the right hand side is with respect to the maximal ideal of R/I. Note that $\hat{I}$ is the completion of I as a R-module.

Proof. Proposition 10.12 in [2] states that completion preserves exactness of sequences of finitely generated modules over a Noetherian ring. As ideals in a Noetherian ring are finitely generated modules, it follows that the image of the short exact sequence

$$0 \to I \to R \to R/I \to 0$$

under completion is also exact, which yields the result. □

PROPOSITION 5.3.12. *If R is a Noetherian local ring, then R is regular if and only if $\hat{R}$ is regular.*

Proof. This is Proposition 11.24 in [2]. □

DEFINITION 5.3.13. A local ring R is *henselian* if for every monic polynomial $f \in R[X]$ and every $a_0 \in R/\mathfrak{m}$ such that $f(a_0) \equiv 0 \mod \mathfrak{m}$ but $f'(a_0) \not\equiv 0 \mod \mathfrak{m}$ there exists an $a \in R$ such that $f(a) = 0$ and $a \equiv a_0 \mod \mathfrak{m}$.

PROPOSITION 5.3.14. *A valued field is henselian if and only if its valuation ring is henselian.*

Proof. This is Theorem 4.1.3 (1) and (4) in [13]. □

PROPOSITION 5.3.15. *A complete local ring is henselian.*

Proof. This is Theorem 7.3 in [11]. □

5.4 The structure of complete local rings

In the proof of Theorem 7.3.3 we use the following well-known result on the structure of complete local rings, which is a one of the cases of Cohen's Structure Theorem.

THEOREM 5.4.1. *Let R be an equicharacteristic complete regular local ring with residue field κ. Then R is isomorphic (as a κ-algebra) to a power series ring over κ in a finite number of variables.*

Proof. This is Theorem 15 in [7]. (Note that that the author's definition of a local ring also requires the ring to be noetherian.) □

PROPOSITION 5.4.2. *Every noetherian equicharacteristic complete local ring is a quotient of a complete regular local ring of the same characteristic.*

Proof. Theorem 29.4 (ii) in [23] states that every noetherian complete local ring A is a quotient of a regular local ring B, say $A \cong B/I$, and by the remark on page 223 in [23], if A is equicharacteristic we can pick B to be equicharacteristic and of the same characteristic. The completion $\hat{B}$ of B is a complete ring that is regular as well by Proposition 5.3.12 and local by Theorem 5.3.8. By Theorem 5.3.11, $\hat{B}$ has a ideal $\hat{I}$ such that

$$\hat{B}/\hat{I} \cong \widehat{B/I} = \hat{A} \cong A,$$

where we used in the last step that A is complete. We see that A is a quotient of a complete regular local ring of the same characteristic. □

5.5 Cohen-Macaulay modules and flatness

DEFINITION 5.5.1. Let R be a ring and M an R-module. An element of R is called *M-regular* if $xM \neq M$ and x is not a zero divisor on M. A sequence of elements $x_1, \ldots, x_n$ in a ring R is said to be *M-regular* if for all i the image of x_{i+1} is regular in $M/(x_1, \ldots, x_i)M$.

DEFINITION 5.5.2. Let R be a noetherian local ring, and M an R-module. M is a *big Cohen-Macaulay module* if there exists a system of parameters in R that is M-regular.
We say M is a *balanced big Cohen-Macaulay module* if it is a big Cohen-Macaulay module, and every system of paramters in R is M-regular.

PROPOSITION 5.5.3. *Let R be a regular local ring. Then every regular system of parameters is R-regular. It follows that every regular local ring is a big Cohen-Macaulay module over itself.*

Proof. By Theorem 17.8 in [23], every regular local ring is a big Cohen-Macaulay module over itself. By Theorem 17.4.(iii) in [23], every system of parameters is a R-regular sequence. □

PROPOSITION 5.5.4. *A big Cohen-Macaulay module M over a noetherian local ring is balanced is every permutation of a M-regular sequence is again M-regular.*

Proof. This is Proposition 3.3.8 in [28]. □

THEOREM 5.5.5. *If M is a balanced big Cohen-Macaulay module over a regular local ring, it is flat.*

Proof. This is the first part of Theorem 3.3.9 in [28]. □

5.6 Excellent rings

For this section, we rely on [8] and the clear description of excellent rings that can be found there. Excellent rings were introduced by Alexander Grothendieck during his work on algebraic geometry, as general noetherian rings sometimes behave pathologically. The definition is technical, and examples of non-excellent noetherian rings are not easy to find.

DEFINITION 5.6.1. We call a chain of prime ideals in a ring R $Q = P_0 \subset P_1 \subset P_2 \subset \cdots \subset P_n = Q'$ *saturated* if there exists no prime ideal P' in R such that

$$P_i \subset P' \subset P_{i+1}$$

for some $0 \leq i < n$.

The following definition is based on Definition 2.1 in [8], but reformulated in terms of commutative algebra, in order not to disrupt the logical order of this thesis.

DEFINITION 5.6.2. A noetherian ring A is *excellent* if it has the following properties:

- (Universally catenary) For every finitely generated A-algebra B and for every two prime ideals $P \subseteq Q$ in B, all saturated chains of prime ideals from P to Q have the same length.
- (Formal fibers are geometrically regular) For every prime ideal P, we have that the ring $\widehat{A_P} \otimes K$ is regular for all finite field extensions K of A_P/M where M is a maximal ideal of A_P, and where $\widehat{A_P}$ is the completion of A_P.
- (Regular loci are open) For all finitely generated A-algebras, there is an ideal I in B such that a prime ideal P of the algebra contains I precisely if the localization at P is not a regular local ring.

PROPOSITION 5.6.3. *A field is excellent. The localization and the homomorphic image of an excellent ring are always excellent.*

Proof. This is shown in [30, Tag 07QW]. □

PROPOSITION 5.6.4. *A ring that is finitely generated over a field is excellent.*

Proof. In §34 of [22] it is shown that a finite algebra over an excellent ring is excellent itself. By Proposition 5.6.3, a field is excellent, so the statement follows. □

PROPOSITION 5.6.5. *The henselization of an excellent ring is excellent.*

Proof. This is discussed on page 17 of [14]. □

Chapter 6

Some notions from algebraic geometry

6.1 Sheaves

DEFINITION 6.1.1. A *sheaf* (of rings) F on a topological space X is a map that sends any open subset $U \subseteq X$ to a ring $F(U)$ and any inclusion $U \subseteq V \subseteq X$ of open subset to a map $\rho_{VU} : F(V) \to F(U)$ (the *restriction map*) such that

- $F(\emptyset) = 0$;
- for all open subsets $U \subseteq X$, $\rho_{UU} = \mathrm{id}_U$;
- for all open subsets $U \subseteq V \subseteq W \subseteq X$, $\rho_{WU} = \rho_{VU} \circ \rho_{WV}$;
- for any covering $\{U_i\}$ of an open subset $U \subseteq X$, if $s \in F(U)$ such that $\rho_{UU_i}(s) = 0$ for all i, then $s = 0$;
- for any covering $\{U_i\}$ of an open subset $U \subseteq X$, if there exist $s_i \in F(U_i)$ such that for all i, j:

  $$\rho_{U_i, U_i \cap U_j}(s_i) = \rho_{U_j, U_i \cap U_j}(s_j)$$

  then there exists a $s \in F(U)$ such that $\rho_{UU_i}(s) = s_i$ for all i.

DEFINITION 6.1.2. Let $f : X \to Y$ be a continuous map of topological spaces, and F a sheaf on X. The *direct image sheaf* f_*F is the sheaf on Y defined by $f_*F(V) = F(f^{-1}(V))$ for all open sets $V \subseteq Y$.

PROPOSITION 6.1.3. *Let F be a sheaf on a topological space X, and let $U \subseteq X$ be an open subset. Then $(U, F|_U)$ is a sheaf on U, where we define*

$$F_U(V) = F(V) \quad \text{for open } V \subseteq U,$$

and the restriction maps of F_V to be those of F.
We call this sheaf the restricted sheaf *of F to U.*

Proof. This is shown on page 65 of [15]. □

DEFINITION 6.1.4. Let F be a sheaf on a topological space X, and let P be a point of X. The *stalk* F_P of F at P is the direct limit $\lim_{U \ni P} F(U)$ where U runs through the open subsets of X containing P. The maps between the rings are the restriction maps.

DEFINITION 6.1.5. Let R be a ring. The *spectrum* $\operatorname{Spec} R$ of R is the set of all prime ideals of R.

PROPOSITION 6.1.6. *Let R be a ring. For any ideal A of R, we write $V(A)$ for $\{P \in \operatorname{Spec} R : P \supseteq A\}$. Then there is a topology on $\operatorname{Spec} R$ in which the subsets of the form $V(A)$ are precisely the closed sets.*

Proof. In Lemma II.2.1 of [15], it is shown that the finite union and the arbitrary intersection of closed sets are closed too. That the empty set and $\operatorname{Spec} R$ itself are closed follows from the fact that they are equal to $V((1))$ respectively $V((0))$. □

EXAMPLE 6.1.7. Under this topology, the subsets $D(f) = \{P \in \operatorname{Spec} R : f \notin P\}$ are open. We call sets of this form *distinguished open sets* and they form a basis with respect to this topology.

In the remainder, we will assume that $\operatorname{Spec} R$ is endowed with this topology.

PROPOSITION 6.1.8. *Let R be a ring. The assignment $D(f) \mapsto R_f$ for any $f \in R$ can be extended to a sheaf on $\operatorname{Spec} R$. The stalk of this sheaf in the point P is equal to R_P.*

Proof. This is shown on page 70 of [15]. □

We write $\mathcal{O}_{\operatorname{Spec} R}$ for this sheaf.

6.2 Schemes

We want a scheme to be an topological space with a sheaf that locally looks like the spectrum of a ring with the sheaf of the previous proposition on it. In order to define this formally we need the concept of a map between such objects.

DEFINITION 6.2.1. A *locally ringed space* is a topological space X with a sheaf $\mathcal{O}_X$ such that all stalks of the sheaf are local rings.

DEFINITION 6.2.2. A *morphism of locally ringed spaces* from $(X, \mathcal{O}_X)$ to $(Y, \mathcal{O}_Y)$ is a continuous map $f : X \to Y$ together with a ring map $f_V^\# : \mathcal{O}_Y(V) \to f_*\mathcal{O}_X(V)$ for all open subsets $V \subseteq Y$, such that for any $P \in X$, the map between the stalks that is induced by the maps $f_V^\# : \mathcal{O}_Y(V) \to f_*\mathcal{O}_X(V)$ for open sets V containing $f(P) \in Y$,

$$f_P^\# : \mathcal{O}_{Y,f(P)} \to \mathcal{O}_{X,P},$$

is a local homomorphism.
An *isomorphism of locally ringed spaces* is a morphism of locally ringed spaces with an inverse, i.e. a pair $(f, f^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ such that f is a homeomorphism and $f_V^\#$ is a ring isomorphism for all open $V \subseteq Y$.

DEFINITION 6.2.3. An *affine scheme* is a locally ringed space isomorphic to $(\operatorname{Spec} R, \mathcal{O}_{\operatorname{Spec} R})$, where R is a ring.
A *scheme* is a locally ringed space $(X, \mathcal{O}_X)$ such that any point in X has a open neighbourhood $U \subseteq X$ such that the restricted sheaf $(U, \mathcal{O}_X|_U)$ is an affine scheme. (Often we write X for the scheme $(X, \mathcal{O}_X)$.)
A *morphism of schemes* is a morphism of locally ringed spaces.

