Math 58R – Selected Topics In Model Theory

o-minimality and Some Applications

Fall 2023

Ayhan Günaydın

December 26, 2023

Contents

Introduction 5

Chapter 1. Basics of Mathematical Logic 7
1. Syntax of First Order Logic 7
2. Semantics 10
3. Formal First Order Theories 15
4. Completeness Theorem 17

Chapter 2. Model Theory 19
1. Basics 19
2. Compactness Theorem 21
3. Another Proof of Compactness Theorem 23
4. Maps Between Structures 26
5. Categoricity 27
6. Definable Sets 30
7. More on ACF 32

Chapter 3. o-minimal Structures 37
1. Ordered Structures 37
2. Definition and Basics 38
3. o-minimal Groups, Rings, and Fields 40
4. Examples of o-minimal Structures 41

Chapter 4. Cell Decomposition 47
1. Cells 47
2. More on Cells 48
3. Cell Decomposition 49
4. Proof of Cell Decomposition 52
5. An Application of Uniform Finiteness Theorem 53

Chapter 5. Dimension Theory for Definable Sets 55
1. Definition and Basic Properties 55
2. Euler Characteristic 58

Chapter 6. Some Basic Algebraic Number Theory 61
1. Absolute Values on Fields 61
2. Absolute Values on Number Fields 65
3. Heights of Algebraic Numbers 68
4. Valuation Ring and Residue Field 70

Chapter 7. Some Basic Algebraic Geometry 73
1. Algebraic Varieties 73
2. Complex Tori and Abelian Varieties 73

Chapter 8. Pila-Wilkie Theorem and Its Applications 77
1. Counting Rational Points on Definable Sets 77
2. The Case of the Multiplicative Group – Theorem of Mann 79
3. The Case of Abelian Varieties – Manin-Mumford Conjecture 84
4. Galois orbits 85

Bibliography 87

Index 89

Introduction

Our ultimate aim in this course is to study some recent applications of *o-minimality* in number theory. These applications go through Pila-Wilkie Theorem ([**20**]) on the number of rational points of a set definable in an o-minimal expansion of the real field, or some variations of it.

Introduced in [**23**], building some ideas from [**7**], o-minimality is a topic in model theory. (Actually, it is more than a mere topic; it has become a sub-branch of the area right after its introduction.) Therefore we first need to establish some basic model theory and hence some mathematical logic. We tend to think that model theory is a way of thinking about algebra (and sometimes even analysis) in a different way than the usual. So we present more than strictly necessary to understand o-minimality. That way, we would like to initiate that way of thinking.

We start with the very basics of mathematical logic, but we proceed very fast. Since we have model theory in mind, we say very little about formal first-order theories and focus on the semantics. As a result we skip the proof of Completeness Theorem. However, we cover its applications in detail. Most applications of Completeness Theorem are actually applications of Compactness Theorem. Among applications are Löwenheim-Skolem Theorems and Łoś-Vaught Test. For mathematical logic, we mostly follow [**13**]. One may read the details of the proof of Completeness Theorem there. Another source is the recent book [**14**] by Hils and Loeser.

Even just to be able to define the concept of 'o-minimal structure', we need the very central concept of *definable set* from model theory. So we shall spend some time discussing that topic. Unfortunately, we cannot study the details of the methods of determining the structure of definable sets. That is really another course. So we state some old results without proofs.

Finally, on Chapter 3 we start our study of o-minimal structures. On a very intuitive level, one may think of these structures as the ones whose *definable functions do not oscillate that much.* After establishing the basics of o-minimality, we move on to the most predominant result about o-minimal structures, namely Cell Decomposition Theorem. This theorem will help us to understand all definable sets and

functions in a very geometric way and that will provide us with tools to do topology in o-minimal theories.

Once we know the essentials of o-minimal theories, we shall be ready to state Pila-Wilkie Theorem; the main theorem of [**20**]. Vaguely speaking, that theorem is about the number of rational points of a set definable in an o-minimal expansion of the real field. The phrase 'the number of rational points of a definable set' does not really make sense, as there are rarely finitely many such elements. For this to make sense, we need to count the rational points of height bounded by a fixed number. There are so many other technicalities on the way and we present all the details in Chapter 4. We also present the generalization of Pila-Wilkie Theorem by Pila to algebraic points of bounded degree rather than rational points; see [**21**]

In the final chapter, we consider arithmetic applications of Pila-Wilkie Theorem. Our main application is a proof of Manin-Mumford Conjecture. This proof is far from being the first proof. There are many different proofs, and the first one is in [**24**] by Raynaud; that proof is in a little bit more restricted setting than the version we present below. Here is the statement that we are going to prove.

THEOREM 0.1 (Manin-Mumford Conjecture-Version 1). *Let* $\mathbf{A}$ *be an abelian variety and let* $X \subseteq \mathbf{A}$ *be an algebraic subvariety. Then* $X \cap \mathrm{Tor}(\mathbf{A})$ *is a finite union of cosets of abelian subvarieties of* $\mathbf{A}$.

This is indeed formally equivalent to the following weaker looking statement.

THEOREM 0.2 (Manin-Mumford Conjecture-Version 2). *Let* $\mathbf{A}$ *be an abelian variety and let* $X \subseteq \mathbf{A}$ *be an algebraic subvariety which does not contain a coset of an abelian subvariety of* $\mathbf{A}$ *of positive dimension. Then* X *contains only finitely many torsion points of* $\mathbf{A}$.

The concept of *abelian variety* in both of these statements is not in a usual undergraduate curriculum. This will be introduced along with some other concepts to be used in the proof.

CHAPTER 1

Basics of Mathematical Logic

We do not directly need most of the results of mathematical logic[1] to be introduced in this chapter in order to work with o-minimal theories later, but it proves to be useful to know the mechanics of logic to have a deeper understanding of the subject. The main result will be Gödel's Completeness Theorem, which in my mind serves as a boundary between logic and model theory. To be more precise, one of its consequences, namely Compactness Theorem can be thought as the beginning of model theory. The reason is that once we have this theorem, we may leave the very formal (and very beautiful) world of logic and start to get some algebraic results. We are aiming to make these vague sentences more precise in the rest of this chapter. While doing so we hope to convey the idea of the proof of Compactness.

1. Syntax of First Order Logic

Vaguely speaking, first order logic has two basic concepts, namely *proof* and *truth*, and Completeness Theorem is the bridge connecting them. Here we give a fairly detailed account of 'truth', but a very limited account of 'proof'. We refer the reader to the lecture notes [**13**] for all kinds of details; in particular the details of 'proof'.

We start by introducing the syntax of first order logic. As a matter of fact, we should talk about first order *logics* since different settings will give different logics. This setting is determined by *languages*[2].

Definition 1.1. A *first order language* L consists of the following:

(1) *Connectives:* $\neg \quad \rightarrow \quad \wedge \quad \vee$
(2) *Parentheses:* $(\quad)$
(3) *Comma:* $,$
(4) *Quantifiers:* $\forall \quad \exists$
(5) *Variables:* $v_1 \quad v_2 \quad \cdots$
(6) *Equality:* $=$
(7) *Function Symbols:* $f_1^{(m_1)} \quad f_2^{(m_2)} \cdots$
(8) *Relation Symbols:* $R_1^{(n_1)} \quad R_2^{(n_2)} \cdots$

[1] After this point on, we simply refer to it as *logic*

[2] *Alphabet* would be a better word for this concept, but 'language' is the more commonly used word in model theory. In the context of logic, they really have different meanings, but it will not matter for us.

(9) *Constant Symbols:* $c_1 \quad c_2 \quad \cdots$

This definition is given in a little bit more minimal way in [**13**]; there we have not put the symbols $\wedge, \vee, \exists$ in the language and defined them in terms of others. It is just a matter of style and in the context of these notes it would be more confusing to do that, so we choose clarity over efficiency.

Note the little integers that appear as superscripts in the function and relation symbols. They are called the *arity* of the symbols; arity is a made-up word generalizing the words *binary*, *ternary*, etc. If a function or a relation symbol has arity n, then we say that it is *n-ary*. So function and relation symbols are more than symbols: they have an integer attached to them. So far they do not have any meaning, like any other symbol in the language.

The first six parts in this definition are the same for every first order language. So a language is determined by the function, relation, and constant symbols in it. We refer to them as *non-logical symbols*. Most of the times we simply list them when we present a particular language as done in the following examples.

EXAMPLE 1.2. Let $L_{\mathrm{o}} = \{<\}$ be the language of orderings. This means that there is only one non-logical symbol, which is a binary relation symbol.

EXAMPLE 1.3. We call $L_{\mathrm{ab}} = \{+, -, 0\}$ as the language of abelian groups. It has one binary function symbol, one unary function symbol, and one constant symbol.

EXAMPLE 1.4. Let $\mathbb{Q}$ be the field of rational numbers. The language $L_{\mathbb{Q}\text{-vs}}$ of $\mathbb{Q}$-vector spaces extends L_{ab} by countably many unary function symbols; one for each rational number q. We denote such a function symbol by s_q.

Next we define *terms* of a given language L. They are just certain finite strings of elements of L; from now on an *expression* of L means a finite string of elements of L. Terms will not have meaning yet either, but one should think them as 'the simplest functions that can be expressed in the setting of L'.

DEFINITION 1.5. The *terms* of a given first order language L are certain expressions of L that are built as follows:

(1) Variables and constant symbols are terms.
(2) If $t_1, \ldots, t_{m_i}$ are terms, then so is $f_i^{(m_i)}(t_1, t_2, \ldots, t_{m_i})$.
(3) Nothing else is a term.

We write L-term in the place of 'terms of L'.

Note that terms did not make use of relation symbols. They will be used to define *formulas* of L.

DEFINITION 1.6. The *formulas* of a first order language L are expressions that are built as follows:

(1) If t_1, t_2 are terms of L, then $t_1 = t_2$ is a formula.
(2) If $t_1, \ldots, t_{n_i}$ are terms of L, then $R_i^{(n_i)}(t_1, t_2 \ldots, t_{n_i})$ is a formula.
(3) If ϕ and ψ are formulas, then so are $(\neg\phi)$, $(\phi \to \psi)$, $(\phi \wedge \psi)$, $(\phi \vee \psi)$, $(\forall v_i \phi)$, $(\exists v_i \phi)$
(4) Nothing else is a formula.

As with terms, we simply write L-formula. Also if the language is clear from the context, we just write formula.

The formulas of the first two kinds will be referred to as *atomic formulas*.

The reader might have realized that there is a strange thing in this definition: the use of parentheses in the third item in the definition of formulas. They seem to be unnecessary, but we need them so that we do not get unparsable expressions. However, once the formula is formed, there is no harm in getting rid of the outmost parentheses. So as a convention, we do this. We have two more similar conventions: After the formula is formed, we remove parentheses around negations and quantifiers. For instance, we write $(v_1 = v_2) \to (\forall v_1 \neg v_3 = v_1)$, rather than $((v_1 = v_2) \to ((\forall v_1(\neg v_3 = v_1))))$.[3]

We use letters x, y, z for variables; possibly with decorations. This way we do not have to distinguish which v_i we are using.

We write a term t as $t(x_1, \ldots, x_n)$ if the variables occurring in t are among $x_1, \ldots, x_n$; if $\vec{x} = (x_1, \ldots, x_n)$ is a tuple of variables, then we simply write $t(\vec{x})$.

Most of the times, we omit the arities of function and relation symbols. Also we use other letters in the neighborhood of f to denote function symbols; again with possible decorations. Most of the times, we use familiar function symbols in the familiar way. For instance, in a while $+$ will denote a binary function and we write $x + y$ rather than $+(x, y)$. Similarly we use letters around R to denote relation symbols and familiar relation symbols are used; such as $<$.

Variable Occurrences. A variable x may appear in a formula with two different roles; after a quantifier ($\forall$, $\exists$) or not. We would like to set some notation for these and more.

Consider a formula of one of the forms $\forall x\phi$ or $\exists x\phi$. We say that ϕ is the *scope* of $\forall x$ or $\exists x$. The formula $\forall x\phi$ might appear as a subformula of a more complicated formula; we still say that ϕ is the scope of $\forall x$.

[3]As long as there is no double meaning any convention is fine in the context of these notes.

It might happen that $\forall x$ or $\exists x$ appears more than once in a formula. In that case, we should make sure scope of which one we are talking about.

DEFINITION 1.7. An occurrence of a variable x in a formula ϕ is said to be *bound* if it is either in $\forall x$ or in the scope of $\forall x$. Otherwise, we say that the occurrence is *free*.

EXAMPLE 1.8. Let $L = \{f, R, c\}$ where f is a binary function symbol, R is a binary relation symbol, and c is a constant symbol. Let x, y, z be distinct variables and let ϕ be the following L-formula:

$$R(f(x,c), f(c,y)) \to ((\forall y(f(x,c) = f(y,c))) \to \neg(\forall z(R(f(c,c), f(x,x))))).$$

All four occurrences of the variable x are free. The first occurrence of y is free, but the next two occurrences are bound. Finally, the only occurrence of the variable z is bound.

Consider $\forall y\, \phi$. Then all the occurrences of y become bound. However, there is a strange thing happening: The third y in ϕ seems to be bound (in $\forall y \phi$) by two different quantifiers. This is not a problem. Later when we interpret this formula, we will see that the second $\forall y$ is the one bounding that y and the first one will have no effect on it.

DEFINITION 1.9. A formula in which there are no free occurrences of any variable is called a *sentence*.

Sentences are mostly denoted with letters σ, τ, ρ, etc., possibly with decorations.

2. Semantics

Let L be a language.

Now we start to give meaning to L-formulas. This is done inside a *structure*, which we define next.

DEFINITION 2.1. An *L-structure* $\mathcal{M}$ is a nonempty set M with an *interpretation* of each of the non-logical symbols of L as follows:

- If f is an n-ary function symbol of L, then $f^{\mathcal{M}} : M^n \to M$ is a function,
- If R is an n-ary relation symbol of L, then $R^{\mathcal{M}}$ is a subset of M^n,
- If c is a constant symbol of L, then $c^{\mathcal{M}}$ is an element of M.

We will call M in this definition the *universe* of $\mathcal{M}$; sometimes the word *domain* is used. Note how we used the same letter in different font for the structure and its universe. We will try to keep doing this in these notes, but there will be some places where it is better use different letters. We generally write

$$\mathcal{M} = (M, f_1^{\mathcal{M}}, \dots, R_1^{\mathcal{M}}, \dots, c_1^{\mathcal{M}}, \dots)$$

to denote a structure with the interpretations of symbols exposed.

EXAMPLE 2.2. Consider $L_{\mathrm{o}} = \{<\}$ from above. One quick remark: Just because the symbol is the ordering symbol, its interpretation does not have to be an ordering. But it will be! The point is symbols are just symbols and we choose them to reflect how they will be interpreted.
An example of an L_{o}-structure is $\mathcal{R} = (\mathbb{R}, <^{\mathcal{R}})$ where $<^{\mathcal{R}}$ is the usual ordering of real numbers.
In general, we may take any partially ordered set and interpret $<$ as the ordering.

EXAMPLE 2.3. Let $L = \{E\}$, where E is a binary relation symbol. Given a set X, we may, for instance, interpret E as an equivalence relation on X.

EXAMPLE 2.4. Consider the language $L_{\mathrm{ab}} = \{+, -, 0\}$. Any abelian group can be thought of as an L_{ab}-structure. Actually, any group can be seen as an L_{ab}-structure, but it won't really be very natural.

Next we interpret terms in a structure. We do this in a somewhat sloppy way; below we remark about the intricate points and the correct way of doing this.

DEFINITION 2.5. Let $x_1, \ldots, x_n$ be a list of distinct variables. Let $\mathcal{M}$ be an L-structure and $\vec{a} = (a_1, \ldots, a_n) \in M^n$. For terms t whose variables are among $x_1, \ldots, x_n$, we define $t^{\mathcal{M}}(\vec{a})$ by recursion as follows:

(1) If t is x_i, then $t^{\mathcal{M}}(\vec{a}) = a_i$.
(2) If t is c, then $t^{\mathcal{M}}(\vec{a}) = c^{\mathcal{M}}$.
(3) If f is an n-ary function symbol, $t_1, \ldots, t_m$ are L-terms, and t is $f(t_1, \ldots, t_n)$, then
$$t^{\mathcal{M}}(\vec{a}) = f^{\mathcal{M}}\big(t_1^{\mathcal{M}}(\vec{a}), \ldots, t_n^{\mathcal{M}}(\vec{a})\big).$$

It is not necessary that all of the listed variables appear in t; actually it is necessary that we allow that, otherwise the recursive definition cannot work. Also this definition depends on the ordering of variables $x_1, \ldots, x_n$. In order to avoid this, we should define $t^{\mathcal{M}}(\vec{a})$ for countable sequences $\vec{a}$ as done in [**13**]. This detail is very important in an introductory logic course, but in these notes, we hope that it will always be clear what we substitute in the place of what.

Once we fix $x_1, \ldots, x_n$, we think of $t^{\mathcal{M}}$ as a function from M^n to M. After a while, we might not even mention the variables x_i.

We save examples of 'interpretations of terms in structures' until the end of the next definition.

DEFINITION 2.6. Let $x_1, \ldots, x_n$ be a list of distinct variables. Let $\mathcal{M}$ be an L-structure, and $\vec{a} = (a_1, \ldots, a_n) \in M^n$. For formulas whose free variables are among $x_1, \ldots, x_n$, we define $\vec{a}$ *satisfying* that formula (in $\mathcal{M}$) by recursion as follows:

(1) $\vec{a}$ satisfies $t_1 = t_2$ if $t_1^{\mathcal{M}}(\vec{a}) = t_2^{\mathcal{M}}(\vec{a})$.

(2) $\vec{a}$ satisfies an atomic formula $R(t_1, \ldots, t_n)$ if
$$\left(t_1^{\mathcal{M}}(\vec{a}), \ldots, t_n^{\mathcal{M}}(\vec{a})\right) \in R^{\mathcal{M}}.$$
(3) $\vec{a}$ satisfies $\neg\phi$ if it doesn't satisfy ϕ.
(4) $\vec{a}$ satisfies $\phi \to \psi$ if either $\vec{a}$ does not satisfy ϕ or $\vec{a}$ satisfies ψ.
(5) $\vec{a}$ satisfies $\phi \wedge \psi$ if $\vec{a}$ satisfy both ϕ and ψ.
(6) $\vec{a}$ satisfies $\phi \vee \psi$ if $\vec{a}$ satisfy one of ϕ or ψ.
(7) $\vec{a}$ satisfies $\forall y\phi$ if for every $b \in M$, the tuple $(a_1, \ldots, a_n, b)$ satisfies ϕ.
(8) $\vec{a}$ satisfies $\exists y\phi$ if $\vec{a}$ does not satisfy $\forall y\neg\phi$.

We can make remarks similar to the remarks about the previous definition. However, the problems with this definition are even bigger. In this case, it is really better in terms of preciseness to define satisfiability for countable tuples, but once again for our purposes this is one is precise enough, and it might even be less confusing.

The most involved part is the seventh one. Since we assume that the free variables of $\forall y\phi$ are among $x_1, \ldots, x_n$, we know that y is none of the variables x_i. Therefore the list $x_1, \ldots, x_n, y$ is distinct and it makes sense to talk about its satisfiability by $(a_1, \ldots, a_n, b)$ for any choice of b. However, it is a little bit unsettling that we have talk about one more number of variables in this recursive definition. Once again, defining this concept for countable tuples as in [**13**] would solve this potential problem.

We denote $\vec{a}$ satisfying ϕ in $\mathcal{M}$ as
$$\mathcal{M} \models \phi(\vec{a}).$$

Note that if σ is a sentence, then either any $\vec{a}$ satisfies it or no $\vec{a}$ satisfies it. So we may talk about a sentence being *true* in $\mathcal{M}$, without referring to any tuple from M.

The *universal closure* of a formula ϕ whose free variables are among $x_1, \ldots, x_n$ is $\forall x_1 \cdots \forall x_n \phi$. (Note that our conventions are in action here.) Clearly, the universal closure of any formula is a sentence. We write $\mathcal{M} \models \phi$ to mean that the universal closure of ϕ is true in $\mathcal{M}$.

2.1. Examples.

Example 2.7. Let's first consider the language $L_{\mathrm{o}} = \{<\}$. First note that the only L_{o}-terms are variables since there are no function or constant symbols. So the only atomic formulas are $x = y$ and $x < y$. Let's write down a few L_{o}-formulas. Let $\phi(x, y)$ be $y < x \vee x = y$, and let $\psi(x, y, z)$ be $x < y \to (x < z \wedge z < y)$. So far, these formulas do not have any meaning. So let's determine some L_{o}-structures. Let $\mathcal{M}_1$, $\mathcal{M}_2$, $\mathcal{M}_3$, and $\mathcal{M}_4$ be the L_{o}-structures whose universes are $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ and the interpretation of $<$ in each of these structures is the usual ordering. It is easy to determine which tuples of elements of these

structures satisfy ϕ and ψ. So we will start to place some quantifiers here and there in ϕ and ψ. Before doing that note that if $m, n \in \mathbb{N}$, then

$$\mathcal{M}_1 \models \phi(m,n) \Leftrightarrow \mathcal{M}_2 \models \phi(m,n) \Leftrightarrow \mathcal{M}_3 \models \phi(m,n) \Leftrightarrow \mathcal{M}_4 \models \phi(m,n).$$

As a matter of fact, the same is true for any L_{o}-formula without quantifiers. Later in this case we are going to say $\mathcal{M}_1$ is a *substructure* of each of $\mathcal{M}_2$, $\mathcal{M}_3$, $\mathcal{M}_4$.

Now consider the formula $\exists y \phi(x,y)$. The only free variable in this formula is x, and it is clear that it is satisfied by every element in each of the structures $\mathcal{M}_1$, $\mathcal{M}_2$, $\mathcal{M}_3$, $\mathcal{M}_4$. In other words, the sentence $\forall x \exists y \phi(x,y)$ holds in each $\mathcal{M}_i$ since every element is equal to itself. How about $\exists x \forall y \phi(x,y)$? It is easy to see that does not hold in any of the $\mathcal{M}_i$, because none of these structures have a 'largest element'. So far, we do not have an example of a formula or a sentence that behaves differently in different $\mathcal{M}_i$. Consider $\exists y \forall x \phi(x,y)$. This sentence says that there is a 'smallest element'. Therefore it holds in $\mathcal{M}_1$ and does not hold in any of the other $\mathcal{M}_i$.

Consider $\forall x \forall y \exists z \psi(x,y,z)$. It is easy to see that his sentence states that this ordering is 'dense'. Hence it holds in $\mathcal{M}_3$ and $\mathcal{M}_4$ and does not hold in $\mathcal{M}_1$ and $\mathcal{M}_2$.

Example 2.8. Let's now consider the language $L_{\mathrm{ab}} = \{+, -, 0\}$. We have two function symbols $+$ and $-$; the former is binary and the latter unary. Let's try to understand terms with only one variable x. It is a good idea to order them according to the number of occurrences of x. If it does not occur, then terms are constructed by just using the constant 0. For instance, 0, $0+0$, -0, $(-0)+0$ are terms. One might think that these are all the same term, but they are not. We will come back to this issue in a bit. Some examples of terms using x only once are $x+0$, $x+(0+0)$, $x+(-0)$, $x+((-0)+0)$, $0+x$, $(0+0)+x$, $(-0)+x$, $((-0)+0)+x$. We could determine all terms with one occurrence of x, but there isn't a very simple way to express them. In general, one could determine all terms.

Now let's consider the following L_{ab}-structures:

$$\mathcal{M}_1 = (\mathbb{Z}, +, -, 0), \mathcal{M}_2 = (\mathbb{Q}, +, -, 0), \mathcal{M}_3 = (\mathbb{Z}/6\mathbb{Z}, +, -, 0),$$

with the natural interpretations of the symbols. We shall see later that $\mathcal{M}_1$ is a substructure of $\mathcal{M}_2$, but let's remark here that in this setting it just means that $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$.

Consider the formula $\phi(x,y)$ defined as $x = y + y$. So in these three groups ϕ holds at (a,b) if and only if twice b is a. It is a little bit more interesting to think about $\exists y \phi(x,y)$; let's call this formula $\psi(x)$. In these groups –indeed in any abelian group– this formula holds at a if and only if a is divisible by 2. For instance, $\mathcal{M}_1 \not\models \psi(1)$, but

$\mathcal{M}_2 \models \psi(1)$. This means that being a substructure is not really that strong a property. It is also clear that $\mathcal{M}_3 \not\models \psi(\overline{1})$ and $\mathcal{M}_3 \models \psi(\overline{2})$. One could show that the following sentence holds in all abelian groups:

$$\forall x_1 \forall x_2((\psi(x_1) \wedge \psi(x_2)) \to \psi(x_1 + x_2)).$$

We could distinguish $\mathcal{M}_1$ and $\mathcal{M}_2$ by the sentence $\exists x \neg\psi(x)$. Actually, this formula distinguishes $\mathcal{M}_2$ and $\mathcal{M}_3$ as well. How can we distinguish $\mathcal{M}_1$ and $\mathcal{M}_3$? We can just say M_3 has 6 elements:

$$\exists x_1 \cdots \exists x_6(\bigwedge_{1 \leq i < j \leq 6} \neg x_i = x_j \wedge \forall y \bigvee_{1}^{6} y = x_i).$$

Here we used shorthands $\bigwedge_{1 \leq i < j \leq 6}$ and $\bigvee_{1}^{6}$. It must be clear what they mean, so we do not make any more comments about them, and we keep using similar shorthands in the rest of the text.

Note that changing the formula above a little, for any $n > 0$, we could write down a sentence in any first order language that expresses that the structure has exactly n elements. Also another sentence that expresses that the structure has at least n elements.

Let's return to the terms listed above. It is really correct that the interpretations of those terms in either of $\mathcal{M}_1$, $\mathcal{M}_2$, $\mathcal{M}_3$ are all equal to the interpretation of the constant symbol 0 in those structures. In a bit we shall state this more precisely, but let's observe that in $\mathcal{M}_1$ and $\mathcal{M}_2$ the interpretation of any term with variables $x_1, \ldots, x_k$ is equal to the interpretation of a term of the form $n_1x_1 + n_2x_2 + \cdots + n_kx_k$, where n_ix_i is short for the sum of n_i many x_i's for positive n_i and similarly is the sum of $-n_i$ many $-x_i$'s for negative n_i. In $\mathcal{M}_3$ we may restrict the integers n_i to vary in $\{0, 1, \ldots, 5\}$.

A little bit more on terms. Again let L be an arbitrary first order language and let $\mathcal{M}$ be an L-structure. We define an equivalence relation on the set of L-terms using $\mathcal{M}$:

$$s \sim_{\mathcal{M}} t \iff s^{\mathcal{M}} = t^{\mathcal{M}}.$$

This requires a little bit explanation. What does it mean that $s^{\mathcal{M}}$ and $t^{\mathcal{M}}$ are equal? It is the equality of functions, but how? Suppose that s has m variables, t has n variables. Recall that we then think of $s^{\mathcal{M}}$ and $t^{\mathcal{M}}$ as functions $M^m \to M$ and $M^n \to M$. If, say $n \leq m$, then we may think of $t^{\mathcal{M}}$ as a function $M^m \to M$, by considering the last $m-n$ variables as dummy variables. Note in particular that when we change a variable in a term with a variable that does not appear in that term, we get an equivalent term.

