Introductory model theory with elements of universal algebra (version 9)

Will Johnson

Autumn 2022

Preface

This is a provisional draft of the course notes for Introductory Model Theory at Fudan University in Autumn 2022. The goal is to present the basic topics of model theory without assuming much background in abstract algebra. Please send any comments or corrections to willjohnson@fudan.edu.cn.

The current draft has no examples, motivations, or explanations after Section 6.4.

There are a number of optional reading sections, marked with the symbols $\diamondsuit$ and $\spadesuit$. The $\diamondsuit$ sections contain additional examples and interesting trivia. The $\spadesuit$ sections contain technical details and more advanced content.

The approach of these notes

Many textbooks in model theory assume a large amount of mathematical background knowledge, especially in abstract algebra. For example, Poizat's *Course in Model Theory*—which is better than most textbooks in this regard—assumes you know the definition of fields, rings, homomorphisms, and ideals.

There is a good reason for this approach: model theory as a subject is mostly about the applications of mathematical logic to other branches of mathematics, especially abstract algebra. However, this works poorly for our class, which is not in the mathematics department and not intended solely for mathematics majors.

In contrast, these notes will try to minimize the required mathematical background. Model theory is a branch of mathematics, so it would be impossible to explain the subject without *any* mathematical background. I assume you know what sets, functions, and ordered pairs are. (Much of this material is reviewed in Appendix A.) But I will not assume any background in abstract algebra. In theory, mathematical logic is a prerequisite for this course, so these notes will assume a little bit of background from mathematical logic, mostly set theory.

One approach would be to avoid the concepts from abstract algebra (fields, rings, etc.) entirely, instead focusing on combinatorial examples like the random graph. Model theory *can* be presented in this way, but one loses much of the motivation, examples, intuition, and applications of the subject.

Instead, we will build up elements of abstract algebra from scratch, defining concepts like fields, rings, homomorphisms, and ideals and proving their basic properties. This will allow us to work through the model theory of algebraically closed fields, which has served as an important example in the history of the subject.

Our approach towards abstract algebra will emphasize ideas from *universal algebra*. Universal algebra is a subject which finds the parallels between ring theory, group theory, lattice theory, and other topics in algebra. For example, "ideals" in ring theory and "normal subgroups" in group theory are both instances of the more fundamental concept of "congruences" in universal algebra.

There are two reasons to use universal algebra in these notes. On a basic level, it allows us to efficiently explain concepts in ring theory and group theory simultaneously. More importantly, universal algebra is tightly connected to model theory. One could say that universal algebra is a special case of model theory, or model theory is a generalization of universal algebra. For example, Chang and Keisler describe model theory as "universal algebra plus logic" in their textbook. Consequently, one of the goals of these notes will be to emphasize the parallels between universal algebra and model theory.

Notation and conventions

We generally follow standard mathematical notation, some of which is reviewed in Appendix A. Here are some points to be aware of:

- $A \subseteq B$ means that A is a subset of B. $A \subsetneq B$ means that A is a proper subset of B. We don't use the symbol $A \subset B$. $A \not\subseteq B$ means that A is not a subset of B.

- $A \subseteq_f B$ means that A is a finite subset of B.

- The powerset of S is written $\mathfrak{P}(S)$.

- The empty set is written $\varnothing$.

- $\bar{x}$ means $(x_1, x_2, \ldots, x_n)$, where n is determined by the context. The symbols $\bar{a}, \bar{b}, \bar{c}, \bar{d}, \bar{y}, \bar{z}, \ldots$ work similarly.

- $f : A \to B$ means that f is a function from A to B. If we are talking about some function f, then $x \mapsto y$ means $f(x) = y$. If $X \subseteq A$, then $f(X)$ denotes the direct image, and if $X \subseteq B$ then $f^{-1}(X)$ denotes the inverse image. The domain and range of f are written $\mathrm{dom}(f)$ and $\mathrm{im}(f)$.

- $x := \ldots$ means "[by the way,] let x be $\ldots$". The notation $\ldots =: x$ means the same thing.

- $\mathbb{N}$ means the natural numbers, including 0:

  $$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$

  We also denote this set by ω or $\aleph_0$.

- $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$, and $\mathbb{C}$ denote the real numbers, the rational numbers, the integers, and the complex numbers, respectively.

- $\forall x$ means "for every x", and $\exists x$ mean "there is an x such that".

- If E is an equivalence relation on some set X and a is an element, then $[a]$ or $[a]_E$ denotes the equivalence class of a, and X/E denotes the set of all equivalence classes.

- If A is a set, we write the cardinality (size) of A as $|A|$.

Introduction

The story of model theory is like a novel that unexpectedly changes genres halfway through. What began as a branch of mathematical logic later became "universal algebra plus logic" in Chang and Keisler's formulation, and then "algebraic geometry minus fields" in Hodges' formulation. This makes the subject a little hard to precisely define.

At the end of the day, model theory is a network of closely connected definitions and tools, all related to the notion of "model." This introduction is a survey of these definitions and tools. The goal of model theory is not so much to understand "models", but instead to build on this network and apply it to other branches of mathematics.

0.1 Models

Mathematical knowledge is obtained through deductive reasoning—through *proofs*. Proofs must begin somewhere, with a set of *axioms*—statements we assume without proof. When reasoning about numbers, one might take the following set of statements as axioms:

1. If x and y are numbers, then $x + y$ and $x \cdot y$ are numbers.

2. If x and y are numbers, then $x + y = y + x$ and $x \cdot y = y \cdot x$.

3. If x, y, and z are numbers, then $x+(y+z) = (x+y)+z$ and $x\cdot(y\cdot z) = (x \cdot y) \cdot z$.

4. If x, y, and z are numbers, then $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

5. There is a number 0 such that $x + 0 = x$ for any number x.

6. There is a number 1 such that $x \cdot 1 = x$ for any number x.

7. For any number x, there is a number called $-x$ such that $x+(-x)=0$.
8. For any number x other than 0, there is a number called x^{-1} such that $x\cdot(x^{-1})=1$.

We can use these axioms to deduce other facts about numbers. Here is an example:

Theorem 0.1.1. *For any number x, $x\cdot 0=0$.*

Proof. If $y=x\cdot 0$, then

$$\begin{aligned} y &\overset{(5)}{=} y+0 \overset{(7)}{=} y+(y+(-y)) \overset{(3)}{=} (y+y)+(-y) \\ &= ((x\cdot 0)+(x\cdot 0))+(-y) \overset{(4)}{=} x\cdot(0+0)+(-y) \\ &\overset{(5)}{=} x\cdot 0+(-y) = y+(-y) \overset{(7)}{=} 0. \end{aligned}$$

□

With more work (Corollary 1.4.14, Theorem 1.4.16), one can prove other algebraic facts, such as

$$x\cdot y=0 \iff (x=0 \text{ or } y=0)$$
$$(-x)\cdot(-y)=x\cdot y.$$

How about the following?

$$x+x=y+y \overset{?}{\Longrightarrow} x=y. \qquad (*)$$

This is certainly true for real numbers, but can we prove $(*)$ from the axioms? Surprisingly, **we cannot**. To see this, suppose we that 0 and 1 are the only "numbers", and that "+" and "·" are defined as follows:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

For example, "$1+1=0$" under this interpretation. By checking all the cases, one can verify that all of Axioms (1)–(8) hold. Anything which is provable from the axioms, such as Theorem 0.1.1, must be true in this interpretation. However, $(*)$ fails:

$$1+1=0+0 \text{ but } 1\neq 0.$$

Therefore $(*)$ cannot be proven from Axioms (1)–(8).

Our strange way of interpreting "number", "0", and "1" is an example of a **model**—in this case a model of Axioms (1)–(8).

Remark 0.1.2. Axioms (1)–(8) are called the *field axioms*, and their models are called *fields*. Fields are one of the central objects of study in the branch of mathematics called *abstract algebra*.

♢ Some history

The toy example above is parallel to an important saga in the history of mathematics. In ancient times, the Hellenistic mathematician Euclid wrote a book called the *Elements* in which he developed geometry from a set of five axioms. Four of these axioms were simple, intuitive statements, like "any two points are on a line" or "any two right angles are congruent." In contrast, the fifth axiom was a complicated geometric statement about parallel lines. This was the so-called *parallel posulate*.

Many people were unhappy with the parallel postulate, because it seemed less obvious and more arbitrary than the other four axioms. It felt like something that should be a theorem or a lemma, not an axiom. Euclid himself avoided using the parallel postulate until absolutely necessary. *If* one could find a proof of the parallel postulate from the other four axioms, the problem would go away: the parallel postulate could be demoted to a theorem and geometry could be developed on the firm foundation of the four intuitive axioms.

In the 2000 years after Euclid, there were many unsuccessful attempts to find such a proof. Eventually the matter was settled in 1868 when the mathematician Beltrami constructed a model of Euclid's first four axioms in which the parallel postulate is false. This model is called *hyperbolic geometry*, and is the precursor to the sort of "curved" geometries used in Einstein's theory of general relativity.

0.2 Complete theories

A *theory* is a set of axioms. If T is a theory, we write $M \models T$ to indicate that M is a model of T, and $M \models \varphi$ to indicate that M satisfies a sentence φ. For example, if T is the field axioms (1)–(8) of the previous section and φ is Statement $(*)$, then the standard real numbers $\mathbb{R}$ satisfy both T and φ

$$\mathbb{R} \models T \text{ and } \mathbb{R} \models \varphi,$$

but we constructed a different model M such that

$$M \models T \text{ and } M \not\models \varphi.$$

A theory T is *complete* if for every sentence φ, either T proves φ or T disproves φ. If we can completely axiomatize a structure, then we can determine all its logical properties:

Fact 0.2.1. *Let T be a complete theory.*

1. *If $M \models T$, then for any sentence φ,*

$$M \models \varphi \iff (\varphi \textit{ is provable from } T)$$

2. *If T is finite or computable, then there is an algorithm which takes a sentence φ as input and outputs whether or not φ is provable from T.*

The problem we ran into in the previous section is that the field axioms are not complete—they neither prove nor disprove the statement $(*)$. Can we fix the problem and write down a complete axiomatization for numbers?