DEFINITION 6.2.4. A morphism of schemes $f : Y \to X$ is a *closed immersion* if f induces a homeomorphism between Y and a closed subset of X as topological spaces, and the induced map on the stalks $f_P^\# : \mathcal{O}_{X,f(P)} \to f_*\mathcal{O}_{Y,P}$ is surjective for every $P \in Y$.

DEFINITION 6.2.5. Let $(X, \mathcal{O}_X)$ be a scheme. The *residue field* of a scheme at a point $P \in X$ is the residue field of the local ring $\mathcal{O}_{X,P}$.

PROPOSITION 6.2.6. *Let R be a ring and X a scheme. There exists a bijection between the set of scheme morphisms from X to* $\operatorname{Spec} R$ *and the set of ring homomorphisms from R to $\mathcal{O}_X(X)$.*

Proof. This is Theorem I-40 in [12]. □

COROLLARY 6.2.7. *The category of affine schemes is isomorphic to the category of rings with arrows reversed.*

DEFINITION 6.2.8. Let X be a scheme. A *scheme over X* is a scheme Y together with a fixed scheme morphism $Y \to X$ (the *structure morphism*). As a shorthand, we will refer to a scheme over $\operatorname{Spec} R$ as a scheme over R.
A *morphism of schemes over X* is a morphism of schemes such that the triangle with the fixed morphisms to X commutes.
As a special case, we say an open subset U of a scheme X over R is *defined over R* if the restriction of the fixed morphism $X \to \operatorname{Spec} R$ to U is a morphism $U \to \operatorname{Spec} R$.

As a direct application of Proposition 6.2.6, we note that an affine scheme $\operatorname{Spec} A$ over a ring R (a scheme morphism $\operatorname{Spec} A \to \operatorname{Spec} R$) corresponds to a ring map $R \to A$, i.e. a R-algebra structure on the ring A. In this context, a morphism of schemes over R corresponds to an R-algebra homomorphism.

DEFINITION 6.2.9. Let X be a scheme, and let Y and Z be schemes over X. The *fibre product* $Y \times_X Z$ is the fiber product in the categorical sense of the fixed morphisms $Y \to X \leftarrow Z$.

PROPOSITION 6.2.10. *This fiber product of two schemes over a third one always exists.*

Proof. This is Theorem II.3.3 in [15]. □

We refer to any commutative square of the form

$$\begin{array}{ccc} Y \times_X Z & \longrightarrow & Y \\ \downarrow & & \downarrow \\ Z & \longrightarrow & X \end{array}$$

as a *cartesian square*.

DEFINITION 6.2.11. Let $f : X \to Y$ be a morphism. The *pullback* (or *base change*) of f by a morphism $h : W \to Y$ is the morphism $\bar{f} : X \times_Y W \to W$ in the cartesian square induced by f and h.

DEFINITION 6.2.12. A morphism of schemes $f : X \to Y$ is *locally of finite type* if there exists an open affine covering of Y by sets $(V_i)_i = (\operatorname{Spec} B_i)_i$ such that $f^{-1}(V_i)$ can be covered by open affine subsets $(U_{ij})_j = (\operatorname{Spec} A_{ij})_j$ where every A_{ij} is a finitely generated B_i-algebra.
The morphism is said to be *of finite type* if the above condition is satisfied and moreover there are only a finite number of affine subsets U_{ij} needed for every value of i.

DEFINITION 6.2.13. A scheme is *quasi-compact* if its underlying topological space is quasi-compact.

DEFINITION 6.2.14. A *locally noetherian scheme* is a scheme X that can be covered by affine open subsets of the form $\operatorname{Spec} A_i$ where A_i is noetherian ring.

DEFINITION 6.2.15. A *noetherian scheme* is a scheme X that is quasi-compact and locally noetherian.

6.3 Rational points

DEFINITION 6.3.1. Let R be a ring and X a scheme over $\operatorname{Spec} R$ via the map $s : X \to \operatorname{Spec} R$. An *$R$-rational point* of X is a scheme morphism $x : \operatorname{Spec} R \to X$ such that $s \circ x = \mathrm{id}_{\operatorname{Spec} R}$.

In the case that X is an affine scheme, say $X = \operatorname{Spec} A$ with A an R-algebra, we see that a R-rational point on X (i.e. a map $\operatorname{Spec} R \to X$) corresponds to a ring map $A \to R$, such that the R-algebra structure of A is respected. So R-rational points on an affine scheme $\operatorname{Spec} A$ correspond bijectively to R-algebra homomorphisms from A to R.

We move to the case where A is finitely generated over R, say A is of the form $R[x_1, \ldots, x_m]/(f_1, \ldots, f_t)$ for some polynomials f_i over $x_1, \ldots, x_m$. We know that R-algebra homomorphisms from A to R correspond bijectively to R-algebra homomorphisms $F : R[x_1, \ldots, x_n] \to R$ such that $f_i \in ker(F)$ for all polynomials f_i. Algebra homomorphisms from a polynomial ring are determined by the image of the variables, so F corresponds to a n-tuple $(r_1, \ldots, r_n)$ in R such that $f_i(r_1, \ldots, r_n) = 0$ for all i. It follows that the R-rational points on the scheme $\operatorname{Spec} R[x_1, \ldots, x_m]/(f_1, \ldots, f_t)$ correspond bijectively to solutions over F of the system of equations $f_1 = \cdots = f_t = 0$.

Definition 6.3.2. If $f : Y \to X$ is a morphism of schemes over $\operatorname{Spec} R$, we say that an R-rational point y on Y is a *lifting* of a point x on X if $f \circ y = x$ as scheme morphisms.
If a lifting of a R-rational point (with respect to some morphism) exists we say the point *admits* a lifting.

When $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$ are affine schemes, a scheme morphism $f : Y \to X$ over R corresponds to an R-algebra homomorphism $\bar{f} : A \to B$. Since R-rational points on X correspond to R-algebra homomorphisms $\phi : A \to R$, we see that a lifting of ϕ to Y is the same as giving an R-algebra homomorphism $\psi : B \to R$ such that $\psi \circ \bar{f} = \phi$.

6.4 Properties of morphisms

Definition 6.4.1. Let $f : X \to Y$ be a morphism of schemes. Now consider the following commutative square.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \mathrm{id}_Y} \\ Y & \xrightarrow{\mathrm{id}_Y} & Y. \end{array}$$

By the universal property of the fibre product, a map $X \to X \times_Y X$ is induced such that its postcomposition with both the projective maps $X \times_Y X \to X$ is f. We call this map $\Delta_{Y/X} : X \to X \times_Y X$ the *diagonal morphism* corresponding to f.

Definition 6.4.2. We call $f : X \to Y$ a *separated morphism* if its associated diagonal morphism $\Delta_{Y/X} : X \to X \times_Y X$ is a closed immersion.

DEFINITION 6.4.3. A morphism of schemes $f : X \to Y$ is *closed* if the image of every closed subset of X under f is a closed set in Y.
A morphism of schemes $f : X \to Y$ is *universally closed* if every pullback of it is closed.

DEFINITION 6.4.4. A morphism of schemes $f : X \to Y$ is a *proper morphism* if it is separated, of finite type and universally closed.

THEOREM 6.4.5 (Valuative Criterion for Properness). *Let $f : X \to Y$ be a scheme morphism of finite type, with X noetherian. Then f is a proper morphism iff the following condition holds.*
For every valuation ring R, let K denotes its fraction field. The inclusion map $R \subseteq K$ induces a map $i : \operatorname{Spec} K \to \operatorname{Spec} R$. For every two morphisms $\operatorname{Spec} K \to X$ and $\operatorname{Spec} R \to Y$ there exists a unique morphism $\operatorname{Spec} R \to X$ that makes the diagram below commute.

$$\begin{array}{ccc} \operatorname{Spec} K & \longrightarrow & X \\ \downarrow{\scriptstyle i} & \nearrow & \downarrow{\scriptstyle f} \\ \operatorname{Spec} R & \longrightarrow & Y \end{array}$$

Proof. This is Theorem II.4.7 in [15]. □

DEFINITION 6.4.6. A morphism of schemes $f : Y \to X$ is *flat* if the induced stalk map $f_y^{\#} : \mathcal{O}_{X,f(y)} \to \mathcal{O}_{Y,y}$ is flat for all $y \in Y$.

DEFINITION 6.4.7. A morphism of schemes $f : Y \to X$ that is locally of finite type is *unramified at $y \in Y$* if $\mathcal{O}_{Y,y}/\mathfrak{m}_x\mathcal{O}_{Y,y}$ is a finite separable field extension of $k(x)$ for $x = f(y)$.
We say a morphism of rings $A \to B$ is *unramified* at a prime ideal of B if the induced morphism $\operatorname{Spec} B \to \operatorname{Spec} A$ is at the corresponding point in $\operatorname{Spec} B$.

PROPOSITION 6.4.8. *A ring homomorphism $A \to B$ of finite type is unramified at the maximal ideal P of B if the image of $f^{-1}(P)$ generates the maximal ideal in B and the residue field of B at P is a finite separable field extension of the residue field of A at $f^{-1}(P)$.*

Proof. This is shown on page 21 of [24]. □

DEFINITION 6.4.9. A morphism of schemes locally of finite type is *étale* at a point if it is flat and unramified at that point.

DEFINITION 6.4.10. A point of a scheme X is *non-singular* if the local ring at that point is a regular ring.

6.5 More on rational points

DEFINITION 6.5.1. Let R be an integral domain and X be a scheme over $\operatorname{Spec} R$. Let $K = \operatorname{Frac}(R)$, and $i : \operatorname{Spec} K \to \operatorname{Spec} R$ the map induced by the inclusion $R \to K$. The *generic fiber* of X is the scheme $X \times_{\operatorname{Spec} R} \operatorname{Spec} K$, which will be denoted by X_K. (We write $j : X_K \to X$ for the pullback of i.)

In the situation of Definition 6.5.1, it holds that

$$X_K \times_X \operatorname{Spec} R = \operatorname{Spec} K,$$

since

$$(X \times_{\operatorname{Spec} R} \operatorname{Spec} K) \times_X \operatorname{Spec} R = \operatorname{Spec} R \times_{\operatorname{Spec} R} \operatorname{Spec} K = \operatorname{Spec} K,$$

by the cancellation property of the fiber product.

Let x be an R-rational point on X. We can now draw the following diagram, in which the small squares are both cartesian:

$$\begin{array}{ccc}
\operatorname{Spec} K & \xrightarrow{i} & \operatorname{Spec} R \\
\downarrow{\scriptstyle x_K} & & \downarrow{\scriptstyle x} \\
X_K & \xrightarrow{j} & X \\
\downarrow & & \downarrow{\scriptstyle s} \\
\operatorname{Spec} K & \xrightarrow{i} & \operatorname{Spec} R
\end{array} \qquad \text{id}$$

We note that the induced map $x_K : \operatorname{Spec} K \to X_K$ is a K-rational point.

DEFINITION 6.5.2. Let R be an integral domain and X be a scheme over $\operatorname{Spec} R$. The *underlying point* of a R-rational point x on X is the pullback of the map $\operatorname{Spec} R \to X$ along the map $X_K \to X$. We write x_K for the underlying point.