We extensively use the following notions.

DEFINITION 2.9. Let σ be a sentence, ϕ, ψ formulas, and Γ a set of formulas.

(1) We say that σ is *logically valid* if $\mathcal{M} \models \sigma$ for every structure $\mathcal{M}$. We denote this as $\models \sigma$.
(2) We say σ is *satisfiable* if there is a structure $\mathcal{M}$ such that $\mathcal{M} \models \sigma$.
(3) ϕ is *logically valid/satisfiable* if its universal closure is logically valid/satisfiable; we still use the notation $\models \phi$.
(4) The set Γ is *satisfiable* if there is a structure $\mathcal{M}$ such that $\mathcal{M} \models \theta$ for every $\theta \in \Gamma$; such a structure $\mathcal{M}$ is called a *model* of Γ, and we write $\mathcal{M} \models \Gamma$.
(5) The formula ϕ is a *logical consequence of* Γ if every model of Γ satisfies ϕ. We write $\Gamma \models \phi$ to denote this.
(6) If $\{\phi\} \models \psi$ and $\{\psi\} \models \phi$, we say that ϕ and ψ are *logically equivalent*.

A sentence σ is logically valid if and only if $\neg\sigma$ is not satisfiable. Also a formula ϕ is satisfiable if there is a structure $\mathcal{M}$ such that every tuple $\vec{a}$ from M satisfies ϕ.

Note that ϕ and ψ are logically equivalent if and only if $\phi \leftrightarrow \psi$ is logically valid.

3. Formal First Order Theories

Before sinking into the depths of model theory, we would like to get Completeness Theorem out of the way. For that, we need to introduce the concept of *proof*. In general, a formal theory has four components:

Alphabet Well-formed formulas Axioms Rules of Inference.

In the case of first order theories, an alphabet is just a first order language L and the well-formulas are just L-formulas. So it remains to introduce axioms and inference rules. After that we could define what a proof in such a formal theory is.

3.1. Axioms. Axioms of an L-theory T are as follows:

(A1) For every pair ϕ, ψ of L-formulas we have the axiom:
$$\phi \to (\psi \to \phi)$$
(A2) For every triple ϕ, ψ, θ of L-formulas we have the axiom:
$$(\phi \to (\psi \to \theta)) \to ((\phi \to \psi) \to (\phi \to \theta))$$
(A3) For every pair ϕ, ψ of L-formulas we have the axiom:
$$(\neg\phi \to \neg\psi) \to ((\neg\phi \to \psi) \to \phi)$$
(A4) If t is a term that is free for a variable x in a formula ϕ, then the following is an axiom:
$$\forall x\phi \to \phi(t/x)$$

(A5) If ϕ is an L-formula that has no free occurrence of a variable x, then the following is an axiom:

$$\forall x(\phi \to \psi) \to (\phi \to \forall x\psi)$$

(E1) $\forall x\, x = x$

(E2) If $\phi(x, y)$ is an L-formula, then the following is an axiom:

$$\forall x \forall y(x = y \to (\phi(x, x) \to \phi(x, y)))$$

(PA) We also have non-logical axioms called *proper axioms*, which are just some L-formulas.

The axiom (A4) contains two concepts we haven't defined yet. First of all, we say that a term t is *free for* a variable x in an L-formula ϕ if no free occurrence of x in ϕ lies within the scope of $\forall y$ for some variable y occurring in t. This is such a complicated looking definition, but one should think this as *no harm is done when we substitute t in the place any free occurrence of x.* When this is the case, the formula obtained by replacing every occurrence of x in ϕ by t is denoted as $\phi(t/x)$. We shall use this notation in later contexts as well.

The set of axioms (PA) is just a set of some L-formulas. There might be none, or there might be infinitely many of them. In our settings, they will generally be L-sentences. Later when we specify L-theories, we just state what their proper axioms are as the rest of the axioms are the same once the language is fixed. We let T_L denote the formal first order L-theory that has no proper axioms; this theory is sometimes called *Predicate Logic (in L).*

3.2. Inference Rules. We have two inference rules:

(MP) Modus Ponens: ψ follows from $\phi \to \psi$ and ϕ.

(Gen_x) Generalization: $\forall x\phi$ follows from ϕ.

The purpose of inference rules will be clear once we define 'proof' from T.

Definition 3.1. Let T be a formal L-theory.

(1) A finite sequence $\phi_1 \ldots, \phi_n$ of L-formulas is called a *proof (in T)*, if for each $i \in \{1, \ldots, n\}$ the formula ϕ_i is either an axiom or follows from previous formulas in the sequence by some inference rule.

(2) If there is a proof $\phi_1 \ldots, \phi_n$ from T with $\phi_n = \phi$ then ϕ is called a *theorem (of T)*; in this case, we write $\vdash_T \phi$.

We simply write $\vdash_L \phi$ in the place of $\vdash_{T_L} \phi$. When the language is clear from the context or is not important we even write $\vdash \phi$.

Note that if Γ is a set of L-formulas, then we may add them in the list of proper axioms and get another formal first order theory; let's say T_Γ. In this case rather writing $\vdash_{T_\Gamma} \phi$, we write $\Gamma \vdash_T \phi$. In accordance

with the previous paragraph, $\Gamma \vdash_L \phi$ will mean that ϕ is a theorem of the L-theory whose proper axioms are elements of Γ; and again we sometimes write $\Gamma \vdash \phi$.

In general, it is quite hard to determine whether given a formula is a theorem or not. The following homework shows that this could be hard even for very simple formulas.

Homework 1.

(1) Show that $\phi \to \phi$ is a theorem of any first order theory for any formula ϕ.
(2) Write down the sentence stating that $=$ is an equivalence relation and show that it is a theorem of every formal first order theory.

The next result makes the process of finding a proof a little bit easier. It is a special case of *Deduction Theorem*; see [**13**]. We do not prove it and refer the reader to [**13**]. This result can be used in solving homework problems.

PROPOSITION 3.2. *Let T be a first-order theory, Γ a set of formulas, σ a sentence, and ψ a formula. If $\Gamma \cup \{\sigma\} \vdash_T \psi$, then $\Gamma \vdash_T \sigma \to \psi$.*

Note that the converse is proposition is quite clear from (MP).

We do not wish to discuss more on the concept of formal proofs, and we would like to directly state Completeness Theorem. There will be some homework on deducing some statements in a given theory, and if you wish to learn more we suggest [**13**], since the notations there are the same as here.

4. Completeness Theorem

We fix a language L and all concepts below are in reference to L.

THEOREM 4.1 (Completeness Theorem – Version 1). *For a set Γ of formulas and a formula ϕ, we have $\Gamma \models \phi$ if and only if $\Gamma \vdash \phi$.*

As a matter of fact, it is quite easy to see that if $\Gamma \vdash \phi$, then $\Gamma \models \phi$. All we need to realize is that axioms are logically valid and Modus Ponens and Generalization preserve satisfaction of formulas. This part of the theorem is mostly referred to as *Soundness Theorem*.

In order to state the second version of Completeness Theorem, we need the concept of consistency and some fact about it.

DEFINITION 4.2. A set Γ of formulas is *inconsistent* if there is a formula ϕ such that $\Gamma \vdash \phi$ and $\Gamma \vdash \neg\phi$; this is denoted as $\Gamma \vdash$. Otherwise Γ is called *consistent*.

LEMMA 4.3. *A set Γ of formulas is inconsistent if and only if $\Gamma \vdash \psi$ for every ψ.*

PROOF. It is clear that if Γ proves every formula, then it proves a formula and its negation. In order to prove the other implication, let $\Gamma \vdash \phi$, $\Gamma \vdash \neg\phi$, and let ψ be an arbitrary formula. Since it is an axiom, Γ proves the formula $(\neg\psi \to \phi) \to ((\neg\psi \to \phi) \to \psi)$. Similarly, Γ proves $\phi \to (\neg\psi \to \phi)$ and $\neg\phi \to (\neg\psi \to \neg\phi)$. Now by using Modus Ponens a few times, we get $\Gamma \vdash \psi$. □

PROPOSITION 4.4. *Let Γ be set of formulas and ϕ a formula. Then $\Gamma \vdash \phi$ if and only if $\Gamma \cup \{\neg\phi\}$ is inconsistent.*

PROOF. It is easy to se that it suffices to prove that $\Gamma \vdash \hat{\phi}$ if and only if $\Gamma \cup \{\neg\hat{\phi}\}$ is inconsistent, where $\hat{\phi}$ is the universal closure of ϕ.

Suppose that $\Gamma \vdash \hat{\phi}$. Then $\Gamma \cup \{\neg\hat{\phi}\} \vdash \hat{\phi}$. But we also have $\Gamma \cup \{\neg\hat{\phi}\} \vdash \neg\hat{\phi}$. Therefore $\Gamma \cup \{\neg\hat{\phi}\}$ is inconsistent.

Conversely, suppose $\Gamma \cup \{\neg\phi\}$ is inconsistent. Then by the previous lemma, $\Gamma \cup \{\neg\hat{\phi}\} \vdash \hat{\phi}$. Using Proposition 3.2, we get that $\Gamma \vdash \neg\hat{\phi} \to \hat{\phi}$. We also have

$$\Gamma \vdash (\neg\hat{\phi} \to \neg\hat{\phi}) \to ((\neg\hat{\phi} \to \hat{\phi}) \to \hat{\phi})$$

and

$$\Gamma \vdash \neg\hat{\phi} \to \neg\hat{\phi}.$$

Now using MP twice, we get $\Gamma \vdash \hat{\phi}$. □

It is clear from Soundness Theorem that a satisfiable set Γ of formulas is consistent. Indeed, for a model $\mathcal{M}$ of Γ it is not possible that $\mathcal{M} \models \phi$ and $\mathcal{M} \models \neg\phi$. The second version of Completeness Theorem is the converse of this.

THEOREM 4.5 (Completeness Theorem – Version 2). *Every consistent set of formulas is satisfiable.*

The following homework asks you to show that the two versions of Completeness Theorem are indeed equivalent.

Homework 2. Prove that the following are equivalent:

(1) For every set Γ of formulas and formula ϕ, if $\Gamma \models \phi$, then $\Gamma \vdash \phi$.
(2) Every consistent set of formulas is satisfiable.

In the next chapter, we study a consequence of Completeness Theorem, namely Compactness Theorem. We shall also study quite a few applications of Compactness Theorem. Even though we are not presenting a proof of Completeness Theorem, we will outline a proof of Compactness Theorem not using Completeness Theorem.

CHAPTER 2

Model Theory

1. Basics

We start with introducing some basic notions of to be used repeatedly.

Elementary Equivalence. The first concept we introduce is elementary equivalence of two structures. For an algebraically trained person, this might look a little bit strange since it does not involve any map between structures and in particular it does not follow that elementarily equivalent structures have the same cardinality. As a matter of fact, one the applications of Compactness Theorem is that for a given structure and cardinal number larger than the cardinality of that structure, there is a structure of that cardinality which is elementarily equivalent to the original structure; this result is called Löwenheim-Skolem Theorem.

DEFINITION 1.1. Two L-structures $\mathcal{M}$ and $\mathcal{N}$ are *elementarily equivalent* if for every L-sentence σ, we have

$$\mathcal{M} \models \sigma \iff \mathcal{N} \models \sigma.$$

This is denoted as $\mathcal{M} \equiv \mathcal{N}$.

We leave it as an exercise to show that this is indeed an equivalence relation on L-structures.[1]

In Example 2.8 above, we have shown that none of the pairs the structures $\mathcal{M}_1$, $\mathcal{M}_2$, $\mathcal{M}_3$ are elementarily equivalent to each other. In general, in order to show that two structures are not elementarily equivalent, all we have to do is to find a mathematical property which is expressible in the language that distinguishes them. We may interpret Löwenheim-Skolem Theorem as stating that cardinality is not expressible in any language.

However, it is not very easy to show that two structures are elementarily equivalent. We will develop some tools in this chapter to be able to do that.

[1]This actually does not really make sense as the set of L-structures is not a set, but it must clear what we mean.

Theories. We have introduced above formal first order theories. Recall that once the language is fixed, such a theory is determined by its proper axioms, which is just a collection of formulas. Starting from now on, an *L-theory* is a consistent set of L-sentences. So it is not really very different than a set of sentences, but we just want to emphasize that it has a model.

An example of a theory is the theory of an L-structure $\mathcal{M}$:

$$\mathrm{Th}(\mathcal{M}) := \{\sigma : \mathcal{M} \models \sigma\}.$$

This theory has the nice property that for any L-sentence σ, either σ or $\neg\sigma$ is in $\mathrm{Th}(\mathcal{M})$. In particular $\mathrm{Th}(\mathcal{M})$ proves one and only one of σ or $\neg\sigma$. According to Completeness Theorem, one and only one of σ or $\neg\sigma$ is a logical consequence of $\mathrm{Th}(\mathcal{M})$. This property has a name:

Definition 1.2. A theory T is called *complete* if for every σ, either $T \models \sigma$ or $T \models \neg\sigma$.

Elementary equivalence can be expressed in terms of theories of structures.

Proposition 1.3. *Let $\mathcal{M}$ and $\mathcal{N}$ be L-structures. Then $\mathcal{M} \equiv \mathcal{N}$ if and only if $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{N})$.*

Proof. Clear. □

For a theory T we define its *logical closure* as the set of all sentences that are logical consequences of T:

$$\mathcal{D}(T) := \{\sigma : T \models \sigma\}.$$

Once again, it is clear from Completeness Theorem that $\mathcal{D}(T)$ is the set of L-sentences that can be deduced from T; that is why we use the letter D, which is short for *deductive closure*. The reason for giving these definitions in terms of truth rather than proofs is that later, we present a proof of Compactness Theorem, not going through Completeness Theorem. So it is important that these definitions are independent of equivalence of truth and provable.

Proposition 1.4. *Let T be an L-theory. Then the following are equivalent:*

(1) *T is complete.*
(2) *$\mathcal{D}(T)$ is complete.*
(3) *for every L-sentence σ, either $\sigma \in \mathcal{D}(T)$ or $\neg\sigma \in \mathcal{D}(T)$.*
(4) *$\mathcal{M} \equiv \mathcal{N}$ for every $\mathcal{M}, \mathcal{N} \models T$.*
(5) *$\mathcal{D}(T) = \mathrm{Th}(\mathcal{M})$ for any model $\mathcal{M}$ of T.*
(6) *$\mathcal{D}(T) = \mathrm{Th}(\mathcal{M})$ for some model $\mathcal{M}$ of T.*

Proof. Exercise. □

EXAMPLE 1.5. Consider the *theory* T_{ab} *of abelian groups* in the language L_{ab}; we do not write down the elements of this theory[2]. It is clearly consistent as there are groups. However, it is also clear that T_{ab} is not complete: there exist groups of different cardinalities. So let's consider the theory $T_{\text{ab},\infty}$ of infinite abelian groups. This is still not complete, because of the following sentence:

$$\forall x \exists y (x = ny).$$

Let's call this sentence as δ_n. So an abelian group satisfies δ_n if and only if it is n-divisible. So let's consider the theory $T^*_{\text{ab},\infty}$ of *divisible abelian groups*. Stil not complete! Consider the sentence τ_n defined as:

$$\exists x (x \neq 0 \wedge nx = 0).$$

An abelian group satisfies τ_n if and only it contains a nonzero torsion element. Let's extend $T^*_{\text{ab},\infty}$ by adding $\neg\tau_n$ for all $n > 0$. Below we prove that this theory is actually complete, and we denote it as DAG.

Reducts and Expansions. Let $L \subseteq L^*$ be languages. An L^*-structure $\mathcal{M}$ can be naturally considered as an L-structure. Let's denote that structure as $\mathcal{M}|_{L^*}$. We say that $\mathcal{M}|_{L^*}$ is the *reduct* of $\mathcal{M}$ (to L).

If $\mathcal{N}$ is an L-structure that is the reduct of an L^*-structure, say $\mathcal{N}^*$, then we say that $\mathcal{N}^*$ is an *expansion* of $\mathcal{N}$. Note that reduct of structure is unique, but there may be many natural ways to expand a structure.

EXAMPLE 1.6. Let $L_{\text{or}} = \{+, \cdot, -, <, 0, 1\}$ be the language of *ordered rings* and let $\mathcal{R} = (\mathbb{R}, +, \cdot, -, <, 0, 1)$ be a structure in that language. Then we way take the reduct of $\mathcal{R}$ to L_{ab}. Namely, $(\mathbb{R}, +, -, 0)$.

2. Compactness Theorem

As promised in the previous chapter, we study Compactness Theorem. This theorem is bread and butter of a model theorist.

THEOREM 2.1 (Compactness Theorem). *Let* Γ *be a set of* L*-sentences. Then there* Γ *has a model if and only if every finite subset of* Γ *has a model.*

PROOF. It is clear that if Γ has a model, then that model is a model of any subset of Γ. So let's assume that every finite subset of Γ has a model and show that Γ itself has a model.

Suppose not. Then by the second version of the Completeness Theorem, Γ is inconsistent. This means that there is an L-sentence σ such that $\Gamma \vdash \sigma$ and $\Gamma \vdash \neg\sigma$. In both cases, the proofs involve only finitely many hypotheses from Γ. Therefore there is a finite subset of Γ which is inconsistent. But then using the second version of the Completeness

[2]Actually, it can be taken to contain only one sentence.

Theorem on the reverse direction, we get that that finite subset of Γ does not have a model, contradicting the assumption. Hence Γ has a model. $\square$

REMARK. There is a possible confusion about Compactness Theorem akin to the usual confusion in the proof of infinitude of primes that is attributed to Euclid. Namely, the models of finite subsets of Γ might not be models of Γ. Actually, generally they are not, otherwise we probably do not need the Compactness Theorem. The next example illustrates this; none of the models of the finite parts work for our purposes.

EXAMPLE 2.2. Consider the structure $\mathcal{R} = (\mathbb{R}, +, \cdot, -, <, 0, 1)$ introduced above. We will show that there is $\mathcal{R}^*$ that is elementarily equivalent to $\mathcal{R}$ and there is $\alpha \in R^*$ which is positive and less than any $1/n$ for any $n > 0$. Obviously, there is no such element in $\mathbb{R}$, and it might sound like this contradicts elementary equivalence of $\mathcal{R}$ and $\mathcal{R}^*$. However, it only shows that existence of such an element cannot be expressed with an L_{or}-sentence.

Let $L^* = L_{\text{or}} \cup \{c\}$ where c is a new constant symbol. Consider the following set of L^*-sentences:

$$\Gamma := \text{Th}(\mathcal{R}) \cup \{0 < c\} \cup \{c < \frac{1}{n} : n > 0\}.$$

Note that if $\mathcal{R}^*_c = (R^*, +, \cdot, -, <, 0, 1, c^{\mathcal{R}_c})$ is a model of Γ, then its reduct $\mathcal{R}^* = (R^*, +, \cdot, -, <, 0, 1)$ to L_{or} satisfies the condition we ask for with $\alpha = c^{\mathcal{R}_c}$.

So we need to show that any finite subset Δ of Γ has a model. Write $\Delta = \Delta_1 \cup \Delta_2$, where $\Delta_1 \subseteq \text{Th}(\mathcal{R})$ and $\Delta_2 \subseteq \{0 < c\} \cup \{c < \frac{1}{n} : n > 0\}$. Since Δ_2 is finite, it is subset of $\{0 < c\} \cup \{c < \frac{1}{1}, c < \frac{1}{2}, \ldots, c < \frac{1}{N}\}$ for some $N > 0$. Now it is clear that $(\mathbb{R}, +, \cdot, -, <, 0, 1, \frac{1}{N+1})$ is a model of Δ.

Note that the universe of the models of each finite subset of Γ is $\mathbb{R}$. So none of those structures can be a model of Γ.

The first application of the Compactness Theorem is that we can find arbitrarily large models of a consistent sets of sentences.

THEOREM 2.3 (Upward Löwenheim-Skolem Theorem). *Let Γ be a theory that has an infinite model, and let κ be a cardinal number. Then there is a model $\mathcal{M}$ of Γ with $|M| \geq \kappa$.*

PROOF. Let C be a set of cardinality κ disjoint from L. We add elements of C to L as constant symbols to get the language L'. Consider the following set of L'-sentences:

$$\Gamma' = \Gamma \cup \{\neg c = d : c, d \in C, c \neq d\}.$$

Clearly it suffices to show that Γ' has a model. So let Δ be a finite subset of Γ'. Then only finitely many sentences of the form $\neg c = d$ appear in Δ. Taking an infinite model of Γ, we may interpret the new constants in a way that all those sentences are correct. So Δ has a model and consequently so does Γ'. By construction that model has cardinality at least κ and is indeed a model of Γ. □

3. Another Proof of Compactness Theorem

We now outline a proof of Compactness Theorem that does not go through Completeness Theorem. Assuming that every finite subset of Γ has a model, we actually construct a model of Γ. This procedure is called *Henkin Construction*.

A set Γ of L-sentences is called *finitely satisfiable* if every finite subset of it is satisfiable. So we assume Γ is finitely satisfiable and show that it is satisfiable. The proof is based on two results. We demonstrate only a sketch of those results. Before presenting them, we first would like to give an idea on what the model to be constructed looks like. Let $\mathcal{T}$ be the set of L-terms that do not contain any variables, and define the following equivalence relation on it:

$$s \sim_\Gamma t \iff \Gamma \models s = t.$$

Now put $\mathcal{M}_\Gamma := \mathcal{T}/\sim_\Gamma$. We construe $\mathcal{M}_\Gamma$ as an L-structure as follows:

$$f^{\mathcal{M}_\Gamma}(t_1/\sim, \dots, t_m/\sim) = f(t_1, \dots, t_m)/\sim,$$
$$(t_1/\sim, \dots, t_n/\sim) \in R^{\mathcal{M}_\Gamma} \iff \Gamma \models R(t_1, \dots, t_n),$$
$$c^{\mathcal{M}_\Gamma} = c/\sim .$$

It is straightforward to check that $\mathcal{M}_\Gamma$ is indeed an L-structure this way; the only problem is that the definitions above can really be made[3] The following is also straightforward.

Homework 3. Let σ be a quantifier-free sentence. Show that $\mathcal{M}_\Gamma \models \sigma$ if and only if $\Gamma \models \sigma$.

Note that a sentence being quantifier-free means that it does not contain any variables.

If the homework above could have been proven for all sentences, then we would be done, since in that case, $\mathcal{M}_\Gamma$ would be a model of Γ. Not only that this is too good to be true, but also there is a bigger problem. If the language does not contain any constant symbols, then $\mathcal{T}$ and hence $\mathcal{M}_\Gamma$ would be the empty set, and we do not allow empty set as the universe of a structure. This might look like a small problem, but it is part of a much larger problem. Below we will see this under the name of 'witness property'.

[3]In other words, they are well-defined.

The first result to be used in the proof is the following.

PROPOSITION 3.1 (Lindenbaum's Lemma). *Let Γ be a finitely satisfiable set of L-sentences. Then there is a finitely satisfiable, complete set Γ^* of L-formulas containing Γ such that for every L-sentence σ if $\Gamma^* \models \sigma$, then $\sigma \in \Gamma^*$.*

Recall the concept $\mathcal{D}(\Gamma^*)$ of logical closure of Γ^*: a sentence σ is in $\mathcal{D}(\Gamma^*)$ if and only if $\Gamma^* \vdash \sigma$. So if we assume Completeness Theorem, then the last property of Γ^* in this proposition could have been written as $\mathcal{D}(\Gamma^*) = \Gamma^*$. We do not need to assume this and we don't. We refer to sets of formulas with this property as *deductively closed*.

The idea of the proof of Lindenbaum's Lemma is to keep adding one of σ or $\neg\sigma$ if neither of them is already added. Of course, sometimes we may add either of them, but most of the times, it is determined which one to add. For instance, it could happen that $\neg\neg\sigma$ is already added.

Using Lindenbaum's Lemma, we may always enrich a given finitely satisfiable set of sentences to a complete and deductively closed set of sentences by keeping finite satisfiability. The next result is that we may enrich it to satisfy even a stronger property. This property is that if $\Gamma \models \exists x\phi(x)$, then there is $t \in \mathcal{T}$ such that $\Gamma \models \phi(t)$; hence $\phi(t) \in \Gamma$ if Γ is deductively closed. This will be called the *witness property*, because we are witnessing the truth of an existential formula by a very special kind of term. Going back to the problem about $\mathcal{M}_\Gamma$ mentioned above, we see that if Γ has the witness property, then $\mathcal{M}_\Gamma$ is not empty, since $\Gamma \models \exists x(x = x)$. Of course, the witness property is much more than this. Note also that this cannot be achieved without extending the language as well.

PROPOSITION 3.2. *Let Γ be a finitely satisfiable set of L-sentences. Then there is a language L^* extending L by constant symbols, and a finitely satisfiable, complete, deductively closed set $\Gamma^* \supseteq \Gamma$ of L^*-sentences that has the witness property.*

Using Lindenbaum's Lemma, we may assume that Γ is deductively closed and complete. Suppose that $\exists x\phi(x)$ is a logical consequence of a finitely satisfiable theory Γ. Let $L' = L \cup \{c_a\}$ and let $\Gamma' = \Gamma \cup \{\phi(c_a)\}$. It is clear then that Γ' has a witness for this particular formula $\exists x\phi(x)$, and it can easily be shown that Γ' is still finitely satisfiable. Actually, this can be done simultaneously for all formulas of the form $\exists x\phi(x)$ by extending L to L_1 by adding constant symbols and by extending Γ to Γ_1 by adding existential formulas. After doing this, we may lose completeness and deductive closedness. So we apply Lindenbaum's Lemma once again. So we apply Lindenbaum's Lemma on the even steps and adding constants and existential formulas procedure on the

odd steps. Then one may show that after countably many steps this procedure gives Γ^* as desired.

Proof of Compactness Theorem. Suppose that Γ is finitely satisfiable. Using Proposition 3.2, construct the language L^* and finitely satisfiable, complete, deductively closed $\Gamma^* \supseteq \Gamma$ that has witnesses. We claim that $\mathcal{M}_{\Gamma^*}$ is a model of Γ^*. We prove by induction on the complexity of sentence that for an L^*-sentence σ we have

$$\sigma \in \Gamma^* \iff \mathcal{M}_{\Gamma^*} \models \sigma.$$

By Homework 3 above, we know this for all quantifier-free sentences, in particular this is the case for atomic formulas. The sentences obtained by $\neg, \to, \wedge, \vee$ from simpler sentences clearly satisfy this as well. The sentences of the form $\forall x \phi(x)$ is logically equivalent to $\neg\exists x \neg\phi(x)$. Therefore it is enough to consider sentences of the form $\exists x \phi(x)$.

Note that

$$\begin{aligned} \mathcal{M}_{\Gamma^*} \models \exists x \phi(x) &\iff \mathcal{M}_{\Gamma^*} \models \phi(t/\sim) \text{ for some } t \in \mathcal{T} \\ &\iff \phi(t) \in \Gamma^* \text{ for some } t \in \mathcal{T} \end{aligned}$$

Since $\exists x \phi(x)$ is a logical consequence of $\phi(t)$, if $\mathcal{M}_{\Gamma^*} \models \exists x \phi(x)$, then we get $\exists x \phi(x) \in \Gamma^*$. Conversely, if $\exists x \phi(x) \in \Gamma^*$, then by witness property, there is $t \in \mathcal{T}$ such that $\phi(t) \in \Gamma^*$. By the equivalences above we get $\mathcal{M}_{\Gamma^*} \models \exists x \phi(x)$. □

Note that the language L^* obtained in Proposition 3.2 has the same cardinality as L[4]. Therefore the model $\mathcal{M}^*_\Gamma$ constructed in the proof of Compactness Theorem has at most as many elements as L. This proves the following.