To begin with, let's add the following axioms:

$$\begin{gathered} 1+1 \neq 0 \\ 1+1+1 \neq 0 \\ 1+1+1+1 \neq 0 \\ \cdots \end{gathered}$$

The first of these axioms gets rid of the bad model M of the previous section, which is a good start. Models of the resulting theory are called *fields of characteristic 0.*

Sadly, the resulting theory is still not complete. For example, consider the statement

> For every number x, there is a number y with $y^2 = x$.

This is true if "number" means "complex number", and false if "number" means "real number." In other words, the two models $\mathbb{C}$ and $\mathbb{R}$ show incompleteness.

We should probably decide whether we are trying to axiomatize the complex numbers $\mathbb{C}$ or the real numbers $\mathbb{R}$. It turns out to be easier to axiomatize $\mathbb{C}$.

Definition 0.2.2. A field is *algebraically closed* if it satisfies the following axiom: for any numbers $a_0, a_1, \ldots, a_{n-1}$, there is a number x such that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

In other words, every polynomial equation has a solution.

The field of complex numbers $\mathbb{C}$ is algebraically closed, a fact known as the *fundamental theorem of algebra*. In contrast, the field of real numbers $\mathbb{R}$ is *not* algebraically closed, as $x^2 + 1 = 0$ has no solutions.

If we combine the axioms defining fields of characteristic zero and the axioms defining algebraically closed fields, we get a theory called ACF_0, whose models are algebraically closed fields of characteristic 0. The complex numbers are a model. In Section 9.4 we will prove the following:

Fact 0.2.3. *The theory* ACF_0 *is complete.*

Consequently:

1. A sentence φ is true in $\mathbb{C}$ if and only if it is provable from the ACF_0 axioms.

2. There is an algorithm which takes φ as input and determines whether φ is true in $\mathbb{C}$.

Remark 0.2.4. There is also a theory called RCF which completely axiomatizes $\mathbb{R}$. Models of RCF are called *real closed fields*.

0.3 Categoricity

Model theory provides a number of methods to prove that a theory T is complete by analyzing the structure of the models of T. One such method is *categoricity*.

Definition 0.3.1. Let κ be an infinite cardinal number like $\aleph_0$ or $\aleph_1$. A theory T is *κ-categorical* if T has exactly one model of size κ.

Fact 0.3.2 (Łoś-Vaught criterion)**.** *If a theory T is κ-categorical and all models of T are infinite, then T is complete.*

Conveniently, it is a theorem in abstract algebra that ACF_0 is κ-categorical for all uncountable κ:

Fact 0.3.3 (Steinitz)**.** *If κ is an uncountable cardinal, then there is exactly one algebraically closed field of characteristic 0 and size κ.*

Algebraically closed fields are infinite (see Theorem 9.2.3), and so ACF_0 is complete by the Łoś-Vaught criterion.

Remark 0.3.4. This technique is less flexible than one might hope for. In fact, algebraically closed fields are the *only* fields which can be completely axiomatized by κ-categorical theories. We will see a little bit of the proof in Section 13.4, but the bulk of the proof requires stability theory and is beyond the scope of this course.

0.4 Definable sets

If M is a model, a subset $D \subseteq M$ is *definable* if $D = \{x \in M : \varphi(x)\}$ where $\varphi(x)$ is a logical statement about x. For example, the set

$$\{x \in \mathbb{R} : x \text{ has a square root}\} = \{x \in \mathbb{R} : x \geq 0\}$$

is definable in the field $\mathbb{R}$. More generally, a set $D \subseteq M^n$ in n variables is definable if

$$D = \{(x_1, \ldots, x_n) \in M^n : \varphi(x_1, \ldots, x_n)\}$$

where $\varphi(x_1, \ldots, x_n)$ is a statement about the variables $x_1, \ldots, x_n$. For example, the unit circle is definable in the field $\mathbb{R}$

$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}. \tag{†}$$

In some models, there are very many definable sets:

Fact 0.4.1 (Robinson)**.** *In the field $\mathbb{Q}$, every computable set $S \subseteq \mathbb{Q}^n$ is definable.*

For example, the set of Fibonacci numbers $\{1, 2, 3, 5, 8, 13, \ldots\}$ is definable. We will see a variant of Fact 0.4.1 in Section 3.9.

In other models, there are very few definable sets:

Definition 0.4.2. In a field K, a set is *constructible* if it is a finite union of sets of the form

$$\begin{aligned}\{(x_1, \ldots, x_n) \in K^n : &P_1(x_1, \ldots, x_n) = P_2(x_1, \ldots, x_n) = \cdots \\ &= P_m(x_1, \ldots, x_n) = 0 \neq Q(x_1, \ldots, x_n)\}\end{aligned}$$

where $P_1, \ldots, P_m, Q$ are polynomials.

For example, the unit circle (†) is constructible.

Fact 0.4.3. *In algebraically closed fields such as $\mathbb{C}$, the definable sets are exactly the constructible sets.*

Constructible sets are a slight generalization of what algebraic geometers call *varieties*, and Fact 0.4.3 is equivalent to a fact called Chevalley's Theorem in algebraic geometry. We will prove Fact 0.4.3 in Section 9.4 as a consequence of *quantifier elimination.*

One consequence of Fact 0.4.3 is that definable sets in one variable are very simple:

Corollary 0.4.4. *If M is an algebraically closed field and $D \subseteq M$ is definable, then D is finite or the complement of a finite set.*

One says that a theory T is *strongly minimal* if the models of T have this property. It turns out that strong minimality is closely connected to categoricity.

Fact 0.4.5 (= Corollary 14.2.7)**.** *If T is strongly minimal and complete, then T is κ-categorical for all $\kappa > \aleph_0$.*

Remark 0.4.6. In more advanced model theory, one can show that if T is κ-categorical for at least one $\kappa > \aleph_0$, then T is tightly connected to a strongly minimal theory in a certain sense. As a consequence, T is κ-categorical for *all* $\kappa > \aleph_0$, a fact known as *Morley's Theorem.*

Strong minimality also has an interesting consequence for definable sets in more than one variable:

Fact 0.4.7. *Let M be a model of a strongly minimal theory. To each definable set $D \subseteq M^n$, we can associate a natural number called the* dimension *of D, written* $\dim(D)$*, with the following properties, among others:*

1. $\dim(X) > 0$ *if and only if D is infinite.*

2. $\dim(M^n) = n$.

3. $\dim(X \cup Y) = \max(\dim(X), \dim(Y))$.

4. $\dim(X \times Y) = \dim(X) + \dim(Y)$.

5. *If $f : X \to Y$ is a definable bijection, then* $\dim(X) = \dim(Y)$.

The intuition is that $\dim(D)$ measures the number of "degrees of freedom" of a value in D. For example, the unit circle $x^2 + y^2 = 1$ has one degree of freedom, because the value x almost determines the pair (x, y). In contrast, the plane $\mathbb{C}^2$ has two degrees of freedom, because x and y can vary freely. We will verify Fact 0.4.7 in Sections 14.5–14.6.

In the case of algebraically closed fields, $\dim(D)$ is something that algebraic geometers call *Krull dimension*. More generally, model theorists like to take concepts from algebraic geometry and extend them from algebraically closed fields to other strongly minimal theories. This is perhaps why Hodges characterizes model theory as "algebraic geometry minus fields" in his textbook.

0.5 An outline of this book

Chapters 1 and 2 are about *universal algebra*, which is the special case of model theory where axioms must be *equations* like the distributive law or associative law

$$\begin{gathered} x \cdot (y + z) = (x \cdot y) + (x \cdot z) \\ x + (y + z) = (x + y) + z \end{gathered}$$

rather than more complicated sentences like

For every x, there is a y such that $y \cdot y = x$ or $y \cdot y = -x$.

An *equational theory* is a set of equations. Many important classes of structures from abstract algebra, such as groups and rings, are defined by equational theories, as we will see in Chapter 1. Moreover, certain algebraic constructions like products and quotients make sense in any equational theory, as we will see in Chapter 2. In fact, these constructions precisely characterize which classes of structures are defined by equational theories, a fact known as *Birkhoff's HSP theorem* (Theorem 2.9.2). Along the way, we will develop basic ring theory, using it as a running example of universal algeba. This ring theory will be used later in Chapter 9 when we axiomatize the complex numbers.

We begin the study of model theory proper in Chapter 3, where we define the basic notions of languages, structures, formulas, satisfaction, theories, models, elementary classes, elementary equivalence, elementary maps, and definable sets. Chapter 4 is about the *compactness theorem*, the most important fundamental tool of model theory. We apply the compactness theorem in Chapter 5 on categoricity, where we prove the Łoś-Vaught criterion (Theorem 5.6.2) mentioned above.

Chapter 6 is about *ultraproducts*, a mysterious construction which plays the same role in general model theory that products, quotients, etc. play in universal algebra. We use ultraproducts to give another proof of the compactness theorem (Theorem 6.2.14), and then discuss some analogues of Birkhoff's HSP theorem using ultraproducts in Sections 6.5–6.6.

In Chapter 7, we review basic pointset topology, and apply it to build the topological space S of complete theories. The compactness theorem can be understood as the statement that S is compact (Theorem 7.3.4), and ultraproducts correspond to a certain kind of limit in this topological space (Theorem 7.3.5). The construction of S serves as a prototype of several constructions appearing later in the book.

Chapter 8 is about types and quantifier elimination, two topics which happen to be interconnected. A *type* is a description of a potential object which may not exist in the current model, but exists in some other model. Most applications of the compactness theorem boil down to *realizing* types—finding the element described by a type. Meanwhile, *quantifier elimination* is an important technical tool that allows us to model-theoretically analyze good theories and structures. For example, quantifier elimination gives control over definable sets, and can be used to detect whether a theory is complete.