This underlying point is a scheme morphism $\operatorname{Spec} K \to X_K$, so the underlying point is always a K-rational point on the generic fiber X_K.

THEOREM 6.5.3. *Let R be a discrete valuation ring with $K = \operatorname{Frac}(R)$. Let X, Y be Noetherian schemes over $\operatorname{Spec} R$, and $f : Y \to X$ a proper morphism. If the underlying point x_K of an R-rational point x admits a K-rational lifting z to Y_K, then x itself admits a R-rational lifting y to Y such that $y_K = z$.*

Proof. This is Proposition 2.2 in [9]. □

Chapter 7

Artin approximation

7.1 The approximation property and Artin approximation

DEFINITION 7.1.1. We say that a local ring R has the *approximation property* if for every tuple $\bar{u} = (u_1, \ldots, u_k)$ in R there exists an *approximation function* $N_{\bar{u}} : \mathbf{N}^2 \to \mathbf{N}$ that depends on R and $\bar{u}$ only, such that the following property holds. If $\{f_i(x_1, \ldots, x_k, y_1, \ldots, y_m) : 1 \leq i \leq t\}$ is a family of polynomials of degree $\leq d$ over $\mathbf{Z}$ such that there exist a m-tuple $\bar{v}$ from R such that for all i

$$f_i(u_1, \ldots, u_k, v_1, \ldots, v_m) \equiv 0 \mod \mathfrak{m}^N,$$

where $N = N_{\bar{u}}(d, m)$, then there exists a m-tuple $\bar{v'}$ from R such that

$$f_i(u_1, \ldots, u_k, v'_1, \ldots, v'_m) = 0.$$

7.2 The approximation property in a power series ring over a field

LEMMA 7.2.1. *Let κ be a field, and let R be the power series ring $\kappa[[T_1, \ldots, T_d]]$ with maximal ideal $\mathfrak{m} = (T_1, \ldots, T_d)$. Let R^* be the ultrapower of R and κ^* the ultrapower of κ, where the ultrapowers are formed with the same non-principal ultrafilter on $\mathbf{N}$. Write $\mathfrak{m}^\infty = \bigcap_{n \in \mathbf{N}} \mathfrak{m}^n R^*$. Then:*

$$R^*/\mathfrak{m}^\infty \cong \kappa^*[[T_1, \ldots, T_d]].$$

Proof. In this proof we will use the multi-index notation: by $\sum_I a_I T^I$ we mean

$$\sum_{(i_1, \ldots, i_d) \in \mathbf{N}^d} a_{(i_1, \ldots, i_d)} T_1^{i_1} \cdots T_d^{i_d}.$$

For multi-indices I, J (i.e. d-tuples from $\mathbf{N}$) we write $I \leq J$ to indicate $i_k \leq j_k$ for all k. In this case, we define $J - I$ to be the multi-index given by $j_k - i_k$ at the k-th place. This allows us to write concisely:

$$\left(\sum_I a_I T^I\right)\left(\sum_J b_J T^J\right) = \sum_K \left(\sum_{I \leq K} a_I b_{K-I}\right) T^K$$

We also introduce the notation $\deg(I)$ as a shorthand for the sum of the indices in the multi-index I. Note that we have $T^I \in \mathfrak{m}^n$ iff $\deg(I) \geq n$.

We will prove the lemma by studying the properties of the following map:

$$f : R^* \to \kappa^*[[T_1, \ldots, T_d]] : [(\sum_I a_{i,I} T^I)_i] \mapsto \sum_I [(a_{i,I})_i] T^I$$

First of all, this assignment is well-defined: if $[(\sum_I a_{i,I} T^I)_i] = [(\sum_I b_{i,I} T^I)_i]$, then

$$\{i \in \mathbf{N} : a_{i,I} = b_{i,I} \text{ for all } I\} \in \mathcal{U},$$

so for every value of I we have $\{i \in \mathbf{N} : a_{i,I} = b_{i,I}\} \in \mathcal{U}$ as it is a larger subset of $\mathbf{N}$. So $[(a_{i,I})_i] = [(b_{i,I})_i]$ for all I, hence $\sum_I [(a_{i,I})_i] T^I = \sum_I [(b_{i,I})_i] T^I$.

The map f is a homomorphism too: it is clear that 1 is mapped to itself, and that f respects the addtition of power series, as this is defined pointwise in the ultrapower. We need to show f respects the multiplication of power series too. We note that a multi-index sum ranging over indices I such that $I \leq K$ for some multi-index K is always a finite sum. Using that the finite sum and multiplication in the ultrapower is defined pointwise, we see that in general:

$$\begin{aligned}
f([(\sum_I a_{i,I} T^I)_i][(\sum_J b_{i,J} T^J)_j]) &= f([(\sum_I a_{i,I} T^I \sum_J b_{i,J} T^J)_j]) \\
&= f([(\sum_K \sum_{I \leq K} a_{i,I} b_{i,K-I} T^K)_i]) \\
&= \sum_K [(\sum_{I \leq K} a_{i,I} b_{i,K-I})_i] T^K \\
&= \sum_K \sum_{I \leq K} [(a_{i,I})_i][(b_{i,K-I})_i] T^K \\
&= \sum_I [(a_{i,I})_i] T^I \sum_J [(b_{i,J})_i] T^J \\
&= f([(\sum_I a_{i,I} T^I)_i]) f([(\sum_J b_{i,J} T^J)_j]).
\end{aligned}$$

Note that f is surjective: consider an element of $\kappa^*[[T_1, \ldots, T_d]]$, say

$$\sum_I [(a_{i,I})_i] T^I.$$

Then clearly $([\sum_I a_{i,I}T^I)_i] \in R^*$ is in its preimage.

We claim that the kernel of f is the ideal $\mathfrak{m}^\infty$ in R^* which is the intersection of all $\mathfrak{m}^n R^*$ for $n \in \mathbf{N}$. First we show that $\ker f \subseteq \mathfrak{m}^n R^*$ for every natural number n. Let $([(\sum_I a_{i,I}T^I)_i]$ be an element of R^* which is mapped to 0 by f, so $\sum_I [(a_{i,I})_i]T^I = 0$, i.e. $[(a_{i,I})_i] = 0$ for all I, which means by definition

$$\{i \in \mathbf{N} : a_{i,I} = 0\} \in \mathcal{U}. \tag{7.1}$$

If we show that

$$([(\sum_I a_{i,I}T^I)_i] = [(\sum_{I,\deg(I)\geq n} a_{i,I}T^I)_i]$$

we are done: every power series of the form $\sum_{I,\deg(I)\geq n} a_{i,I}T^I$ is in $\mathfrak{m}^n$, so the element of R^* on the right hand side is inside $\mathfrak{m}^n R^*$. Showing this equality amounts to proving

$$\{i \in \mathbf{N} : \sum_I a_{i,I}T^I = \sum_{I,\deg(I)\geq n} a_{i,I}T^I\} \in \mathcal{U},$$

i.e.

$$\{i \in \mathbf{N} : a_{i,I} = 0 \text{ for all } I \text{ with } \deg(I) < n\} \in \mathcal{U},$$

Since there are only finitely many multi-indices I with $\deg(I) < n$, we can write the set on the left hand side as a finite intersection:

$$\{i \in \mathbf{N} : a_{i,I} = 0 \text{ for all } I \text{ with } \deg(I) < n\} = \bigcap_{I,\deg(I)<n} \{i \in \mathbf{N} : a_{i,I} = 0\}.$$

By (7.1), every set in the intersection is in the ultrafilter $\mathcal{U}$, and as ultrafilters are closed under finite intersections, we see that we have shown our desired equality in R^*. So $\ker f \subseteq \mathfrak{m}^n R^*$, and as this holds for all $n \in \mathbf{N}$ we have $\ker f \subseteq \mathfrak{m}^\infty$.

Now assume $[(\sum_I a_{i,I}T^I)_i] \in \mathfrak{m}^\infty$. We want to show this element is in the kernel of f, i.e. we want to show that for every multi-index I we have $[(a_{i,I})_i] = 0$. Take n such that $\deg(I) < n$. By assumption $[(\sum_I a_{i,I}T^I)_i] \in \mathfrak{m}^n R^*$. As $[(\sum_{I,\deg(I)\geq n} a_{i,I}T^I)_i] \in \mathfrak{m}^n R^*$ as well, we see that $[(\sum_{I,\deg(I)<n} a_{i,I}T^I)_i] \in \mathfrak{m}^n R^*$. Since every element of $\mathfrak{m}^n$ is of the form $\sum_{I,\deg(I)\geq n} b_I T^I$, every element of $\mathfrak{m}^n R^*$ is a class with a representative of the form $(\sum_{I,\deg(I)\geq n} b_{i,I}T^I)_i$. So we should have $[(\sum_{I,\deg(I)<n} a_{i,I}T^I)_i] = [(\sum_{I,\deg(I)\geq n} b_{i,I}T^I)_i]$ for some coefficients $(b_{i,I})$, and that can only happen if $[(a_{i,I})_i] = 0$ for every I with $\deg(I) < n$. This proves our claim that $\ker f = \mathfrak{m}^\infty$.

The observations above show that f induces the isomorphism we were looking for. □

LEMMA 7.2.2. *The ultrapower of an henselian discrete valuation ring is henselian.*

Proof. This is shown on page 192 in [3]. □

THEOREM 7.2.3. *Let R be an excellent henselian local ring. Then every finite system of polynomial equations over R has a solution in R iff it has a solution in its completion $\hat{R}$.*

Proof. This is Theorem 1.3 in [26]. □

THEOREM 7.2.4. *The power series ring in a finite number of variables over a field has the approximation property.*

Proof. We consider the power series ring $R = \kappa[[T_1, \ldots, T_r]]$ over the field κ with maximal ideal $\mathfrak{m} = (T_1, \ldots, T_r)$. Let $\bar{u} = (u_1, \ldots, u_k)$ be a fixed k-tuple from R, and let d and m be fixed integers. Now we show the approximation property holds by contradiction.

Assume that for every $N \in \mathbf{N}$ we can find a family of t_N polynomials

$$f_N^{(1)}, \ldots, f_N^{(t_N)} \in \mathbf{Z}[U_1, \ldots, U_k, V_1, \ldots, V_m]$$

such that there is a m-tuple $v_{\bar{N}}$ in R such that for all i:

$$f_N^{(i)}(\bar{u}, v_{\bar{N}}) \equiv 0 \mod \mathfrak{m}^N \tag{7.2}$$

and there is no tuple $\bar{v}'$ in R such that

$$f_N^{(i)}(\bar{u}, \bar{v}') = 0 \tag{7.3}$$

for all values of i simultaneously.

As we will only substitute elements of R in the polynomials $f_N^{(i)}$, we can take our coefficients in $\mathbf{Z}/p\mathbf{Z}$ where p is the characteristic of R and κ. In turn, $\mathbf{Z}/p\mathbf{Z}$ can be embedded in κ so we can assume our polynomials to be in $\kappa[U_1, \ldots, U_k, V_1, \ldots, V_m]$, which is useful when we want to apply Lemma 7.2.1.