Theorem 3.3 (Downward Löwenheim-Skolem). *Suppose that Γ is an L-theory. Then there is a model of Γ of cardinality at most $|L|$.*

Putting the two Löwenheim-Skolem Theorems and Completeness Theorem together we get the following consequence.

Corollary 3.4. *Let Γ be a set of L-sentences that has an infinite model and let $\kappa \geq |L|$ be a cardinal number. Then Γ has a model of cardinality κ.*

Proof. Let C a set of cardinality κ disjoint from L, and let $L' = L \cup C$, where elements of C are added as constant symbols. Note that L' has cardinality κ. Then by the proof of Theorem 2.3, there is a model of

$$\Gamma' = \Gamma \cup \{\neg c = d : c, d \in C, c \neq d\}.$$

[4]Recall that every language contains at least countably many variables, hence is always infinite.

So applying Theorem 3.3, Γ' has a model $\mathcal{M}$ of cardinality at most $|L'| = \kappa$. However models of Γ' has at least κ many elements. Therefore $\mathcal{M}$ has cardinality exactly κ. □

4. Maps Between Structures

Let L be a language and $\mathcal{M}$ and $\mathcal{N}$ be L-structures. A function $F : M \to N$ is called a *homomorphism* if the following hold for every n-ary function symbol f, n-ary relation symbol R, constant symbol c and $\vec{a} = (a_1, \ldots, a_n) \in M^n$:

(1) $F(f^{\mathcal{M}}(\vec{a})) = f^{\mathcal{N}}(F(\vec{a}))$,
(2) If $\vec{a} \in R^{\mathcal{M}}$, then $F(\vec{a}) \in R^{\mathcal{N}}$,
(3) $F(c^{\mathcal{M}}) = c^{\mathcal{N}}$.

(Here and later, $F(\vec{a}) = (F(a_1), \ldots, F(a_n))$.)

We sometimes write '$F : \mathcal{M} \to \mathcal{N}$ is a homomorphism'.

Note that we only require that $F(R^{\mathcal{M}}) \subseteq R^{\mathcal{N}}$. Sometimes a homomorphism that has equality here instead of inclusion for every R is called a *strong homomorphism*. However, we do not need this definition except for the next definition: A strong homomorphism that is also injective is called an *embedding*. If an embedding is also surjective, then it is called an *isomorphism*. If there is an isomorphism between two structures $\mathcal{M}$ and $\mathcal{N}$, then we say that they are *isomorphic*, and we denote this as $\mathcal{M} \simeq \mathcal{N}$. An isomorphism of a structure $\mathcal{M}$ with itself is called an *automorphism*.

Homework 4. Let $F : \mathcal{M} \to \mathcal{N}$ be a homomorphism of $\mathcal{L}$-structures and let t be an $\mathcal{L}$-term whose variables are among $x_1, \ldots, x_n$. Show that for any $\vec{a} = (a_1, \ldots, a_n) \in M^n$, we have

$$t^{\mathcal{N}}(F(\vec{a})) = F(t^{\mathcal{M}}(\vec{a})).$$

Homework 5. Show that L-isomorphism gives an equivalence relation on the class of L-structures. [5]

Homework 6. Show that the set of automorphisms of a structure forms a group with composition as the group operation.

Suppose that $\mathcal{M}$ and $\mathcal{N}$ are structures such that $M \subseteq N$. If the inclusion map $M \to N$ is an embedding, then we say that $\mathcal{M}$ is a *substructure* of $\mathcal{N}$ and we denote this as $\mathcal{M} \subseteq \mathcal{N}$.

[5] Once again, this does not exactly make sense, but it is clear what is meant.

EXAMPLE 4.1. Let's study these concepts in structures of more algebraic content. Let $L_{\mathrm{r}} = \{+, \cdot, -, 0, 1\}$, where $+, \cdot$ are binary function symbols, $-$ is a unary function symbol, and $0, 1$ are constant symbols. We may interpret $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ as L_{r}-structures in a natural way, and all excepts $\mathbb{C}$ are naturally L_{or}-structures. Moreover, the smaller ones are substructures of bigger ones. However, they are not elementarily equivalent to each other.

Homework 7. Suppose that $\mathcal{M} \subseteq \mathcal{N}$, and let σ be a sentence that does not have any occurrence of $\forall$ or $\exists$. Show that $\mathcal{M} \models \sigma$ if and only if $\mathcal{N} \models \sigma$.

Homework 8. Show that if $\mathcal{M} \simeq \mathcal{N}$, then $\mathcal{M} \equiv \mathcal{N}$.

A stronger type of a function is defined as follows.

DEFINITION 4.2. An embedding $f : \mathcal{M} \to \mathcal{N}$ is called an *elementary embedding* of for every formula $\phi(\vec{x})$ and $\vec{a} \in M^n$ we have

$$\mathcal{M} \models \phi(\vec{a}) \iff \mathcal{N} \models \phi(f(\vec{a})).$$

A substructure $\mathcal{M}$ of $\mathcal{N}$ is called an *elementary substructure* if the inclusion map is an elementary embedding; this is denoted as $\mathcal{M} \preceq \mathcal{N}$. It is clear that if $\mathcal{M} \preceq \mathcal{N}$, then $\mathcal{M} \equiv \mathcal{N}$. However, the converse is not correct.

Homework 9. Find two structures $\mathcal{M}$ and $\mathcal{N}$ such that $\mathcal{M} \subseteq \mathcal{N}$ and $\mathcal{M} \equiv \mathcal{N}$, but $\mathcal{M} \not\preceq \mathcal{N}$.

5. Categoricity

It is somehow[6] important that a theory has a single model of a given cardinality; so we give it a name.

DEFINITION 5.1. Let κ be a cardinal number and let L be a language with $|L| \leq \kappa$. An L-theory T with infinite models is called *κ-categorical* if any two models of cardinality κ are isomorphic.

EXAMPLE 5.2. A well-known theorem of Cantor states that any two countable densely ordered sets without end points are isomorphic. This is to say that the the following theory, denoted as DLO, expressed in the language L_{o}, is $\aleph_0$-categorical:

- $<$ is a linear (total) ordering:
  - $\forall x \neg x < x$
  - $\forall x \forall y (x < y \to \neg y < x)$
  - $\forall x \forall y \forall z ((x < y \wedge y < z) \to x < z)$
  - $\forall x \forall y (x = y \vee x < y \vee y < x)$

[6] See Theorem 5.4 below.

- The ordering is dense: $\forall x \forall y (x < y \to \exists z (x < z \wedge z < y))$
- The ordering has no end points: $\forall x \exists y (x < y) \wedge \forall z \exists w (w < z)$

Homework 10. Prove Cantor's Theorem.

EXAMPLE 5.3. Now let's consider the L_{ab}-theory that consists of the following sentences:

- Abelian group axiom(s); we are not going to write down this sentence(s).
- $\exists x \, x \neq 0$.
- For each $n > 0$, the following axiom: $\forall x \exists y x = ny$.
- For each $n > 0$, the following axiom: $\neg \exists x (x \neq 0 \wedge nx = 0)$.

The second item is not one axiom, but infinitely many axioms; such things are sometimes called axiom schemes. First two parts state that the models need to be divisible abelian groups. Similarly the last part is an axiom scheme and added on top the previous parts it says that models are torsion-free. This theory is called the theory of divisible torsion-free abelian groups, and it is denoted as DAG.[7]

It is easy (and standard) to see that models of DAG are exactly nonzero $\mathbb{Q}$-vector spaces. Note that $\mathbb{Q}$-vector spaces are generally considered in a different language; namely $L_{\mathbb{Q}\text{-vs}}$. However, this is not our concern. So models of DAG have $\mathbb{Q}$-bases and hence $\mathbb{Q}$-dimensions. We also know that two $\mathbb{Q}$-vector spaces are isomorphic if and only if they have the same dimension. Now it requires a little bit thought, but it is not a very complicated thing that the dimension of an uncountable model of DAG is the same as its cardinality. As a result, DAG is κ-categorical for all uncountable κ.

Homework 11. Show that DAG is not $\aleph_0$-categorical.

Homework 12. Let p be either 0 or a prime.

(1) Write down the theory of "algebraically closed fields of characteristic p" in the language $L_r := \{+, \cdot, -, 0, 1\}$. Denote this theory as ACF_p
(2) Show that ACF_p is not $\aleph_0$-categorical.
(3) Show that ACF_p is κ-categorical for all uncountable κ.

(Hint: Transcendence degree.)

THEOREM 5.4 (Łoś-Vaught Test). *Let κ be a cardinal number and L a language of cardinality at most κ. Also let T be a κ-categorical theory that does not have finite models. Then T is complete.*

[7]Unfortunately being torsion-free is not reflected in the notation.

PROOF. Let $\mathcal{M}$ and $\mathcal{N}$ be models of Γ. By Proposition 1.4, we need to show that $\mathcal{M} \equiv \mathcal{N}$. By Corollary 3.4 both $\mathrm{Th}(\mathcal{M})$ and $\mathrm{Th}(\mathcal{M})$ have models of cardinality κ; say $\mathcal{M}'$ and $\mathcal{N}'$ respectively. Note that $\mathcal{M}'$ and $\mathcal{N}'$ are models of T as well. So by categoricity assumption, we get $\mathcal{M}' \simeq \mathcal{N}'$. So $\mathcal{M}' \equiv \mathcal{N}'$ by Homework 8. Therefore

$$\mathcal{M} \equiv \mathcal{M}' \equiv \mathcal{N}' \equiv \mathcal{N}.$$

□

COROLLARY 5.5. *The theories* DLO*,* DAG*, and* $\mathrm{ACF_p}$ *are complete.*

We close this section with an application of Compactness Theorem involving ACF_0. This is a special case of a theorem of J. Ax in [**1**]. Later, we will give another proof this result as direct consequence of *Lefschetz Principle*.

THEOREM 5.6. *Every injective polynomial map* $f : \mathbb{C}^n \to \mathbb{C}^n$ *is surjective.*

PROOF. Suppose that this is not correct and let $f = (f_1, \ldots, f_n)$ be a counterexample. For each i, let d_i be the (total) degree of f_i. So we may write f_i as follows:

$$f_i = \sum_{|\vec{j}| \leq d_i} a_{i\vec{j}} \vec{X}^{\vec{j}},$$

where $\vec{X} = (X_1, \ldots, X_n)$ is an n-tuple of indeterminates, $\vec{j} = (j_1, \ldots, j_n)$ runs through $\mathbb{N}^n$, with $|\vec{j}| = j_1 + \cdots + j_n$, and $\vec{X}^{\vec{j}}$ denotes the product $X_1^{j_1} X_2^{j_2} \cdots X_n^{j_n}$.

Fix a finite set J of multi-indices $\vec{j}$ such that –possibly after adding some $a_{i\vec{j}} = 0$– we have $f_i = \sum_{\vec{j} \in J} a_{i\vec{j}} \vec{X}^{\vec{j}}$.

Let σ be the following L_{r}-sentence

$$\exists_{i \in [n], \vec{j} \in J} x_{i\vec{j}} \Big(\big(\forall y_1 \cdots \forall y_n \forall z_1 \cdots \forall z_n \bigwedge_{i=1}^{n} \sum_{\vec{j} \in J} x_{i\vec{j}} \vec{y}^{\vec{j}} = \sum_{\vec{j} \in J} x_{i\vec{j}} \vec{z}^{\vec{j}} \to \vec{y} = \vec{z} \big) \wedge$$

$$\big(\exists s_1 \cdots \exists s_n \forall t_1 \cdots \forall t_n \bigvee_{i=1}^{n} \sum_{\vec{j} \in J} x_{i\vec{j}} \vec{t}^{\vec{j}} \neq s_i \big) \Big).$$

Then $\mathbb{C} \models \sigma$, and hence by completeness of ACF_0, we have $\mathrm{ACF}_0 \models \sigma$. Using Compactness Theorem, there is a finite subset Γ of ACF_0 with $\Gamma \models \sigma$. Note that there is $N > 0$ such that for every prime $p > N$ we have $\mathrm{ACF_p} \models \Gamma$, hence $\mathrm{ACF_p} \models \sigma$. So $\overline{\mathbb{F}}_p \models \sigma$. Then there is an injective polynomial map $f : \overline{\mathbb{F}}_p^n \to \overline{\mathbb{F}}_p^n$ which is not surjective. Take $\vec{\alpha} \in \overline{\mathbb{F}}_p^n$ that is not in the image of f.

Let F be subfield of $\overline{\mathbb{F}}_p$ that is a finite extension of $\mathbb{F}_p$ such that $\vec{\alpha} \in F^n$ and $f \in F[\vec{X}]$. Note that f maps F^n to F^n and $f|_{F^n}$ is still injective and not surjective as $\vec{\alpha} \in F^n$. However, F is a finite field, hence every injective map from F^n to itself must be surjective. This is a contradiction, so every injective polynomial map $f : \mathbb{C}^n \to \mathbb{C}^n$ is surjective. □

6. Definable Sets

Let $\mathcal{M}$ be an L-structure. We consider formulas of the form $\phi(\vec{x}, \vec{a})$ where as usual $\vec{x}$ is a tuple of variables, and $\vec{a}$ is a tuple of elements of M. It is clear what this formula should mean, but to be precise it is not an L-formula. In order to do this correctly, let A be a subset of M. Let L_A be the language obtained by augmenting L by a new constant symbol for each element of A. We may than expand $\mathcal{M}$ to an L_A-structure by interpreting a new constant symbol as the element it names. We do not distinguish the constant symbol and its interpretation. Sometimes we denote this expansion as $\mathcal{M}_A$, but most of the times we simply write $\mathcal{M}$. Now $\phi(\vec{x}, \vec{a})$ is just an L_A-formula, where $\vec{a}$ is just a tuple of constant symbols naming elements of A. Sometimes we suppress $\vec{a}$ and simply say $\phi(\vec{x})$ is an L_A-formula.

Given an L_M-formula $\phi(\vec{x})$ we let

$$\phi(\mathcal{M}) := \{\vec{b} \in M^n : \mathcal{M} \models \phi(\vec{b})\}.$$

A set of this form is called a *definable set*; in this case we say that it is *defined by* ϕ. If we want to emphasize the parameters used, then we say that a set is *definable over* A or A*-definable* provided that it is defined by an L_A-formula.

Obviously, $\emptyset$ and M^n are definable sets. It is also clear that definable sets are closed under Boolean combinations. This means that if X, Y are definable sets, then so are $X \cup Y$, $X \cap Y$, $X \setminus Y$. Also logically equivalent formulas define the same sets.

A function $f : X \to M$ is called *definable* if its graph

$$\Gamma(f) := \big\{(x, f(x)) \in M^{n+1} : x \in X\big\}$$

is a definable set. Note that this forces X to be definable.

In general, it can be very hard to analyze definable sets in a given structure. For this purpose, it is crucial to find good representatives for formulas in the sense of logical equivalence. For instance, it could happen that in $\mathcal{M}$, every formula is equivalent to a formula in which neither $\forall$ nor $\exists$ occurs; such formulas are called *quantifier-free*. If that is the case, then each formula is a Boolean combination of formulas of atomic formulas. Recall that they are formulas of the form $R(t_1, \ldots, t_m)$ for an m-ary relation symbol R and terms $t_1, \ldots, t_m$. So it boils down to understanding terms.

Let us make this a little bit more precise. Let T be an L-theory. We say that T *eliminates quantifiers* or *has quantifier-elimination* if for every L-formula $\phi(\vec{x})$, there is a quantifier-free L-formula $\psi(\vec{x})$ such that

$$T \models \forall \vec{x}(\phi(\vec{x}) \leftrightarrow \psi(\vec{x})).$$

In the previous paragraph, we were talking about definable sets in a structure, and here we start to talk about theories. First of all, it is easier to express this in terms of formulas and this is really a more general approach. We say that an L-structure $\mathcal{M}$ has quantifier elimination if $\mathrm{Th}(\mathcal{M}_M)$ has quantifier elimination. Note that $\mathrm{Th}(\mathcal{M}_M)$ is a theory in the language L_M.

Note that having quantifier-elimination heavily depends on the language. Indeed, by enriching the language, one may obtain quantifier-elimination, but then the terms will be quite complicated. This process is called *Morleyization*, and we prefer not to get into the details.

We finish the discussion of quantifier-elimination for the moment, by stating some facts. The proofs of these require developing some more methods. As we do not want to turn this course into a model theory course, we skip them. They can be found in [**16**] or [**19**].

Fact 6.1. The theories DLO, DAG, $\mathrm{ACF_p}$ have quantifier-elimination.

Actually, the (incomplete) theory ACF of algebraically closed fields also has quantifier-elimination. We sketch a proof of this in the next section, assuming a model theoretic fact.

Fact 6.2. Let L^*_{ab} be language extending L_{ab} by a unary relation symbol D_n for each $n > 0$. Let $\mathcal{Z}$ be the expansion of $(\mathbb{Z}, +, -, 0)$ to an L^*_{ab}-structure by interpreting D_n as $n\mathbb{Z}$. Then $\mathcal{Z}$ eliminates quantifiers.

Fact 6.3. Let L_{oab} be language extending L_{ab} by a binary relation symbol $>$, and let DAOG be the L_{oab}-theory of densely ordered divisible abelian groups. Then DOAG eliminates quantifiers.

Note that the L_{ab}-reduct of a model of DAOG is a model of DAG.

Fact 6.4 (Tarski-Seidenberg Theorem). The L_{or}-structure $\mathcal{R} = (\mathbb{R}, +, \cdot, -, 0, 1, <)$ eliminates quantifiers.

Note that $<$ is definable in the L_{r}-structure $(\mathbb{R}, +, \cdot, -, 0, 1)$ since the non-negative elements of reals are precisely the squares. So they have more the same definable sets. However, the structure $(\mathbb{R}, +, \cdot, -, 0, 1)$ does not eliminate quantifiers, because the definition of $<$ has quantifiers and they cannot be eliminated. The L_{r}-theory of $(\mathbb{R}, +, \cdot, -, 0, 1)$ is axiomatized as the theory of *real closed fields*.

Generally, $\mathrm{Th}(\mathbb{R}, +, \cdot, -, 0, 1, <)$ is denoted as RCF. Hence we may restate the fact above as "RCF has quantifier elimination".[8]

[8]This is not precisely correct; we leave it to the reader why.

Later we shall use some of these facts to obtain examples of o-minimal structures.

A notion slightly weaker than having quantifier-elimination is being model complete.

DEFINITION 6.5. A theory T is *model complete* if for any two models $\mathcal{M}$ and $\mathcal{N}$ with $\mathcal{M} \subseteq \mathcal{N}$, we have $\mathcal{M} \preceq \mathcal{N}$.

Homework 13. Show that the following are equivalent:

(1) T is model complete.
(2) Any formula whose free variables are among $\vec{x}$ is equivalent in T to a formula of the form $\exists \vec{y} \phi(\vec{x}, \vec{y})$, where ϕ is a quantifier free formula.
(3) For any two models $\mathcal{M} \subseteq \mathcal{N}$, any quantifier free formula $\phi(\vec{x}, \vec{y})$, and $\vec{a} \in M^n$ we have
$$\mathcal{M} \models \exists \vec{y} \phi(\vec{a}, \vec{y}) \iff \mathcal{N} \models \exists \vec{y} \phi(\vec{a}, \vec{y}).$$

PROPOSITION 6.6. *If an L-theory has quantifier elimination, then it is model complete.*

PROOF. It is clear from the homework above. □

6.1. Definable families and sections.

DEFINITION 6.7. Let $X \subseteq M^n \times M^k$ be a definable set and let $\vec{b} \in M^k$. The *section of X over $\vec{b}$* is
$$X_{\vec{b}} := \{\vec{a} \in M^n : (\vec{a}, \vec{b}) \in X\}.$$
For a definable set $Y \subseteq M^k$, the collection $(X_{\vec{a}})_{\vec{a} \in Y}$ is called a *family of definable sets*.

If $(X_{\vec{a}})_{\vec{a} \in Y}$ is a definable family, then
$$X = \bigcup_{\vec{a} \in \pi(X)} \{\vec{a}\} \times X_{\vec{a}}$$
where $\pi : M^{n+k} \to M^k$ the projection onto the last k coordinates. More generally, for a subset Z of Y, we have
$$\pi^{-1}(Z) \cap X = \bigcup_{\vec{a} \in Z} \{\vec{a}\} \times X_{\vec{a}}.$$

7. More on ACF

We give a proof of QE for ACF by assuming the following.

PROPOSITION 7.1. *Let T be an L-theory. Suppose that for any $\mathcal{M}, \mathcal{N} \models T$ the following holds:*

For any common substructure $\mathcal{A}$ of $\mathcal{M}$ and $\mathcal{N}$ and quantifier-free L_A-formula $\phi(y)$ we have $\mathcal{M} \models \exists y \phi(y)$ if and only of $\mathcal{N} \models \exists y \phi(y)$.

Then T has quantifier elimination.

THEOREM 7.2. *The L_r-theory* ACF *has quantifier elimination.*

PROOF. Let K, L be algebraically closed fields with a common subring A. By taking algebraic closures in K and L of the fraction field of A, we may assume that A is algebraically closed. Note then that K and L have the same characteristic.

Now let $\phi(y)$ be an L_A-formula and let $K \models \phi(\alpha)$ for some $\alpha \in K$. We would like to find $\beta \in L$ with $L \models \phi(\beta)$.

We know that $\phi(y)$ is logically equivalent to a formula of the form

$$\bigvee_{i=1}^{m} \bigwedge_{j=1}^{n} \phi_{ij}(y),$$

where $\phi_{ij}(y)$ is either $p_{ij}(y) = 0$ or $p_{ij}(y) \neq 0$ for a polynomial $p_{ij}(y)$ with coefficients from A.

For our purposes we may assume that ϕ is actually of the form

$$\bigwedge_{j=1}^{n} \phi_j(y).$$

This can be written as

$$\bigwedge_{j=1}^{m} p_j(y) = 0 \wedge \bigwedge_{j=m+1}^{n} p_j(y) \neq 0.$$

For some polynomials $p_1, \ldots, p_n \in A[y]$.

If $m \neq 0$, then $\alpha \in A$ since A is an algebraically closed field, and hence $\alpha \in L$. Thus we may assume that ϕ is of the form

$$\bigwedge_{j=1}^{n} p_j(y) \neq 0.$$

Since α satisfies these inequalities, each p_j is a nonzero polynomial, hence has finitely many roots. Therefore we may find $\beta \in L$ satisfying ϕ. □

By Proposition 6.6, we know that ACF is model complete. This gives another proof of its completeness of ACF_p: Let K, L be algebraically closed field of characteristic p. Then $\overline{\mathbb{F}}_p$[9] is a common substructure of K and L, which happens to be a model of ACF_p as well. Therefore $\mathbb{F}_p \preceq K$ and $\mathbb{F}_p \preceq L$. Hence $K \equiv L$. Note that this idea can be used to prove that if T is model complete and T has a model that embeds in every model of T, then T is complete. Indeed, this observation is the reason for the expression *model complete*.

[9]We set $\mathbb{F}_0 = \mathbb{Q}$.

One may think of completeness of ACF_0 as *Lefschetz Principle*. This also gives a *Local-global Principle* as follows.

THEOREM 7.3. *Let σ be an L_{r}-sentence. Then the following are equivalent.*

(1) $\mathbb{C} \models \sigma$.
(2) $K \models \sigma$ *for some algebraically closed field of characteristic* 0.
(3) $\mathrm{ACF}_0 \models \sigma$.
(4) *There is* $N > 0$ *such that* $\mathrm{ACF}_p \models \sigma$ *for all* $p > N$.
(5) $\mathrm{ACF}_p \models \sigma$ *for infinitely many primes* p.
(6) *There are infinitely many primes* p *such that there is a model of* ACF_p *in which* σ *holds.*

PROOF. Equivalence of $(1), (2), (3)$ is just completeness of ACF_0, and equivalence of (5) and (6) is just completeness of ACF_p.

$((3) \Rightarrow (4))$ Suppose $\mathrm{ACF}_0 \models \sigma$. Then $\mathrm{ACF}_0 \cup \{\sigma\}$ has no model and by Compactness Theorem $\Gamma \cup \{\neg\sigma\}$ has no model for a finite subset of ACF_0. Then $\Gamma \models \sigma$ and for large enough p we have $\mathrm{ACF}_p \models \Gamma$. Therefore $\mathrm{ACF}_p \models \sigma$ for large enough p.

$((4) \Rightarrow (5))$ This is clear.

$((5) \Rightarrow (3))$ Assume that $\mathrm{ACF}_p \models \sigma$ for all $p > N$. If it were the case that $\mathrm{ACF}_0 \not\models \sigma$, then $\mathrm{ACF}_o \models \neg\sigma$ since ACF_0 is complete. But then by $(3) \Rightarrow (4)$, we would have $\mathrm{ACF}_p \models \neg\sigma$ for large enough p, which contradicts with our assumption. So $\mathrm{ACF}_0 \models \sigma$. □

We now prove an abstract result, which will help us to prove a stronger local-global principle. We need to introduce two concepts for this result.

Let L be a language. An L-formula of the form $\forall x_1 \cdots \forall x_m \exists y_1 \cdots \exists y_n \phi$ where ϕ is a quantifier-free L-formula is called a $\forall\exists$-*formula*.

Let $\mathcal{M}_n$ be an L-structure for each $n > 0$ such that $\mathcal{M}_m \subseteq \mathcal{M}_n$ for $m \leq n$. In this case we say that $(\mathcal{M}_n)_{n>0}$ is a *chain of L-structures*. When $(\mathcal{M}_n)_{n>0}$ is a chain, then the union $\bigcup_{n>0} M_n$ can be endowed with an L-structure in a natural way; we shall denote it as $\bigcup_{n>0} \mathcal{M}_n$.

PROPOSITION 7.4. *Let $(\mathcal{M}_n)_{n>0}$ be a chain and let σ be a $\forall\exists$-formula such that $\mathcal{M}_n \models \sigma$ for all $n > 0$. Then $\bigcup_{n>0} \mathcal{M}_n \models \sigma$.*

PROOF. Exercise. □

This result has many other applications, but we do not elaborate on them.

THEOREM 7.5. *Let σ be a $\forall\exists$-sentence in the language L_{r} of rings. If σ holds in every finite field, then* $\mathrm{ACF} \models \sigma$.