In Chapter 9, we begin studying the model theory of algebraically closed fields, leading to the complete axiomatization of the complex numbers in Corollary 9.4.7. We continue to develop the model theory of algebraically closed fields in later chapters, using it as a running example.

The next two chapters are about models where "anything which can happen does happen", in two slightly different senses. Chapter 10 is about *existentially closed models*. Existentially closed models are a useful way of constructing new models of a given theory—for example, we will use them to show that algebraically closed fields *exist*. Existentially closed models can also be used to construct new theories and prove quantifier elimination.

Meanwhile, Chapter 11 is about *monster models*—models where every "small" type is realized. Monster models exist (Theorem 11.4.8), and possess a number of nice properties with respect to definable sets, types, and automorphisms (Sections 11.2–11.3). In advanced model theory, it is common to fix a monster model $\mathbb{M}$ and always work inside $\mathbb{M}$. Monster models also provide a nice way of thinking about quantifier elimination (see Theorem 11.5.4).

The final three chapters return to the theme of categoricity. Recall that a theory is κ-categorical if it has exactly one model of size κ. Chapter 12 is about *countable categoricity*, the case where $\kappa = \aleph_0$. It turns out that a structure M can be axiomatized by an $\aleph_0$-categorical theory if and only if M satisfies certain structural properties with respect to types, definable sets, and automorphisms (Theorems 12.3.5 and 12.3.6). Chapter 13 is a digression on abstract *closure operations* and the special family of closure operations known as *pregeometries* or *matroids*. We use pregeometries to classify vector spaces, getting more examples of κ-categorical theories (Corollary 13.7.6).

Finally, Chapter 14 is about *strongly minimal theories*, a special class of uncountably categorical theories including algebraically closed fields. Using pregeometries, we prove that strongly minimal theories are uncountably categorical (Corollary 14.2.7), and we develop the dimension theory described in Section 0.4 above. In fact, this dimension theory works in *any* uncountably categorical theory, but the proof is beyond the scope of this book.

Contents

Chapter 1

Algebras and equational classes

In this chapter, we introduce several important classes of structures from abstract algebra, including *monoids*, *groups*, *rings*, and *fields*. The definitions of these concepts look very similar to each other on an abstract level. Each definition has the form

> A Foo is a set together with some operations, satisfying a certain list of equations,

where Foo is "monoid", "group", "ring", and so on.

This suggests the abstract notion of an *equational class*—a class of structures defined by a set of equations. The class of monoids is an equational class, and the same holds for groups and rings. We precisely define equational classes in Section 1.3. Equational classes allow us to uniformly treat certain concepts in algebra. For example, in Section 1.4, we define the important algebraic concepts of *homomorphisms* and *isomorphisms* in a uniform way across all equational classes.

The study of equational classes is called *universal algebra*, and is the subject of this chapter and Chapter 2. Model theory proper, which begins in Chapter 3, can be seen as a generalization of universal algebra. We will use universal algebra as both a source of inspiration for model theory, and as a technical tool to develop the ring theory we will need later when we axiomatize the complex numbers in Chapter 9.

1.1 Monoids and groups

Let A be a set. For $k \geq 0$, a *k-ary operation* or *k-ary function* on A is a function $f : A^k \to A$, that is, a function which takes k inputs from A and outputs one value in A. *Binary*, *unary*, and *nullary* mean 2-ary, 1-ary, and 0-ary, respectively.

For example, the function

$$\max(x, y) = \begin{cases} x & \text{if } x \geq y \\ y & \text{if } x \leq y \end{cases}$$

is a function $\mathbb{R}^2 \to \mathbb{R}$, so it is a binary (2-ary) operation on $\mathbb{R}$. Other binary operations on $\mathbb{R}$ include $+$, $-$, and $\times$. Most binary operations are written in infix notation, like $2 + 3$, rather than prefix notation, like $+(2, 3)$.

Note that A^0 has one element $()$. Therefore, we can identify nullary fuctions $f : A^0 \to A$ with elements of A via the correspondence

$$f \mapsto f().$$

For example, we identify the element $8 \in \mathbb{R}$ with the function $f : \mathbb{R}^0 \to \mathbb{R}$ sending the one element $()$ in $\mathbb{R}^0$ to the element $8 \in \mathbb{R}^1$.

A *magma* is a pair $(A, \star)$ where A is a set and $\star$ is a binary operation on A. For example, $(\mathbb{R}, +)$ and $(\mathbb{R}, -)$ are magmas. A magma $(A, \star)$ is a semigroup if $\star$ is associative, meaning that:

$$x \star (y \star z) = (x \star y) \star z$$

for all $x, y, z \in A$. For example, $(\mathbb{R}, +)$ and $(\mathbb{R}, \max)$ are semigroups, because

$$x + (y + z) = (x + y) + z$$
$$\max(x, \max(y, z)) = \max(x, y, z) = \max(\max(x, y), z).$$

On the other hand, $(\mathbb{R}, -)$ is not a semigroup, because

$$5 - (3 - 2) = 4 \neq (5 - 3) - 2 = 0.$$

Let $(A, \star)$ be a semigroup. An element $e \in A$ is is an *identity element* if

$$x \star e = x = e \star x$$

holds for all $x \in A$. For example, 0 is an identity element in the semigroup $(\mathbb{R}, +)$ because $x + 0 = 0 + x = x$. Similarly, 1 is an identity element in the semigroup $(\mathbb{R}, \cdot)$, because $x \cdot 1 = 1 \cdot x = x$. In contrast, $(\mathbb{R}, \max)$ has no identity element.

Theorem 1.1.1. *If $(A, \star)$ is a semigroup, there is at most one identity element.*

Proof. Suppose e_1, e_2 are identity elements. Then $e_1 \star e_2 = e_1$ (because e_2 is an identity element), and $e_1 \star e_2 = e_2$ (because e_1 is an identity element. Therefore $e_1 = e_2$. □

Consequently, we can talk about "the" identity element, when it exists.

Definition 1.1.2. A *monoid* is a triple $(A, \star, e)$ where $(A, \star)$ is a semigroup and e is an identity element.

For example, $(\mathbb{R}, +, 0)$ and $(\mathbb{R}, \cdot, 1)$ are monoids.

Remark 1.1.3. The traditional definition of "monoid" is "a semigroup in which an identity element exists." With the traditional definition, $(\mathbb{R}, +)$ is a monoid, rather than $(\mathbb{R}, +, 0)$. However, there is a clear correspondence between the traditional definition and Definition 1.1.2, thanks to Theorem 1.1.1. Definition 1.1.2 works slightly better for the purposes of universal algebra.

Let $(A, \star, e)$ be a monoid. If $x \in A$, then an *inverse* of x is an element $x' \in A$ such that $x \star x' = x' \star x = e$.

Example 1.1.4. In the monoid $(\mathbb{R}, \cdot, 1)$, the element $2/3$ is an inverse of $3/2$, while the element 0 has no inverse.

Theorem 1.1.5. *Let $(A, \star, e)$ be a monoid. If $x \in A$, then x has at most one inverse.*

Proof. Suppose y, z are both inverses of x. Then

$$y = y \star e = y \star (x \star z) = (y \star x) \star z = e \star z = z. \qquad \square$$

Consequently, we can talk about "the" inverse of x, when it exists.

Definition 1.1.6. A *group* is a 4-tuple $(A, \star, e, (-)')$ where $(A, \star, e)$ is a monoid and $(-)'$ is a unary function $A \to A$ such that x' is an inverse of x for every $x \in A$.

Equivalently, a group is a 4-tuple $(A, \star, e, (-)')$ where A is a set, $\star$ is a binary operation on A, $e \in A$ is a nullary operation (an element), and $(-)'$ is a unary operation such that the following equations hold for all $x, y, z \in A$.

$$\begin{gathered} x \star (y \star z) = (x \star y) \star z \\ x \star e = e \star x = x \\ x \star x' = x' \star x = e. \end{gathered}$$

Example 1.1.7. $(\mathbb{R}, +, 0, -)$ is a group, where $-$ is the unary negation function $-x$.

Again, the traditional definition of "group" is slightly different—a group is a monoid $(A, \star)$ in which every element has an inverse. With this definition, $(\mathbb{R}, +)$ is a group rather than $(\mathbb{R}, +, 0, -)$. Again, there is a clear correspondence between the traditional definition and Definition 1.1.6, and Definition 1.1.6 is better for universal algebra.

A semigroup, monoid, or group is *commutative* if the equation

$$x \star y = y \star x$$

holds for any x, y. Commutative groups are usually called *abelian groups.* So far, all our examples have been commutative. Here is an important example of a non-abelian group.

Example 1.1.8. Let S be a set. Let $\mathrm{Perm}(S)$ be the set of bijections $f : S \to S$. Then $\mathrm{Perm}(S)$ is a group $(\mathrm{Perm}(S), \circ, \mathrm{id}, (-)^{-1})$, where

1. $f \circ g$ is the function composition $(f \circ g)(x) := f(g(x))$.

2. $\mathrm{id} : S \to S$ is the identity function $\mathrm{id}(x) = x$.

3. f^{-1} is the inverse function of f.

$\mathrm{Perm}(S)$ is usually non-abelian, since function composition is non-abelian in general. For example, if $f, g \in \mathrm{Perm}(\mathbb{R})$ are

$$f(x) = x + 1$$
$$g(x) = 2x$$

then $(f \circ g)(x) = 2x + 1$ and $(g \circ f)(x) = 2(x + 1) = 2x + 2$, so $f \circ g \neq g \circ f$.

When S is $\{1, 2, \ldots, n\}$, the group $\mathrm{Perm}(S)$ is called the *nth symmetric group.*

Example 1.1.9. If you know linear algebra, the group of $n \times n$ invertible matrices is a group with respect to matrix multiplication. This group is called the *nth general linear group*, usually written $GL(n)$ or $GL_n(\mathbb{R})$.

Remark 1.1.10. Groups are usually written using multiplicative or additive notation.