If a number of equations of the form $f_j(X_1, \ldots, X_s) = 0$ is satisfied simultaneously by some s-tuple, then every linear combination of those polynomials also assumes 0 for that tuple. So we can assume that our polynomials are linearly independent. The space of polynomials of degree $\leq d$ in $k + m$ variables over the field κ is finite-dimensional, as it is generated by the monomials of degree $\leq d$, so we can assume the sequence $(t_N)_N$ of the number of polynomials we needed for the counterexample modulo $\mathfrak{m}^N$ is bounded above by some N. We will therefore write assume we have the same number of polynomials for every N.

Here we will employ the theory of ultrapowers: let R^* be the ultrapower of R, and κ^* the ultrapower of κ. Let $\bar{v}$ be the m-tuple in R^* determined by the sequence $(v_N)_N$. We let $\bar{u}$ be the k-tuple corresponding to the constant sequence

$(\bar{u})_i$. For $1 \leq i \leq t$, we let $f^{(i)}$ be the element of $\kappa^*[[U_1, \ldots, U_k, V_1, \ldots, V_m]]$ determined by the sequence $(f_N^i)_N$, via the map described in Lemma 7.2.1.

As every element in the sequence $(f_N^i)_N$ is a polynomial of degree $\leq d$, it follows that the resulting element $f^{(i)}$ must also be a polynomial of degree $\leq d$, so in fact $f^{(i)} \in \kappa^*[U_1, \ldots, U_k, V_1, \ldots, V_m]$.

If we substitute elements of R in a polynomial over its residue field, we obtain an element of R. So we have

$$f^{(i)}(\bar{u}, \bar{v}) = (f_N^{(i)}(\bar{u}, \bar{v}_N)_N \in R^*.$$

In fact, by (7.2), $f_N^{(i)}(\bar{u}, \bar{v}_N) \in \mathfrak{m}^N$, so all terms of this sequence except a finite number belong to $\mathfrak{m}^N$ for every $N \in \mathbf{N}$. Since $\mathcal{U}$ is non-principal it contains all cofinite sets, so it follows that $f^{(i)}(\bar{u}, \bar{v}) \in \mathfrak{m}^n R^*$ for all n, i.e.

$$f^{(i)}(\bar{u}, \bar{v}) \in \mathfrak{m}^\infty.$$

From Lemma 7.2.1 it now follows that the image of $f^{(i)}(\bar{u}, \bar{v})$ in $\kappa^*[[T_1, \ldots, T_r]]$ is 0. We will show this implies that $f^{(i)}(\bar{u}, \bar{v}') = 0$ in R^* as well, for some m-tuple $\bar{v}'$.

Let A be the localization of $\kappa^*[T_1, \ldots, T_r, \bar{u}]$ at its maximal ideal

$$\mathfrak{m}\kappa^*[[T_1, \ldots, T_r]] \cap \kappa^*[T_1, \ldots, T_r, \bar{u}].$$

As A is finitely generated over the field κ^*, by Proposition 5.6.4 A is excellent.

Note that the completion of A is $\kappa^*[[T_1, \ldots, T_r]]$, as it is the completion of its subring $\kappa^*[T_1, \ldots, T_r]$. We consider the henselization $\tilde{A}$ of A, which is contained in this completion. Note that the henselization of an excellent ring is excellent as well by Proposition 5.6.5.

The finite system of equations $f^{(i)}(\bar{u}, V_1, \ldots, V_m) = 0$ (with $1 \leq i \leq t$) over $A[V_1, \ldots, V_m]$ has a solution in $\kappa^*[[T_1, \ldots, T_r]]$, namely $(V_1, \ldots, V_m) = \bar{v}'$. Using the excellence of $\tilde{A}$, we now apply Theorem 7.2.3 to this ring and its completion, and we see that there must exist a m-tuple $\bar{w}$ in $\tilde{A}$ that solves the system as well.

Note R^* is a henselian ring by Lemma 7.2.2. It follows from Lemma 7.2.1 that $\kappa^*[T_1, \ldots, T_r]$ is contained in R^*. By noting that $\bar{u}$ is a tuple from R^*, it follows that there is a map $A \to R^*$. This means we can apply the universal property of the henselization (Theorem 4.3.9): this gives us a unique A-algebra map $\tilde{A} \to R^*$. Let $\bar{w}'$ be the image of $\bar{w}$ in R^* under this map.

As our system of equation is defined over A, we see that $f^{(i)}(\bar{u}, \bar{w}) = 0$ in $\tilde{A}$ implies $f^{(i)}(\bar{u}, \bar{w}') = 0$ in R^*, as we desired. We will now show this is impossible.

Let $\bar{w}' = [(w'_N)_N]$ in R^*. Then

$$\{N \in \mathbf{N} : f_N^{(i)}(\bar{u}, w'_N) = 0\} \in \mathcal{U}$$

by Theorem 3.6.10. However, as $f_N^{(i)}(\bar{u}, V_1, \ldots, V_m) = 0$ has no solutions for every $N \in \mathbf{N}$, we see that this set is the empty set. But $\mathcal{U}$ cannot contain the empty set, and we have reached a contradiction. □

7.3 Proving the approximation property in the general case

LEMMA 7.3.1. *Let R be a excellent henselian local ring. If the completion of R has the approximation property, then so does R.*

Proof. Suppose that the approximation property holds for the completion $\hat{R}$ of R. Let $\bar{u}$ be a k-tuple from R, and let $N_{\bar{u}}$ be the function whose existence is implied by the definition of the approximation property of $\hat{R}$. We will show that this function is an approximation function for R as well.

Fix positive integers d and m, and let $N = N_{\bar{u}}(d, m)$. Let $(f_i(X_1, \ldots, X_k, Y_1, \ldots, Y_m))_i$ be a finite family of polynomials of degree $\leq d$ and $\bar{v}$ be a m-tuple from R such that for all i:

$$f_i(\bar{u}, \bar{v}) \equiv 0 \mod \mathfrak{m}^N$$

where $\mathfrak{m}$ is the maximal ideal of R. We need to show that there is a m-tuple $\bar{v}'$ in R such that $f_i(\bar{u}, \bar{v}') = 0$ for all i.

As R is excellent, it is Noetherian and by Corollary 5.3.5 it embeds in $\hat{R}$. So $\mathfrak{m}$ embeds in the maximal ideal $\hat{\mathfrak{m}}$ of $\hat{R}$, and

$$f_i(\bar{u}, \bar{v}) \equiv 0 \mod \hat{\mathfrak{m}}^N$$

for all i. By the approximation property of $\hat{R}$, there is a m-tuple $\bar{v}''$ in $\hat{R}$ such that $f_i(\bar{u}, \bar{v}'') = 0$ holds for all i in $\hat{R}$.

By Theorem 7.2.3 (here we use the henselianity of R), this means that there is a solution $\bar{v}' \in R^m$ already such that $f_i(\bar{u}, \bar{v}') = 0$ for all i. □

LEMMA 7.3.2. *Let R be a noetherian local ring with the approximation property, and A an ideal of R. Then R/A has the approximation property.*

Proof. Assume R has the approximation property, so that for every k-tuple $\bar{u}$ from R we have an approximation function $N_{\bar{u}}$. Since R is noetherian, we know that A is finitely generated, say by $a_1, \ldots, a_\ell$. Let $\bar{u}'$ be a k-tuple in R/A and $\bar{u}$ an tuple in R such that the image of $\bar{u}$ in R/A is $\bar{u}'$.

Suppose we have a family of polynomials $\{f_i(X_1, \ldots, X_k, Y_1, \ldots, Y_m) : 1 \leq i \leq t\}$ of degree $\leq d$ over $\mathbf{Z}$. We want to show that there exists a constant M such that the existence of a m-tuple $\bar{v}$ in R/A such that

$$f_i(\bar{u}', \bar{v}) \equiv 0 \mod \mathfrak{m}^M(R/A) \tag{7.4}$$

implies that there is a solution to $f(\bar{u}', Y_1, \ldots, Y_m) = 0$ in R/A.

We claim that $M = N_{\bar{u}}(\max(2, d), m + \ell t)$. Indeed, (7.4) implies that there exist a family of constants $\{b_{ij} : 1 \leq i \leq t, 1 \leq j \leq \ell\}$ such that in R we have

$$f_i(\bar{u}, \bar{v}) \equiv \sum_{j=1}^{\ell} b_{ij} a_j \mod \mathfrak{m}^M \tag{7.5}$$

for all $1 \leq i \leq t$.

Now we use the approximation property of R on the following family of polynomials indexed by $1 \leq i \leq t$:

$$F_i(X_1, \ldots, X_k, Y_1, \ldots, Y_m, A_1, \ldots, A_\ell, B_{11}, \ldots, B_{t\ell}) = f_i(X_1, \ldots, Y_m) - \sum_{j=1}^{\ell} B_{ij} A_j.$$

As f_i has degree $\leq d$ and the terms of the sum have degree 2, we see that F_i has degree $\leq \max(2, d)$.

By (7.5), the family $\{F_i : 1 \leq i \leq t\}$ has a solution modulo $\mathfrak{m}^M$. As

$$M = N_{\bar{u}}(d + 1, m + \ell t),$$

we see by the approximation property that the equation

$$f_i(\bar{u}, Y_1, \ldots, Y_m) - \sum_{j=1}^{\ell} B_{ij} a_j = 0$$

has a solution in R. As every solution $(\bar{v}, (b_{ij})_{ij})$ of this equation satisfies $f_i(\bar{u}, \bar{v}) = 0$ in R/A, we see that $f(\bar{u}', Y_1, \ldots, Y_m) = 0$ has a solution there, so R/A has the approximation property. □

THEOREM 7.3.3. *Every excellent equicharacteristic henselian local ring has the approximation property.*

Proof. Let R be an excellent equicharacteristic henselian local ring. Consider its completion $\hat{R}$, which is a local ring by Theorem 5.3.8. Since R is excellent, it is noetherian and so is its completion by Theorem **??**, hence by Proposition 5.4.2, $\hat{R}$ is a quotient of a complete regular local ring S.

As R is equicharacteristic, so is $\hat{R}$ by Corollary 5.3.10. We applied Proposition 5.4.2 to obtain S which can be chosen to be of the same characteristic as $\hat{R}$. As a local ring has the same residue field as a quotient of it, we see that S is equicharacteristic. This means that we can apply Theorem 5.4.1: it follows that S is a power series ring over the residue field of R in a finite number of variables.

By Theorem 7.2.4, S has the approximation property. We apply Lemma 7.3.2 to see that its quotient $\hat{R}$ has the approximation property, and by Lemma 7.3.1 R itself has the approximation property, as R is henselian. □

Part III

Solving the problem

Chapter 8

The geometric approach

8.1 Non-singular rational points are locally dense

In this section we show that a scheme satisfying with a R-rational point that is non-singular actually has a lot of R-rational points. For this proof we use a lot of machinery from algebraic geometry: for clarity, some steps have been placed in a lemma.

Definition 8.1.1. Let R be a integral domain, $K = \mathrm{Frac}(R)$, and X a scheme over $\operatorname{Spec} R$. We say that a R-rational point x is *non-singular* if the underlying point x_K is a non-singular point of the generic fiber X_K.

Lemma 8.1.2. *Let R be a local ring with fraction field K, and let A be a R-algebra. Suppose we have a R-algebra homomorphism $\phi : A \to R$, with kernel P. Let $A_K = A \otimes_R K$, and $P' = P \cdot A_K$. Suppose $(A_K)_{P'}$ is a regular local ring of Krull dimension h. Any choice of a regular system of parameters for this ring induces a scheme morphism from X_K to the affine h-space over K is étale at x_K.*

Proof. By Definition 5.2.6, there are $t_1/s_1, \ldots, t_h/s_h \in (A_K)'_P$ that generate P' in $(A_K)_{P'}$, where h is the dimension of this ring. In fact, the elements $t_1/1, \ldots, t_h/1$ also generate P' in $(A_K)_{P'}$: since these elements are divisors of the original generators, their span is at least P' and since all t_i are in P' any linear combination also has to be in P'.