PROOF. Recall that for any prime p we have $\overline{\mathbb{F}}_p = \bigcup_{n>0} \mathbb{F}_{p^n}$. Therefore $\overline{\mathbb{F}}_p \models \sigma$ by Proposition 7.4. Using Theorem 7.3, we get ACF $\models \sigma$. □

This gives another proof of Ax's Theorem (namely Theorem 5.6): For each $d \geq 0$ and $n > 0$, there is an L_{r}-term $t_{dn}(x_1, \ldots, x_m, y_1, \ldots, y_n)$ such that for any field K any polynomial in indeterminates $Y_1, \ldots, Y_n$ of total degree at most d is of the form $t_{dn}(a_1, \ldots, a_m, Y_1, \ldots, Y_n)$ for some $a_1, \ldots, a_n \in K$. Using this term, we may express that *"every injective polynomial map $\mathbb{C}^n \to \mathbb{C}^n$ of total degree d is surjective"* in the language L_{r} as a $\forall\exists$ the sentence, say σ_{dn}. We would like to show that $\mathbb{C} \models \sigma_{dn}$. By Theorem 7.5, we even have ACF $\models \sigma_{dn}$ since every finite field satisfies σ_{nd}.

CHAPTER 3

o-minimal Structures

1. Ordered Structures

In this chapter all the languages contain a binary relation symbol $<$. Moreover, in every structure, the interpretation of this symbol will be a dense linear ordering of that structure with no end points. In other words the reduct of every structure to the language $\{<\}$ will be a model of DLO. As a result all the theories are extensions of DLO.

We show structures as $\mathcal{M} = (M, <, \dots,)$ and call them *ordered structures*. For notational reasons we define $M_\infty := M \cup \{-\infty, \infty\}$ and we order it in the most natural way: $-\infty$ is smaller than all the elements of M and ∞ is larger than all the elements of M. We may form intervals (a, b), where $a, b \in M_\infty$, and such intervals provide an open basis for a topology on M. In other words we endow M with the topology whose open sets are arbitrary unions of intervals. We also put product topology on M^n for each $n > 0$. Therefore a basis for the topology on M^n consists of boxes as below:

$$B(\vec{a}, \vec{b}) := \{\vec{x} \in M^n : a_i < x_i < b_i \text{ for } i = 1, \dots, n\},$$

where $\vec{a}, \vec{b} \in M^n$ with $a_i < b_i$ for all i.

We reserve the word interval for open intervals as above. Other kinds of intervals will be referred to as *closed intervals* or *half open/closed intervals*.

Given subset X of M^n, we make the following usual definitions of *closure* and *interior*:

$$y \in \mathrm{cl}(X) \Leftrightarrow \text{every open } U \text{ containing } y \text{ contains a point of } X,$$

$$y \in \mathrm{int}(X) \Leftrightarrow \text{there is an open } U \subseteq X \text{ containing } y.$$

We also define the *boundary* and the *frontier* of a set X:

$$\mathrm{bd}(X) := \mathrm{cl}(X) \setminus \mathrm{int}(X), \quad \mathrm{fr}(X) := \mathrm{cl}(X) \setminus X.$$

These definitions are totally topological; meaning that they are generally given for abstract topological spaces. In our case they can be expressed in terms of intervals. For instance, for $X \subseteq M$ we have

$$y \in \mathrm{bd}(X) \Leftrightarrow \text{every interval containing } y \text{ meets both } X \text{ and } M \setminus X.$$

PROPOSITION 1.1. *Suppose that $X \subseteq M^n$ is definable in $\mathcal{M} = (M, <, \dots)$. Then* $\mathrm{cl}(X)$, $\mathrm{int}(X)$, $\mathrm{bd}(X)$, *and* $\mathrm{fr}(X)$ *are also definable in $\mathcal{M}$.*

PROOF. First, note that it is enough to show that $\mathrm{cl}(X)$ and $\mathrm{int}(X)$ are definable.

Let $\phi(\vec{x})$ define X. Then $\mathrm{cl}(X)$ is defined by the following formula:

$$\forall y_1 \cdots \forall y_n \forall z_1 \cdots \forall z_n (\bigwedge_{i=1}^{n} y_i < x_i < z_i \to \exists t_1 \cdots \exists t_n (\phi(\vec{t}) \wedge \bigwedge_{i=1}^{n} y_i < t_i < z_i))$$

We leave writing down the formula defining $\mathrm{int}(X)$ as an exercise.

□

PROPOSITION 1.2. *Let $X \subseteq Y \subseteq M^n$ be definable in an ordered structure $\mathcal{M}$. Suppose that X is open in Y; that is $X = Y \cap U$ for some open subset U of M^n. Then $X = V \cap Y$ where $Y \subseteq M^n$ is open and definable in $\mathcal{M}$.*

PROOF. Let $\phi(\vec{x})$ and $\psi(\vec{x})$ define X and Y respectively. The set V defined by the following $\vec{x}$-formula works:

$$\exists \vec{a} \exists \vec{b} (\vec{x} \in B(\vec{a}, \vec{b}) \wedge \forall \vec{z} ((\vec{z} \in B(\vec{a}, \vec{b}) \wedge \psi(\vec{z})) \to \phi(\vec{z}))).$$

□

2. Definition and Basics

DEFINITION 2.1. An ordered structure $\mathcal{M} = (M, <, \dots)$ is *o-minimal* if every definable subset of M is a finite union of points and intervals.

We first observe some obvious topological facts about o-minimal structures.

PROPOSITION 2.2. *Let $\mathcal{M} = (M, <, \dots)$ be o-minimal.*

1. *For every definable $X \subseteq M$, there is $a \in M_\infty$ such that $a \leq x$ for all $x \in X$ and it is the maximal such element in the sense that if $b \leq x$ for all $x \in X$, then $b \leq a$. We call this element as the* infimum of X *and it is denoted as* $\inf(X)$.
2. *For every definable $X \subseteq M$, there is $a \in M_\infty$ such that $x \leq a$ for all $x \in X$ and it is the minimal such element in the sense that if $x \leq b$ for all $x \in X$, then $a \leq b$. We call this element as the* supremum of X *and it is denoted as* $\sup(X)$.

Consider the example $(\mathbb{Q}, <)$; we will show in a bit that this structure is indeed o-minimal. No interval in this structure is connected: take $t \in \mathbb{R} \setminus \mathbb{Q}$ from the interpretation of that interval in $\mathbb{R}$. Then we can separate the original interval into two parts as *left* and *right* of t. The point here is that this separation is not done in a definable way in $(\mathbb{Q}, <)$ and this motivates the next definition.

DEFINITION 2.3. Let X be a set definable in an o-minimal structure $\mathcal{M}$. We say that X is *definably connected* if there are no nonempty open subsets U, V of X that are definable in $\mathcal{M}$ such that $U \cap V = \emptyset$ and $U \cup V = X$.

This definition makes sense in any ordered structure, but from now on most of our structures are o-minimal. So we just defined it in that case.

Note that intervals are indeed definably connected in an o-minimal structure. This is not correct in general. For instance, consider the structure $(\mathbb{Q}, <, (0, \sqrt{2}) \cap \mathbb{Q})$, where $(0, \sqrt{2}) \cap \mathbb{Q}$ is the interpretation of a unary relation symbol. Then $(0, 2) \cap \mathbb{Q}$ is not definably connected.

It is easy to see that all the definably connected subsets of M in an o-minimal $\mathcal{M}$ are the empty set, singletons, and all kinds of intervals. Hence we could say that definable subsets of M have finitely many definably connected components; here, as usual, *definably connected component* means a definably connected subset that is maximal with respect to set inclusion.

A question rises: Let $\mathcal{M}$ be o-minimal and let $\mathcal{N}$ be an elementary extension of $\mathcal{M}$. Can a definable subset of M have more definably connected components in $\mathcal{N}$ than in $\mathcal{M}$? As a matter of fact, it is not even clear whether $\mathcal{N}$ is o-minimal. So perhaps a definable subset of M has infinitely many definably connected components in $\mathcal{N}$. That does not happen and we shall show it later. In other words, we shall show that being o-minimal is expressible in a first-order way.

In this chapter all ordered structures are o-minimal as long as it is not stated otherwise.

We record some facts about definable connectedness.

PROPOSITION 2.4. *Let $X, Y \subseteq M^n$ be definable in $\mathcal{M}$. Suppose that X is definably connected and that $X \subseteq Y \subseteq \mathrm{cl}(X)$. Then Y is also definably connected.*

PROOF. Suppose that $Y = U \cup V$ for some disjoint definable open subsets U, V. Then $X \cap U$ and $X \cap V$ are also definable open subsets of X and $X = (X \cap U) \cup (X \cap V)$. Then one of $X \cap U$ or $X \cap V$ must be empty. If, say, $X \cap U = \emptyset$, then X is contained in the closed set $M^n \setminus U$. This is a contradiction as $Y \subseteq \mathrm{cl}(X)$. □

PROPOSITION 2.5. *Let X, Y be definably connected subsets of M^n with $X \cap Y \neq \emptyset$. Then $X \cup Y$ is also definably connected.*

PROOF. Exercise. □

PROPOSITION 2.6. *Let $f : M^m \to M^n$ be a definable continuous map and let $X \subseteq M^m$ be definably connected. Then $f(X)$ is also definably connected.*

PROOF. Suppose that $f(X) = U \cup V$ where U, V are nonempty open definable subsets of $f(X)$. Then $X \subseteq f^{-1}(U) \cup f^{-1}(V)$. Therefore $U' := X \cap f^{-1}(U)$ and $V' := X \cap f^{-1}(V)$ are open subsets of X and $X = U' \cup V'$. Therefore $U' \cap V'$ is not empty and hence $U \cap V$ is not empty. □

COROLLARY 2.7 (Definable Intermediate Value Property). *Suppose that $f : [a, b] \to M$ is a definable continuous map. Then for every $y \in M$ that is between $f(a)$ and $f(b)$, there is $x \in [a, b]$ with $f(x) = y$.*

3. o-minimal Groups, Rings, and Fields

An *ordered group* is a group $(G, \cdot)$ equipped with a linear ordering $<$ such that for every x, y, z from G if $x < y$, then $xz < yz$ and $zx < zy$. We say that the triple $(G, \cdot, <)$ is an ordered group. Examples of order groups are $(\mathbb{Z}, +, <)$, $(\mathbb{Q}, +, <)$, $(\mathbb{R}, +, <)$, $(\mathbb{R}^{>0}, \cdot, <)$, etc.

Note that ordered groups are torsion-free since $1 < g$ implies that $g^n < g^{n+1}$ for all $n > 0$.

Let $\mathcal{G} = (G, \cdot, <, \dots)$ be an o-minimal structure[1] such that $(G, \cdot, <)$ is an ordered group, we simply say that $\mathcal{G}$ is an *o-minimal group*. Note that models of DLO are infinite, hence o-minimal groups are nontrivial.

PROPOSITION 3.1. *Suppose that $(G, \cdot, <, \dots)$ is an o-minimal group. Then the only definable subgroups[2] of G are the trivial subgroup and G itself.*

PROOF. Let H be a definable subgroup of G. Suppose that H is not trivial.

We first show that H needs to be convex: for every $x, y \in H$ and $z \in (x, y)$, we have $z \in H$. If that is not the case, then there are $h \in H$ and $g \in G \setminus H$ such that $1 < g < h$. Then $h^n < gh^n < h^{n+1}$ for all $n \leq 0$. Since $gh^n \notin H$ we see that H needs to have infinitely many definably connected components, which is a contradiction.

Let $g = \sup(H)$ and let $h \in H$ be such that $1 < h < g$. Then $1 < h^{-1}g < g$ and hence $h^{-1}g \in H$ by convexity. However, then we get $g = hh^{-1}g \in H$ and $g < hg$, contradicting the definition of g. Therefore $g = \infty$ and $H = G$ as required.

□

This proposition has so many consequences about the structure of o-minimal groups. For instance, noting that the centralizer $C_G(a)$ of a given element $a \in G$ is definable and nontrivial, we see that G needs to be abelian. Because of this, we start to denote the group operation

[1] So the language contains a binary function symbol $\cdot$.

[2] By *definable subgroup*, all we mean is a definable subset that happens to be a subgroup as well.

by $+$ from now on. Note that for $n > 0$, the elements of G divisible by n forms a nontrivial subgroup of G. Hence G is divisible. Putting these together we see that if $\mathcal{G} = (G, +, <, \dots)$ is an o-minimal group, then $(G, +, <)$ is a model of DOAG.

DEFINITION 3.2. An *ordered ring* is a ring $(R, +, \cdot)$ equipped with a linear ordering $<$ such that

(1) $(R, +, <)$ is an ordered group.
(2) $0 < 1$.
(3) For every $x, y, z \in R$, if $x > 0$ and $y < z$, then $xy < xz$.

Let's call element x of an ordered ring *positive*(*negative*) if $0 < x$ ($x < 0$); we denote the set of positive elements as $R^{>0}$. It follows that $R^{>0}$ is closed under multiplication and that the inverse of a positive invertible element is again positive. Clearly, a nonzero element is positive if and only if its additive inverse is negative. So $R = -R^{>0} \cup \{0\} \cup R^{>0}$. Note also that for every $x \neq 0$, the element x^2 is positive.

The ring of integers becomes an ordered ring with the usual ordering and the ring morphism $\mathbb{Z} \to R$; $n \mapsto n \cdot 1$ is increasing. In particular, it is an embedding and hence we may consider $\mathbb{Z}$ as a subring of any ordered ring R.

An ordered ring that happens to be a field is called an *ordered field*. Note that the positive elements of an ordered field becomes an ordered group. Hence it is torsion-free. For instance, the field $\mathbb{C}$ of complex numbers cannot be linearly ordered in a way that it becomes an ordered field.

If $\mathcal{K} = (K, +, \cdot, <, \dots)$ is an ordered structure expanding an ordered field, then all polynomial functions are definable in $\mathcal{K}$. If $\mathcal{K}$ is also o-minimal, then polynomial functions being continuous definable functions they satisfy the Intermediate Value property: if $p \in R[X]$ and $a < b$, then for any d between $f(a)$ and $f(b)$, there is $c \in [a, b]$ with $f(c) = d$. Fields satisfying this property are called *real closed*. For an alternative (and more common) definition and more detailed study of real closed fields, we refer the reader to Lang's Algebra; [**17**].

For the above argument, we do not really need K to be a field. In a similar way to o-minimal groups being abelian, o-minimal rings are automatically fields.

4. Examples of o-minimal Structures

Most of our examples follow from the facts at the end of the previous chapter. Those facts are not that hard to prove once some model theoretic technology is developed. It is much harder to show that our last two examples are indeed o-minimal; both of them are quite important and famous results.

4.1. Dense linear orderings without end points. Let $\mathcal{M} = (M, <)$ be a model of DLO. We claim that $\mathcal{M}$ is o-minimal. For this we use Fact 6.1; namely that DLO has quantifier elimination. Note that $L_{\mathrm{o},M}$-terms[3] are just variables and constants due to the lack of function symbols. Therefore atomic $L_{\mathrm{o},M}$-formulas are the following:

$$x = y \quad x = c \quad c = d \quad x < y \quad x < c \quad c < x \quad c < d,$$

where x, y are variables and c, d are constants from M; we also have $c = x$, but using the fact that $=$ is always interpreted as equality, we always overlook this kind of distinctions.

One could analyze all the definable sets using this, however our current interest is only in the unary definable sets. so let's fix a variable, say x. So the sets defined by atomic formulas above with the variable y replaced by x are:

$$M \quad \{c\} \quad \text{either } \emptyset \text{ or } M \quad \emptyset \quad (-\infty, c) \quad (c, \infty) \quad \text{either } M \text{ or } \emptyset.$$

By the quantifier elimination fact, we know that all definable subsets of M are Boolean combinations of these. It is easy to see that such sets are exactly finite unions of points and intervals as desired. Actually, putting these together with some observations from before, we see that a structure $\mathcal{M} = (M, <)$ is o-minimal if and only if it is a model of DLO.

More concrete examples would be $(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$. A less standard example could be constructed on $\mathbb{R} + \mathbb{R}T$, where T is a variable and the ordering extends the one on $\mathbb{R}$ by declaring $0 < T < r$ for all $r \in \mathbb{R}$. So

$$a + bT < c + dT \iff a < c \text{ or } (a = c \text{ and } b < d).$$

Therefore $(\mathbb{R} + \mathbb{R}T, <)$ is really isomorphic to $(\mathbb{R} \times \mathbb{R}, <)$ where the ordering is the lexicographic ordering. It is easy to see that this is not isomorphic to $(\mathbb{R}, <)$.

4.2. Divisible Ordered Abelian Groups. This class of examples consist of the models of DOAG; namely structures of the form $\mathcal{M} = (M, +, -, 0, <)$ where $(M, +, <)$ is an ordered group that is divisible. Recall that being an ordered group forces the group to be torsion-free and it is easy to see that divisibility provides that the ordering is dense. (Actually, 2-divisible would be enough.) We already know that an o-minimal group needs to be a model of DOAG. We are aiming to show that all such groups are o-minimal.

As in the previous example, let's start by observing the sets defined by atomic formulas. Then we could analyze all definable sets using Fact 6.3.

[3]Recall that given a language L and set A, L_A means the extension of L by one constant symbols for each element of A. In this case, the language itself already has a subscript, we write the constants next to that subscript.

Fix a model $\mathcal{M} = (M, +, -, 0, <)$ of DOAG. First note that up-to equivalence, $L_{\text{oab},M}$-terms in variables $x_1, \ldots, x_n$ are

$$k_1 x_1 + \cdots + k_n x_n + a$$

where $k_1, \ldots, k_n \in \mathbb{Z}$ and $a \in M$. Therefore up-to logical equivalence, atomic $L_{\text{oab},M}$-formulas are

$$k_1 x_1 + \cdots + k_n x_n + a = 0 \quad \text{and} \quad k_1 x_1 + \cdots + k_n x_n + a < 0.$$

Once again, we specialize to the case $n = 1$. So atomic $L_{\text{oab},M}$-formulas in one variable x are

$$kx = a \quad \text{and } kx < a.$$

for some integer k and $a \in M$.

If $k = 0$ and $a \neq 0$, then the first formula defines the empty set. If $k = 0$ and $a = 0$, then it defines M. Suppose $k \neq 0$. Then realization of the first formula is just the singleton $\{\frac{1}{k}a\}$. Now let's consider the second formula. If $k = 0$ and $0 < a$, then it defines M, and if $k = 0$ and $a \leq 0$, then it defines the empty set. So again we may assume $k \neq 0$. If $k > 0$, then the formula defines the interval $(-\infty, \frac{1}{k}a)$. If $k < 0$, then it defines the interval $(\frac{1}{k}a, \infty)$.

It is now clear that the Boolean combinations of atomic $L_{\text{oab},M}$-formulas are finite unions of points and intervals. Hence all definable sets are so by the quantifier elimination for DOAG, and $\mathcal{M}$ is o-minimal.

Remember that we discussed the models of DAG being vector spaces over $\mathbb{Q}$. In particular, L_{ab}-reducts of models of DOAG are also vector spaces over $\mathbb{Q}$. However, they are a little bit more than that. Namely, they are *ordered vector spaces* over the ordered field $\mathbb{Q}$. This means that $\mathbb{Q}$ considered as an ordered field, the scaler multiplication by its positive elements preserves the order of M. The theories DOAG and the theory (in the appropriate language) of ordered vector spaces over $\mathbb{Q}$ are so-called *bi-interpretable*.[4] The second theory is more open to generalizations. We could fix any ordered field K and we let $L_{K\text{-ovs}}$ be the language expanding L_{oab} by a unary function symbol s_a for each element a of K. Then we could define the $L_{K\text{-ovs}}$-theory of "ordered vector spaces over K". Each model of that theory turns out to be o-minimal; for details see the seventh section of the first chapter of van den Dries' book ([**8**]).

4.3. Real Closed Fields. Recall that an ordered field is *real closed* if it satisfies the Intermediate Value Property for polynomial functions. Another characterization is that any polynomial of odd order has a root. Note that this latter property has nothing to do with

[4]We do not define this notion precisely as we shall not use it again, but the reader might have a few guesses about what it should mean.

the ordering; so it could be expressed in the language of rings. However, the theory would not have quantifier elimination in that language. So we consider the models of L_{or}-theory RCF.

In order to show that any model of RCF, we analyze the formulas. Let $\mathcal{K} = (K, +, -, \cdot, 0, 1, <)$ be a model of RCF. Up-to equivalence of terms, $L_{\text{or},K}$-terms are polynomials. More precisely, each $L_{\text{or},K}$-term whose variables are among $x_1, \ldots, x_n$ is equivalent to an element of $K[x_1, \ldots, x_n]$ considered as a term. As a result atomic $L_{\text{or},K}$-formulas are

$$p(x_1, \ldots, x_n) = 0 \quad \text{and} \quad p(x_1, \ldots, x_n) < 0.$$

By quantifier elimination result Fact 6.4, we know that all definable sets are Boolean combinations of sets defined by these formulas. Such formulas are generally closed *semi-algebraic* sets. So the Tarski-Seidenberg result could be interpreted as saying that definable subsets of real closed fields are exactly semi-algebraic sets.

Atomic formulas in one variable x are $p(x) = 0$ and $p(x) < 0$. The first one defines either a finite set or the whole K. It could happen that p is always non-negative valued. In that case the second formula defines the empty set. If p always gets negative values, then the second formula defines K. So suppose that p has both positive and negative values. By the Intermediate Value Property p has roots and the changes of sign could only happen at zeros of p. Therefore $p(x) < 0$ defines a finite union of intervals. So semi-algebraic subsets of K are finite unions of points and intervals and $\mathcal{K}$ is o-minimal.

4.4. Real Exponential Field. Let $L_{\exp} := L_{\text{or}} \cup \{\exp\}$, where exp is a unary function symbol. We consider the $L_{\exp}$-structure

$$\mathcal{R}_{\exp} = (\mathbb{R}, +, -, \cdot, 0, 1, <, \exp),$$

where exp is the usual exponential function.

In this example, we just state the result proven by A. Wilkie in [**27**], building on results of Gabrielov ([**11**]).

THEOREM 4.1. *The theory of $\mathcal{R}_{\exp}$ is model complete.*

This is related to the o-minimality of $\mathcal{R}_{\exp}$ as follows.

Homework 14. Suppose that $\mathcal{R} = (\mathbb{R}, <, \ldots)$ is an expansion of the ordered reals that has a model complete theory and that every quantifier-free definable subset of $\mathbb{R}^n$ (for any n) has finitely many definably connected components. Then $\mathcal{M}$ is o-minimal.

A theorem of Khovanskii ([**15**]) guarantees that $\mathcal{R}_{\exp}$ has the property that every quantifier-free definable set has finitely many definably connected components. So Wilkie's theorem coupled with the homework above gives that $\mathcal{R}_{\exp}$ is o-minimal.

4.5. Restricted Analytic Functions. Let $\mathcal{F}$ be the class of functions $f|_{[0,1]^n}$ where $f : V \to \mathbb{R}$ is an analytic function on an open set V containing $[0,1]^n$. Let $\mathcal{R}_{\text{an}}$ be the expansion of the real field by elements of $\mathcal{F}$. Using the paper [**11**] mentioned above, one may deduce that $\mathbb{R}_{\text{an}}$ is model complete. Then using the Khovanskii result from [**15**] we again get that $\mathcal{R}_{\text{an}}$ is o-minimal.

This could be obtained from the paper [**6**] of Denef and van den Dries as well, where they prove that $\mathcal{R}_{\text{an}}$ has quantifier elimination in a slightly richer language.

4.6. Restricted Analytic Functions with Global Exponentiation. We may put the previous two examples together. Namely, we may expand $\mathcal{R}_{\text{an}}$ by adding the function exp to get the structure $\mathcal{R}_{\text{an,exp}}$. It is shown by van den Dries and Miller in [**10**], that $\mathcal{R}_{\text{an,exp}}$ is also o-minimal.

CHAPTER 4

Cell Decomposition

In this chapter, we follow van den Dries' book ([**8**]) very closely in terms of proofs. The order of topics is slightly different.

In what follows $\mathcal{M} = (M, \dots)$ is an o-minimal structure.

1. Cells

Let $f : X \to M$ and $g : X \to M$ be definable in $\mathcal{M}$ such that $f(x) < g(x)$ for all $x \in X$. We let (f, g) denote the following set:

$$\big\{(x, y) \in M^{n+1} : x \in X \text{ and } f(x) < y < g(x)\big\}.$$

We extend this definition by allowing f to be $-\infty$, and g to be ∞ in a natural way.

Definition 1.1. We define *cells* in M^n by induction on $n > 0$.

Cells in M: For any $x \in M$, the singleton $\{x\}$ is a cell, and for any $x, y \in M$ with $x < y$, the interval (x, y) is a cell. Nothing else is a cell in M.

Cells in M^{n+1}: Suppose that cells in M^n are already defined. The cells in M^{n+1} are the following:

- $\Gamma(f)$ for some definable continuous function $f : C \to M$ where C is a cell in M^n
- (f, g) where $f : C \to M$ and $g : C \to M$ are definable continuous functions on a cell C in M^n with $f(x) < g(x)$ for all $x \in C$.
- $(-\infty, g)$ for some definable continous function $g : C \to M$ where C is a cell in M^n.
- (f, ∞) for some definable continuous function $f : C \to M$ where C is a cell in M^n.

Right away, we can state a weak version of the fundamental theorem.

Theorem 1.2 (Weak Cell Decomposition). *Let $f : X \to M$ be definable in $\mathcal{M}$ where $X \subseteq M^n$. Then there are cells $C_1, \dots, C_t$ in M^n with the following properties:*

(1) *$C_i \cap C_j = \emptyset$ for all $i \neq j$.*
(2) *$X = C_1 \cup \cdots \cup C_t$.*
(3) *$f|_{C_i}$ is continuous for all i.*

COROLLARY 1.3. *Any definable set $X \subseteq M^n$ can be partitioned into finitely many cells; that is there are pairwise disjoint cells $C_1, \dots, C_t$ in M^n such that $X = C_1 \cup \cdots \cup C_t$.*

One can easily generalize this corollary to the following.

COROLLARY 1.4. *Let $X_1, \dots, X_k$ be subsets of M^n definable in $\mathcal{M}$. Then there is a partitioning $C_1 \cup \cdots \cup C_k$ of $X_1 \cup \cdots \cup X_k$ into cells such that each X_j is a finite union of some of the cells C_i.*

2. More on Cells

For the Cell Decomposition Theorem to be useful, it is necessary that cells have some good properties. They do, and we collect some of those in this section. We state some of them without a proof, because it is either easy enough to be left as an exercise, or a little bit too technical. See van den Dries' book for the details.

It is clear by construction that the projection of a cell in M^{n+1} onto the first n-coordinates is again a cell. It is actually not hard to see that if $\pi : M^{m+n} \to M^m$ is projection to the first m coordinates and $C \subseteq M^{m+n}$ is a cell, then $\pi(C)$ is still a cell.

The cells that happen to be open are the ones whose construction does not involve graphs of functions. We trust the understandability of this vague statement and not elaborate more on it. If a cell is not open, then they indeed have empty interior. However, for every cell $C \subseteq M^n$, there is a coordinate projection $\pi : M^n \to M^k$ such that $\pi|_C$ is a homeomorphism of C with its image, which is an open cell.

Recall that a subset of a topological space is *locally closed* if it is the intersection of an open set and a closed set. The next homework gives a few conditions equivalent to local closedness.

Homework 15. Let Y be a subest of a topological space X. Show that the following conditions are equivalent:

(1) Y is locally closed.
(2) Y is open in a closed set.
(3) Y is open in its closure.
(4) $\mathrm{cl}(Y) \setminus Y$ is closed in X.
(5) for every $y \in Y$, there is an open subset U of X such that $Y \cap U$ is closed in U.

(Note that the second condition is just the restatement of being locally closed.)