	Multiplicative notation	Additive notation
$x \star y$	$x \cdot y$	$x + y$
e	1	0
x'	x^{-1}	$-x$

When using multiplicative notation, one uses the usual abbreviations for multiplication, writing $xy^{-1}z$ instead of $x \cdot (y^{-1}) \cdot z$. Here are the group axioms in multiplicative notation:

$$\begin{gathered} x(yz) = (xy)z \\ x \cdot 1 = 1 \cdot x = x \\ xx^{-1} = x^{-1}x = 1 \end{gathered}$$

Additive notation is traditionally reserved for abelian groups. Here are the abelian group axioms in additive notation:

$$\begin{gathered} x + (y + z) = (x + y) + z \\ x + 0 = 0 + x = x \\ x + (-x) = (-x) + x = 0 \\ x + y = y + x. \end{gathered}$$

1.2 Rings and fields

Definition 1.2.1. A *ring* is a 6-tuple $(A, +, \cdot, -, 0, 1)$ such that

1. $(A, +, 0, -)$ is an abelian group.
2. $(A, \cdot, 1)$ is a commutative monoid.
3. The distributive law holds for $x, y, z \in A$:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z).$$

For example, $(\mathbb{R}, +, \cdot, -, 0, 1)$ is a ring, where $+, \cdot, -, 0, 1$ have their usual meanings. Similarly, $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{C}$ are rings with respect to the usual operations.

Definition 1.2.2. A *field* is a ring $(K, +, \cdot, -, 0, 1)$ such that $0 \neq 1$ and any $x \neq 0$ has an inverse x^{-1} in the monoid $(K, \cdot, 1)$.

For example, the rings $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{C}$ are fields. On the other hand, $\mathbb{Z}$ is not, because, for example, $2 \in \mathbb{Z}$ does not have a multiplicative inverse.

Remark 1.2.3. 1. Again, the traditional definition of "ring" is slightly different, so that $(\mathbb{R}, +, \cdot)$ is a ring rather than $(\mathbb{R}, +, \cdot, -, 0, 1)$, but the two definitions are equivalent and Definition 1.2.1 is better for universal algebra.

2. What we are calling "rings" should really be called "commutative rings." We will follow the conventions of comutative algebra and assume all rings are commutative. In noncommutative rings, $(A, +)$ is an abelian group but $(A, \cdot)$ is a monoid, not necessarily commutative. One needs *two* distributive laws

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$
$$(x + y) \cdot z = (x \cdot z) + (y \cdot z),$$

as these are no longer equivalent without commutativity. A typical example of a noncommutative ring is the ring $M_n(\mathbb{R})$ of $n \times n$ matrices of real numbers, with $+$ and $\cdot$ given by matrix addition and matrix multiplication.

3. In some fields of mathematics, rings are not assumed to have a multiplicative identity element $1 \in A$, so that $(A, \cdot)$ is a semigroup rather than a monoid. In this case, what we are calling "rings" should be called "commutative unital rings."

When working with rings, we use the usual notational abbreviations from algebra. For example, $x^2y - yz$ means $((x \cdot x) \cdot y) + (-(y \cdot z))$.

1.3 Languages, algebras, and equational classes

Each of the concepts *magma*, *semigroup*, *monoid*, *group*, *abelian group*, and *ring* is defined by a list of operations and a set of equations. More generally, an *equational class* is a class of "algebras" defined by a set of "equations". In this section, we make these notions precise.

Before we can define equations and algebras, we need to deal with the fact that there are different kinds of algebras with different signatures. It doesn't make sense to talk about a semigroup $(G, \cdot)$ satisfying the distributive law

$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$, because semigroups don't have an addition operation $x + y$. The concept of *languages* allows us to distinguish between these different types of algebras.

Definition 1.3.1. A *(functional) language* $\mathcal{L}$ is a set of *function symbols* and a map assigning to each function symbol f an integer $n_f \in \mathbb{N}$ called the *arity* of f. An *n-ary function symbol* is a function symbol of arity n. Nullary function symbols are usually called *constant symbols*.

In Chapters 1–2, all "languages" will be functional languages. Later, we wil see a more general notion of "language" (Definition 3.1.1). Languages are also called *signatures*, which is probably a better name. But at least in model theory, the term "language" is more common than "signature," for historical reasons.

Example 1.3.2. The *language of abelian groups* has one binary function symbol $+$, one constant symbol 0, and one unary function symbol $-$.

Definition 1.3.3. Given a language $\mathcal{L}$, an *$\mathcal{L}$-algebra* $\mathcal{A}$ is a set A and a map assigning to each n-ary function symbol f in $\mathcal{L}$ a corresponding n-ary function $f^{\mathcal{A}} : A^n \to A$. The set A is called the *underlying set* of $\mathcal{A}$, and $f^{\mathcal{A}}$ is called the *interpretation of f in $\mathcal{A}$*.

Usually we don't distinguish between an algebra $\mathcal{A}$ and its underlying set A, writing both as A.

Example 1.3.4. If $\mathcal{L}$ is the language of abelian groups, then an $\mathcal{L}$-algebra is essentially a 4-tuple $(A, +^A, 0^A, -^A)$ where A is a set, $+^A$ is a binary operation on A, $0^A \in A$, and $-^A$ is a unary operation on A.

Fix some infinite set $\mathcal{V} = \{x, y, z, \ldots\}$ of "variable symbols."

Definition 1.3.5. An *$\mathcal{L}$-term* is a string generated by the following rules:

- If x is a variable symbol, then x is a term.
- If f is an n-ary function symbol in $\mathcal{L}$, and $t_1, \ldots, t_n$ are $\mathcal{L}$-terms, then $f(t_1, \ldots, t_n)$ is an $\mathcal{L}$-term.

Example 1.3.6. These are terms in the language of abelian groups:

$$x + (-y),\ 0 + (x + 0),\ z,\ -(-(0 + x)),\ 0.$$

When we say "let $t(x_1, \ldots, x_n)$ be a term," we mean that $t(x_1, \ldots, x_n)$ is a term and the variables occurring in $t(x_1, \ldots, x_n)$ are contained in $\{x_1, \ldots, x_n\}$. If $s_1, \ldots, s_n$ are terms and $t(x_1, \ldots, x_n)$ is a term, then $t(s_1, \ldots, s_n)$ denotes the result of replacing x_i with s_i in $t(x_1, \ldots, x_n)$.

Example 1.3.7. if $t(x, y)$ is a term in the language of abelian groups, then $t(x, y)$ might be $x + (-y)$ or $x + (x + 0)$, but not $x + z$. If $t(x, y)$ is $x + (-y)$, then $t(0, w + z)$ is $0 + (-(w + z))$.

A *closed term* is a term with no variables, like $-(0 + 0)$ in the language of abelian groups. If t is a closed term and A is an $\mathcal{L}$-algebra, we define the *interpretation of* t *in* A, written t^A, recursively as follows:

$$f(t_1, \ldots, t_k)^A = f^A(t_1^A, \ldots, t_k^A).$$

Example 1.3.8. If $\mathcal{L}$ is the language of abelian groups, then the interpretation of the closed $\mathcal{L}$-term $(0 + (-0)) + 0$ in an $\mathcal{L}$-algebra $(A, +^A, 0^A, -^A)$ is the value $(0^A +^A (-^A 0^A)) +^A 0^A$.

It would be nice if we could also interpret terms with variables. If we substitute values $a_1, \ldots, a_n \in A$ into an $\mathcal{L}$-term $t(x_1, \ldots, x_n)$, the resulting expression $t(a_1, \ldots, a_n)$ is no longer an $\mathcal{L}$-term, but instead an $\mathcal{L}(A)$*-term* for some new language $\mathcal{L}(A)$. The language $\mathcal{L}(A)$ consists of $\mathcal{L}$ with each element of A added as a new constant symbol. We regard A as an $\mathcal{L}(A)$-algebra by interpreting each new constant symbol as the corresponding element of A, so that $c^A = c$ for $c \in A$. If $t(x_1, \ldots, x_n)$ is an $\mathcal{L}$-term and $a_1, \ldots, a_n \in A$, then $t(a_1, \ldots, a_n)$ is a closed $\mathcal{L}(A)$-term. The *interpretation of* t *in* A, written t^A, is the function $t^A : A^n \to A$ defined by

$$t^A(a_1, \ldots, a_n) = (t(a_1, \ldots, a_n))^A.$$

Example 1.3.9. If $\mathcal{L}$ is the language of abelian groups and $t(x, y) = (-x) + (0 + y)$, then the interpretation of t in an $\mathcal{L}$-algebra $(A, +^A, 0^A, -^A)$ is the function

$$t^A(a, b) = ((-a) + (0 + b))^A = (-^A a) +^A (0^A +^A b).$$

Definition 1.3.10. An $\mathcal{L}$*-equation* is a formal expression of the form

$$t(x_1, \ldots, x_n) = s(x_1, \ldots, x_n)$$

for two $\mathcal{L}$-terms $t(\bar{x})$ and $s(\bar{x})$. An $\mathcal{L}$-algebra A *satisfies* an equation $(t(\bar{x}) = s(\bar{x}))$ if for any $\bar{a} \in A^n$,

$$t^A(\bar{a}) = s^A(\bar{a}).$$

The notation $A \models \varphi$ means that A satisfies φ.

The group $(\mathbb{R}, +)$ satisfies the equation $x \cdot y = y \cdot x$, but the non-abelian group $(\mathrm{Perm}(S), \circ)$ does not:

$$\begin{gathered}(\mathbb{R}, +) \models x \cdot y = y \cdot x \\ (\mathrm{Perm}(S), \circ) \not\models x \cdot y = y \cdot x.\end{gathered}$$

Definition 1.3.11. An *equational $\mathcal{L}$-theory* is a set Σ of $\mathcal{L}$-equations. Elements of Σ are called *axioms* of Σ. If Σ is an equational $\mathcal{L}$-theory, and A is an $\mathcal{L}$-algebra, then A is a *model* of Σ, written $A \models \Sigma$, if $A \models \varphi$ for every $\varphi \in \Sigma$. The class of models of Σ is written $\mathrm{Mod}(\Sigma)$. An *equational class* is a class of the form $\mathrm{Mod}(\Sigma)$ for some Σ.