Now consider the following map of K-algebras:

$$\psi : K[X_1, \ldots, X_h] \to A_K : X_i \mapsto t_i.$$

We write $\mathfrak{n}$ for the maximal ideal $(X_1, \ldots, X_h)$ in $K[X_1, \ldots, X_h]$, so that $\psi(\mathfrak{n}) = P'$. Now ψ induces the following map on the localizations:

$$\bar{\psi} : K[X_1, \ldots, X_h]_{\mathfrak{n}} \to (A_K)_{P'}.$$

We will now show that this map $\bar{\psi}$ has certain properties. First of all $(A_K)_{P'}$ is a big Cohen-Macaulay module over $K[X_1, \ldots, X_h]$, as the sequence $(t_1, \ldots, t_h)$ is the image of a system of parameters in $K[X_1, \ldots, X_h]$ that is regular in $(A_K)_{P'}$ by Proposition 5.5.3. In fact, as $K[X_1, \ldots, X_h]$ is a big balanced Cohen-Macaulay module over itself, it follows that $(A_K)'_P$ is a big balanced Cohen-Macaulay module over $K[X_1, \ldots, X_h]$. By Theorem 5.5.5 it follows that the map $\bar{\psi}$ is flat.

We see that $\bar{\psi}$ is unramified at P' by Proposition 6.4.8: the inverse image of the maximal ideal $P'(A_K)_{P'}$ is the maximal ideal $\mathfrak{n}$ in $K[X_1, \ldots, X_h]_{\mathfrak{n}}$, and as the residue field of both the domain and codomain of $\bar{\psi}$ is K we see that trivially the residue field of the codomain is a finite separable extension of the residue field of the domain.

It follows from Definition 6.4.9 that $\bar{\psi}$ is an étale morphism at P'. Consequently, ψ is étale at P', and so the corresponding morphism of schemes $X_K \to \mathbf{A}^h_K$ is étale at the point x_K. □

LEMMA 8.1.3. *A morphism $f : Y \to X$ of locally Noetherian schemes is étale if and only if for every $y \in Y$ there are affine open neighbourhoods $V = \operatorname{Spec} C$ of y and $U = \operatorname{Spec} A$ of $f(y)$ such that for some n polynomials $f_1, \ldots, f_n$ in n variables $T_1, \ldots, T_n$ it holds that*

$$C \cong A[T_1, \ldots, T_n]/(f_1, \ldots, f_n),$$

such that the Jacobian $\det(\partial f_i/\partial T_j)$ is a unit in C.

Proof. This is Corollary 3.16 in [24]. □

THEOREM 8.1.4. *Let R be a Henselian local integral domain with maximal ideal $\mathfrak{m}$ and fraction field K, and X a scheme of finite type over $\operatorname{Spec} R$. If there is a non-singular R-rational point x on X, there exists an open subset $X' \subseteq X$ over R that admits x as a R-rational point such that any open subset of X' over R admits an R-rational point.*

Proof. Since R is local, we can pick an affine open subset X_0 of X containing the image under x of $\mathfrak{m} \in \operatorname{Spec} R$. On this affine subset x is a R-rational point as well, since $x^{-1}(X_0)$ is an open subset of $\operatorname{Spec} R$ containing the closed point $\mathfrak{m}$, i.e. the whole of $\operatorname{Spec} R$. So we assume $X = \operatorname{Spec} A$ for some ring A.

We will first show that we can assume A is a finitely generated R-algebra.

We let $\phi : A \to R$ be the R-algebra homomorphism corresponding to $x : \operatorname{Spec} R \to \operatorname{Spec} A$, and let $P = \ker(\phi)$ which is a prime ideal. By the discussion

above, the generic fiber X_K of X is now $\operatorname{Spec} A_K$ where we write $A_K = A \otimes_R K$. The image of P under the map $A \to A \otimes_R K$ is denoted $P' = P \cdot A_K$ and this maximal ideal corresponds to the underlying point x_K of x.

We assumed x is a non-singular R-rational point, so x_K is a non-singular point of X_K. This means the local ring of x_K, $(A_K)'_P$, is regular. If we assume its Krull dimension is h, we are in the situation of Lemma 8.1.2, which allows us to conclude that the induced scheme morphism $f : X_K \to \mathbf{A}^h_K$ is étale at x_K. Note that this morphism depends which regular system of parameters we pick in $(A_K)_{P'}$. We can assume x_K is sent to the origin of $\mathbf{A}^h_K$, if we postcompose f with a translation, as a translation on affine space is always étale and the composition of étale maps is étale.

Affine schemes are locally noetherian, so we can now apply Lemma 8.1.3 to the morphism f. This gives us n polynomials $f_1, \ldots, f_n$ over K in $h + n$ variables $X_1, \ldots, X_h, T_1, \ldots, T_n$ such that

$$A_K \cong K[X_1, \ldots, X_h, T_1, \ldots, T_n]/(f_1, \ldots, f_n). \tag{8.1}$$

and the determinant of the matrix $(\partial f_i/\partial T_j)_{ij}$ is a unit at the point x_K. As K is the fraction field of R, by multiplying by suitable constants we can ensure all polynomials f_i are over R.

Let d_0 be the determinant of $(\partial f_i/\partial T_j)_{ij}$ evaluated at the origin. As it is a unit in K, it cannot be zero. Since we have chosen the polynomials f_i over R, we see that the determinant evaluated at a point must also be in R. So $d_0 \in R$.

We define the R-algebra

$$B = R[X_1, \ldots, X_h, T_1, \ldots, T_n]/(f_1, \ldots, f_n),$$

and we write $Y = \operatorname{Spec} B$. By (8.1), we see that

$$Y_K = \operatorname{Spec} B_K = K[X_1, \ldots, X_h, T_1, \ldots, T_n]/(f_1, \ldots, f_n) = \operatorname{Spec} A_K = X_K.$$

We can now find neighbourhoods U in X and V in Y such that x is an R-rational point on U and y an R-rational point on V such that $U \cong V$ as schemes over $\operatorname{Spec} R$, and x and y have the same underlying point. We see that it is enough to prove the statement for spectra of finitely generated R-algebras, which concludes the first part of the proof.

We will now show that the statement holds for the scheme Y. Using an argument that is a form of Néron desingularization (which is described as Claim 2.5 in [9]), we can assume that d_0 is in fact equal to 1.

Let W be an non-empty open subset of Y. As any non-empty open subset contains an non-empty open subset of the form $X \backslash V(f_0)$ for some $f_0 \in R[X_1, \ldots, X_h, T_1, \ldots T_n]$, it suffices to prove that any open subset of this form has an R-rational point.

As $V(f_0)$ is not-empty, f_0 is not in the ideal $(f_1, \ldots, f_n)$. The ideal $(f_1, \ldots, f_n)$ has height n, and so $(f_0, \ldots, f_n)$ has height $n+1$.

The polynomial $X_1 - a$ cannot be in $(f_0, \ldots, f_n)$ for all values $a \in \mathfrak{m}$. As we pick one value a_1 for which this holds, we see that $(f_0, \ldots, f_n, X_1 - a_1)$ has height $n+2$. Continuing in this fashion, we see that

$$(f_0, \ldots, f_n, X_1 - a_1, \ldots, X_{h-1} - a_{h-1})$$

has height $n+h$. This means that we can pick $a_h \in \mathfrak{m}$ such that this ideal together with the generator $X_h - a_h$ is the unit ideal in $K[X_1, \ldots, X_h, T_1, \ldots, T_n]$.

By plugging these values $(a_1, \ldots, a_h)$ into f_i we define

$$F_i(T_1, \ldots, T_n) = f_i(a_1, \ldots, a_h, T_1, \ldots, T_h)$$

for $0 \leq i \leq n$. We see $(F_0, \ldots, F_n)$ is the unit ideal in $K[T_1, \ldots, T_h]$.

Since all f_i have a root at the origin, there are no constant terms. So from the fact that all a_i are in the ideal $\mathfrak{m}$ it follows that

$$F_i(0, \ldots, 0) = f_i(a_1, \ldots, a_h, 0, \ldots, 0)$$

must be in $\mathfrak{m}$ too. We now use the henselianity of R: modulo $\mathfrak{m}$ the polynomials $F_1, \ldots, F_n$ have a root on $(0, \ldots, 0)$, but as the determinant of these polynomials is a unit (as $d_0 = 1$), we see that this root is simple.

So there must exists a root of these polynomials in R itself, say $(t_1, \ldots, t_n)$. As the ideal generated by $F_0, \ldots, F_n$ is the unit ideal, they cannot have a common root. So $F_0(t_1, \ldots, t_n)$ cannot be 0, and consequently $(a_1, \ldots, a_h, t_1, \ldots, t_n)$ must be an R-rational point on $X \backslash V(f_0)$. This concludes the proof. □

8.2 Resolution of singularities

We start with the classical example of a blow-up.

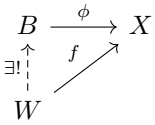
EXAMPLE 8.2.1. Let us work in a field. The affine curve C defined by $x^2 = y^2 + y^3$ has a singular point, namely $(0, 0)$. We consider the following subset C' of $\mathbf{A}^2 \times \mathbf{P}^1$: the set of $((x, y), (z, w))$ such that $x^2 = y^2 + y^3$ and $xw = zy$. Now the map $C' \to C$ that projects to the first factor has the property that the inverse image of any point except $(0, 0)$ is a point, and the inverse image of $(0, 0)$ is a copy of $\mathbf{P}^1$. We can show that C' has no singular points.

This example has some characteristics that are of interest: given a variety with a singular point (i.e. a point where the local ring is not regular), we look at another variety with less singular points and a map from the latter to the former that is an isomorphism 'almost everywhere'.

We can define this more generally in the language of schemes.

DEFINITION 8.2.2. Let X be a scheme, and Y a closed subscheme of an open subscheme of X. We call Y a *Cartier subscheme* in X if for all $P \in X$ there is an affine neighbourhood $U = \operatorname{Spec} A$ of P such that $Y \cap U = V(f) \subseteq U$ for some $f \in A$ such that f is not a zerodivisor.

DEFINITION 8.2.3. Let X be a scheme, and let Y a closed subscheme of an open subscheme X. The *blow-up of X along Y* is the morphism $\phi : B \to X$ with the following properties: $\phi^{-1}(Y)$ is a Cartier subscheme of B, and every morphism $f : W \to X$ such that $f^{-1}(Y)$ is a Cartier subscheme in W factors uniquely through ϕ in the following way:



In this situation, we call $\phi^{-1}(Y)$ the *exceptional divisor* of the blow-up and Y the *centre* of the blow-up. In Section IV.2 of [12] it is shown that the blow-up always exists, and as we defined it by its universal property it is unique up to isomorphism.