PROPOSITION 2.1. *Each cell is locally closed.*

PROOF. We proceed by induction on n to show that each cell in M^n is locally closed. The case $n = 1$ is clear. So suppose that each cell in M^n is locally closed and let C be a cell in M^{n+1}. Then $\pi(C) \subseteq M^n$ is

locally closed, where π is the projection on the the first n coordinates. So $\mathrm{cl}(\pi(C)) \setminus \pi(C)$ is closed, say K.

First consider the case, that $C = \Gamma(f)$ for some definable continuous map $f : \pi(C) \to M$. It is easy to check that

$$\mathrm{cl}(C) \setminus C = \mathrm{cl}(C) \cap (K \times M).$$

Hence $\mathrm{cl}(C) \setminus C$ is closed.

Now let $C = (f, g)$ for definable continuous maps $f, g : \pi(C) \to M$. In this case, $\mathrm{cl}(C) \setminus C$ equals the closed set

$$\mathrm{cl}(C) \cap (K \times M \cup \mathrm{cl}(\Gamma(f)) \cup \mathrm{cl}(\Gamma(g)).$$

This argument can also be used for the cases where f, g are allowed to be $-\infty$ and ∞. □

PROPOSITION 2.2. *Each cell is definably connected.*

PROOF. Once again, we prove that cells in M^n are definably connected by induction on n. The case $n = 1$ is clear as we know that intervals and points are definably connected. So let $C \subseteq M^{n+1}$ be a cell. Then the cell $\pi(C) \subseteq M^n$ is definably connected by the induction hypothesis.

If $C = \Gamma(f)$ for some continuous definable function : $f : \pi(C) \to M$, then by Proposition 2.6, $C = f(\pi(C))$ is also definably connected.

Now let $C = (f, g)$, for continuous definable functions $f, g : \pi(C) \to M$. Then for each $x \in \pi(C)$, the fiber $\pi^{-1}(x) \cap C = \{x\} \times (f(x), g(x))$ is homeomorphic to an interval and thus is definably connected. Hence if $C = U \cup V$ with disjoint nonempty open definable U, V, then for any $x \in \pi(C)$ one of $U \cap \pi^{-1}(x) \cap C$ or $V \cap \pi^{-1}(x) \cap C$ is empty. This means that $\pi(U) \cap \pi(V) =$. Since projections are open maps we also have that $\pi(U)$ and $\pi(V)$ are open. But then this show that $\pi(C)$ is not definably connected. Therefore C is definably connected. □

3. Cell Decomposition

Weak Cell Decomposition Theorem (WCD) above reflects the idea of the Cell Decomposition Theorem (CD). It is just that CD is a fine tuning of WCD. Not only that this makes it more applicable, but also it is easier to prove. This is because, we proceed by induction and stronger inductive hypothesis is more useful.

A *decomposition* of M is a partition of M into finitely many cells. Such a partition has be of the following form:

$$M = (-\infty, a_1) \cup (a_1, a_2) \cup \cdots \cup (a_{m-1}, a_m) \cup (a_m, \infty) \cup \{a_1, \ldots, a_m\}$$

for some $a_1 < \cdots < a_m$. (We think of the case $M = (-\infty, \infty)$ as the $m = 0$ case.)

Now let $n > 0$. A *decomposition* of M^{n+1} is a finite partition of M^{n+1} into cells such that the projection onto the first n coordinates of cells in this partition forms a decomposition of M^n.

THEOREM 3.1 (Cell Decomposition Theorem). *Let $n > 0$.*

- (CD_n) *For any collection $X_1, \ldots, X_t$ of definable subsets of M^n, there is a decomposition $\mathcal{C}$ of M^n such that for each $C \in \mathcal{C}$ and for each $i = 1, \ldots, t$ either $C \cap X_i = \emptyset$ or $C \subseteq X_i$.*
- (LC_n) *For any definable function $f : X \to M$ with $X \subseteq M^n$, there is a decomposition $\mathcal{C}$ of M^n partitioning X such that for each $C \in \mathcal{C}$, the function $f|_C$ is continuous.*

We prove this theorem by induction on n. Note that (CD_1) is almost the definition of o-minimality. The next proposition is a stronger version of (LC_1). We do not prove this here. There are nice topological arguments in the proof, which can be checked from van den Dries' book. There will be similar topological arguments in the rest of the proof of Cell Decomposition.

PROPOSITION 3.2 (Monotonicity Theorem). *Let $f : (a, b) \to M$ be a definable function. Then there is a decomposition*

$$M = (-\infty, a_1) \cup (a_1, a_2) \cup \cdots \cup (a_{m-1}, a_m) \cup (a_m, \infty) \cup \{a_1, \ldots, a_m\}$$

such that $f|_{(a_i, a_{i+1})}$ is continuous and it is strictly monotone if it is not constant.

Now let us assume (CD_1),...,(CD_n), (LC_1),...,(LC_n), and let's prove (CD_{n+1}) and (LC_{n+1}).

We start with the following fundamental result to be proved using the assumptions above and to be used in the proof of (CD_{n+1}) and (LC_{n+1}).

THEOREM 3.3 (Uniform Finiteness). *Let $X \subseteq M^{n+1}$ be definable with the property that for every $a \in M^n$, the fiber X_a is finite. Then there is a natural number $N = N(X)$ such that $|X_a| \leq N$ for all $a \in M$.*

The proof of this result will be through a series of lemmas. Let (UF_n) be the statement of the theorem for a fixed n and fix X as in the statement. We prove (UF_n) from (CD_1),...,(CD_n), (LC_1),...,(LC_n).

DEFINITION 3.4. A point $a \in M^n$ is called *X-good* if there is a definably connected open set $U \subseteq M^n$ containing a such that for all $(b, c) \in X$ with $b \in U$, there is an interval I containing c such that for every $d \in U$, there is a unique $e \in I$ with $(d, e) \in X$.

REMARKS. (1) If $a \notin \mathrm{cl}(\pi(X))$, then it is vacuously X-good. Similarly, if $a \in \mathrm{cl}(\pi(X)) \setminus \mathrm{int}(\pi(X))$, then a is not X-good. So non-trivial X-good points are in $\mathrm{int}(\pi(X))$.

(2) Suppose that a is X-good witnessed by neighborhood U. Then for every $(b, c) \in X$ with $b \in U$, there are an interval I around c and a definable map $f : U \to M$ such that $X \cap (U \times I) = \Gamma(f)$. By using (LC_n) and possibly making U smaller, we may also assume that f is continuous.
(3) In the definition of X-good, we may replace the phrase 'definably connected open set ' by the word 'box'. This means that that seemingly stronger definition is not really stronger.
(4) The set $G_X \subseteq M^n$ of X-good points is definable.

LEMMA 3.5. *Suppose that $a \in M^n$ is X-good with $|X_a| = k > 0$. Then there exist a definably connected open U containing a and continuous definable functions $f_1, \ldots, f_k : U \to M$ such that*

$$X \cap (U \times M) = \Gamma(f_1) \cup \cdots \cup \Gamma(f_k).$$

Moreover, after reordering, we have $f_1 < f_2 < \cdots < f_k$.

PROOF. Let the elements of X_a be $b_1 < \cdots < b_k$. Also let U be as in the definition of X-goodness. Then there are intervals $I_1, \ldots, I_k$ around $b_1, \ldots, b_k$ and continuous definable functions $f_1, \ldots, f_k : U \to M$ with $X \cap (U \times I_i) = \Gamma(f_i)$ for each i. In particular, $b_i = f_i(a)$. We claim that these functions work.

CLAIM. *For every i, j, the set $\{c \in U : f_i(c) = f_j(c)\}$ is open.*

PROOF. Suppose this set is nonempty and let $f_i(c) = f_j(c)$. Then $f_j(c)$ is in the open set $f_j^{-1}(I_i)$. By definition $X \cap (U \times I_i) = \Gamma(f_i)$. So $f_i = f_j$ on $f_j^{-1}(I_i)$, finishing the proof of the claim. □

It is clear that the sets $\{c \in U : f_i(c) < f_j(c)\}$ and $\{c \in U : f_i(c) > f_j(c)\}$ are open. However, U is the union of these three sets and hence by definable connectedness, it equals one of them. Since $b_i < b_j$ for $i < j$, we see that $f_i < f_j$ on U.

Now let $(c, d) \in X \cap (U \times M)$. Then there is a continuous definable $f : U \to M$ such that $d = f(c)$. Also $f(a) = b_i$ for some i. Then the argument above gives $f = f_i$ on U. □

LEMMA 3.6. *Suppose that $Y \subseteq M^n$ is a definably connected set, whose all points are X-good. Then there are continuous definable functions $f_1 < \cdots < f_k$ on Y such that $X \cap (Y \times M) = \Gamma(f_1) \cup \cdots \cup \Gamma(f_k)$.*

PROOF. The arguments from the proof of Lemma 3.5 shows that for every $k \in \mathbb{N}$, the set $\{c \in M^n : |X_c| = k\}$ is a both closed and open. So by definable connectedness of Y, there is k such that each fiber over elements of Y has k elements. Then $X \cap (Y \times M)$ is locally a union of k many graphs of continuous functions. By using Lemma 3.5 once again, we see that that happens globally. □

LEMMA 3.7. *Every open cell in M^n has an X-good point.*

PROOF. Left as an exercise for now. But let's keep in mind that this uses both (CD_n) and (LC_n). □

PROOF OF THEOREM 3.3. Using (CD_n) take a decomposition of M^n partitioning G_X. So each cell in this decomposition either disjoint from G_X or is included in it. Let C be an open cell from this decomposition. Then by Lemma 3.7, $C \cap G_X$ is not empty, hence $C \subseteq G_X$ and we are done by Lemma 3.6.

Now let C be a cell from the decomposition that is not open. Then there is a coordinate projection π_C that is a homeomorphism of C with an open cell in M^m. Suppose $X \cap (C \times M)$ is nonempty and consider the map $p : X \cap (C \times M) \to M^{m+1}$ defined as $p(x, y) = (\pi_C(x), y)$. Now apply the arguments for open cells with X replaced by the definable set $p(X \cap (C \times M))$.[1] □

4. Proof of Cell Decomposition

Remember that we assume (CD_1),...,(CD_n), (LC_1),...,(LC_n).

PROOF OF (CD_{n+1}). Let $X_1, \ldots, X_t \subseteq M^{n+1}$ be definable and put

$$B := \{(x, r) \in M^{n+1} : r \in \mathrm{bd}((X_i)_x), \text{ for some } i = 1, \ldots, t\}.$$

Note that B_x is finite for all $x \in M^n$. Therefore by Theorem 3.3, there is $N \geq 0$ such that B_x has at most N elements for all $x \in M^n$. For $j = 0, \ldots, N$ let D_j be the set of $x \in M^n$ such that $|B_x| = j$, and define functions $f_{j1}, \ldots, f_{jj}$ on D_j such that for all $x \in D_j$ we have

$$B_x = \{f_{j1}(x), \ldots, f_{jj}(x)\} \text{ with } f_{j1}(x) < \cdots < f_{jj}(x).$$

Also for $i = 1, \ldots, t$, $1 \leq k \leq j \leq N$ define the sets

$$E_{ijk} := \{x \in D_j : f_{jk}(x) \in (X_i)_x\},$$

$$F_{ijk} := \{x \in D_j : (f_{jk}(x), f_{j(k+1)}(x)) \subseteq (X_i)_x\}.$$

Now using (CD_n), take a decomposition of M^n partitioning all D_j, E_{ijk}, F_{ijk}, using also (LC_n), we may assume that each f_{jk} is continuous on the cells of that decomposition.

Now it is easy to check that the following cells of the form $\Gamma(f_{jk}|_C)$ and $(f_{jk}|_C, f_{j(k+1)}|_C)$ where C is a cell from the decomposition above form a decomposition of M^{n+1} partitioning $X_1, \ldots, X_t$. □

[1] In this argument $m = \dim(C) = 0$ is possible. That case can be handled separately since there are finitely many such cells. So no need to project down to M^0.

PROOF OF (LC_{n+1}). Let $f : X \to M$ be a definable function, where $X \subseteq M^{n+1}$. Using (CP_{n+1}), we may assume that X is a cell, and it suffices to show that there are definable subsets $X_1, \ldots, X_t$ partitioning X such that f is continuous on each X_i.

First suppose that X is not open. Then take a projection π of M^{n+1} onto M^k with $k \leq n$, which is a homeomorphism on X. Now $f \circ \pi^{-1}$ is a map on $\pi(X)$. Then by (LC_k), we have a decomposition of M^k partitioning $\pi(X)$ such that $f \circ \pi^{-1}$ is continuous on each cell of this decomposition. Carrying this to X via π^{-1} gives the desired partition of X.

Now assume that X is an open cell.

We say that f is *well-behaved* at a point (x, y) of X if there is a box $B \in M^n$ and an interval (a, b) such that $(x, y) \in B \times (a, b) \subseteq X$, for all $c \in B$ the function $f(c, -)$ is continuous and monotone on (a, b), and for all $z \in (a, b)$, the function $f(-, z)$ is continuous at x. Clearly, the points at which f is well-behaved form a definable subset of X; let's denote that set as X^*. We claim that any box $B \times (a, b)$ that is contained in X intersects X^*; hence X^* is dense in X. Given $x \in B$, there is a largest $\lambda(x) \in (a, b]$ such that the function $f(x, -)$ is continuous and monotone on $(a, \lambda(x))$. Note that this λ gives a definable function from B into M, hence there is a cell $C \subseteq B$ on which it is continuous. By shrinking C, there is $c \in (a, b)$ such that $\lambda(x) \geq c$ for all $x \in C$. Now for $y \in (a, c)$, the function $f(-, y)$ is continuous on a cell $C' \subseteq C$. Now it's easy to see that f is well-behaved at each (x, y) of X with $x \in C'$. This proves the claim.

Using (CP_{n+1}) take a decomposition of M^{n+1} partitioning both X and X^*. Consider a cell $C \subseteq X$ in this decomposition. Then $C \subseteq X^*$ by the claim above. So for all $(x, y) \in C$, the function $f(-, y)$ is continuous on at x and hence C is a union of boxes $D \times (a, b)$ witnessing the well-behavedness of of their points. In particular, $f(x, -)$ is continuous and monotone on such boxes D and $f(-, y)$ are continuous on each point. By a standard topological argument f is continuous on such $D \times (a, b)$, finishing the proof. □

5. An Application of Uniform Finiteness Theorem

We mentioned above that it is not clear whether o-minimality is first order expressible. This means that we do not know if an ordered structure elementarily equivalent to an o-minimal structure is itself o-minimal. We will prove this in a bit. First, some notations.

DEFINITION 5.1. Let $\mathcal{M}$ be an o-minimal structure, and take an element $s = (s_1, \ldots, s_t)$ of $\{0, 1\}^t$. We say that a definable subset X of M is *of the shape* s if it has t many components and the i^{th} component is of dimension s_i.

Note that a definable set $X \subseteq M^{1+n}$, the set of $\vec{a} \in M^n$ such that $X_{\vec{a}}$ is of shape s is a definable subset of M^n.

The proof of the following result is very instructive, so we leave it as a homework.

PROPOSITION 5.2. *Let $\mathcal{M} = (M, <, \dots)$ be an o-minimal structure, and let $X \subseteq M^{1+n}$ be a definable family. Show that there is $N = N(X) > 0$ such that for every $\vec{a} \in M^n$, the section $X_{\vec{a}}$ has at most N many definably connected components.*

PROOF. Exercise. □

PROPOSITION 5.3. *Let $\mathcal{M}$ be an o-minimal structure and let $\mathcal{N}$ be elementarily equivalent to $\mathcal{M}$. Then $\mathcal{N}$ is o-minimal.*

PROOF. Let $Y \subseteq N$ be definable in $\mathcal{N}$. Take a $\emptyset$-definable $X \subseteq N^{1+n}$ and $\vec{a} \in N^n$ such that $Y = X_{\vec{a}}$. We actually show that every section $X_{\vec{b}}$ is a finite union of points and intervals; hence in particular Y will be so.

Let $\phi(x, \vec{y})$ define X and let $X^{\mathcal{M}}$ be the definable subset of M^{1+n} defined by ϕ. Using Proposition 5.2, there is N such that for each $\vec{c} \in M^n$, the section $X_{\vec{c}}$ has at most N components. Let $S = \bigcup_{t \leq N} \{0,1\}^t$.

For $s \in S$, let $\psi_s(\vec{y})$ be the formula such that

$$\mathcal{M} \models \psi_s(\vec{c}) \iff X_{\vec{c}}^{\mathcal{M}} \text{ is of shape } s.$$

Then we have

$$\mathcal{M} \models \forall \vec{y} \bigvee_{s \in S} \psi_s(\vec{y}).$$

Therefore

$$\mathcal{N} \models \forall \vec{y} \bigvee_{s \in S} \psi_s(\vec{y}).$$

Therefore $Y = X_{\vec{a}}$ has shape s for some $s \in S$, and hence $X_{\vec{a}}$ is a finite union of points and intervals. □

CHAPTER 5

Dimension Theory for Definable Sets

1. Definition and Basic Properties

Here we develop the basic dimension theory for sets definable in an o-minimal structure. So fix an o-minimal structure $\mathcal{M}$; all concepts are with respect to this structure unless stated otherwise.

We fist define the dimension, $\dim(C)$ of a cell $C \subseteq M^n$ by induction on n.

$\underline{n = 1:}$ Dimension of a point is 0 and dimension of an interval is 1.

$\underline{n \rightsquigarrow n+1:}$ Let $f : C \to M$ and $g : C \to M$ be continuous definable maps defined on a cell $C \subseteq M^n$ such that $f < g$ on C. Then

$$\dim(\Gamma(f)) = \dim(C), \text{ and } \dim((f,g)) = \dim(C) + 1.$$

It is easy to see using inductive arguments that if $C_1 \subseteq C_2$ are cells in M^n, then

$$\dim(C_1) \leq \dim(C_2) \leq n.$$

This can be proven using Proposition 1.2 below. That proposition does not rest on this fact, hence we assume it with a clear conscience.

We define the *dimension*, $\dim(X)$ of a definable set X to be

$$\max\{\dim(C) : C \text{ is a cell, } C \subseteq X\}.$$

The remark on the dimensions of cells show that two definitions of dimension for cells agree. This is to say that for a cell C, there are no cells contained in C that are of larger dimension than C. For the same reason, it is also clear that if $X \subseteq Y$ are definable subsets of M^n, then

$$\dim(X) \leq \dim(Y) \leq n.$$

It would be more useful to define the dimension of a definable set X as the maximum among the dimensions of cells appearing in a cell decomposition of X. The problem with that definition would be proving that it is independent of the choice of the cell decomposition. We shall show that that definition is actually equivalent to ours after a series of results on dimension.

The first result is of topological nature.

LEMMA 1.1. *Let $C \subseteq M^n$ be an open cell and let $f : C \to M^n$ be an injective definable map. Then the image $f(C)$ contains an open set.*

PROOF. We prove this by induction on n. The $n = 1$ case follows easily from Monotonicity Theorem (Proposition 3.2). So let $n > 1$ and suppose the result holds for smaller natural numbers. Let $f(C) = C_1 \cup \cdots \cup C_t$ be a partitioning of $f(C)$ into cells. Then one of $f^{-1}(C_i)$ contains an open set, say $f^{-1}(C_1)$ does, and let B be a box in it. By Cell Decomposition, we may assume that f is continuous on B. We claim that $f(B)$ contains an open set. Suppose not, then C_1 is not open and let $\pi : M^n \to M^{n-1}$ be a projection whose restriction to C_1 is a injective. Also write $B = B' \times (a, b)$. Then for each $c \in (a, b)$, we have an injective definable map $g_c : M^{n-1} \to M^{n-1}$ given by $g_c(x) = \pi(f(x, c))$. Therefore by induction hypothesis $g_c(B')$ contains an open set, say U. Take $x \in B'$ with $g_c(x) \in U$. Then by continuity of f on B, for $c' \in (a, b)$ close enough to c we have $\pi(f(x, c')) \in U$. Hence for each such $c' \neq c$ there is $x' \in B'$ with $\pi(f(x, c')) = \pi(f(x', c))$. This contradicts the injectivity of $\pi \circ f$; finishing the proof. □

PROPOSITION 1.2. *Let X and Y be two definable sets in bijection through a definable function. Then* $\dim(X) = \dim(Y)$.

PROOF. Let $f : X \to Y$ be a definable bijection, and let $d = \dim(X)$ and $\dim(Y) = e$. We show that $d \leq e$, which will finish the proof by symmetry. So let C be a cell of dimension d contained in X. Using the usual projection trick, we may assume that C is an open set contained in M^d. Suppose that $e < d$ and let $D \subseteq Y$ be a cell of dimension e. Also let $\pi : M^m \to M^e$ be a projection that is injective on D. Then the map $g : M^d \to M^d$ defined by $g(x) = (\pi(f(x)), a, \ldots, a)$, where the element a appearing in the last $d - e$ coordinates is a randomly chosen element of M. It is clear that g is injective on C. However, this contradicts with Lemma 1.1 as $g(C)$ cannot contain an open set. □

Homework 16.

(1) Show that an interval is not in definable bijection with the union of two disjoint intervals.
(2) Suppose that $\mathcal{M}$ is an o-minimal expansion of a field. Show that an interval is in definable bijection with the union of two disjoint intervals and a point. Explain why we need the field structure.

According to the first part of this homework, the converse of this proposition is obviously false: Both an interval and the union of two intervals are of dimension 1. One might think that the problem is the number of connected components, but the second part of the homework says it is not the case. So dimension is a definable invariant, but it is not a complete invariant.

PROPOSITION 1.3. *Let X, Y be definable subsets of M^n. Then* $\dim(X \cup Y) = \max\{\dim(X), \dim(Y)\}$.

PROOF. Let $d = \dim(X \cup Y)$ and let $C \subseteq X \cup Y$ be of dimension d. Take a projection $\pi : M^n \to M^d$ that is injective on C and $\pi(C)$ is an open cell. Then $\pi(C) = \pi(C \cap X) \cup \pi(C \cap Y)$. Then one of $\pi(C \cap X)$ and $\pi(C \cap Y)$ contains an open set, hence an open box B. Therefore one of $C \cap X$ and $C \cap Y$ contains an open box of dimension d and thus is of dimension d. □

It follows from this result that dimension of a definable set is the maximal dimension of cells in any cell decomposition of X.

PROPOSITION 1.4. *Let $(X_{\vec{a}})_{\vec{a} \in Y}$ be a definable family of subsets of M^n and let $0 \leq d \leq n$, Then the set*

$$X(d) := \left\{\vec{a} \in Y : \dim(X_{\vec{a}}) = d\right\}$$

is definable. Moreover,

$$\dim\left(\bigcup_{\vec{a} \in X(d)} \{\vec{a}\} \times X_{\vec{a}}\right) = \dim(X(d)) + d.$$

PROOF. By the inductive construction of cells, for any cell $C \subseteq M^{n+k}$ and projection $\pi : M^n \to M^k$ onto the last k coordinates, we have that $\dim(\pi^{-1}(\vec{a}))$ is the same, say d, for any $\vec{a} \in \pi(C)$. Note that $\pi^{-1}(\vec{a}) \cap C = \{\vec{a}\} \times C_{\vec{a}}$. Hence, in the notations of the statement, the set $C(d) = \pi(C)$, and $C(e) = \emptyset$ for $e \neq d$. It is also clear that $\dim(C) = \dim(\pi(C)) + d$. Therefore the result is correct when X is a cell.

For the general case, let $X = C_1 \cup \cdots \cup C_t$ be a cell decomposition of X, and for $i = 1, \ldots, t$ let $d_i = \dim(\pi^{-1}(\vec{a}) \cap C_i)$ for any/some $\vec{a} \in \pi(C_i)$. By the previous paragraph, another way to express d_i is $\dim(C_i) - \dim(\pi(C_i))$.

Let $D_1, \ldots, D_s$ be collection of distinct cells among $\pi(C_1), \ldots, \pi(C_t)$ partitioning $\pi(X)$. For a fixed $j = 1, \ldots, s$ let

$$e_j := \max\{d_i : \pi(C_i) = D_j\}.$$

Then $X(d) = \bigcup_{e_j=d} D_j$ is a definable set, and we have[1]

$$\begin{aligned}
\dim\left(\bigcup_{\vec{a}\in X(d)} \{\vec{a}\} \times X_{\vec{a}}\right) &= \dim\left(\bigcup_{e_j=d}\bigcup_{\vec{a}\in D_j} \{\vec{a}\} \times X_{\vec{a}}\right) \\
&= \max_{e_j=d}\left\{\dim\left(\bigcup_{\vec{a}\in D_j} \{\vec{a}\} \times X_{\vec{a}}\right)\right\} \\
&= \max_{e_j=d}\left\{\dim\left(\bigcup_{\pi(C_i)=D_j}\bigcup_{\vec{a}\in D_j} \{\vec{a}\} \times (C_i)_{\vec{a}}\right)\right\} \\
&= \max_{e_j=d}\max_{\pi(C_i)=D_j}\{\dim(C_i)\} \\
&= \max_{e_j=d}\max_{\pi(C_i)=D_j}\{d_i + \dim(D_j)\} \\
&= \dim(X(d)) + d.
\end{aligned}$$

□

It is clear from this proposition that for any definable $X \subseteq M^{m+k}$, we have $\dim(X) = \max_{0\le d\le n}\{\dim(X(d)) + d\}$. It is also clear that $\dim(X \times Y) = \dim(X) + \dim(Y)$ for any definable sets X, Y.

Now let's take X to be the graph of a definable function $f : X \to M^k$. Then $X(d)$ is the set of $\vec{a} \in M^k$ such that $\dim(f^{-1}(\vec{a})) = d$. Thus assuming that $X(d) = M^k$, we see that $\dim(X) = k + d$.

The next result is very important. However, the proof is a little bit technical; so we skip it. One may read it from [**8**].

THEOREM 1.5. *Let X be a nonempty definable set. Then*

$$\dim(\mathrm{fr}(X)) < \dim(X).$$

As a consequence, we have that $\mathrm{cl}(X)$ has the same dimension as X.

2. Euler Characteristic

Euler characteristic is a much less intuitive invariant for definable sets. Even its definition requires some preparation.

The Euler characteristic of a cell C is defined to be

$$\chi(C) = (-1)^{\dim(C)}.$$

Now let's consider a general definable set $X \subseteq M^n$. Let $\mathcal{P} = \{C_1, \ldots, C_t\}$

[1]The last equality requires a little bit of thought.

be a collection of cell that partition X. As a temporary definition, we present the *Euler characteristic of X with respect to $\mathcal{P}$* as follows:

$$\chi_{\mathcal{P}}(X) = \sum_{i=1}^{t} \chi(C_i).$$

Note that this can be written as $\sum_{d=0}^{n}(-1)^d k_d$, where k_d is the number of d dimensional cells in $\mathcal{P}$.

The first order of business is to show that this definition is indeed independent of the choice of $\mathcal{P}$.