Example 1.3.12. Let $\mathcal{L}$ be the language of abelian groups. The *theory of abelian groups* consists of the equations

$$\begin{gathered}x + (y + z) = (x + y) + z \\ x + 0 = x \\ x + (-x) = 0 \\ x + y = y + x.\end{gathered}$$

Models are abelian groups.

Example 1.3.13. The classes of rings, groups, monoids, semigroups, and magmas are equational classes.

Warning 1.3.14. The class of fields is *not* an equational class. We will see a couple proofs of this in the next chapter (Examples 2.1.6 and 2.2.6). Nevertheless, we can still learn useful facts about fields by applying the tools of universal algebra to rings.

Example 1.3.15. An *idempotent monoid* is a monoid $(A, \star, e)$ in which the equation $x \star x = x$ holds. Idempotent monoids form an equational class.

Example 1.3.16. A *boolean algebra* is a 6-tuple $(B, \wedge, \vee, \neg, 0, 1)$ where $(B, \vee, 0)$ is an idempotent commutative monoid, $(B, \wedge, 1)$ is an idempotent commutative monoid, and $\neg : B \to B$ is a unary operation such that the following equations hold:

$$\begin{aligned} x \wedge \neg x &= 0 \\ x \vee \neg x &= 1 \\ x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z) \\ x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z) \end{aligned}$$

Boolean algebras form an equational class. If S is a set, then the powerset $\mathfrak{P}(S)$ is a boolean algebra with

$$\begin{aligned} x \wedge y &= x \cap y \\ x \vee y &= x \cup y \\ 0 &= \varnothing \\ 1 &= S \\ \neg x &= S \setminus x \end{aligned}$$

Another important boolean algebra is the set of truth values $\{\textsc{False}, \textsc{True}\}$, with $\wedge, \vee, \neg$ interpreted as the basic logical operations:

$$\begin{aligned} x \wedge y &= x \textsc{ And } y \\ x \vee y &= x \textsc{ Or } y \\ \neg x &= \textsc{Not } x \\ 0 &= \textsc{False} \\ 1 &= \textsc{True}. \end{aligned}$$

The fact that these two examples satisfy the axioms of boolean algebras can be checked directly. We will see later in Example 2.2.14 that there is a reason why any equation satisfied by the boolean algebra of truth values must also be satisfied by the boolean algebra $\mathfrak{P}(S)$.

Warning 1.3.17. In universal algebra, equational classes are usually called *varieties*. We will avoid this terminology because "variety" tends to mean something completely different in model theory. Confusingly, "equational theory" also has a technical meaning in model theory, though it is much less common.

Note that languages are allowed to have infinitely many symbols, and theories are allowed to have infinitely many axioms. Here is an important example:

Definition 1.3.18. Let $(G, \cdot)$ be a group and S be a set. An *action* of G on S is a map

$$\star : G \times S \to S$$

satisfying the following axioms for $g, h \in G$ and $x \in S$:

$$(g \cdot h) \star x = g \star (h \star x)$$
$$1 \star x = x$$

Group actions are usually written using $\cdot$ rather than $\star$.

Example 1.3.19. Suppose S is a set and $\mathrm{Perm}(S)$ is the group of permutations on S (Example 1.1.8). There is a natural action of $\mathrm{Perm}(S)$ on S given by $f \cdot x = f(x)$. The axioms of group actions hold as follows:

$$(f \cdot g) \cdot x = (f \circ g)(x) = f(g(x)) = f \cdot (g \cdot x)$$
$$1 \cdot x = \mathrm{id}(x) = x.$$

Example 1.3.20. If you know linear algebra, another example is the group of invertible $n \times n$ matrices, which acts by matrix multiplication on the space of $n \times 1$ column vectors.

Fix a specific group G.

Definition 1.3.21. A *G-set* is a pair $(S, \cdot)$ where S and $\cdot$ is an action of G on S.

This doesn't immediately fit into the framework of universal algebra, because the binary operator $\cdot$ involves two different sets, one of which is fixed. However, the following equivalent definition works:

Definition 1.3.22. A *G-set* is a set S and a unary operator μ_g for each $g \in G$, satisfying the following identities:

$$\mu_{g \cdot h}(x) = \mu_g(\mu_h(x)) \text{ for each } g, h \in G$$
$$\mu_1(x) = x$$

The translation between Definitions 1.3.21 and 1.3.22 is

$$\mu_g(x) = g \cdot x.$$

Definition 1.3.22 fits into the framework of universal algebra. Note that the language of G-sets has one symbol for each element of G. When G is an infinite group, we need infinitely many symbols. Likewise, the theory of G-sets needs infinitely many equations (when G is infinite).

Remark 1.3.23. If you know what vector spaces are, the same thing happens: for any fixed field K, the class of K-vector spaces is an equational class. We will review vector spaces later, in Section 13.6.

1.4 Homomorphisms and isomorphisms

Fix a language $\mathcal{L}$.

Definition 1.4.1. Let A, B be $\mathcal{L}$-algebras. A *homomorphism* from A to B is a function $\alpha : A \to B$ such that for any k-ary function symbol $f \in \mathcal{L}$, and any $a_1, \ldots, a_k \in A$,

$$\alpha(f^A(a_1, \ldots, a_k)) = f^B(\alpha(a_1), \alpha(a_2), \ldots, \alpha(a_k)). \tag{$*$}$$

An *isomorphism* is a bijective homomorphism. Two $\mathcal{L}$-algebras A, B are *isomorphic*, written $A \cong B$, if there is an isomorphism $\alpha : A \to B$.

In what follows, we extend functions to tuples componentwise, so that $\alpha(a_1, \ldots, a_k) := (\alpha(a_1), \ldots, \alpha(a_k))$. Then $(*)$ can be rewritten as $\alpha(f^A(\bar{a})) = f^B(\alpha(\bar{a}))$.

Remark 1.4.2. The idea of $(*)$ is that α "preserves" the function symbol f. It may help to rewrite $(*)$ as the following logically equivalent condition:

$$f^A(a_1, \ldots, a_k) = b \implies f^B(\alpha(a_1), \ldots, \alpha(a_k)) = \alpha(b).$$

Example 1.4.3. Let $\mathcal{L} = \{+, 0, -\}$ be the language of abelian groups. Let $h : \mathbb{Z} \to \mathbb{Z}$ be $h(x) = 2x$. Then h is a homorphism from $\mathbb{Z}$ to $\mathbb{Z}$, because

$$\begin{gathered} 2(x + y) = (2x) + (2y) \\ 2(0) = 0 \\ 2(-x) = -(2x). \end{gathered}$$

However, h is not an isomorphism, because h is not surjective.

Here is another example which is slightly more subtle.

Example 1.4.4. Let $\mathcal{L} = \{\cdot, 1\}$ be the language of monoids. The exponential map $\exp(x) = e^x$ is a homomorphism from the monoid $(\mathbb{R}, +, 0)$ to $(\mathbb{R}, \cdot, 1)$, because

$$\begin{aligned} \exp(x + y) &= \exp(x)\exp(y) \\ \exp(0) &= 1 \end{aligned}$$

If this looks confusing, remember that the interpretation of "$\cdot$" in the monoid $(\mathbb{R}, +, 0)$ is $+$, and the interpretation of "1" is 0.

The exponential map is not an isomorphism, as it is not surjective. On the other hand, if $\mathbb{R}_{>0}$ denotes the set of positive real numbers, then exp is an isomorphism from the monoid $(\mathbb{R}, +, 0)$ to the monoid $(\mathbb{R}_{>0}, \cdot, 1)$.

Example 1.4.5. An action of G on a set S (Definition 1.3.18) can be thought of as a map assigning to each element $g \in G$ a permutation $\mu_g \in \mathrm{Perm}(S)$ satisfying the conditions

$$\begin{aligned} \mu_{g\cdot h} &= \mu_g \circ \mu_h \\ \mu_1 &= \mathrm{id}_S \end{aligned}$$

(See Definition 1.3.22.) These conditions precisely say that $g \mapsto \mu_g$ is a monoid homomorphism $(G, \cdot, 1) \to (\mathrm{Perm}(S), \circ, \mathrm{id}_S)$. We will see later that such a homomorphism must actually be a group homomorphism (Theorem 1.4.13). Therefore, an action of G on S is equivalent to a group homomorphism from G to $\mathrm{Perm}(S)$.

The next theorem expresses some basic facts about homomorphisms and isomorphisms: we can compose homomorphisms and take inverses of isomorphisms.

Theorem 1.4.6. *Let $\mathcal{L}$ be a language and A, B, C be $\mathcal{L}$-algebras.*

1. *Let $\alpha : A \to B$ and $\beta : B \to C$ be homomorphisms. Then $\beta\circ\alpha : A \to C$ is a homomorphism.*

2. *The identity map $\mathrm{id}_A : A \to A$ is an isomorphism.*

3. *If $\alpha : A \to B$ is an isomorphism, then $\alpha^{-1} : B \to A$ is an isomorphism.*

Proof. 1. If $f \in \mathcal{L}$ is a k-ary function symbol, then

$$\beta(\alpha(f^A(\bar{a}))) = \beta(f^B(\alpha(\bar{a}))) = f^C(\beta(\alpha(\bar{a})))$$

because β and α are homomorphisms.

2. If $f \in \mathcal{L}$ is a k-ary relation symbol, then

$$\mathrm{id}(f(\bar{a})) = f(\bar{a}) = f(\mathrm{id}(\bar{a})).$$

3. Suppose $f \in \mathcal{L}$ is a k-ary function symbol and $b_1, \ldots, b_k \in B$. Let $a_i = \alpha^{-1}(b_i) \in A$. Then $b_i = \alpha(a_i)$. As α is a homomorphism,

$$\alpha(f^A(\bar{a})) = f^B(\alpha(\bar{a})) = f^B(\bar{b}).$$

Applying α^{-1} to both sides, we see that

$$\alpha^{-1}(f^B(\bar{b})) = f^A(\bar{a}) = f^A(\alpha^{-1}(\bar{b})).$$ □

Corollary 1.4.7. *The relation of isomorphism is an equivalence relation on $\mathcal{L}$-algebras:*

1. *$A \cong A$ for any $\mathcal{L}$-algebra A.*

2. *If $A \cong B$, then $B \cong A$.*

3. *If $A \cong B$ and $B \cong C$, then $A \cong C$.*

Proof. 1. $\mathrm{id}_A : A \to A$ is an isomorphism.