As we have seen above, blow-ups can be used to make singularities in schemes disappear. It is widely believed that we can find a blow-up for any reduced scheme such that its blow-up is non-singular. The following statement is known as Resolution of Singularities:

CONJECTURE 8.2.4. *Let X be a reduced scheme of finite type over a field K. Then there exists a morphism $f : \tilde{X} \to X$ of schemes of finite type over K such that $\tilde{X}$ is non-singular and f is a blow-up with a nowhere dense centre defined over K.*

Note that a set is nowhere dense if there is no non-empty open set contained it it.

We follow [16] for a brief overview of the partial results in this matter and the progress in proving the statement in its entirety.

The strategy is to tackle the problem by blowing up subschemes that consist solely of singular points. The goal is to end up with schemes with less singularities. However, this is not always possible, so one has to come up with more sophisticated ways to measure the complexity of a singular point. If we restrict ourselves to hypersurfaces for a second, an example of this is given by the order of vanishing of the defining polynomial in a point of the hypersurface.

In the characteristic 0 case it turns out that singularities are better behaved under blow-ups. As a consequence, a proof of the conjecture is already available: it was given by Hironaka in 1964.

Returning to the case of positive characteristic, we note that in lower dimensions results have been achieved as well. As all singular points on a curve are isolated, we can blow up singular points in any order, and after a finite number of steps we end up with a non-singular variety.

For surfaces the situation is more complicated: here singular points are either isolated points or lie on a curve. However, if such a curve is itself singular, it cannot be taken as the centre of a blow-up, as the behaviour is unpredictable in that case.

In dimension 3 no definitive result has been reached. However, work has been done by Abhyankar, which was later improved by Cutkosky, Cossart and Piltant.

8.3 Decidability and rational points

THEOREM 8.3.1. *Let R be an equicharacteristic excellent henselian local integral domain. Let $\bar{u} = (u_1, \ldots, u_k)$ be a tuple in R. Then the positive $L(\bar{u})$-existential theory of R is decidable if we can decide the existential theory of the residue field of R and the $L(\bar{u})$-diagram of R.*

Proof. We first show we can decide the truth of a sentence of the following form:

$$\exists v_1 \cdots \exists v_m \, f_1(\bar{u}, v_1, \ldots, v_m) = \cdots = f_t(\bar{u}, v_1, \ldots, v_m) = 0, \tag{8.2}$$

where $\bar{u}$ is a tuple from R and every f_i is a polynomial with coefficients in $\mathbf{Z}$.

By Theorem 7.3.3, we know that there exists a solution in R to (8.2) if there exists a solution modulo $\mathfrak{m}^N$, where N depends on the maximal degree of the polynomials f_i, and m and $\bar{u}$.

As $R/\mathfrak{m}^N$ is a vector space over the residue field of finite dimension (why?), determining whether there exists a solution to an equation can always be done in a finite number of steps. □

THEOREM 8.3.2. *Let R be an equicharacteristic excellent henselian local integral domain with residue field κ. Let X and Y be schemes of finite type over R, and $f : Y \to X$ be a morphism of finite type. We can obtain a morphism $\bar{f} : \bar{Y} \to \bar{X}$ of finite type between schemes of finite type over κ such that for every R-rational point x over X we can find a κ-rational point $\bar{x}$ over $\bar{X}$ such that x admits a R-rational lifting to Y iff the fibre $\bar{Y}_{\bar{x}}$ admits a κ-rational point.*

Proof. This is the second part of Theorem 3.5 in [9]. □

PROPOSITION 8.3.3. *Let R be a integral domain with $K = \mathrm{Frac}(R)$. Let X be a scheme of finite type over* $\operatorname{Spec} R$. *Then there is a closed subscheme Y of X such that Y_K is the reduced closed subscheme of X_K and every R-rational point on X lies already on Y, and there exists an algorithm that computes Y.*

Proof. This is Theorem 4.2 in [9]. □

THEOREM 8.3.4. *If Conjecture 8.2.4 is true, then the existential theory of every excellent equicharacteristic Henselian discrete valuation ring is decidable if we can decide the existential theory of its residue field and its L-diagram.*

Proof. This is Theorem 4.3 in [9]. □

COROLLARY 8.3.5. *If Conjecture 8.2.4 is true, then the existential theory of* $\mathbf{F}_p[[t]]$ *is decidable if we can decide its L-diagram.*

Proof. We apply Theorem 8.3.4 to the ring $\mathbf{F}_q[[t]]$, and note that the residue field of $\mathbf{F}_q[[t]]$ is finite, which means that we can decide the truth of all statements in it by substituting all elements of the field $\mathbf{F}_q$ in the variables. □

Chapter 9

The model-theoretic approach

9.1 Tame valued fields

In this section, we give a very brief overview of the results in [18], regarding a special type of valued fields. In this thesis we only consider valued fields with a positive residue field characteristic, so like in [1] we define tame valued fields just in this case. For the more general definition the reader is referred to [18].

Definition 9.1.1. We call a valued field (K, v) with $\operatorname{char} Kv = p$ *tame* if

- Kv is perfect;
- (K, v) is henselian;
- vK is p-divisible;
- (K, v) is defectless.

In the next section, we will see some examples of tame valued fields.

Theorem 9.1.2. *Let (K, v) be a valued field. Then there exists an extension (K^t, v^t) such that*

- *(K^t, v^t) is tame;*
- *K^t is a perfect field;*
- *$v^t K^t = \frac{1}{p^\infty} vK$;*

- *K^tv^t is the perfect hull of Kv.*

Proof. The existence of such an extension is shown in [19]. Throughout this article, the assumption is made that (K, v) is henselian. However, this assumption is not material: if we have shown the statement for henselian fields, it follows for every valued field.

We can see this in the following way: look at the henselization (K^h, v^h) of every valued field (K, v). By assumption we can find an extension $(K', v') \supseteq (K^h, v^h)$ such that (K', v') is tame and K' perfect. By Theorem 4.3.10, $v^hK^h = vK$ and $K^hv^h = Kv$, so $v'K' = \frac{1}{p^\infty}v^hK^h = \frac{1}{p^\infty}vK$ and similarly $K'v'$ is the perfect hull of K^hv^h which is equal to Kv. So (K', v') is the desired extension of (K, v).

We now show the statement for henselian fields (K, v). Theorem 2.1 in [19] implies the existence of a subfield (L, v) of the algebraic closure of K that is an algebraic K-complement of the ramification field of K, a concept that we will not define here. By Lemma 2.3 in the same article, this field L is perfect, and by Theorem 4.5(i) there, we have $vL = \frac{1}{p^\infty}vK$ and that Lv is the perfect hull of Kv.

It remains to be shown that (L, v) is a tame valued field. For this we introduce – for the duration of this proof – the concept of a purely wild extension of (K, v): this is a finite extension $(L, v) \supseteq (K, v)$ such that $[vL : vK]$ is a p-power and the field extension $Lv \supseteq Kv$ is purely inseparable.

By Theorem 4.3 in [19], (L, v) is a maximal algebraic purely wild extension of (K, v). This means that every proper algebraic extension of (L, v) is not purely wild. By Theorem 3.2 in [18], this is equivalent to (L, v) being tame. This concludes the proof. □

THEOREM 9.1.3. *Let (F, u) be a valued field with tame extensions (K, v) and (L, w), and suppose the following conditions hold:*

- *(F, u) is defectless;*
- *(L, w) is $|K|^+$-saturated;*
- *vK/uF is torsion-free;*
- *there exists an embedding $vK \to wL$ over uF;*
- *$Kv \supseteq Fu$ is separable;*
- *there exists an embedding $Kv \to Lw$ over Fu.*

Then there exists an embedding $\iota : (K, v) \to (L, w)$ that is the identity on (F, u) and respects the embeddings mentioned above.

Proof. This is Theorem 7.1 in [18]. □

THEOREM 9.1.4. *Let (K, v) and (L, w) be tame valued fields. Suppose $Kv \preccurlyeq Lw$ and $vK \preccurlyeq wL$. Then $(K, v) \preccurlyeq (L, w)$.*

Proof. This is Theorem 1.4 in [18]. □

THEOREM 9.1.5. *Let Γ be a p-divisible ordered abelian group. Then $(\mathbf{F}_q((\Gamma)), v_t)$ is a tame valued field.*

Proof. By Proposition 4.4.19, $(\mathbf{F}_q((\Gamma)), v_t)$ is henselian. Since its residue field is $\mathbf{F}_q$, its residue characteristic is p. The value group is equal to Γ which is p-divisible by assumption, and $(\mathbf{F}_q((\Gamma)), v_t)$ is defectless since it is maximal by Lemma 4.4.20. □

THEOREM 9.1.6. *Let $E \supseteq \mathbf{F}_q((t))$ be a finite extension of valued fields, and suppose the residue field of E is equal to $\mathbf{F}_q$. Then E is isomorphic to $(\mathbf{F}_q((s)), v_s)$.*

Proof. This follows from Proposition 2.3 and 2.5 in [29]. □

THEOREM 9.1.7. $(\mathbf{F}_q(t)^h, v_t) \preccurlyeq_\exists (\mathbf{F}_q((t)), v_t)$.

Proof. This is Theorem 5.12 in [18]. □

THEOREM 9.1.8. *$\mathbf{F}_q((t))^{\mathbf{Q}}$ is tame.*

Proof. We need to demonstrate the four properties from Definition 9.1.1 to show $\mathbf{F}_q((t))^{\mathbf{Q}}$ is tame. Three of those are straightforward. The residue field of $\mathbf{F}_q((t))^{\mathbf{Q}}$ is $\mathbf{F}_q$ (as the field is between $\mathbf{F}_q((t))$ and $\mathbf{F}_q((\mathbf{Q}))$), which is finite and hence perfect. By Proposition 4.4.19 we see that $\mathbf{F}_q((t))$ is an henselian field. Every algebraic extension of an henselian field is also henselian, so $\mathbf{F}_q((t))^{\mathbf{Q}}$ is henselian.

The value group of $\mathbf{F}_q((t))^{\mathbf{Q}}$ is enclosed between $\mathbf{Z}$ and $\mathbf{Q}$ (since $v_t\mathbf{F}_q((\Gamma)) = \Gamma$), and in fact it is $\mathbf{Q}$, since the element $t^{m/n} \in \mathbf{F}_q((\mathbf{Q}))$ (for $m \in \mathbf{Z}, n \in \mathbf{Z}_{>0}$) is in the algebraic closure of $\mathbf{F}_q((t))$: it is a root of the equation $x^n - t^m = 0$. The valuation map sends $t^{m/n}$ to m/n, which implies that all rationals are in the range of v_t on $\mathbf{F}_q((t))^{\mathbf{Q}}$. So $v_t\mathbf{F}_q((t))^{\mathbf{Q}} = \mathbf{Q}$, and since $\mathbf{Q}$ is divisible it is also p-divisble.

It remains to show that $\mathbf{F}_q((t))^{\mathbf{Q}}$ is defectless. We let $\mathbf{F}_q((t))^{\mathbf{Q}} \subseteq E$ be a finite extension, of degree n. Note that there are no non-trivial finite extensions of the value group by Proposition 2.4.4, so $v_tE = \mathbf{Q}$ and $[v_tE : \mathbf{F}_q((t))^{\mathbf{Q}}] = 1$ must hold. We now try to determine the residue field of E.

By Proposition 4.4.16, $\mathbf{F}_q((\mathbf{Q}))$ is a perfect field. We use this to show that $\mathbf{F}_q((t))^{\mathbf{Q}}$ is a perfect field too, i.e. (by Proposition 2.6.8) that the extension $\mathbf{F}_q((t))^{\mathbf{Q}} \subseteq E$ is separable.