Let $C \subseteq M^n$ be a cell and let $\mathcal{D}^*$ be a decomposition of M^n that partitions C. Recall that this means that $\mathcal{D}^*$ is a collection $\{D_1, \ldots, D_t\}$ of cells such that $M^n = D_1 \cup \cdots \cup D_t$ and for each i, either $D_i \subseteq C$ or $D_i \cap C = \emptyset$. Suppose that $D_i \subseteq C$ for $i = 1, \ldots, s$ and $D_i \cap C = \emptyset$ for $i > s$. Let $\mathcal{D} = \{D_1, \ldots, D_s\}$. We claim that $\chi_{\mathcal{D}}(C) = \chi(C)$. As usual, this is done by induction on n. Let $n = 1$. If C is a point, then there is nothing to do and if C is an interval, then $\mathcal{D}$ contains k many intervals and $k-1$ many points. Hence

$$\chi_{\mathcal{D}}(C) = (k-1) - k = 1 = (-1)^1 = \chi(C).$$

Now let $n > 0$. Assume that C is of the for (g, h) where

$$g, h : \pi(C) \to M$$

are continuous definable functions. Since $\pi(\mathcal{D}) = \{\pi(D_1), \ldots, \pi(D_s)\}$ partitions $\pi(C)$, by the induction hypothesis, we have

$$\chi_{\pi(\mathcal{D})}(\pi(C)) = \chi(\pi(C)).$$

Let $E \in \pi(\mathcal{D})$ be of dimension d, and let $f_0, \ldots, f_q : E \to M$ be continuous definable functions such that $f_j < f_{j+1}$ for all j, and the element of $\mathcal{D}$ above E are

$$\Gamma(f_1), \ldots, \Gamma(f_{q-1}), (f_0, f_1), \ldots, (f_{q-1}, f_q).$$

Then the contribution of these cells to $\chi_{\mathcal{D}}(C)$ is

$$(q-1)(-1)^d + q(-1)^{d+1} = (-1)^{d+1} = -\chi(E).$$

Therefore we have

$$\chi_{\mathcal{D}}(C) = -\sum_{E \in \pi(\mathcal{D})} \chi(E) = -\chi_{\pi(D)}(\pi(C)) = \chi(C).$$

The case that C is the graph of a continuous definable function can ben handled similarly.

Let's record this:

LEMMA 2.1. *Let C be a cell and let $\mathcal{D}$ be a partition of C into cells whose projections partition the cell $\pi(C)$. Then $\chi_{\mathcal{D}}(C) = \chi(C)$.*

Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be tow collections of cells partitioning a definable set $X \subseteq M^n$. Take a decomposition $\mathcal{P}$ of M^n that partitions each member of $\mathcal{P}_1 \cup \mathcal{P}_2$. Then $\mathcal{P}$ refines both $\mathcal{P}_1$ and $\mathcal{P}_2$, and using 2.1 we get that

$$\chi_{\mathcal{P}}(X) = \sum_{C \in \mathcal{P}_1} \chi_{\mathcal{P}}(C) = \sum_{C \in \mathcal{P}_1} \chi(C) = \chi_{\mathcal{P}_1}(X).$$

Similarly, $\chi_{\mathcal{P}}(X) = \chi_{\mathcal{P}_2}(X)$. Hence $\chi_{\mathcal{P}_1}(X) = \chi_{\mathcal{P}_2}(X)$, and as promised Euler characteristic of X is independent of the choice of the partition $\mathcal{P}$ into cells. So we denote it as $\chi(X)$.

If $X, Y \subseteq M^n$ are disjoint definable sets, then $\chi(X \cup Y) = \chi(X) + \chi(Y)$. If they are not necessarily disjoint, then

$$\begin{aligned}\chi(X \cup Y) &= \chi((X \setminus (X \cap Y)) \cup (X \setminus (X \cap Y)) \cup X \cap Y) \\ &= \chi(X \setminus (X \cap Y)) + \chi(Y \setminus (X \cap Y)) + \chi(X \cap Y) \\ &= \chi(X) + \chi(Y) - \chi(X \cap Y).\end{aligned}$$

Next we would like to investigate the behavior of Euler characteristic in definable families. As usual, let's do this first for cells. For $m, n \geq 0$ let π denote the projection from M^{n+m} to M^n. Let $C \subseteq M^{n+m}$ be a cell. Then it is easy to see –if you wish by induction– that the Euler characteristic of $C_{\vec{a}}$ is the same for each $\vec{a} \in \pi(C)$, and that $\chi(C) = \chi(\pi(C))\chi(C_{\vec{a}})$ for any $\vec{a} \in \pi(C)$.

Now let $X \subseteq M^{n+m}$ be a definable set and let $\mathcal{D}$ be a decomposition of M^{n+m} partitioning X. Then by the previous paragraph, for any $D \in \pi(\mathcal{D})$, the sections over D have the same Euler characteristics, and hence for $e \in \mathbb{Z}$, the set

$$\{\vec{a} \in M^m : \chi(X_{\vec{a}}) = e\}$$

is definable. Moreover, for any $D \in \pi(\mathcal{D})$ and $\vec{a} \in D$, we have

$$\chi(X \cap \pi^{-1}(D)) = \chi(D)\chi(X_{\vec{a}}).$$

Note in particular that $\chi(X \times Y) = \chi(X)\chi(Y)$ for every definable X, Y.

We close this chapter with two fundamental results. The first states that Euler characteristic is invariant under definable bijections as is the case for dimension. The second result says that for expansions of fields, they are complete invariants. We do not present a proof for either of them. The proof of the former one is not too complicated, but a little bit technical, but the proof of the latter is quite hard.

THEOREM 2.2. *Let $f : X \to M^n$ be an injective definable map. Then $\chi(f(X)) = \chi(X)$. In particular, if X and Y are in definable bijection, then they have the same Euler characteristic.*

THEOREM 2.3. *Let $\mathcal{R} = (R, +, \cdot, <, \dots)$ be an o-minimal expansion of a real closed field. Then two definable sets X and Y are in definable bijection if and only if $\dim(X) = \dim(Y)$ and $\chi(X) = \chi(Y)$.*

CHAPTER 6

Some Basic Algebraic Number Theory

We recall some definitions and facts about the study of number fields. As in the case of logic and model theory, we cover more than strictly necessary, but we again believe that it is very useful to be acquainted with number theoretical objects to grasp the importance of the theorem we prove at the end. We do however sweep quite a few details under the rug. Also we assume some background in the algebra; mostly in Galois theory.

What we strictly need is the concept of the *height* of an algebraic number. As a matter of fact, we could have defined only the height of a rational number –which can be defined in very non-technical terms– and say that the general definition is similar to that. However, we feel like that would veil some of the ideas about the use of heights in arithmetic.

We follow the path of the book [**3**]. We first introduce absolute values, valuations, and places on fields; these are more or less the same concepts. We investigate how to extend them to field extensions and then specialize to number fields, which are just finite extensions of $\mathbb{Q}$. Finally, we define the (absolute) height of an algebraic number using places on number fields.

1. Absolute Values on Fields

DEFINITION 1.1. An *absolute value* on a field K is a function $|\cdot| : K \to \mathbb{R}^{>0}$ such that

(1) For each $x \in K$, $|x| = 0$ is and only if $x = 0$,
(2) $|xy| = |x||y|$ for all $x, y \in K$,
(3) $|x + y| \leq |x| + |y|$ for all $x, y \in K$.

Observe that $|1| = |-1| = 1$ and $|-x| = |x|$ for all $x \in K$.

An absolute value gives a metric on K by defining $d_{|\cdot|}(x, y) = |x - y|$. We never use the notation $d_{|\cdot|}$ again, and mostly refer to the topology given by the absolute value. A basis for this topology consists of the balls:

$$B(a, r) := \{x \in K : |x - a| < r\}.$$

If $|\cdot|$ is an absolute value and $s \in \mathbb{R}^{>0}$, then it is easy to see that $|\cdot|^s$ is also an absolute value, and that $|\cdot|$ and $|\cdot|^s$ define equivalent

topologies on K. The other way around is also correct, but it is much harder to prove.

THEOREM 1.2. *Let $|\cdot|_1$ and $|\cdot|_2$ are two absolute values on a field K that define the same topology. Then there is $s \in \mathbb{R}^{>0}$ with $|\cdot|_2 = |\cdot|_1^s$*

PROOF. See Lemma 3.2 of [**5**]. □

We are mostly interested in absolute values on $\mathbb{Q}$ and its finite extensions. The next two examples below contain infinitely many absolute values on $\mathbb{Q}$. As a matter fact, we later mention that these are the only examples. So we will keep returning to these examples again and again.

EXAMPLE 1.3. The usual absolute value on $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are absolute values in the above sense. We denote all these absolute values as $|\cdot|_\infty$. The topology it gives on $\mathbb{R}$ and $\mathbb{C}$ are the usual Euclidean topology.

EXAMPLE 1.4. Let p be a prime. We define another absolute value $|\cdot|_p$ on $\mathbb{Q}$ depending on this p. Note that if $\frac{a}{b} \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$, $b > 0$, then $|\frac{a}{b}|_p = \frac{|a|_p}{|b|_p}$. Moreover, we may assume that a is also non-negative. So it is enough to define $|\cdot|_p$ for natural numbers. So let $a \in \mathbb{N}$. If $a = 0$, then $|a|_p = 0$ and if it is nonzero, then let $a = p^k b$, where $k \in \mathbb{N}$ and $p \not| b$. In this case we define $|a|_p = p^{-k}$. This absolute value is called the *p-adic absolute value* on $\mathbb{Q}$. The topology given by the p-adic absolute value is a little bit strange. We investigate this below.

EXAMPLE 1.5. Let $K = F(T)$, where F is a field and T is an indeterminate. Also let $f \in K$ be irreducible. We proceed to define the *f-adic absolute value* $|\cdot|_f$ on K in a similar way to the definition of p-adic absolute value on $\mathbb{Q}$. Again it is enough to define it on $F[T]\setminus\{0\}$. So let g be a nonzero polynomial with coefficients from F and write is as $g = f^k h$ where $k \in \mathbb{N}$ and $f \not| h$. At this stage the construction changes a little bit since we do not have a canonical choice as $\frac{1}{p}$. So instead we fix $c \in (0, 1)$ and let $|g|_f = c^k$. By Theorem 1.2, the choice of c does not matter much in terms of topology. The topology here is strange as well, just as in the case of p-adic absolute value.

Consider the special case when $F = \mathbb{C}$; or any algebraically closed field for that matter. Then the irreducible polynomials are exactly the linear polynomials $T - a$ for $a \in \mathbb{C}$. In that case, the $(T - a)$-adic absolute value somehow counts the multiplicity at the point a.

In the definition of absolute value, if instead of (3), the following condition holds, then the absolute value is said to be *non-archimedean*:

(3*) $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$.

If this does not hold, then we say that the absolute value is *archimedean*.

The absolute value $|\cdot|_\infty$ on either of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ is archimedean. For each p, the p-adic absolute value is non-archimedean, and similarly the f-adic absolute value on $F(T)$ is non-archimedean.

LEMMA 1.6. *Let $|\cdot|$ be a non-archimedean absolute value on K, and let $x, y \in K$ be such that $|x| < |y|$. Then $|x + y| = |y|$.*

PROOF. Just note that for such x, y we have

$$|y| = |x + y - x| \leq \max\{|x + y|, |x|\} \leq |y|.$$

So $\max\{|x + y|, |x|\} = |x + y| = |y|$ □

PROPOSITION 1.7. *Let $|\cdot|$ be a non-archimedean absolute value on K. Then any point of any open ball is the center of the ball; in other words for every $r > 0$ and $x, y \in K$, if $y \in B(x, r)$, then*

$$B(x, r) = B(y, r).$$

PROOF. Suppose that $y \in B(x, r)$. By symmetry, it suffices to show that $B(x, r) \subseteq B(y, r)$. So let $z \in B(x, r)$. Then $|x - y| < r$ and $|x - z| < r$. Therefore

$$|y - z| = |(x - z) - (x - y)| \leq \max\{|x - z|, |x - y|\} < r.$$

Hence $z \in B(y, z)$.

□

Homework 17. An absolute value $|\cdot|$ on a field K is archimedean if and only if for every $x \in K$, there is $n \in \mathbb{Z}$ such that $|x| < |n|$.

Recall that a metric space is called *complete* if every Cauchy sequence has a limit. It is clear that $\mathbb{Q}$ is not complete with respect to the usual absolute value $|\cdot|_\infty$. For $p > 3$, one take $a \in \{2, \ldots, p - 1\}$ and consider the sequence $(a^{p^n})_{n\in\mathbb{N}}$. One may easily show that this sequence is Cauchy, but does not have a limit in $\mathbb{Q}$. For $p = 2, 3$, one may come up with ad-hoc sequences to prove that $\mathbb{Q}$ is not complete with respect any of the p-adic absolute values.

We construct the *completion* of a field K with respect to an absolute value $|\cdot|$: There is a field extension L of K equipped with an absolute value $|\cdot|_*$ extending $|\cdot|$ such that L is complete with respect to $|\cdot|_*$, and K is a dense subset of L with respect to the topology determined by $|\cdot|_*$. We do not get into the details of the construction of L, but we would like to say that it is very similar to the construction of $\mathbb{R}$ from $\mathbb{Q}$ with respect to $|\cdot|_\infty$. It is also very important that the completion is unique up to isomorphism fixing the base field; that isomorphism is actually an isometry.

The completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is called the *field of p-adic numbers* and it is denoted as $\mathbb{Q}_p$.

We state the following results, usually known as Ostrowski Theorems, without proofs. (For this kind of results Cassel's book, [**5**] is a good source.)

THEOREM 1.8. (1) *Every non-trivial absolute value on $\mathbb{Q}$ is equivalent either to $|\cdot|_\infty$ or to $|\cdot|_p$ for some p.*
(2) *The only fields with complete archimedean absolute values on them are $\mathbb{R}$ and $\mathbb{C}$.*

DEFINITION 1.9. A *place* on a field K is the equivalence class of absolute values on K. We generally denote places with letters v, w and a choice of absolute value in the class v will be denoted as $|\cdot|_v$.

If $K \subseteq L$ are fields with places v and w on them such that any representative of w extends a representative of v, we say that w *extends* v and it is denoted as $w|v$.

One important task is to find extensions of places or absolute values to finite extensions. The way to do this is via the norm function attached to finite extensions. Let $L|K$ be a finite extension of fields, and let $\alpha \in L$. Suppose that $\alpha_1, \ldots, \alpha_n$ are the roots of the minimal polynomial of α over K; counted with multiplicity if the extension is not separable. We define the *norm* of α over K as

$$N_{L|K}(\alpha) := (\alpha_1 \cdots \alpha_n)^{[L:K]/n}.$$

Note that this quantity is in K; actually it is the constant term of the minimal polynomial raised to the power $\frac{[L:K]}{n}$. Therefore we may take its absolute value. If K complete, one could check that

$$|\alpha|_w := |N_{L|K}(\alpha)|_v^{1/[L:K]}$$

is indeed an absolute value on L and that it is unique. The uniqueness is not a trivial task; one could check the related chapter in Lang's book ([**17**]). Moreover, L becomes complete with respect to $|\cdot|_w$.

This is not exactly correct when K is not complete. We need to first go up to the completion of K. Let's do this in details; so let $|\cdot|_v$ be an absolute value on K. Let K_v be the completion of K with respect to $|\cdot|_v$; we continue to denote the absolute value on K_v as $|\cdot|_v$. Take α from an algebraic closure of K with minimal polynomial f over K. Decompose f in K_v as $f_1^{k_1} \cdots f_t^{k_t}$. [1] Let L_j be an extension of K_v generated by a root of f_j; for instance $K_v[T]/\langle f_j \rangle$. Then by the above construction, $|\cdot|_v$ has a unique extension to L_j, denote it as $|\cdot|_j$; recall that $|\cdot|_j = |N_{L_j/K_v}(\cdot)|_v^{\frac{1}{[L_j:K_v]}}$. Now L embeds into L_j by sending α to a root of f_j in L_j; for instance to $\overline{T}$. Hence $|\cdot|_j$ restricts to an absolute value on L extending $|\cdot|_v$. It is not hard to see that the image of L under this embedding is dense in L_j, hence it is indeed a completion of

[1] Note that if the characteristic of K is 0, then each k_j is 1.

L with respect to $|\cdot|_j$. Using the uniqueness of completions, it is easy to see that L_j's are distinct. Similarly, any extension of $|\cdot|_v$ to L is a restriction of one of the absolute values $|\cdot|_j$. We summarize these for separable extensions as follows.

THEOREM 1.10. *Let $L = K(\alpha)$ be a finite separable extension of K, and let $|\cdot|_v$ be an absolute value on K.*

1. *There are finitely many places w on L extending v; more precisely the number of them is the same as the number of irreducible components in $K_v[X]$ of the minimal polynomial of α over K.*
2. *The completion L_w of L with respect to an absolute value w extending v can be identified with a finite extension of K_v.*
3. *$[L : K] = \sum_{w|v}[L_w : K_v]$.*
4. *If $L|K$ is Galois, then for any w_1, w_2 extending v, the fields L_{w_1} and L_{w_2} are isomorphic over K_v. Also there is $\sigma \in \mathrm{Gal}(K/L)$ such that $|\cdot|_{w_2} = |\sigma(\cdot)|_{w_1}$ on L.*

2. Absolute Values on Number Fields

We are mostly interested in the case of number fields; meaning finite extensions of $\mathbb{Q}$. So all extensions we'll be talking about will be separable. So let K be a number field.[2] We know by Ostrowski's theorem that a place w on K extends places corresponding either to $|\cdot|_\infty$ or to $|\cdot|_p$ for some p. First consider $|\cdot|_\infty$. We know that the completion of $\mathbb{Q}$ in this case is $\mathbb{R}$ and by the other part of Ostrowski's theorem, the completion of K with respect to w must be either $\mathbb{R}$ or $\mathbb{C}$ with $|\cdot|_\infty$ on them; in the former case w is called a *real place* and in latter case it is called a *complex place*. So w is determined by embeddings of K into $\mathbb{C}$. If we have an embedding whose image is not in $\mathbb{R}$, then the composition of it with complex conjugation gives another embedding, but these two embeddings determine the same place. By Theorem 1.10, other than this situation all embeddings determine different places. In either case, a representative of w is given as the restriction of the complex absolute value $|\cdot|_\infty$; note that

$$|N_{\mathbb{C}/\mathbb{R}}(a+bi)|^{1/[\mathbb{C}:\mathbb{R}]} = \sqrt{a^2+b^2} = |a+bi|_\infty.$$

There is no simple explanation for the extensions of p-adic places as $\mathbb{Q}_p$ could have all kinds of finite algebraic extensions. Still $|\cdot|_p$ extend to each in a unique way, and hence the absolute values on K extending $|\cdot|_p$ are determined by embeddings of K into $\overline{\mathbb{Q}}_p$.

We would like to choose a 'normal' representative for the places extending the p-adic place on $\mathbb{Q}$ as follows:

$$|x|_w = |N_{K_w/\mathbb{Q}_p}(x)|_p^{1/[K:\mathbb{Q}]}.$$

[2]Note that this K corresponds to L in Theorem 1.10, and $\mathbb{Q}$ to K there.

Note that $|x|_w = (|N_{K_w/\mathbb{Q}_p}(x)|_p^{\frac{1}{[K_w:\mathbb{Q}_p]}})^{[K_w:\mathbb{Q}_p]/[K:\mathbb{Q}]}$. Therefore for $x \in \mathbb{Q}$, we have

$$|x|_w = |x|_p^{\frac{[K_w:\mathbb{Q}_p]}{[K:\mathbb{Q}]}}.$$

So we have $w|p$, but unless $K = \mathbb{Q}$, it is not correct that $|\cdot|_w$ extends $|\cdot|_p$. Now combining this with the third part of Theorem 1.10, we see that $\prod_{w|p} |x|_w = |x|_p$ for $x \in \mathbb{Q}$.

We let M_K denote the set of absolute values chosen this way. Note that $M_\mathbb{Q}$ simply consists of the usual absolute value $|\cdot|_\infty$ and the p-adic absolute values $|\cdot|_p$.

Let's see these in examples.

EXAMPLE 2.1. Let $K = \mathbb{Q}(\sqrt{2})$. First consider the archimedean absolute value. In this case, both roots $\sqrt{2}$ and $-\sqrt{2}$ of the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ are in $\mathbb{R}$. Hence the place ∞ has two extensions to K, say w_1 and w_2, and moreover $K_{w_1} = K_{w_2} = \mathbb{R}$. These extensions correspond to embeddings of K into $\mathbb{R}$. One of them is the inclusion map and the other one is the one sending $\sqrt{2}$ to $-\sqrt{2}$. So the normalized choices for representatives of w_1 and w_2 are as follows:

$$|a + b\sqrt{2}|_{w_1} = |a + b\sqrt{2}|_\infty^{1/2} \text{ and } |a + b\sqrt{2}|_{w_2} = |a - b\sqrt{2}|_\infty^{1/2}.$$

Now consider a non-archimedean place p. One can determine, using Newton method, the primes p for which 2 has a square root in each $\mathbb{Q}_p$; one must be careful when applying calculus methods since our metric is a little bit different, for instance $\sum_{n=0}^{\infty} 3^n = -1$ in $\mathbb{Q}_3$. This can be done using Hensel's Lemma and Quadratic Reciprocity as well. We use the fact that the 2-adic absolute values of elements $\mathbb{Q}_2$ are still in $2^\mathbb{Z}$ to see that 2 has no square root in $\mathbb{Q}_2$: If $\beta \in \mathbb{Q}_2$ we a root of 2, then $|\beta|_2^2 = |\beta^2|_2 = |2|_2 = 1/2$, and hence we would have $|\beta|_2 = 1/\sqrt{2} \notin 2^\mathbb{Z}$. So for $p \neq 2$, K embeds into $\mathbb{Q}_p$ in two ways and when K embeds into a quadratic extension of $\mathbb{Q}_2$ in a unique way.

EXAMPLE 2.2. For this example, let $K = \mathbb{Q}(\sqrt[3]{2})$. This time, the archimedean place ∞ has one real extension w_1, and one complex extension w_2. The representatives of these are

$$|a + b\sqrt[3]{2} + c\sqrt[3]{4}|_{w_1} = |a + b\sqrt[3]{2} + c\sqrt[3]{4}|_\infty^{1/3}$$

and

$$|a + b\sqrt[3]{2} + c\sqrt[3]{4}|_{w_1} = |a + b\zeta_3\sqrt[3]{2} + c\zeta_3\sqrt[3]{4}|_\infty^{1/3},$$

where ζ_3 is a primitive third root of unity and the first $|\cdot|_\infty$ is in $\mathbb{R}$ and the second in $\mathbb{C}$.

For the non-archimedean absolute values, one could use the Hensel's lemma to determine when 2 is a cube root in in $\mathbb{Q}_p$ and whether the other two roots are there as well or not. Then proceed as in the previous example.

For a second, let's consider a very special case by taking $K = \mathbb{Q}$ and let $\alpha = \frac{a}{b}$ be nonzero with $\gcd(a, b) = 1$ and $b > 0$. Then $|\alpha|_p = 1$ for all but finitely many p, namely the prime divisors of a and b. So the product $\Pi_p |\alpha|_p$ makes sense and it actually equals $1/|\alpha|_\infty$. We write this in the following way:

$$\prod_{v \in M_{\mathbb{Q}}} |\alpha|_v = 1.$$

We claim that both these properties hold for M_K as well.

We first show that for any non-zero $\alpha \in K$, there is a finite set $W \subseteq M_K$ such that $|\alpha|_w \leq 1$ for all $w \notin W$. Since this is correct for $1/\alpha$ as well, we'll get that $|\alpha|_w = 1$ except for finitely many w. Let

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$$

be the minimal polynomial of α over $\mathbb{Q}$. Each $v \in M_{\mathbb{Q}}$ extends to finitely many elements of M_K. In particular, there are only finitely many archimedean places on K and hence it is enough to consider non-archimedean w, which is to say that $w|p$. We know that $|a_i|_w = |a_i|_p^{\frac{[K_w:\mathbb{Q}_p]}{[K:\mathbb{Q}]}} \neq 1$ for all but finitely many $w \in M_K$. So there is a finite subset W of M_K such that $|a_i|_w \leq 1$ for all i and for all $w \notin W$. Now

$$|\alpha|_w^n \leq \max\{|\alpha|_w^{n-1}|a_{n-1}|_w, \ldots, |a_0|_w\}$$

for all w. Therefore $|\alpha|_w \leq 1$ for all $w \notin W$ as desired.

Now let $\alpha \in K$ be nonzero. Recall that $|\alpha|_w = |N_{K_w/\mathbb{Q}_p}(\alpha)|_p^{1/[K:\mathbb{Q}]}$ for $w|p$. It is not hard to see from the way K_w constructed from $\mathbb{Q}_p$ that

$$\prod_{w|p} N_{K_w/\mathbb{Q}_p}(\alpha) = N_{K/\mathbb{Q}}(\alpha).$$

Therefore

$$\prod_{w|p} |\alpha|_w = (\prod_{w|p} |N_{K_w/\mathbb{Q}_p}(\alpha)|_p)^{1/[K:\mathbb{Q}]} = |N_{K/\mathbb{Q}}(\alpha)|_p^{1/[K:\mathbb{Q}]}.$$

Hence

$$\begin{aligned}
\prod_{w \in M_K} |\alpha|_w = \prod_{v \in M_{\mathbb{Q}}} \prod_{w|v} |\alpha|_w &= \prod_{v \in M_{\mathbb{Q}}} |N_{K/\mathbb{Q}}(\alpha)|_v^{1/[K:\mathbb{Q}]} \\
&= (\prod_{v \in M_{\mathbb{Q}}} |N_{K/\mathbb{Q}}(\alpha)|_v)^{1/[K:\mathbb{Q}]} \\
&= 1^{1/[K:\mathbb{Q}]} \\
&= 1.
\end{aligned}$$

This last property we proved for M_K is called the *product formula*. Even though K will always be a number field in the rest of this chapter, most of the results go through for a field L equipped with a set M_L of

absolute values on it such that for any $x \in L^\times$ we have $|x|_v \neq 1$ for only finitely many $v \in M_L$ and M_L satisfies the product formula.

3. Heights of Algebraic Numbers

Height of a number is a measure of how complicated it is; for instance even though they are very close to each other (in the Euclidean topology), the numbers 1 and $\frac{99999}{100000}$ are quite different and it seems like the latter should be considered more complicated.

As usual, we do more than what is strictly necessary for our purposes and define the height of a tuple of algebraic numbers. Actually, even more: We define the height function on the projective space $\mathbb{P}^n(\overline{\mathbb{Q}})$. Recall that the elements of $\mathbb{P}^n(\overline{\mathbb{Q}})$ are classes of a certain equivalence relation on $\overline{\mathbb{Q}}^{n+1} \setminus \{\vec{0}\}$. Two elements $(x_0, \ldots, x_n)$ and $(y_0, \ldots, y_n)$ of $\overline{\mathbb{Q}}^{n+1} \setminus \{\vec{0}\}$ are equivalent if

$$(y_0, \ldots, y_n) = (\lambda x_0, \ldots, \lambda x_n) \text{ for some } \lambda \in \overline{\mathbb{Q}}^\times.$$

So one could think of elements of $\mathbb{P}^n(\overline{\mathbb{Q}})$ as the set of lines in $\overline{\mathbb{Q}}^{n+1}$ passing through the origin. An element of $\mathbb{P}^n(\overline{\mathbb{Q}})$ will be written as $\mathbf{x} = (x_0 : \cdots : x_n)$. If, for instance $x_0 \neq 0$, then

$$(x_0 : x_1 : \cdots : x_n) = (1 : \frac{x_1}{x_0} : \cdots : \frac{x_n}{x_0})$$

This can be done with any $x_i \neq 0$. So there are $n+1$ ways to embed $\overline{\mathbb{Q}}^n$ into $\mathbb{P}^n(\overline{\mathbb{Q}})$.