2. If $\alpha : A \to B$ is an isomorphism, then $\alpha^{-1} : B \to A$ is an isomorphism.

3. If $\alpha : A \to B$ and $\beta : B \to C$ are isomorphisms, then $\beta \circ \alpha : A \to C$ are isomorphisms. □

Example 1.4.8. Here is an example of an isomorphism. Let S be $\{\{x\} : x \in \mathbb{R}\}$, the set of one element subsets of $\mathbb{R}$. Define operations on S as follows:

$$\begin{gathered}\{x\} + \{y\} := \{x + y\} \\ \{x\} \cdot \{y\} := \{x \cdot y\} \\ -\{x\} = \{-x\} \\ 1 := \{1\} \\ 0 := \{0\}.\end{gathered}$$

For example, $\{2\} + \{3\} \cdot \{5\} = \{17\}$. This makes $(S, +, \cdot, -, 0, 1)$ into a ring. Then there is an isomorphism from the ring $\mathbb{R}$ to the ring S given by

$$f : \mathbb{R} \to S$$
$$f(x) = \{x\}.$$

The intuition you should have is that the ring S is a poorly disguised copy of $\mathbb{R}$. On some level, S is "the same thing" as $\mathbb{R}$.

This is the intuition we have for isomorphisms in general—if two algebras A and B are isomorphic, then we think of them as being two "copies" of the same algebra. In algebra and model theory, the objects of study are not so much algebras as isomorphism classes of algebras.

This mindset has the following corollary: if two algebras A and B are isomorphic, then they should have identical properties. For example, A and B will have the same cardinality because the isomorphism $f : A \to B$ is a bijection, showing that $|A| = |B|$.

Of course, not all properties respect isomorphisms. In our example above, the property "contains 7" is true for $\mathbb{R}$ but false for S. What we should conclude from this is that the property "contains 7" is a stupid property, or an *evil property* as they would say on the website nLab. The "meaningful" or "good" properties of algebras are the ones that respect isomorphisms. In the remainder of this section, we show that the properties defined by equations are good properties. In other words, we will show that isomorphic algebras satisfy the same equations (Theorem 1.4.11).

The next theorem shows that homomorphisms preserve not only the basic function symbols, but also all terms. This is intuitively reasonable, since terms are expressions built up from function symbols.

Theorem 1.4.9. *Let $\alpha : A \to B$ be a homomorphism of $\mathcal{L}$-algebras. Let $t(x_1, \ldots, x_n)$ be an $\mathcal{L}$-term. Then for any $a_1, \ldots, a_n \in A$, we have*

$$\alpha(t^A(\bar{a})) = t^B(\alpha(\bar{a})). \tag{$\dagger$}$$

Proof. Proceed by induction on the complexity of t.

- If $t(\bar{x}) = x_i$, then both sides of ($\dagger$) are $\alpha(a_i)$.
- Suppose $t(\bar{x}) = f(s_1(\bar{x}), \ldots, s_k(\bar{x}))$ for some k-ary function symbol f and some simpler $\mathcal{L}$-terms $s_1, \ldots, s_k$. By definition of t^A,

$$\alpha(t^A(\bar{a})) = \alpha(f^A(s_1^A(\bar{a}), \ldots, s_k^A(\bar{a}))).$$

As α is a homomorphism,

$$\alpha(f^A(s_1^A(\bar{a}),\ldots,s_k^A(\bar{a}))) = f^B(\alpha(s_1^A(\bar{a})),\ldots,\alpha(s_k^A(\bar{a}))).$$

By induction,

$$\alpha(s_i^A(\bar{a})) = s_i^B(\alpha(\bar{a})).$$

for each i. Therefore,

$$f^B(\alpha(s_1^A(\bar{a})),\ldots,\alpha(s_k^A(\bar{a}))) = f^B(s_1^B(\alpha(\bar{a})),\ldots,s_k^B(\alpha(\bar{a}))).$$

By definition, the right hand side is $t^B(\alpha(\bar{a}))$. □

Lemma 1.4.10. *Let $\alpha : A \to B$ be a surjective homomorphism of $\mathcal{L}$-algebras, and let φ be an $\mathcal{L}$-equation. Then $A \models \varphi \implies B \models \varphi$.*

Proof. Suppose φ is $t(x_1,\ldots,x_n) = s(x_1,\ldots,x_n)$. Suppose $b_1,\ldots,b_n \in B$. By surjectivity, we can write b_i as $\alpha(a_i)$ for some $a_i \in A$. Then

$$\begin{aligned} t^B(\bar{b}) = t^B(\alpha(\bar{a})) = \alpha(t^A(\bar{a})) \\ s^B(\bar{b}) = s^B(\alpha(\bar{a})) = \alpha(s^A(\bar{a})) \end{aligned}$$

by Theorem 1.4.9, as α is a homomorphism. Because $A \models \varphi$, the right hand sides are equal. Therefore the left hand sides are equal, meaning

$$t^B(\bar{b}) = s^B(\bar{b}).$$ □

This allows us to complete the proof that isomorphic algebras satisfy the same equations.

Theorem 1.4.11. *Suppose $A \cong B$.*

1. $A \models s = t \iff B \models s = t$.

2. $A \models \Sigma \iff B \models \Sigma$

3. $A \in \mathrm{Mod}(\Sigma) \iff B \in \mathrm{Mod}(\Sigma)$.

4. *If $\mathcal{K}$ is an equational class, then $A \in \mathcal{K} \iff B \in \mathcal{K}$.*

Group homomorphisms

In this section, we study homomorphisms of groups, learning something useful about rings and fields along the way.

Lemma 1.4.12 (Cancellation)**.** *Let G be a group. If $ax = ay$, then $x = y$. Similarly, if $xa = ya$, then $x = y$.*

Proof. If $ax = ay$, then

$$x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = 1y = y.$$

The other case is similar. □

Theorem 1.4.13. *Let G, H be groups. If $f : G \to H$ is a semigroup homomorphism, meaning that f preserves multiplication*

$$f(xy) = f(x)f(y),$$

then f also preserves 1 and $(-)^{-1}$:

$$\begin{gathered} f(1) = 1 \\ f(x^{-1}) = f(x)^{-1}, \end{gathered}$$

and so f is a group homomorphism.

Proof. First note that

$$f(1) \cdot f(1) = f(1 \cdot 1) = f(1) = f(1) \cdot 1.$$

Canceling $f(1)$ from both sides, we see $f(1) = 1$. Next,

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(1) = 1 = f(x)f(x)^{-1}.$$

Canceling $f(x)$ from both sides, we see $f(x^{-1}) = f(x)^{-1}$. □

Corollary 1.4.14. *Let R be a ring. Then the following equations hold, for $a, x \in R$:*

$$\begin{gathered} 0a = 0 \\ (-x)a = -(xa) \\ (-1)a = -a \end{gathered}$$

Proof. Let $\mu_a(x) = ax$. Then μ_a is a semigroup homomorphism $(R, +) \to (R, +)$, by the distributive law:

$$a(x + y) = ax + ay.$$

Thus μ_a preserves zero and negation:

$$\begin{aligned} \mu_a(0) &= 0 \\ \mu_a(-x) &= -\mu_a(x), \end{aligned}$$

which are the first two equations. The third equation holds by taking $x = 1$ in the second equation. □

Lemma 1.4.15. *The following holds in any field K:*

$$xy = xz \implies y = z \text{ when } x \neq 0.$$

Proof. Multiply both sides of $xy = xz$ by x^{-1}, as in Lemma 1.4.12. □

Theorem 1.4.16. *If K is a field and $x, y \in K$, then*

$$xy = 0 \iff (x = 0 \text{ or } y = 0)$$

Proof. If $x = 0$ or $y = 0$, then $xy = 0$ by the zero law (Corollary 1.4.14). Conversely, suppose $xy = 0$, but $x \neq 0$ and $y \neq 0$. Then

$$xy = 0 = x0$$

by the zero law. Cancelling x from both sides, $y = 0$, a contradiction. □

1.5 ♢ More examples of equational classes

We have seen a number of examples of equational classes so far, including magmas, semigroups, commutative semigroups, monoids, commutative monoids, groups, abelian groups, rings, boolean algebras, and G-sets. Here are some additional examples:

Sets: If $\mathcal{L}$ is the language with no symbols, then $\mathcal{L}$-algebras are sets and homomorphisms are functions. If T is the equational $\mathcal{L}$-theory with no axioms, then models of T are sets.

Vector spaces: Vector spaces are an important concept in linear algebra. A *real vector space* is an abelian group $(V, +, 0, -)$ with an function $\cdot : \mathbb{R} \times V \to V$ called scalar multiplication satisfying the axioms

$$\begin{aligned} a \cdot (v + w) &= a \cdot v + a \cdot w \\ 1 \cdot v &= v \\ (a + b) \cdot v &= a \cdot v + b \cdot v \\ a \cdot (b \cdot v) &= (a \cdot b) \cdot v. \end{aligned}$$

For example, the set $\mathbb{R}^3$ of real vectors of length 3 is a vector space if we define addition componentwise

$$(x_1, x_2, x_3) + (y_1, y_2, y_3) = (x_1 + y_1, x_2 + y_2, x_3 + y_3)$$

and define scalar multiplication in the usual way

$$a \cdot (x_1, x_2, x_3) = (a \cdot x_1, a \cdot x_2, a \cdot x_3).$$

Real vector spaces don't fit into the framework of universal algebra because of the fixed set $\mathbb{R}$. However, we can do the same thing we did for G-sets (Definition 1.3.22), and replace the binary operation $\cdot : \mathbb{R} \times V \to V$ with a family of unary operations $\mu_a(x) = a \cdot x$, one for each $a \in \mathbb{R}$. Then the axioms above become axiom schemas. For example, there is an axiom

$$\mu_{a+b}(x) = \mu_a(x) + \mu_b(x)$$

for each $a, b \in \mathbb{R}$. From this point of view, real vector spaces are an equational class. We will say more about vector spaces in Section 13.6, going so far as to classify them (Theorem 13.7.3). The classification roughly says that things like $\mathbb{R}^n$ are the *only* examples of vector spaces, though n may need to be infinite.