We lift the extension to $\mathbf{F}_q((\mathbf{Q})) \subseteq E\mathbf{F}_q((\mathbf{Q}))$: this is an algebraic extension too. Since $\mathbf{F}_q(\mathbf{Q})$ is perfect, this extension is separable. By Corollary VIII.4.7 in [20], we see that $\mathbf{F}_q((t))^{\mathbf{Q}} \subseteq E$ is separable.

By the Primitive Element Theorem, there is an $\alpha \in \overline{\mathbf{F}_q((t))^{\mathbf{Q}}}$ such that $E = \mathbf{F}_q((t))^{\mathbf{Q}}(\alpha)$. By Proposition 2.6.15

$$[E\mathbf{F}_q((\mathbf{Q})) : \mathbf{F}_q((\mathbf{Q}))] = [E : \mathbf{F}_q((t))^{\mathbf{Q}}].$$

Since $\mathbf{F}_q((\mathbf{Q}))$ is a henselian valued field (by Proposition 4.4.19), there is a unique extension of v_t to $E\mathbf{F}_q((\mathbf{Q}))$. This extension of valued fields is defectless by Lemma 4.4.20. Since there are no non-trivial finite extensions of the value group by Proposition 2.4.4, we must have $v_t\mathbf{F}_q((\mathbf{Q})) = v_tE\mathbf{F}_q((\mathbf{Q})) = \mathbf{Q}$. It follows that $[E\mathbf{F}_q((\mathbf{Q}))v_t : \mathbf{F}_q((\mathbf{Q}))v_t] = n$, so $E\mathbf{F}_q((\mathbf{Q}))v_t = \mathbf{F}_{q^n}$.

By Theorem 4.4.10, we see that we can embed $\mathbf{F}_{q^n}$ in $E\mathbf{F}_q((\mathbf{Q}))$: we already have a partial section $\mathbf{F}_q \to \mathbf{F}_q((\mathbf{Q})) \subseteq E\mathbf{F}_q((\mathbf{Q}))$ (see Example 4.4.9), and since $\mathbf{F}_q \subseteq \mathbf{F}_{q^n}$ is separable (as $\mathbf{F}_q$ is perfect) and $E\mathbf{F}_q((\mathbf{Q}))$ is henselian (as it is an algebraic extension of an henselian field) this extends to a section $\mathbf{F}_{q^n} \to E\mathbf{F}_q((\mathbf{Q}))$.

E is algebraically closed in $E\mathbf{F}_q((\mathbf{Q}))$ by Proposition 2.6.15. Since $E \subseteq E\mathbf{F}_{q^n}$ is an algebraic subextension (it is a lift of $\mathbf{F}_q \subseteq \mathbf{F}_{q^n}$) of $E \subseteq E\mathbf{F}_q((\mathbf{Q}))$, it follows that $E = E\mathbf{F}_{q^n}$, so $\mathbf{F}_{q^n} \subseteq E$. We see that $\mathbf{F}_{q^n} \subseteq Ev_t$, as every valuation is trivial on finite fields. As the residue field of the larger field $E\mathbf{F}_q(\mathbf{Q}))$ is $\mathbf{F}_{q^n}$, we see that in fact equality must hold. We can now conclude:

$$[E : \mathbf{F}_q((t))^{\mathbf{Q}}] = n = n \cdot 1 = [\mathbf{F}_{q^n} : \mathbf{F}_q][\mathbf{Q} : \mathbf{Q}] = [Ev_t : \mathbf{F}_q((t))^{\mathbf{Q}}v_t][v_tE : v_t\mathbf{F}_q((t))^{\mathbf{Q}}].$$

Hence $\mathbf{F}_q((t))^{\mathbf{Q}}$ is defectless, so it is a tame field. □

9.2 Transfer between henselian fields with finite residue field with q^k elements

In this section, we write L_{vf} for the language of the valued fields. The language of rings (and fields) will be denoted by L_{ring}.

For a language L, we write $L(F)$ to denote the language that is the union of L and a family of constants c_f indexed by $f \in F$ that will always be interpreted as its index, as described on page 34.

Definition 9.2.1. By $\mathbf{T}$ we denote the following L_{vf}-theory which states the following about a L_{vf}-model (K, v):

- (K, v) is a non-trivial henselian valued field;

- $\operatorname{char} K = \operatorname{char} Kv = p$;
- $Kv \cong \mathbf{F}_q$ as fields.

EXAMPLE 9.2.2. A model of $\mathbf{T}$ is $\mathbf{F}_q((t))$ with the valuation v_t.

DEFINITION 9.2.3. By $\mathbf{H}$ we denote the collection of tuples (K, v, i) where (K, v) is a L_{vf}-model and i is a map $\mathbf{F}_q \to Kv$, satisfying

- (K, v) is a non-trivial henselian valued field;
- $\operatorname{char} K = \operatorname{char} Kv = p$;
- i is a field embedding.

EXAMPLE 9.2.4. A member of $\mathbf{H}$ is $(F((t)), v_t)$ for every (possibly infinite) field F of characteristic p with at least q elements, if we specify an embedding $\mathbf{F}_q \to Kv$.

THEOREM 9.2.5. *Let ϕ be an $\exists$-sentence in $L_{\mathrm{vf}}(\mathbf{F}_q)$, and let Γ be an ordered abelian group. If $(\mathbf{F}_q((\Gamma)), v_t, \mathbf{F}_q)$ models ϕ, then $(\mathbf{F}_q(t)^h, v_t, \mathbf{F}_q)$ models ϕ.*

Proof. We assume $(\mathbf{F}_q((\Gamma)), v_t, \mathbf{F}_q) \models \phi$.

Let Δ be the divisible hull of Γ. Note that we can embed $\mathbf{Q}$ and Γ in Δ by Corollary 2.4.6. This induces the following embeddings:

$$(\mathbf{F}_q((\Gamma)), v_t, \mathbf{F}_q) \subseteq (\mathbf{F}_q((\Delta)), v_t, \mathbf{F}_q)$$

and

$$(\mathbf{F}_q((\mathbf{Q})), v_t, \mathbf{F}_q) \subseteq (\mathbf{F}_q((\Delta)), v_t, \mathbf{F}_q).$$

The valued field $\mathbf{F}_q((t))^{\mathbf{Q}}$ is by definition a subfield of $\mathbf{F}_q((\mathbf{Q}))$, and it follows from the above that we have an embedding

$$(\mathbf{F}_q((t))^{\mathbf{Q}}, v_t, \mathbf{F}_q) \subseteq (\mathbf{F}_q((\Delta)), v_t, \mathbf{F}_q) \tag{9.1}$$

Since existential statements remain true in larger models, we see

$$(\mathbf{F}_q((\Delta)), v_t, \mathbf{F}_q) \models \phi.$$

We want to apply Theorem 9.1.4 to (9.1). The two valued fields are tame by Theorem 9.1.5 and 9.1.8. The residue fields of both valued fields are $\mathbf{F}_q$, and the value groups are $\mathbf{Q}$ and Δ. We have $\mathbf{Q} \subseteq \Delta$, so by Theorem 3.4.7 we have $\mathbf{Q} \preccurlyeq \Delta$. Since the conditions of the theorem are satisfied,

$$(\mathbf{F}_q((t))^{\mathbf{Q}}, v_t, \mathbf{F}_q) \preccurlyeq (\mathbf{F}_q((\Delta)), v_t, \mathbf{F}_q)$$

and hence $(\mathbf{F}_q((t))^{\mathbf{Q}}, v_t, \mathbf{F}_q) \models \phi$.

Let us write $\phi = \exists \bar{x} \psi(\bar{x})$ with ψ quantifier-free, and take a tuple $\bar{a} \in \mathbf{F}_q((t))^{\mathbf{Q}}$ such that $\psi(\bar{a})$ is true. Since $\mathbf{F}_q((t))^{\mathbf{Q}}$ is the algebraic closure of $\mathbf{F}_q((t))$, all elements in $\bar{a}$ are algebraic over $\mathbf{F}_q((t))$, so there is a finite extension E of $\mathbf{F}_q((t))$ that contains the elements of $\bar{a}$, which implies $(E, v_t, \mathbf{F}_q) \models \phi$.

Now we apply Theorem 9.1.6: E is a finite extension of $\mathbf{F}_q((t))$ with residue field $\mathbf{F}_q$ (since it is between two fields with residue field $\mathbf{F}_q$). So $(E, v_t, \mathbf{F}_q) \cong (\mathbf{F}_q((t)), v_t, \mathbf{F}_q)$, and hence $(\mathbf{F}_q((t)), v_t, \mathbf{F}_q) \models \phi$.

Finally, by Theorem 9.1.7 existential statements true in $\mathbf{F}_q((t))$ also are true in $\mathbf{F}_q(t)^h$, so $(\mathbf{F}_q(t)^h, v_t, \mathbf{F}_q) \models \phi$, which is what we wanted to prove. □

THEOREM 9.2.6. *Write R for the residue field of $(\mathbf{F}_q(t)^h, v_t)$. Let ϕ be an $\exists$-sentence in $L_{\mathrm{vf}}(\mathbf{F}_q)$. If $(\mathbf{F}_q(t)^h), v_t, \mathbf{F}_q)$ models ϕ, then all $(K, v, i) \in \mathbf{H}$ model ϕ, where we replace the residue field parameters by their image under i.*

Proof. We write $\phi = \exists \bar{x} \psi(\bar{x}; \bar{r})$, where $\bar{x}$ are variables and $\bar{r}$ are parameters in the residue field $R = \mathbf{F}_q(t)^h v_t$.

Assume $\mathbf{F}_q(t)^h$ models ϕ. Let $\bar{a}$ be a tuple of elements such that $\psi(\bar{a}; \bar{r})$ holds.

Let K_0 be the prime field of K. As $\operatorname{char} K = p$, there exists a isomorphism $j : K_0 \to \mathbf{F}_p$. As K_0 is finite, the restriction of the valuation v to it is trivial, hence $K_0 v \cong K_0$. With these isomorphisms, we can find a partial section $f : K_0 v \to K : xv \mapsto x$. Now the image of $\mathbf{F}_q$ under i is a field between $K_0 v$ and Kv. As $K_0 v$ is perfect (as it is finite), the finite field extension $K_0 v \subseteq i(\mathbf{F}_q)$ is separable by 2.6.8 and by Theorem 4.4.10 we can extend the partial section f to a partial section $g : i(\mathbf{F}_q) \to K$.

Now we precompose this map with i to obtain $h = g \circ i : \mathbf{F}_q \to K$ which is in fact an $L_{\mathrm{vf}}(\mathbf{F}_q)$-embedding, where $\mathbf{F}_q$ has the trivial valuation. On the image $h(\mathbf{F}_q) \subseteq K$ the valuation v is trivial, and since v is non-trival there must be an element $s \in K$ with $v(s) > 0$, which cannot be algebraic over $h(\mathbf{F}_q)$.