Definition 3.1. Let $\mathbf{x} = (x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n(\overline{\mathbb{Q}})$. We define the *height* of $\mathbf{x}$ as

$$h(\mathbf{x}) = \sum_{v \in M_K} \max_j \log(|x_j|_v),$$

where K is a number field containing every x_j. We also use the notation $H(\mathbf{x}) = e^{h(\mathbf{x})}$.

It is easy to see, using arguments as in the previous section that $h(\mathbf{x})$ is independent of the choice of K.

Also using the product formula one could see that it is also independent of the choice of the coordinates $(x_0, \ldots, x_n)$ as follows: Let $\mathbf{x} = \mathbf{y}$, say

$(y_0, \dots, y_n) = (\lambda x_0, \dots, \lambda x_n)$ for $\lambda \neq 0$. Then

$$\begin{aligned} h(\mathbf{y}) &= \sum_{v \in M_K} \max_j \log(|\lambda x_j|_v) \\ &= \sum_{v \in M_K} \log(|\lambda|_v) + \sum_{v \in M_K} \max_j \log(|x_j|_v) \\ &= 0 + \sum_{v \in M_K} \max_j \log(|x_j|_v) \\ &= \sum_{v \in M_K} \max_j \log(|x_j|_v) \\ &= h(\mathbf{x}). \end{aligned}$$

If $(x_1, \dots, x_n)$ is a tuple of algebraic numbers we may define its height as the height of $(1 : x_1 : \cdots : x_n) \in \mathbb{P}^n(\overline{\mathbb{Q}})$. Suppose that $x_j \in \mathbb{Q}$ for each j, say $x_i = \frac{a_i}{a_0}$ with $a_0, a_1, \dots, a_n \in \mathbb{Z}$ and $a_0 > 0$. Let $\gamma = \gcd(a_0, \dots, a_n)$ and put $b_j = \frac{a_j}{\gamma}$. Then

$$\begin{aligned} h(x_1, \dots, x_n) &= h(1 : x_1, \dots, x_n) \\ &= h(a_0 : a_1 : \cdots : a_n) \\ &= h(b_0 : b_1 : \cdots : b_n) \\ &= \sum_{v \in M_{\mathbb{Q}}} \max_j \log(|b_j|_v) \\ &= \max_j \log(|b_j|_\infty). \end{aligned}$$

In particular, the height of a rational number a/b in simplest terms is the largest of $\log|a|$ and $\log|b|$. For instance, the height of 1 is 1 and that of $99999/100000$ is $\log 100000$.[3]

Let's present a little piece of notation to express somethings in simpler ways. Let $\log^+ x = \max\{0, \log x\}$ for $x \in \mathbb{R}$; define $\log 0 = -\infty$. Then for a tuple $(x_1, \dots, x_n)$ of algebraic numbers we have

$$h(x_1, \dots, x_n) = \sum_{v \in M_K} \max_j \log^+ |x_j|_v$$

So for a single algebraic number x, we have $h(x) = \sum_{v \in M_K} \log^+ |x|_v$.

If x is a root of unity, then $|x|_v = 1$ for every v extending an element of $M_{\mathbb{Q}}$. Therefore $h(x) = 0$. As a matter of fact, roots of unity are exactly the algebraic numbers with height 1. This is a theorem of Kronecker, which we state without a proof.

THEOREM 3.2 (Kronecker's Theorem). *The height of an algebraic number is* 0 *if and only if it is a root of unity.*

[3]One reason we use the logarithms is that this way the height of an integer is almost the number of its digits.

Let $K|\mathbb{Q}$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. For any $v \in M_{\mathbb{Q}}$, $w \in M_K$ with $w|v$, and $\sigma \in G$, we have that $|\sigma(\cdot)|_w$ is also in M_K and it still extends v. In other words, for a fixed $v \in M_{\mathbb{Q}}$, the group G acts on the extensions of v in M_K.

Now let $(x_1, \ldots, x_n)$ be a tuple of algebraic numbers such that each x_j is in K as above. Then for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we have

$$\begin{aligned} h(x_1, \ldots, x_n) &= \sum_{v \in M_{\mathbb{Q}}} \sum_{w|v} \max_j \log |x_j|_w \\ &= \sum_{v \in M_{\mathbb{Q}}} \sum_{w|v} \max_j \log |\sigma(x_j)|_w \\ &= h(\sigma(x_1, \ldots, x_n)). \end{aligned}$$

Actually, the choice of field K is not important. So we may summarize this as follows:

THEOREM 3.3. *Let $P \in \overline{\mathbb{Q}}^n$ and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $h(P) = h(\sigma(P))$.*

We do not present the proof of the following theorem.

THEOREM 3.4 (Northcott's Theorem). *For every $d, h \geq 0$, there are only finitely many algebraic numbers α with $\deg(\alpha) \leq d$ and $h(\alpha) \leq h$.*

4. Valuation Ring and Residue Field

In this last section of this chapter, we introduce some algebraic objects attached to a non-archimedean place on a field K.

Until the end of this chapter, all absolute values and places are non-archimedean.

DEFINITION 4.1. Let v be a non-archimedean place on K and let $|\cdot|_v$ be a representative of it. The *valuation ring of v* is

$$\mathcal{O}_v := \{\alpha \in K : |\alpha|_v \leq 1\}.$$

Note that this is just the closed unit disc centered at 0, and hence it is clear that this definition does not depend on the choice of the representative $|\cdot|_v$. The open unit disc forms an ideal of $\mathcal{O}_v$, it is denoted as $\mathfrak{m}_v$. Note that $\mathcal{O}_v \setminus \mathfrak{m}_v$ consists of elements of absolute value 1 and hence are units in $\mathcal{O}_v$. This means that $\mathfrak{m}_v$ is the unique maximal ideal and $\mathcal{O}_v$ is a local ring. The quotient $\mathcal{O}_v/\mathfrak{m}_v$ is a field; it is called the *residue field* of v, and it is denoted by k_v. The projection $r_v \colon \mathcal{O}_v \to k_v$ is called the *residue map*.

The image of $K^\times$ under $|\cdot|_v$ is a (multiplicative) subgroup of $\mathbb{R}^{>0}$, and different representatives give isomorphic groups. It is easy to show that a subgroup of $\mathbb{R}^{>0}$ is either cyclic, in which case it is a discrete subset, or is dense in $\mathbb{R}^{>0}$. Let's concentrate on the discrete case; in this case

we call the place *discrete*. Suppose that the image of $K^\times$ is $c^{\mathbb{Z}}$ for some $0 < c < 1$. Then elements of $\mathfrak{m}_v$ are the ones whose absolute value is c^m with $m > 0$. In particular, there is $\alpha \in \mathfrak{m}_v$ with $|\alpha|_v = c$ and any other such elements is of the form $u\alpha$ where $u \in \mathcal{O}_v^\times$. It follows that $\mathfrak{m}_v = \langle \alpha \rangle$. A generator of $\mathfrak{m}_v$ is called a *local parameter*. Two local parameters differ by a unit and they do not depend on the choice of a representative $|\cdot|_v$

The proper ideals of $\mathcal{O}_v$ are exactly $\mathfrak{m}_v^n = \langle \alpha^n \rangle$ for some $n > 0$. So not only that $\mathcal{O}_v$ is a PID, but also the ideals form a chain. Using this, we may define a function $v : K^\times \to \mathbb{Z}$ as follows: If $\beta \in \mathcal{O}_v$, then $v(\beta)$ is the smallest $n \in \mathbb{N}$ such that $\beta \in \mathfrak{m}_v^n$; here $\mathfrak{m}_v^0 = \mathcal{O}_v$. Note that $K = \mathcal{O}_v \cup \mathcal{O}_v^{-1}$, where $\mathcal{O}_v^{-1}$ denotes the inverses of elements of $\mathcal{O}_v$. More simply $K = \mathfrak{m}_v \cup \mathcal{O}_v^\times \mathfrak{m}_v^{-1}$ and here these unions are disjoint. So if $\beta \notin \mathcal{O}_v$, then $\beta^{-1} \in \mathcal{O}_v$. In that case, we define $v(\beta) = -v(\beta^{-1})$.

This function v can be defined in a more direct way. Namely, fixing a local parameter α of v, and $\beta \in K^\times$ we define $v(\beta) = \log_{|\alpha|_v}(|\beta|_v)$. This definition clearly does not depend on the choice of $|\cdot|_v$. Such a function is called a *valuation*.

EXAMPLE 4.2. Consider $\mathbb{Q}$ with the place p. We have

$$\mathcal{O}_p = \{\frac{a}{b} : \gcd(a,b) = 1, p \not| b\},$$

and

$$\mathfrak{m}_p = \{\frac{a}{b} : \gcd(a,b) = 1, p|a, p \not| b\} = p\mathcal{O}_v,$$

Then $k_p \simeq \mathbb{F}_p$ and the value group is $(\frac{1}{p})^{\mathbb{Z}} = p^{\mathbb{Z}}$. Note that $\mathcal{O}_p$ is the localization of $\mathbb{Z}$ at the prime ideal $p\mathbb{Z}$.

It follows from the general construction of completion that elements of $\mathbb{Q}_p$ are sort of Laurent series over $\mathbb{F}_p$: They are of the form

$$\sum_{i=k}^{\infty} a_i p^i, \text{ where } k \in \mathbb{Z}, a_i \in \{0, 1, \ldots, p-1\}, a_k \neq 0.$$

Here let v_p denote the valuation. Then $v_p(\sum_{i=k}^\infty a_i p^i) = k$ and hence the value group is still $(\frac{1}{p})^{\mathbb{Z}}$. The valuation ring is denoted as $\mathbb{Z}_p$ and it consists of $\sum_{i=0}^\infty a_i p^i$, where a_0 could be 0; such an element is called a *p-adic integer*. The elements of the maximal ideal are $\sum_{i=1}^\infty a_i p^i$. It follows that the residue field is still $\mathbb{F}_p$.

EXAMPLE 4.3. Consider the field $K = \mathbb{C}(T)$ of rational functions over $\mathbb{C}$ with the T-adic absolute value. Note that K can be seen as a subfield of the field $\mathbb{C}((T))$ of (formal) Laurent series over $\mathbb{C}$. To see this, note that if $a \neq 0$, then

$$\frac{1}{T-a} = -\frac{1}{a}(1 + \frac{T}{a} + \frac{T^2}{a^2} + \cdots).$$

Then the valuation counts the multiplicity of the rational function at 0; when it is negative, it means that the function hasa pole at 0. The residue field is $\mathbb{C}$. The completion is $\mathbb{C}((T))$, and the valuation ring of $\mathbb{C}((T))$ consists of $\sum_{i=0}^{\infty} a_i T^i$, and the residue field is still $\mathbb{C}$.

Hensel's lemma gives a very useful criterion for the existence of zeros of polynomials over complete fields. We do not give a proof; we'll just say that it is a version of Newton approximation method.

THEOREM 4.4 (Hensel's Lemma). *Let K be a field that is complete with respect to a non-archimedean absolute value $|\cdot|_v$. Let $f \in \mathcal{O}_v[x]$ and let $\alpha \in \mathcal{O}_v$ be such that $f(\alpha) \in \mathfrak{m}_v$ and $f'(\alpha) \notin \mathfrak{m}_v$. Then there is $a \in \mathcal{O}_v$ such that $f(a) = 0$ and $a \equiv \alpha \mod \mathfrak{m}_v$.*

This result can be interpreted as follows: Let $f \in \mathcal{O}_v[x]$ be such that $r_v(f) \in k_v$ has a single zero in k_v –so it is a root, but not a double root– then f has a root in $\mathcal{O}_v$.

CHAPTER 7

Some Basic Algebraic Geometry

1. Algebraic Varieties

TO BE FILLED IN.

2. Complex Tori and Abelian Varieties

Manin-Mumford Conjecture concerns arithmetic structure of abelian varieties. The actual definition of an abelian variety requires quite a lot of knowledge of algebraic geometry. However, here we are interested only in abelian varieties over $\mathbb{C}$, which will be identified with their $\mathbb{C}$-points. In this case, they can be defined in a more elementary way. They are certain complex tori, so with start with the definition of that.

A *lattice* Λ in $\mathbb{C}^n$ is an free abelian subgroup of $\mathbb{C}^n$ that is generated by $2n$ many elements that are linearly independent over $\mathbb{R}$. In other words, it is a subgroup of $\mathbb{C}^n$ generated by a basis of $\mathbb{C}^n$ as a vector space over $\mathbb{R}$. So letting $\lambda_1, \ldots, \lambda_{2n}$ be a generating set we could write $\Lambda = \mathbb{Z}\lambda_1 + \cdots + \mathbb{Z}\lambda_{2n}$. As a result $\mathbb{C}^n = \mathbb{R}\lambda_1 + \cdots + \mathbb{R}\lambda_{2n}$.

Let $A = \mathbb{Z}a_1 + \cdots + \mathbb{Z}a_{2n}$ be a free abelian subgroup of $\mathbb{C}^n$ of rank $2n$. Fixing a basis, for instance the standard basis $\{e_1, \ldots, e_n\}$, of $\mathbb{C}^n$, we may define the *period matrix* P_A of A as

$$P_A = (a_{ij}) \in M_{n\times n}(\mathbb{C}), \text{ where } a_j = \sum_{j=1}^{n} a_{ij} e_j.$$

So $A = P_A\mathbb{Z}^{2n}$; in other words considering P_A as a linear map, A is the image of the subgroup $\mathbb{Z}^{2n}$.

It is easy to see that A is a lattice if and only if the $2n \times 2n$ matrix

$$\begin{bmatrix} P_A \\ \overline{P}_A \end{bmatrix}$$

is invertible. (Here $\overline{P}_A$ is the matrix obtained by applying complex conjugate to the entries of P_A.)

A *complex torus* is a the quotient group $\mathbb{C}^n/\Lambda$ for a lattice Λ endowed with the quotient topology. Actually, it also has the complex manifold structure induced from $\mathbb{C}^n$; so it is complex Lie group. As such it is still of dimension n. We let $\pi_\Lambda : \mathbb{C}^n \to \mathbb{C}^n/\Lambda$ denote the canonical projection.

When are two complex tori $\mathbb{C}^n/\Lambda_1$ and $\mathbb{C}^m/\Lambda_2$ isomorphic as Lie groups? Such an isomorphism preserves the analytic structure and also the group structure. To begin with, they need to have the same dimension, hence $m = n$. Also any isomorphism between two such tori must be induced from an invertible linear map $f : \mathbb{C}^n \to \mathbb{C}^n$; hence f is given by a matrix $A \in \mathrm{GL}_n(\mathbb{C})$. We also need f to map Λ_1 onto Λ_2. So the columns of AP_{Λ_1} must form a basis of Λ_2. So the final question is how do two bases of a lattice differ from each other. The general theory of free modules over PID's tell us that it happens through an invertible matrix with integer coefficients; more precisely, there is $B \in \mathrm{GL}_{2n}(\mathbb{Z})$ such that $P_{\Lambda_2} = AP_{\Lambda_1}B$. Let's record this.

THEOREM 2.1. *Let $T_1 = \mathbb{C}^n/\Lambda_1$ and $T_2 = \mathbb{C}^m/\Lambda_2$ be two complex tori. Then T_1 and T_2 are isomorphic (as complex Lie gorups) if and only if $m = n$ and there are $A \in \mathrm{GL}_n(\mathbb{C})$ and $B \in \mathrm{GL}_{2n}(\mathbb{Z})$ such that*

$$P_{\Lambda_2} = AP_{\Lambda_1}B.$$

EXAMPLE 2.2. Let us consider the case of $n = 1$. So $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, where ω_1, ω_2 are $\mathbb{R}$-linearly independent complex numbers. First of all, $\{\omega_1\}$ is a basis of $\mathbb{C}$ (as a $\mathbb{C}$-vector space). Then we may assume that $\omega_1 = 1$ and hence the period matrix P_Λ is $[1 \quad \omega]$, where $\omega = \frac{\omega_2}{\omega_1}$. This corresponds to multiplying the period matrix by $A = \frac{1}{\omega_1}$ as in Theorem 2.1. Also we may assume that ω is in the upper half-plane; if necessary replace ω by $-\omega$. This corresponds to taking

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

in Theorem 2.1. So the period matrix of Λ can always be taken to be $[1 \quad \omega]$ where ω is in the upper half-plane. In other, words Λ is $\mathbb{Z} + \mathbb{Z}\omega$; so we write Λ_ω to denote this lattice and T_ω to denote the torus determined by this lattice. Using Theorem 2.1 again, we get that T_{ω_1} and T_{ω_2} are isomorphic if and only if there is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

such that $\omega_2 = \frac{b+d\omega_1}{a+c\omega_1}$. Note that this matrix has to be in $\mathrm{SL}_2(\mathbb{Z})$ since both ω_1 and ω_2 are in the upper half-plane. We will return to this example later.

Abelian varieties over $\mathbb{C}$ are certain complex tori. There are various ways to express the property that singles them out among the complex tori. One way is to define abelian varieties as complex tori that can be embedded into a projective space $\mathbb{P}^N(\mathbb{C})$; this means that T is an abelian variety if there is a holomorphic map $T \to \mathbb{P}^N(\mathbb{C})$ for some N that is injective and the image is a Zariski closed subset of $\mathbb{P}^N(\mathbb{C})$. This definition is not very good for our purposes since we have not defined most of the concepts involved, and more importantly it is hard

to validate this property. Also it is not very suitable for our purposes. For our definition, we need to recall some basic linear algebra concepts.

Let Λ be a lattice in $\mathbb{C}^n$ and let $\mu : \Lambda \times \Lambda \to \mathbb{Z}$ be an alternating bilinear map; that is to say that μ is $\mathbb{Z}$-linear in both coordinates and $\mu(a, a) = 0$ for all $a \in \Lambda$. This also gives $\mu(a, b) = -\mu(b, a)$ for all $a, b \in \Lambda$. First of all μ can be extended to $\mu_{\mathbb{R}} : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{R}$ via linearity; this is an alternating $\mathbb{R}$-bilinear map. Then the map $\nu(v, w) := \mu_{\mathbb{R}}(iv, w)$ is still an $\mathbb{R}$-bilinear map. If ν is symmetric, then we have a Hermitian form $H : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ given by

$$H(v, w) = \nu(v, w) + i\mu_{\mathbb{R}}(v, w).$$

If H is positive definite, then μ is called a *Riemann form* on Λ.

We could have gone the other way around. Meaning we could have started with a positive definite Hermitian form $H : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ and ask for $\mathrm{Im}(H) \restriction_{\Lambda \times \Lambda}$ to be $\mathbb{Z}$-valued.

DEFINITION 2.3. A complex torus $\mathbb{C}^n/\Lambda$ is an *abelian variety* if there is a Riemann form on Λ.

The fact mentioned above that says abelian varieties are exactly the complex tori that can be embedded into a complex projective space as a Zariski closed set is a terrific result due top Riemann. This property is also equivalent to T having a positive line bundle on it.[1]

One may express a bilinear map μ on Λ with a basis $\mathcal{B} = \{\lambda_1, \ldots, \lambda_{2n}\}$ by a $2n \times 2n$ matrix $A_{\mathcal{B}}$:

$$\mu(\sum k_i \lambda_i, \sum l_i \lambda_i) = \vec{k}^T A_{\mathcal{B}} \vec{l},$$

where $\vec{k}$ and $\vec{l}$ are (column) vectors of integers and $\vec{k}^T$ denotes the transpose of $\vec{k}$. Note that the ij^{th} entry a_{ij} of $A_{\mathcal{B}}$ is simply $\mu(\lambda_i, \lambda_j)$. This also explains how to extend μ to $\mu_{\mathbb{R}}$:

$$\mu_{\mathbb{R}}(v, w) = v^T A_{\mathcal{B}}\, w.$$

We leave the proof of the following as an exercise.

PROPOSITION 2.4. *Let $T = \mathbb{C}^n/\Lambda$ be a complex torus with a $\mathbb{Z}$-linear map μ on $\Lambda \times \Lambda$. Then μ gives a Riemann form if and only if there is a basis of $\mathcal{B}$ of Λ such that*

$$A_{\mathcal{B}} = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix},$$

where D is a diagonal $n \times n$ matrix with non zero integer entries $d_1, \ldots, d_n$ with $d_i | d_{i+1}$.

Let's see this in the case of $n = 1$ as a continuation of Example 2.2.

[1] More words that are not defined and not to be defined.

EXAMPLE 2.5. Let $\Lambda = \mathbb{Z}+\mathbb{Z}\omega$ be a lattice in $\mathbb{C}$ with ω in the upper half-plane. Define $\mu(a + b\omega, c + d\omega) = ad - bc$. It is straightforward to check that μ is indeed a Riemann form on Λ. This means that any 1-dimensional complex torus $T = \mathbb{C}/\Lambda$ is indeed and abelian variety. In this case, we may even embed T into $\mathbb{P}^2(\mathbb{C})$ in a relatively elementary way. Consider the following map:

$$\wp_\Lambda(z) := \frac{1}{z^2} + \sum_{\lambda\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right).$$

This function is meromorphic with poles of order 2 at each element of Λ; moreover it is periodic with periods being elements of Λ. It is called the *Weierstrass elliptic function* (with respect to Λ). Because of periodicity, defining $\wp_\Lambda$ on $T \setminus \{0\}$ makes sense and actually it is an analytic function on it. Then the function

$$z \mapsto (1 : \wp(z), \frac{1}{2}\wp'(z)), \quad 0 \mapsto (0 : 1 : 1)$$

sends T into $\mathbb{P}^2(\mathbb{C})$ in a holomorphic way and the image is the set of points $(x : y : z)$ satisfying an equation of the form $y^2z = x^3+axz^2+bz^3$. (This is just a homogenized version of $Y^2 = X^3 + aX + b$.) So it is a curve; such a curve is called an *elliptic curve*. One may show that each such curve arises from a torus $\mathbb{C}/\Lambda$.

One place where abelian varieties appear is as Jacobians of curves. We do not get into that phenomenal theory, instead we refer the reader to the classical book 'Principles of Algebraic Geometry' by Griffiths and Harris, [**12**].

CHAPTER 8

Pila-Wilkie Theorem and Its Applications

In this last part of the notes, we finally prove the promised theorem. We still need to introduce the concept of abelian variety and we still need to state the main ingredient of the proof, namely Pila-Wilkie Theorem. After doing these preparatory work, we outline the Pila-Zannier proof of the Manin-Mumford Conjecture. We leave two more black boxes; if time allows we could cover them as well.

Scanlon's expository paper [**26**] is an excellent source to understand the strategy at hand.

1. Counting Rational Points on Definable Sets

Before starting to work in the definable setting, we would like to mention some earlier results that already have the ideas of the Pila-Wilkie Theorem.

For a set $X \subseteq \mathbb{R}^n$, and $t > 0$, let

$$X(\mathbb{Q}, t) := \{\vec{x} \in X \cap \mathbb{Q}^n : H(\vec{x}) \leq t\}.$$

This set is clearly finite; if you wish, using Northcott's Theorem. The question is how is it related to t? Note that it could be $O(t^n)$; say by taking X to be $\mathbb{R}^n$. The idea of the theorems below is that it is sub-linear for suitable X. We first consider the case of a curve from the paper [**4**].

THEOREM 1.1 (Bombieri-Pila-1989). *Let X be the graph of a transcendental real analytic funtion $f : [0,1] \to \mathbb{R}$ and let $\epsilon > 0$. Then there is a constant $c = c(X, \epsilon)$ such that*

$$|X(\mathbb{Q}, t)| \leq ct^{\epsilon}$$

for any $t > 0$.

So in this case the cardinality of $X(\mathbb{Q}, t)$ is $O(t^{\epsilon})$; of course, the constant depends on ϵ. Note that it is really necessary that f is transcendental; for instance this does not work for $f(x) = x$. How to change this assumption for larger dimensions? This is where the o-minimality comes into the picture. It is provably hard to determine zero sets of (real) polynomials in $\mathbb{Q}^n$. This corresponds to finding rational points on real algebraic sets; such sets are definable in $(\mathbb{R}, +, \cdot, <, 0, 1)$; actually we do not really need the ordering to define an algebraic set. So it is really hopeless to answer this question as long as we allow X to

contain algebraic sets. Actually, we take out all connected infinite semi-algebraic sets, which are precisely the sets definable in $(\mathbb{R}, +, \cdot, <, 0, 1)$.

DEFINITION 1.2. Let $X \subseteq \mathbb{R}^n$. We define the *algebraic part* X_{alg} of X to be the union of all infinite connected semi-algebraic sets that are contained in X. We let the *transcendental part* to be $X_{tr} = X \setminus X_{alg}$.

The algebraic part is far from being definable in an o-minimal structure. It might be quite complicated. Let's consider an example, which is taken from the paper [**20**]. Let

$$X := \{(x, y, z) \in \mathbb{R}^3 : z = x^y, x, y \in [1, 2]\}.$$

Being the graph of a restricted analytic function, X is definable in $\mathcal{R}_{\text{an}}$. For every $q \in [2, 3] \cap \mathbb{Q}$, the set $\{(x, q, x^q) : x \in \mathbb{R}\}$ is a semi-algebraic set that is contained in X. It is not so easy, but one can actually prove that X_{alg} is the union of such sets.

THEOREM 1.3 (Pila-Wilkie [**20**]). *Let $X \subseteq \mathbb{R}^n$ be definable in an o-minimal expansion $\mathcal{R}$ of the real field, and let $\epsilon > 0$. Then there is $c = c(X, \epsilon) > 0$ such that*

$$|X_{tr}(\mathbb{Q}, t)| \leq ct^{\epsilon}$$

for all $t > 0$.

This version of the theorem will be enough for our applications, but for more complicated applications one might need to consider points of X in a number field, rather than $\mathbb{Q}$. Such a theorem can be proven using the methods of [**20**]. However, Pila later improved this result to "algebraic points of bounded degree". For this, we need a little more notation.

DEFINITION 1.4. Let $X \subseteq \mathbb{R}^n$, $t > 0$, and $d > 0$. Then we let $X(k, t)$ to denote the set

$$\{\vec{x} \in X : H(\vec{x}) \leq t, [\mathbb{Q}(\vec{x}) : \mathbb{Q}] \leq d\}.$$

Note that $X(\mathbb{Q}, t)$ is just $X(1, t)$.

THEOREM 1.5 (Pila [**21**]). *Let $X \subseteq \mathbb{R}^n$ be definable in an o-minimal expansion $\mathcal{R}$ of the real field, $d >$, and let $\epsilon > 0$. Then there is $c = c(X, k, \epsilon) > 0$ such that*

$$|X_{tr}(k, t)| \leq ct^{\epsilon}$$

for all $t > 0$.

Proofs of both of these theorems are very involved and are out of the scope of these notes. So we skip it. It is so far the biggest black box we assume in these notes.