Of course, we can replace $\mathbb{R}$ with any other field K, getting *K-vector spaces*. The same definitions make sense when we replace $\mathbb{R}$ with a ring R, in which case the result is called an *R-module* rather than an R-vector space. However, R-modules are much harder to classify than vector spaces over fields.

Non-commutative rings: A *non-commutative ring* is an algebra $(R, +, \cdot, 0, 1, -)$ where $(R, +, 0, -)$ is an abelian group and $(R, \cdot, 1)$ is a monoid, *not necessarily commutative*, and the two distributive laws hold:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$
$$(x + y) \cdot z = (x \cdot z) + (y \cdot z).$$

Non-commutative rings form an equational class. A well-known example of a non-commutative ring is the class of $n \times n$ matrices over the real numbers, with $x + y$ and $x \cdot y$ defined as the standard addition and multiplication of matrices.

Another important non-commutative ring is the ring of *quaternions* $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$, where i, j, k are set up so that $i^2 = j^2 = k^2 = ijk = -1$. The quaternions have the unusual property that every non-zero x has a multiplicative inverse, making them something like a non-commutative field. (The usual terminology is "division ring" or "skew field.") The quaternions are connected to the group of rotations in three dimensios, and they have applications to computer graphics.

Non-commutative rings are important in group theory and number theory. One way that non-commutative rings arise in group theory is through *endomorphism rings*. If A is an algebra, an *endomorphism* of A is a homomorphism from A to A. When A is an abelian group $(A, +, 0, -)$, the set $\mathrm{End}(A)$ of endomorphisms naturally has the structure of a non-commutative ring, where $f \cdot g$ is the composition of f and g, and $f + g$ is pointwise addition:

$$(f \cdot g)(x) = f(g(x))$$
$$(f + g)(x) = f(x) + g(x).$$

Quasigroups: Traditionally, a *quasigroup* is a magma $(G, *)$ such that for any $a, b \in G$, the equatios $x * b = a$ and $a * y = b$ have unique solutions. We can convert this into an equational theory by adding binary function symbols a/b for the unique solution of $x * b = a$, and $a\backslash b$ for the unique solution of $a * y = b$. Then the class of quasigroups is defined by the equations

$$\begin{aligned}(x * y)/y &= x\\ (x/y) * y &= x\\ x\backslash(x * y) &= y\\ x * (x\backslash y) &= y.\end{aligned}$$

The words "quasigroup" and "semigroup" both mean "half group," and interestingly, $(G, *)$ is a group if and only if $(G, *)$ is both a semigroup and a quasigroup. Quasigroups are closely connected to "Latin squares" in combinatorics.[1]

Lie algebras: A (real) *Lie algebra* is a real vector space with a binary operation $[x, y]$ satisfying the axioms:

$$\begin{gathered}[a \cdot x, y] = a \cdot [x, y] \text{ for } a \in \mathbb{R}\\ [x, a \cdot y] = a \cdot [x, y] \text{ for } a \in \mathbb{R}\\ [x + y, z] = [x, z] + [y, z]\\ [x, y + z] = [x, y] + [x, z]\\ [x, x] = 0\\ [x, [y, z]] = [[x, y], z] + [y, [x, z]].\end{gathered}$$

This list of axioms looks cryptic, but one motivating example is the class of $n \times n$ matrices, with $[x, y]$ defined to be $xy - yx$. Lie algebras turn out to be very closely connected to *Lie groups*, which are a cross between a group and a topological manifold. In fact, the classification of simple Lie groups works by classifying simple Lie algebras. Lie groups and Lie algebras play an important role in differential topology.

Lattices: A *bounded lattice* can be defined in two ways that are non-obviously equivalent:

1. A bounded lattice is a partially ordered set $(M, \leq)$ such that any finite subset $S \subseteq M$ has a supremum (i.e., a least upper bound) and an infimum (i.e., a greatest lower bound).

[1] A Latin square is an $n \times n$ grid of symbols, such that each symbol occurs exactly once in each row and once in each column. If the symbols are $1, \ldots, n$, then a Latin square is the same thing as a multiplication table for a quasigroup. Latin squares are the inspiration for Sudoku.

2. A bounded lattice is an algebra $(M, \wedge, \vee, 0, 1)$ satisfying the axioms

$$\begin{aligned} x \vee (y \vee z) &= (x \vee y) \vee z & \qquad x \wedge (y \wedge z) &= (x \wedge y) \wedge z \\ x \vee 0 &= x & x \wedge 1 &= x \\ x \vee y &= y \vee x & x \wedge y &= y \wedge x \\ x \vee x &= x & x \wedge x &= x \\ (x \vee y) \wedge y &= y & (x \wedge y) \vee y & \end{aligned}$$

Note that definition (2) defines an equational class of algebras. The conversion between the two definitions is as follows:

$$\begin{gathered} x \vee y = \sup\{x, y\} \\ x \wedge y = \inf\{x, y\} \\ 0 = \sup \varnothing = \min M \\ 1 = \inf \varnothing = \max M \\ x \leq y \iff x \vee y = y \iff x = x \wedge y. \end{gathered}$$

(It takes a bit of work to show that everything is well-defined and works out.) As an example, the powerset $\mathfrak{P}(S)$ is a bounded lattice with

$$\begin{gathered} X \vee Y = X \cup Y \\ X \wedge Y = X \cap Y \\ 0 = \varnothing \\ 1 = S \\ X \leq Y \iff X \subseteq Y. \end{gathered}$$

A *lattice* is defined the same way as a bounded lattice, except that in definition (1), we only require finite *non-empty* sets to have suprema and infima, and in definition (2) we drop the identity elements 0 and 1 and their associated axioms. A typical example of an unbounded lattice is the linear order $(\mathbb{R}, \leq)$, where

$$\begin{gathered} x \vee y = \max(x, y) \\ x \wedge y = \min(x, y). \end{gathered}$$

More generally, any linear order is a lattice.

Lattices are prevalent throughout universal algebra and logic.[2] For example, boolean algebras (Example 1.3.16) can be seen as lattices with additional properties. Jumping ahead a bit, if A is an algebra and $\mathcal{S}$ is the class of *subalgebras* of A (Definition 2.1.1), then $(\mathcal{S}, \subseteq)$ is a bounded lattice, with

$$\begin{gathered} X \wedge Y = X \cap Y \\ 1 = S \\ X \vee Y = \langle X \cup Y \rangle \\ 0 = \langle \varnothing \rangle, \end{gathered}$$

where $\langle X \rangle$ denotes the subalgebra generated by X (Definition 2.1.7). More generally, closure operators (see Chapter 13) always give rise to lattices.

Squags and sloops: A *Steiner triple system* is an object in combinatorics consisting of a set S and a family $\mathcal{T}$ of subsets of S called *triples* such that

- Each triple $X \in \mathcal{T}$ has exactly three elements.
- For any distinct[3] $x, y \in S$, there is a unique $z \in S$ such that $\{x, y, z\}$ is a triple.

Given a Steiner triple system $(S, \mathcal{T})$, define a binary operation $*$ as follows:

- $x * x = x$
- If $x \neq y$, then $x * y$ is the unique z such that $\{x, y, z\}$ is a triple.

The resulting operation $*$ satisfies the equations

$$\begin{gathered} x * x = x \\ x * y = y * x \\ x * (x * y) = y. \end{gathered}$$

[2] In fact Burris and Sankappanavar's textbook on universal algebra devotes its first chapter to lattice theory.

[3] . . . meaning $x \neq y$

Conversely, any algebra $(S, *)$ satisfying these equations corresponds to a Steiner triple system $(S, \mathcal{T})$. Such algebras are called *Steiner quasigroups* or *squags*.[4] This gives a way to regard Steiner triple systems as models of some equational theory.

There is a second, different way to turn Steiner triple systems into algebras. Let $(S, \mathcal{T})$ be a Steiner triple system. Let 0 be an element outside of S. Define a binary operation $\oplus$ on $S \cup \{0\}$ as follows:

- $x \oplus 0 = 0 \oplus x = x$ for any x.
- $x \oplus x = 0$ for any x.
- If $x, y \in S$ and $x \neq y$, then $x \oplus y$ is the same as $x * y$.

The resulting algebra $(S \cup \{0\}, \oplus, 0)$ satisfies the axioms

$$\begin{gathered} x \oplus y = y \oplus x \\ x \oplus 0 = x \\ x \oplus (x \oplus y) = y. \end{gathered}$$

Conversely, any algebra $(A, \oplus, 0)$ satisfying these axioms comes from a Steiner triple system on $A \setminus \{0\}$. Models of these axioms are called *Steiner loops* or *sloops*.[5]

In the next chapter, we will see several operations to produce new models of an equational theory. Applying these operations to squags and sloops, and using the conversion between squags and sloops, one can produce complicated examples of Steiner triple systems.

Keis and quandles: A *kei* or *involutive quandle* is an algebra $(A, \triangleleft)$ satisfying the axioms:

$$\begin{gathered} x \triangleleft (y \triangleleft z) = (x \triangleleft y) \triangleleft (x \triangleleft z) \\ x \triangleleft x = x \\ x \triangleleft (x \triangleleft y) = y \end{gathered}$$

The first of these says that $\triangleleft$ is "self-distributive"—it is distributive over itself the same way that multiplication is distributive over addition $(x \cdot (y + z) = x \cdot y + x \cdot z)$.