We extend the map h to the following embedding by sending t to the transcendental element s.

$$h' : (\mathbf{F}_q(t), v_t) \to (K, v).$$

By Theorem 4.4.6 and the fact that K is henselian there is a unique embedding extending h':

$$h'' : (\mathbf{F}_q(t)^h, v_t) \to (K, v)$$

Since $(\mathbf{F}_q(t)^h, v_t) \models \phi(\bar{a}; \bar{r})$, we see $(K, v) \models \phi(h''(\bar{a}), h''(\bar{r}))$, so

$$(K, v) \models \exists \bar{x} \phi(\bar{x})$$

which completes our proof. □

THEOREM 9.2.7. *Let $\psi(\bar{x})$ be an $\exists$-formula in $L_{\mathrm{vf}}(\mathbf{F}_q)$, where $\bar{x}$ is a sequence of variables of the residue field sort. Suppose there exists a model (K, v) that models $\mathbf{T} \cup \{\forall \bar{x} \psi(\bar{x})\}$. (Note that the universal quantors are of the residue field sort, i.e. $\forall \bar{x} \psi(\bar{x})$ is a $\forall^k \exists$-formula in the sense of Definition 4.5.4.) Then for all $(L, w, i) \in \mathbf{H}$, for every residue field tuple $\bar{a}$ from the image of i in L the formula $\psi(\bar{a})$ holds.*

Proof. Since $(K, v) \models \mathbf{T}$, we have that $\mathbf{F}_q \cong Kv$. We will write f for such an isomorphism.

As in the proof of Theorem 9.2.6 we have a partial section $K_0 v \to K : xv \to x$, where K_0 is the prime field of K (which is isomorphic to $\mathbf{F}_p$), which can be extended to a partial section $f(\mathbf{F}_q) \to K$ by using Theorem 4.4.10. If we precompose this with i we obtain a map $h : \mathbf{F}_q \to K$, which is an embedding of valued fields. Note that $h(\mathbf{F}_q)v = Kv$.

Consider the extension $(K, v) \subseteq (K^t, v^t)$ as described in Theorem 9.1.2. We write $\Gamma = v^t K^t = \frac{1}{p^\infty} vK$. We consider the valued field extension $(K, v) \subseteq (\mathbf{F}_q((\Gamma)), v_t)$ as well.

We want to apply Theorem 9.1.3. Note that (K^t, v^t) is tame by Theorem 9.1.2 and that $(\mathbf{F}_q((\Gamma)), v_t)$ is tame by Theorem 9.1.5. Their common subfield $\mathbf{F}_q$ is defectless as its finite extensions only admit the trival valuation. We employ Theorem 3.5.6 to obtain a $|K|^+$-saturated elementary extension of $(\mathbf{F}_q((\Gamma)), v_t)$, which we will denoted by $(\mathbf{F}_q((\Gamma)), v_t)^*$.

Note that the valuation group of (K^t, v^t) is equal to $\frac{1}{p^\infty} vK$ and the residue field to $\mathbf{F}_q$ (as it is a perfect field). The valuation group of $(\mathbf{F}_q, v_0)$ is the trival group and the residue field is $\mathbf{F}_q$. The extension $\mathbf{F}_q \subseteq \mathbf{F}_q$ is trivially separable, and the quotient group $\frac{1}{p^\infty} vK$ is torsion-free.

We obtain embeddings of the value group by noting that K^t and $\mathbf{F}_q((\Gamma))$ have the same value group and the same residue field and composing this with the induced maps to the saturated extension. We see that we satisfy the hypotheses of Theorem 9.1.3.

It follows that there is a $L_{\mathrm{vf}}(\mathbf{F}_q)$-embedding

$$(K^t, v^t) \to (\mathbf{F}_q((\Gamma)), v_t)^*. \tag{9.2}$$

Assume $(K, v) \models \forall \bar{x} \psi(\bar{x})$, i.e. every tuple $\bar{a}$ in Kv satisfies $\psi(\bar{a})$. We write

$$\Psi = \{\psi(\bar{a}) : \bar{a} \text{ is a tuple in } h(\mathbf{F}_q)v\},$$

and then $(K, v) \models \Psi$.

The collection Ψ of existential formulas holds in larger models as well, so

$$(K^t, v^t) \models \Psi.$$

Via the embedding in (9.2) it follows that

$$(\mathbf{F}_q((\Gamma)), v_t)^* \models \Psi,$$

and since this is an elementary extension of $\mathbf{F}_q((\Gamma)), v_t)$, we see that

$$(\mathbf{F}_q((\Gamma)), v_t) \models \Psi.$$

Theorem 9.2.5 gives us

$$(\mathbf{F}_q(t)^h, v_t) \models \Psi$$

and Theorem 9.2.6 allows us to conclude

$$(L, w) \models \Psi$$

and we see that for all residue field tuples $\bar{a}$ from the image of $\mathbf{F}_q$ under i in L the formula $\psi(\bar{a})$ holds. □

9.3 On the decidability of $\mathbf{F}_q((t))$

THEOREM 9.3.1. *Let ϕ be a $\forall^k\exists$-formula in L_{vf}. Then either $\mathbf{T} \models \phi$ or $\mathbf{T} \models \neg\phi$.*

Proof. We want to show that $\mathbf{T}$ is $\forall^k\exists$-complete. Suppose $\mathbf{T} \not\models \neg\phi$. Then there exists a model (K, v) of $\mathbf{T}$ that does not model $\neg\phi$, i.e. that models ϕ. We want to show $\mathbf{T} \models \phi$, so we take a model (L, w) of $\mathbf{T}$ and demonstrate that it models ϕ.

Let us write $\phi = \forall^k \bar{x}\psi(\bar{x})$, with ϕ a $\exists$-formula in L_{vf}. Since (K, v) models ϕ, it follows that for every tuple $\bar{a}$ in Kv the statement $\psi(\bar{a})$ holds.

Every model of $\mathbf{T}$ is also in $\mathbf{H}$ if we take the map i to be the isomorphism from $\mathbf{F}_q$ to the residue field. So by Theorem 9.2.7 we see that all tuples $\bar{b}$ in Lw the statement $\psi(\bar{b})$ holds, so $(L, w, E) \models \phi$ and we are done. □

THEOREM 9.3.2. *The existential theory of $\mathbf{F}_q((t))$ is decidable.*

Proof. The effectively axiomatisable subtheory $\mathbf{T}$ of $\mathrm{Th}(\mathbf{F}_q((t))$ is $\exists$-complete by Theorem 9.3.1. We will show that this implies the existential theory of $\mathbf{F}_q((t))$ is decidable, following Corollary 15.7 in [4].

Informally speaking we proceed as follows: the theory $\mathbf{T}$ is effectively axiomatizable, so we can build a Turing machine that starts with the axioms of $\mathbf{T}$ and derives all consequences of these axioms. Since for every existential sentence ϕ either $\mathbf{T} \models \phi$ or $\mathbf{T} \models \neg\phi$ by Theorem 9.3.1, we either encounter ϕ or $\neg\phi$ after a finite amount of time. Since $\mathbf{T} \models \mathbf{F}_q((t))$, we then know whether $\mathbf{F}_q((t)) \models \phi$ or $\mathbf{F}_q((t)) \models \neg\phi$, so existential statements are decidable in $\mathbf{F}_q((t))$. □

Bibliography

[1] S. Anscombe and A. Fehm, *The existential theory of equicharacteristic henselian valued fields*, Algebra & Number Theory, 10 (2016), pp. 665–683.

[2] M. F. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[3] J. Becker, J. Denef, L. Lipshitz, and L. van de Dries, *Ultraproducts and approximation in local rings I*, Inventiones Mathematicae, 51 (1979), pp. 189–203.

[4] G. S. Boolos, J. P. Burgess, and R. C. Jeffrey, *Computability and Logic*, Cambridge University Press, 5th ed., 2007.

[5] C. C. Chang and H. J. Keisler, *Model Theory*, vol. 73 of Studies in Logic and the Foundations of Mathematics, North-Holland, 3rd ed., 1990.

[6] R. Cluckers, *Motivic integration and transfer principles.* http://rcluckers.perso.math.cnrs.fr/prints/notes_ETH.pdf, 2015. Seminar notes; accessed online on July 16th, 2020.

[7] I. Cohen, *On the structure and ideal theory of complete local rings*, Transactions of the American Mathematical Society, 59 (1946), pp. 54–106.

[8] R. Datta and K. E. Smith, *Excellence in prime characteristic*, in Local and Global Methods in Algebraic Geometry, vol. 712 of Contemporary Mathematics, 2018, pp. 105–116.

[9] J. Denef and H. Schoutens, *On the decidability of the existential theory of* $\mathbf{F}_p[[t]]$, in Valuation theory and its applications, vol. II, F.-V. K. et al., ed., vol. 33 of Fields Institute Communication, American Mathematical Society, 2003, pp. 43–60.

[10] I. Efrat, *Valuations, Orderings and Milnor K-Theory*, vol. 124 of Mathematical Surveys and Monographs, American Mathematical Society, 2006.

[11] D. Eisenbud, *Commutative Algebra with a view towards Algebraic Geometry*, vol. 150 of Graduate Texts in Mathematics, Springer, 1st ed., 1995.

[12] D. Eisenbud and J. Harris, *The Geometry of Schemes*, vol. 197 of Graduate Texts in Mathematics, Springer, 2000.

[13] A. J. Engler and A. Prestel, *Valued Fields*, Monographs in Mathematics, Springer, 2005.

[14] E. Freitag and R. Kiehl, *Etale Cohomology and the Weil Conjecture*, vol. 13 of Series of Modern Surveys in Mathematics, Springer, 1988.

[15] R. Hartshorne, *Algebraic Geometry*, vol. 52 of Graduate Texts in Mathematics, Springer, 1977.

[16] H. Hauser, *On the problem of resolution of singularities in positive characteristic*, Bulletin of the American Mathematical Society, 47 (2010), pp. 1–30.

[17] T. Jech, *Set Theory*, Monographs in Mathematics, Springer, 3rd ed., 2002.

[18] F.-V. Kuhlmann, *The algebra and model theory of tame valued fields*, Journal für die reine und angewandte Mathematik, 719 (2016), pp. 1–43.

[19] F.-V. Kuhlmann, M. Pank, and P. Roquette, *Immediate and purely wild extensions of valued fields*, Manuscripta Mathematica, 55 (1986), pp. 39–67.

[20] S. Lang, *Algebra*, vol. 211 of Graduate Texts in Mathematics, Springer, revised 3rd ed., 2002.

[21] D. Marker, *Model Theory, an Introduction*, vol. 217 of Graduate Texts in Mathematics, Springer, 2002.

[22] H. Matsumura, *Commutative Algebra*, Mathematics Lecture Notes, Benjamin/Cummings, 2nd ed., 1980.

[23] ——, *Commutative Ring Theory*, Cambridge University Press, 1989.

[24] J. S. Milne, *Étale Cohomology*, vol. 33 of Princeton Mathematical Series, Princeton University Press, 1980.

[25] B. Poonen, *Maximally complete fields*, L'Enseignement Mathématique, 39 (1993), pp. 87–106.

[26] D. Popescu, *General Néron desingularization and approximation*, Nagoya Mathematical Journal, 104 (1986), pp. 85–115.

[27] A. Prestel and C. N. Delzell, *Mathematical Logic and Model Theory*, Universitext, Springer, 2011.

[28] H. Schoutens, *The Use of Ultraproducts in Commutative Algebra*, vol. 1999 of Lecture Notes in Mathematics, Springer, 2010.

[29] J.-P. Serre, *Local fields*, vol. 67 of Graduate Texts in Mathematics, Springer, 1979.

[30] The Stacks Project Authors, *Stacks Project*. https://stacks.math.columbia.edu, 2020.

Index