2. The Case of the Multiplicative Group – Theorem of Mann

Before handling the Manin-Mumford Conjecture, we present a proof of a similar result with $(\mathbb{C}^\times)^n$ in the place of an abelian variety; we write $\mathbb{G}^n$ for this group. This is a theorem of H. Mann from [**18**]. The proof here is quite different than the original proof. Not only that Mann's proof is more elementary, but also the result is stronger than the result we prove. However, our aim is to illustrate Pila-Zannier strategy in a more amenable setting. The idea of presenting this result as a practice for the abelian variety case is not original; we borrowed it from the paper [**25**] by Scanlon. We do not follow the proof there; we give a somewhat easier one in the sense that one needs to know less to understand it. Some arguments appearing in this proof could be traced back to Section 5 of [**9**].

As mentioned above, in Mann's theorem we work in a power of the multiplicative group $\mathbb{C}^\times$ the complex field. The torsion subgroup of that group consists of the tuples of roots of unity; we denote this group as $\mathbb{U}^n$. So the result should involve points in a given algebraic set whose coordinates are roots of unity. We prove that the set of such elements is finite union of cosets of algebraic subgroups of $\mathbb{G}^n$. The formal result is as follows.

THEOREM 2.1. *Let $V \subseteq (\mathbb{C}^\times)^n$ be an algebraic set defined over a number field K. Then*

$$V \cap \mathbb{U}^n = \bigcup_{i=1}^{t} \alpha_i T_i \cap \mathbb{U}^n,$$

where T_i are algebraic subgroups of $\mathbb{G}^n$.

The assumption that V defined over a number field is just to skip a reduction step in the proof. So we might have assumed that that V is defined over $\mathbb{C}$.

2.1. Algebraic subgroups of $\mathbb{G}^n$. We review a very limited part of the theory of algebraic subgroups of $\mathbb{G}^n$; only the part that we need. For a more complete treatment of the subject, we refer the reader to the third chapter of [**3**].

For $k = (k_1, \ldots, k_n) \in \mathbb{Z}^n$, we define the group homomorphism

$$\chi_k : \mathbb{G}^n \to \mathbb{G}^1; \quad \chi_k(x) = x_1^{k_1} \cdots x_n^{k_n}.$$

We sometimes write x^k rather than $\chi_k(x)$, if there is no possible confusion.

For $M \in M_{l\times n}(\mathbb{Z})$, we define

$$\chi_M : \mathbb{G}^n \to \mathbb{G}^l; \quad \chi_M(x) = (\chi_{m_1}(x), \ldots, \chi_{m_l}(x)),$$

where $m_1, \dots, m_l$ are the rows of M. We sometimes write x^M in the place of $\chi_M(x)$.

Algebraic subgroups of $\mathbb{G}^n$ are exactly the kernels of χ_M for various M and l. We denote $\ker \chi_M$ as T_M. Such groups are irreducible if and only if they are connected. Moreover, a connected subgroup is isomorphic to $\mathbb{G}^{n-r}$, where r is the rank of M. For instance, consider T_M where

$$M = \begin{pmatrix} 2 & 1 \\ 6 & 1 \end{pmatrix}.$$

Then T_M consists of eight points: $(\pm 1, \pm 1)$, $(\pm i, \pm 1)$. The dimension of T_M is $2 - 2 = 0$, and it is not irreducible even though M has full rank.

Given an algebraic subgroup T, the irreducible component containing the identity turns out to be an algebraic subgroup of T and it is called the *connected component of* T, and is denoted as T^0. The index of T^0 in T is always finite. The connected component of T above is the identity, and hence its index is 8. Consider another example T_N, where

$$N = \begin{pmatrix} 6 & 4 \end{pmatrix}.$$

Then T_N is not connected and its connected component is T_{N^0}, where

$$N^0 = \begin{pmatrix} 3 & 2 \end{pmatrix}.$$

We leave finding the index of T_{N^0} in T_N as an exercise.

2.2. Interpreting Theorem 2.1 in the Pila-Wilkie Setting. Let $D := \{z \in \mathbb{C} : \mathrm{Re}(z) \in [0, 1)\}$, and define

$$E : D^n \to \mathbb{G}^n, \quad E(z_1, \dots, z_n) := (\exp(2\pi i z_1), \dots, \exp(2\pi i z_n)).$$

Below we let z denote a tuple, and sometimes we simply write $\exp(2\pi i z)$ in the place of $E(z)$. Note that E is a bijective map and is analytic on a neighborhood of D^n. (Actually it is the restriction of an entire function to D^n.)

Returning to Theorem 2.1, recall that we would like to understand $V \cap \mathbb{U}^n$ for an algebraic variety V in $\mathbb{G}^n$ defined over a number field K. More precisely, we would like to show that

$$V \cap \mathbb{U}^n = \bigcup_{i=1}^{t} \alpha_i D_i \cap \mathbb{U}^n,$$

where D_i are algebraic subgroups of $\mathbb{G}^n$. Since the collection of sets as in the right hand side of the equality is closed under finite intersections, we may assume that V is a hyper-surface. So let $V = V(f)$ for some $f \in K[x]$, and write $f(x) = \sum_{i \in I} a_i x^i$, where I is a set of multi-indices.

Let

$$X = E^{-1}(V) = \big\{z \in D^n : f(\exp(2\pi i z_1), \dots, \exp(2\pi i z_n)) = 0\big\}.$$

Let's identify $\mathbb{C}^n$ with $\mathbb{R}^{2n}$ via

$$(x_1 + iy_1, \ldots, x_n + iy_n) \mapsto (x_1, y_1, \ldots, x_n, y_n).$$

We still denote elements of $\mathbb{C}^n$ as $(z_1, \ldots, z_n)$.

With this identification E becomes definable in $\mathcal{R}_{\text{an,exp}}$; in particular the set $D^n \subseteq \mathbb{R}^{2n}$ is definable $\mathcal{R}_{\text{an,exp}}$, even though it is really definable in a simpler o-minimal structure $(\mathbb{R}, <)$. Therefore X is also definable in $\mathcal{R}_{\text{an,exp}}$.

Note that $E^{-1}(V \cap \mathbb{U}^n) = X \cap \mathbb{Q}^n$. Hence we may apply Pila-Wilkie Theorem (1.3) to obtain some information on the set we are interested in.

2.3. Determining X_{alg}. The first order of business is to determine X_{alg}. The following theorem of Ax from [**2**] is relevant for this purpose.

THEOREM 2.2. *Let $y_1, \ldots, y_n \in T\,\mathbb{C}[[T]]$ be linearly independent over $\mathbb{Q}$. Then*

$$\operatorname{trdeg}(\mathbb{C}(T)(y_1, \ldots, y_n, \exp y_1, \ldots, \exp y_n)/\mathbb{C}(T)) \geq n.$$

Now we can determine X_{alg} as the union of all cosets of infinite algebraic subgroups that are wholly contained in X. To be more precise let $\mathcal{T}$ be the collection of all cosets αT of infinite algebraic subgroups T of $\mathbb{G}^n$ with $\alpha T \subseteq V$, and let $\mathcal{L}$ be the collection of $(\alpha + L) \cap D^n$ in $\mathbb{C}^n$ such that $\exp((\alpha + L) \cap D^n) \in \mathcal{T}$.

PROPOSITION 2.3. *Let X be as above. Then*

$$X_{alg} = \bigcup_{A \in \mathcal{L}} A.$$

PROOF. Let $z \in X_{alg}$. This means that there is an irreducible infinite semialgebraic set S containing z such that $S \subseteq X$. We may assume that S is of o-minimal dimension 1. It follows from the quantifier elimination for RCF that S is a part of a real-algebraic curve; an irreducible Zariski closed subset of $\mathbb{R}^{2n}$ of dimension 1 intersected with an open subset of $\mathbb{R}^{2n}$. This curve is given by a function $s : (0, 1) \to D^n$ whose coordinates are given by Taylor series $s_1(t), \ldots, s_n(t)$. Let $z \in S$ and for each i let $s_i^* = s_i - z_i$. Since S is a real-algebraic curve, we have

$$\operatorname{trdeg}(\mathbb{C}(s_1^*, \ldots, s_n^*)/\mathbb{C}) = 1.$$

Therefore

$$\operatorname{trdeg}(\mathbb{C}(t)(s_1^*, \ldots, s_n^*)/\mathbb{C}(t)) = 0.$$

Also as $(\exp s_1, \ldots, \exp s_n) \in V$, we have

$$\operatorname{trdeg}(\mathbb{C}(t)(\exp s_1^*, \ldots, \exp s_n^*)/\mathbb{C}(t)) < n.$$

Hence by Theorem 2.2, the curve S is contained in an infinite affine space $\alpha + L$ over $\mathbb{Q}$; that is L is

$$\{z \in \mathbb{C}^n : k_1 z_1 + \cdots + k_n z_n = 0\}$$

for some integers $k_1, \ldots, k_n$ that are not all 0. Let $\alpha + L$ be a minimal such affine space, say of dimension d. We claim that $\exp(\alpha + L) \subseteq V$. Without loss of generality, $s_1^*, \ldots, s_d^*$ are linearly independent over $\mathbb{Q}$. Then $\exp s_1^*, \ldots, \exp s_d^*$ needs to be algebraically independent, otherwise we would get a contradiction by applying Theorem 2.2 once again. The algebraic group $D = \exp(L)$ is of dimension d as well and hence so does the coset βD, where $\beta = \exp \alpha$. Now $\exp(z) \in \beta D$ and is of transcendence degree d, then $\beta D \subseteq V$. □

It might look like at least the algebraic part of X is of the required form, but we need it to be the union of finitely many such cosets.

Definition 2.4. An element α of V is called *degenerate* if

$$\sum_{i \in I'} a_i \alpha^i = 0$$

for some nonempty proper subset I' of I. Let V_{dg} denote the set of degenerate elements of V.

We are aiming to show that $E^{-1}(V_{dg})$ is more or less X_{alg}. The obstacle is the following algebraic subgroup of $\mathbb{G}^n$:

$$B_f := \{\alpha \in \mathbb{G}^n : \alpha^i = \alpha^{i'} \text{ for all } i, i' \in I\}.$$

For $\alpha \in B_f$, we have $f(\alpha) = \sum_{i \in I} a_i \alpha^i = \beta \sum_{i \in I} a_i$, where $\beta = \alpha^i$ for some/all $i \in I$. It follows that if $V \cap B_f \neq \emptyset$, then $B_f \subseteq V$. Moreover, for any $\beta \in V$, the coset βB_f is contained in V as well. So if B_f is not the trivial group, then $X_{alg} = X$.

Proposition 2.5. *Let $T \leq \mathbb{G}^n$ be an infinite connected algebraic subgroup such that $T \nsubseteq B_f$, and let $\beta \in \mathbb{G}^n$. Suppose that $\beta T \subseteq V$, then $\beta T \subseteq V_{dg}$.*

Proof. Let $\dim T = d > 0$. Since T is connected there is an algebraic group embedding $\mathbb{G}^d \to \mathbb{G}^n$ whose image is T. Such an embedding is given as $\chi_M(y) = y^M$ for some $n \times d$ matrix M with integer entries. So elements of βT are of the form

$$(\beta_1 y^{m_1}, \ldots, \beta_n y^{m_n}) = \beta y^M,$$

where $m_1, \ldots, m_n$ are the rows of M. Therefore we have

$$\sum_{i \in I} a_i (\beta y^M)^i = \sum_{i \in I} a_i \beta^i y^{iM} = 0$$

for all $y \in \mathbb{G}^d$.

Since $T \not\subseteq B_f$, the set $J := \{iM : i \in I\}$ has at least two elements. Letting $b_j = \sum_{iM=j} a_i \beta^i$, we have

$$\sum_{j \in J} b_j y^{iM} = \sum_{j \in J} b_j \chi_j(y) = 0,$$

for all $y \in \mathbb{G}^d$. By linear independence of characters, we get $b_j = 0$ for all $j \in J$. Thus

$$b_j y^j = \sum_{iM=j} a_i \beta^i y^{iM} = 0,$$

for each $j \in J$. This means that $\sum_{iM=j} a_i x^i = 0$ for all $x \in T$, which means that $T \subseteq V_{dg}$. □

COROLLARY 2.6. *Let $T \subseteq \mathbb{G}^n$ be an infinite algebraic group such that $T^0 \not\subseteq B_f$, and let $\beta \in \mathbb{G}^n$. If $\beta T \subseteq V$, then $\beta T \subseteq V_{dg}$.*

PROOF. Write $T = T^0 \cup \alpha_1 T^0 \cup \cdots \cup \alpha_t T^0$. Then

$$\beta T = \beta T^0 \cup \beta\alpha_1 T^0 \cup \cdots \cup \beta\alpha_t T^0$$

Hence $\beta\alpha_i T^0 \subseteq V$ for each i; where $a_0 = 1$. Then $\beta\alpha_i T^0 \subseteq V_{dg}$ by the proposition above. Therefore $\beta T \subseteq V_{dg}$. □

COROLLARY 2.7. *Let $V_{alg} := E(X_{alg})$. Then $V_{alg} \subseteq V_{dg} \cup B_f$.*

The last piece for the proof of Theorem 2.1 is that $V \setminus V_{alg}$ is finite. This part will make use of the Pila-Wilkie Theorem.

PROPOSITION 2.8. *The set $(V \setminus V_{alg}) \cap \mathbb{U}^n$ is finite.*

PROOF. We show that elements of $X \setminus X_{alg}$ have bounded height, which will conclude the proof. Assume that this is not the case. Then for arbitrarily large $t \in \mathbb{N}$ we have $|X_{tr}(\mathbb{Q}, t-1)| < |X_{tr}(\mathbb{Q}, t)|$.

Let $x \in X_{tr}(\mathbb{Q}, t)$. This means that $x = (\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n})$ for integers $a_1, \ldots, a_n, b_1, \ldots, b_n$ with $0 \leq a_i < b_i \leq t$, $\gcd(a_i, b_i) = 1$, and

$$f(\exp(2\pi i \frac{a_1}{b_1}), \ldots, \exp(2\pi i \frac{a_n}{b_n})) = 0.$$

Let $L := K(\exp(2\pi i \frac{a_1}{b_1}), \ldots, \exp(2\pi i \frac{a_n}{b_n}))$. Note that $L|K$ is Galois and conjugates of $\exp(2\pi i \frac{a_i}{b_i})$ are of the form $\exp(2\pi i \frac{a}{b_1})$, where $0 < a < b_i$ with $\gcd(a, b_i) = 1$. So there are $\phi(b_i)$ many of them. It follows that the orbit of $\exp(2\pi i \frac{a_i}{b_i})$ under the action of $\mathrm{Gal}(L/K)$ contains at least $\frac{\phi(b_i)}{[K:\mathbb{Q}]}$ many elements. Note that this number is a rational number and it could even be less than 1. However, since $[K : \mathbb{Q}]$ is a fixed number, it gets larger as b_j gets larger. Since $|X_{tr}(\mathbb{Q}, t-1)| < |X_{tr}(\mathbb{Q}, t)|$ for arbitrarily large $t \in \mathbb{N}$, we see that $|X_{tr}(\mathbb{Q}, t)| \geq \frac{\phi(t)}{[K:\mathbb{Q}]}$ for arbitrarily large t, which is against Theorem 1.3. □

PROOF OF THEOREM 2.1. We proceed by induction on $|I|$. In the case when I is a singleton, there is nothing to prove; so let's assume $|I| > 1$.

For a nonempty $P \subseteq I$ we let

$$V_P := \Big\{\alpha \in \mathbb{G}^n : \sum_{i\in P} a_i x^i = 0\Big\}.$$

By the induction hypothesis, each $V_P \cap \mathbb{U}^n$ is a finite union of cosets $\alpha T \cap \mathbb{U}^n$, where T is an algebraic subgroup of $\mathbb{G}^n$.

Note that

$$V_{dg} = \bigcup_{\emptyset\neq P\neq I} (V_P \cap V_{I\setminus P}).$$

Therefore V_{dg} is also in the required form.

By Corollary 2.7 and Proposition 2.8, we know that $(V\setminus(V_{dg}\cup B_f))\cap\mathbb{U}^n$ is finite. Therefore $V \cap \mathbb{U}^n$ is a finite union of cosets $\alpha T \cap \mathbb{U}^n$, where T is an algebraic subgroup of $\mathbb{G}^n$. □

3. The Case of Abelian Varieties – Manin-Mumford Conjecture

The proof strategy from the previous section is due to Pila and Zannier appearing in [**22**], where it is applied to prove Manin-Mumford Conjecture mentioned in the introduction. We restate the result and present a proof. We skip a few proofs as they require a little more detailed understanding of abelian varieties than the amount we provided in these notes.

THEOREM 3.1 (Manin-Mumford Conjecture). *Let A be an abelian variety and let $V \subseteq A$ be an algebraic subvariety defined over a number field K. Then $V \cap \mathrm{Tor}(A)$ is a finite union of cosets of abelian subvarieties of A.*

Note that this version is slightly weaker than the version appearing in the introduction, because we assume that V is defined over a number field. As in the case of $\mathbb{G}^n$, this is not really a restriction; reducing the general statement to this one is a routine job once enough geometry is known.

3.1. Interpreting the statement in the o-minimal setting. Let $A = \mathbb{C}^n/\Lambda$ with $\Lambda = \mathbb{Z}\lambda_1 + \cdots + \mathbb{Z}\lambda_{2n}$. We identify $\mathbb{C}^n$ with $\mathbb{R}^{2n}$ in a different way than before: We know that $\mathbb{C}^n = \mathbb{R}\lambda_1 + \cdots + \mathbb{R}\lambda_{2n}$ and we identify $r_1\lambda_1 + \cdots + r_{2n}\lambda_{2n}$ with $(r_1, \ldots, r_{2n}) \in \mathbb{R}^{2n}$. Let $\pi : \mathbb{R}^{2n} \to A$ be the map sending $(r_1, \ldots, r_{2n})$ to $r_1\lambda_1 + \cdots + r_{2n}\lambda_{2n} + \Lambda$. This is an analytic map.

Let $F = [0, 1)^{2n}$. Clearly, F is definable in $(\mathbb{R}, <)$. Note that $\pi|_F$ is a bijective definable map; from now on π will refer to this restriction.

Note that $\pi^{-1}(\mathrm{Tor}(A)) = F \cap \mathbb{Q}^{2n}$. Moreover, we know that A is a Zariski closed subset of $\mathbb{P}^N(\mathbb{C})$ for some N, which can be embedded into $\mathbb{R}^M$ as a definable set in $(\mathbb{R}, +, \cdot)$.[1] This way π becomes definable in $\mathcal{R}_{\mathrm{an}}$ and $X := \pi^{-1}(V)$ a definable subset of F. Therefore our interest is in the set $X \cap \mathbb{Q}^{2n}$, and hence we could apply Pila-Wilkie Theorem.

3.2. Structure of X_{alg}. We do not get into the details of this. We will just say that there is a version of Ax's theorem about power series and their exponentials by Bertrand and Pillay that is suitable for this case.[2] As a result one may prove that X_{alg} is a union of affine linear spaces intersected with F.

Recall that the arguments in the case of $\mathbb{G}^n$ to show that X_{alg} is a finite union of affine linear spaces was very elementary in spirit, and were using the equations for V. This is why that path does not generalize to the case of abelian varieties, because even writing down the equations of A itself is a notoriously hard business. So we skip this as well and just state without proof that

$$X_{alg} = \alpha_1 + B_1 \cup \cdots \cup \alpha_t + B_t$$

where $B_1, \ldots, B_t$ are infinite abelian subvarieties of A.

4. Galois orbits

[1] This is not a trivial thing to do, but it is a routine model theoretic argument.

[2] We also let the reader figure out why the original version does not work out.

TO DO

(1) Add sections on *Nonstandard Analysis* and *Ultrproducts*.
(2) Add section on *Basic Algebraic Geometry*.
(3) Finish the proof of Manin-Mumford.
(4) Describe the Jacobian of a curve.
(5) Add some words on Mordell-Lang and André-Oort.

Bibliography

[1] James Ax. Injective endomorphisms of varieties and schemes. *Pacific J. Math.*, 31:1–7, 1969.

[2] James Ax. On Schanuel's conjectures. *Ann. of Math. (2)*, 93:252–268, 1971.

[3] E. Bombieri and W. Gubler. *Heights in Diophantine Geometry*. New Mathematical Monographs. Cambridge University Press, 2006.

[4] E. Bombieri and J. Pila. The number of integral points on arcs and ovals. *Duke Math. J.*, 59(2):337–357, 1989.

[5] J. W. S. Cassels. *Local fields*, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1986.

[6] J. Denef and Lou van den Dries. p-adic and real subanalytic sets. *Ann. of Math. (2)*, 128(1):79–138, 1988.

[7] Lou van den Dries. Remarks on Tarski's problem concerning $(\mathbf{R}, +, \cdot, \exp)$. In *Logic colloquium '82 (Florence, 1982)*, volume 112 of *Stud. Logic Found. Math.*, pages 97–121. North-Holland, Amsterdam, 1984.

[8] Lou van den Dries. *Tame topology and o-minimal structures*, volume 248 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1998.

[9] Lou van den Dries and Ayhan Günaydın. The fields of real and complex numbers with a small multiplicative group. *Proc. London Math. Soc. (3)*, 93(1):43–81, 2006.

[10] Lou van den Dries and Chris Miller. On the real exponential field with restricted analytic functions. *Israel J. Math.*, 85(1-3):19–56, 1994.

[11] A. M. Gabrièlov. Projections of semianalytic sets. *Funkcional. Anal. i Priložen.*, 2(4):18–30, 1968.

[12] Phillip Griffiths and Joseph Harris. *Principles of algebraic geometry*. Pure and Applied Mathematics. Wiley-Interscience [John Wiley & Sons], New York, 1978.

[13] A. Günaydın. Mathematical logic – lecture notes. available at `http://web.boun.edu.tr/ayhan.gunaydin/Logic_Notes.pdf`.

[14] Martin Hils and François Loeser. *A first journey through logic*, volume 89 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2019.

[15] A. G. Hovanskiĭ. A class of systems of transcendental equations. *Dokl. Akad. Nauk SSSR*, 255(4):804–807, 1980.

[16] Jonathan Kirby. *An invitation to model theory*. Cambridge University Press, Cambridge, 2019.

[17] S. Lang. *Algebra*. Addison-Wesley Publishing Co. Inc., Reading, Mass., 1997.

[18] H. Mann. On linear relations between roots of unity. *Mathematika*, 12:107–117, 1965.

[19] D. Marker. *Model Theory. An Introduction.* Graduate Texts in Mathematics, 217. Springer-Verlag, New York, 2002.

[20] J. Pila and A. J. Wilkie. The rational points of a definable set. *Duke Math. J.*, 133(3):591–616, 2006.

[21] Jonathan Pila. On the algebraic points of a definable set. *Selecta Math. (N.S.)*, 15(1):151–170, 2009.

[22] Jonathan Pila and Umberto Zannier. Rational points in periodic analytic sets and the Manin-Mumford conjecture. *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl.*, 19(2):149–162, 2008.

[23] Anand Pillay and Charles Steinhorn. Definable sets in ordered structures. I. *Trans. Amer. Math. Soc.*, 295(2):565–592, 1986.

[24] M. Raynaud. Sous-variétés d'une variété abélienne et points de torsion. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 327–352. Birkhäuser Boston, Boston, MA, 1983.

[25] Thomas Scanlon. Counting special points: logic, Diophantine geometry, and transcendence theory. *Bull. Amer. Math. Soc. (N.S.)*, 49(1):51–71, 2012.

[26] Thomas Scanlon. A proof of the André-Oort conjecture via mathematical logic [after Pila, Wilkie and Zannier]. Number 348, pages Exp. No. 1037, ix, 299–315. 2012. Séminaire Bourbaki: Vol. 2010/2011. Exposés 1027–1042.

[27] A. J. Wilkie. Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function. *J. Amer. Math. Soc.*, 9(4), 1996.

Index

L_{or}, 21
$L_{\mathbb{Q}\text{-vs}}$, 8
L_{ab}, 8
L_{o}, 8
$R^{>0}$, 41
$\mathcal{R}_{\text{an}}$, 45
$\mathbb{Q}_p$, 63
$\forall\exists$-formula, 34
κ-categorical, 27
$\mathcal{R}_{\text{exp}}$, 44
ACF_p, 28
ACF, 28
DAG, 28
DLO, 27
DOAG, 31
f-adic absolute value, 62
p-adic absolute value, 62
p-adic integer, 71
p-adic numbers, 63
Łoś-Vaught Test, 28

Absolute value, 61
Algebraic part of a set, 78
Archimedean, 63
Arity, 8
Atomic formula, 9
Automorphism, 26
Ax's Theorem, 29
Axioms of a Formal Theory, 15

Bound variable, 10
Boundary, 37

Cell, 47
Cell Decomposition Theorem, 50
Chain of structures, 34
Closure, 37
Compactness Theorem, 21
Complete absolute value, 63
Complete theory, 20
Completeness Theorem, 17, 18
Completion of an absolute value, 63
Connected component of an algebraic group, 80
Consistent, 17

Decomposition, 50
Deduction Theorem, 17
Deductively closed, 24
Definable function, 30
Definable set, 30
Definably Connected, 39
Dimension, 55
Discrete place, 71
Divisible Ordered Abelian Groups, 28

Elementarily equivalent, 19
Elementary equivalence, 19
Elliptic curve, 76
Embedding, 26
Equivalence of terms, 14
Euler characrteristic, 58
Euler characteristic, 60
Expansion, 21

Family of definable sets, 32
First order language, 7
Formal first order theories, 15
Formula, 9
Free variable, 10
Frontier, 37

Generalization, 16

Height, 68
Henkin Construction, 23
Hensel's lemma, 72
Homomorphism, 26

Inconsistent, 17
Inference Rules, 16
Interior, 37

Intermediate Value Property, 40
Interpretation, 10
Isomorphic, 26
Isomorphism, 26

Kronecker's Theorem, 69

Language, 7
Language of abelian groups, 8
Language of orderings, 8
Language of vector spaces over $\mathbb{Q}$, 8
Lattice, 73
Lefschetz Principle, 34
Lindenbaum's Lemma, 24
Local parameter, 71
Local-global Principle, 34
Logical closure, 20
Logical consequence, 15
Logically equivalent, 15
Logically valid, 15
Löwenheim-Skolem Theorem, 22, 25

Manin-Mumford Conjecture, 6, 84
Mann's Theorem, 79
Model, 15
Modus Ponens, 16
Monotonicity Theorem, 50

Non-archimedean, 62
Norm, 64
Northcott's Theorem, 70

o-minimal group, 40
o-minimal structure, 38
Ordered field, 41
Ordered group, 40
Ordered ring, 41
Ordered structure, 37
Ordered vector space, 43
Ostrowski Theorems, 64

Period matrix, 73
Pila-Wilkie Theorem, 78
Place, 64
Predicate Logic, 16
Product formula, 67
Proof, 16

Quantifier elimination, 31
Quantifier-free formula, 30

Reduct, 21
Residue field, 70
Residue map, 70
Riemann form, 75

Satisfaction (of a formula), 11
Satisfiable, 15
Scope, 9
Section, 32
Semi-algebraic set, 44
Sentence, 10
Strong homomorphism, 26
Structure, 10
Substructure, 26

Tarski-Seidenberg Theorem, 31
Term, 8
Theorem, 16
Theory, 20
Transcendental part of a set, 78

Uniform Finiteness, 50
Universe, 10

Valuation, 71
Valuation ring, 70

Weak Cell Decomposition Theorem, 47
Weierstrass Elliptic Function, 76