[4] They are quasigroups with $x/y = x\backslash y = x * y$.

[5] A *loop* is a quasigroup with an identity element. In this case, 0 is the identity element.

For example $(\mathbb{R}, \lhd)$ is a kei if we define $x \lhd y$ to be $2x - y$. This can be understood geometrically as the reflection of y over x. More generally, if $(G, \cdot)$ is a group and we define $x \lhd y$ to be $xy^{-1}x$, then $(G, \lhd)$ is a kei. Keis turn out to be useful in knot theory, giving rise to knot invariants.

A *quandle* is an algebra $(A, \lhd, \rhd)$ satisfying the axioms

$$\begin{gathered} x \lhd (y \lhd z) = (x \lhd y) \lhd (x \lhd z) \\ x \lhd x = x \\ x \lhd (y \rhd x) = y = (x \lhd y) \rhd x. \end{gathered}$$

The final line says that $- \rhd x$ is the inverse of $x \lhd -$. Any kei gives a quandle by taking $x \rhd y := y \lhd x$. Other examples of quandles include the following:

1. Any group G becomes a quandle by setting

$$\begin{gathered} x \lhd y := xyx^{-1} \\ y \rhd x := x^{-1}yx \end{gathered}$$

2. For any non-zero $t \in \mathbb{R}$, we can make $\mathbb{R}$ into a quandle by defining

$$\begin{gathered} x \lhd y := (1-t)x + ty \\ y \rhd x := (1-t^{-1})x + t^{-1}y \end{gathered}$$

Like keis, quandles give rise to invariants in knot theory.

Chapter 2

New algebras from old

Let Σ be an equational theory, like the theory of rings or the theory of groups. In this chapter, we will meet three ways to build new models of Σ from old models: *subalgebras*, *products*, and *quotients*, in Sections 2.1, 2.2, and 2.4, respectively. These constructions can roughly be described as follows:

- A *subalgebra* of A is an algebra that sits inside A, the way that the ring $\mathbb{Z}$ sits inside $\mathbb{R}$ and $\mathbb{R}$ sits inside $\mathbb{C}$.

- A *product* of two algebras A and B is the algebra where we carry out operations from A and B in parallel, a bit like vector addition in linear algebra. One can also form products of more than two algebras, even taking the product of infinitely many algebras.

- A *quotient* of an algebra A is an algebra obtained by "collapsing" A, forcing certain elements of A to become equal. For example, there is a way to collapse the ring $\mathbb{Z}$ making all the even numbers be equal to 0 and all the odd numbers be equal to 1. This gives a ring called $\mathbb{Z}/2\mathbb{Z}$ with two elements.

Each of these constructions respects equational theories: if we start with models of Σ, the result will be a model of Σ. For example, a product of models is a model, and a quotient of a model is a model. This provides a new source of models. For example, in Section 2.5, we use quotients to construct new examples of rings, including finite fields.

At the same time, this shows the limits of what can be expressed by equational theories. For example, a product of two fields is not a field, so the class of fields cannot be defined by an equational theory (Example 2.2.6). On the other hand, we will see in Theorem 2.9.2 that if a class of structures $\mathcal{K}$ is closed under products, subalgebras, and quotients, then $\mathcal{K}$ *is* defined by an equational theory, a fact known as *Birkhoff's HSP Theorem.* This gives a structural characterization of equational classes.

A further significance of these constructions is that they reveal the inner structure of homomorphisms. The *fundamental theorem of homomorphisms* (Theorem 2.6.7) shows that if $f : A \to B$ is a homomorphism, then the image of f, which is a subalgebra of B, is isomorphic to a quotient of A. We apply this to rings in Section 2.7, to define *characteristic*, an important invariant of rings and fields. We will see further applications of these ideas when we study algebraically closed fields in Chapter 9.

2.1 Subalgebras and generators

Definition 2.1.1. Let A be an $\mathcal{L}$-algebra. A *subalgebra* is a subset $B \subseteq A$ such that for any k-ary relation symbol $f \in \mathcal{L}$,

$$b_1, \ldots, b_k \in B \implies f^A(b_1, \ldots, b_k) \in B.$$

Example 2.1.2. $\mathbb{Z}$ is a subalgebra of the ring $(\mathbb{R}, +, \cdot, -, 0, 1)$, because

$$\begin{gathered} x, y \in \mathbb{Z} \implies x + y \in \mathbb{Z} \\ x, y \in \mathbb{Z} \implies xy \in \mathbb{Z} \\ x \in \mathbb{Z} \implies -x \in \mathbb{Z} \\ 0 \in \mathbb{Z} \\ 1 \in \mathbb{Z}. \end{gathered}$$

If B is a subalgebra of an $\mathcal{L}$-algebra A, then we can make B into an $\mathcal{L}$-algebra by defining f^B to be the restriction of f^A to B, for each function symbol f:

$$f^B(b_1, \ldots, b_k) := f^A(b_1, \ldots, b_k) \in B.$$

In this way, we regard subalgebras as algebras, not just sets.

Theorem 2.1.3. *Suppose B is a subalgebra of A.*

1. *The inclusion $B \to A$ is a homomorphism.*

2. *If* $A \models s = t$*, then* $B \models s = t$*.*

3. *If* $\mathcal{K} = \mathrm{Mod}(\Sigma)$ *is an equational class, then* $A \in \mathcal{K} \implies B \in \mathcal{K}$*.*

Proof. (1) holds by choice of the structure on B. For (2), note that

$$t^B(\bar{b}) = t^A(\bar{b})$$
$$s^B(\bar{b}) = s^A(\bar{b})$$

for $\bar{b}$ in B by Theorem 1.4.9 and (1). If $t^A = s^A$, then $t^B = s^B$. Finally, (3) follows directly from (2). □

Example 2.1.4. A subalgebra of a monoid is a monoid, and a subalgebra of a group is a group.

Remark 2.1.5. Note that this *wouldn't work* if we had used the traditional definitions of monoids and groups (see Remark 1.1.3). For example, if we use the traditional definition then the algebra $(\mathbb{R}, +)$ is a group, but the subalgebra $(\mathbb{N}, +)$ is not, and the subalgebra $(\{1, 2, 3, \ldots\}, +)$ is not even a monoid. Including the identity element 0 and the inverse map $-x$ as part of the structure makes things work.

Because a subalgebra of a *foo* is usually a *foo*, we often say sub*foo* instead of subalgebra. For example, we say "subgroup" when working with groups, and "subring" when working with rings.

Example 2.1.6. Theorem 2.1.3 can be used to show that certain classes are not equational classes. For example, the ring $\mathbb{R}$ is a field, but the subring $\mathbb{Z}$ is not. Therefore, fields are not an equational class. Of course, maybe this problem could be fixed the same way we fixed monoids and groups, by adding the division operation $\div$ as part of the structure. In Example 2.2.6, we will see that this doesn't work, and there is no sensible way to make fields into an equational class.

Definition 2.1.7. If S is a subset of an algebra A, then $\langle S \rangle$ or $\langle S \rangle_A$ denotes the set

$$\{t^A(\bar{b}) : t(x_1, \ldots, x_n) \text{ is an } \mathcal{L}\text{-term and } \bar{b} \in S^n\} \qquad (*)$$

We often omit brackets $\{,\}$ inside $\langle , \rangle$, using abbreviations like

$$\langle a_1, \ldots, a_n \rangle = \langle \{a_1, \ldots, a_n\} \rangle$$
$$\langle A, b \rangle = \langle A \cup \{b\} \rangle.$$

Remark 2.1.8. $\langle S\rangle$ is the smallest subalgebra of A containing S. To see this, first note that by taking $t(x) = x$, we get $b = t(b) \in \langle S\rangle$ for any $b \in S$, and so $S \subseteq \langle S\rangle$. If A' is a subalgebra of A containing S, then $\langle S\rangle \subseteq A'$ because if $t(\bar{x})$ is a term and $\bar{b} \in S^n$, then $t^A(\bar{b}) = t^{A'}(\bar{b}) \in A'$. The final step is to show that $\langle S\rangle$ is itself a subalgebra. This is a little confusing to formally prove; here is one approach. For $\bar{b} \in S^n$, let

$$A_{\bar{b}} = \{t^A(\bar{b}) : t(x_1, \dots, x_n) \text{ is a term}\} \subseteq \langle \bar{b}\rangle.$$

It is easy to see that $A_{\bar{b}}$ is a subalgebra containing $b_1, \dots, b_n$. Then $\langle\bar{b}\rangle \subseteq A_{\bar{b}}$, equality holds, and $\langle\bar{b}\rangle$ equals the subalgebra $A_{\bar{b}}$. This shows that $\langle S\rangle$ is a subalgebra when S is finite.

For the case where S is infinite, take a k-ary function symbol f and elements $a_1, \dots, a_k \in \langle S\rangle$. Each a_i is in $\langle S_i\rangle$ for some finite $S_i \subseteq_f S$. Let $S' = \bigcup_{i=1}^n S_i$. Then $a_1, \dots, a_k \in \langle S'\rangle$, and $\langle S'\rangle$ is a subalgebra (by the finite case), and so $f^A(a_1, \dots, a_k) \in \langle S'\rangle \subseteq \langle S\rangle$.

Definition 2.1.9. The subalgebra $\langle S\rangle$ is called the subalgebra *generated* by S. We say that A is *finitely generated* if $A = \langle S\rangle$ for some finite $S \subseteq A$.

Example 2.1.10. The subring of $\mathbb{R}$ generated by $\{\sqrt{2}, \sqrt{3}\}$ contains all the expressions built up from $\sqrt{2}$ and $\sqrt{3}$ using the ring operations, such as

$$\sqrt{2} + \sqrt{3}, \ -\sqrt{2}, 1 + \sqrt{3}, 1 + 1, \sqrt{3} \cdot (\sqrt{2} + 1).$$

In fact, one can show that

$$\langle\sqrt{2}, \sqrt{3}\rangle = \{w + x\sqrt{2} + y\sqrt{3} + z\sqrt{6} : w, x, y, z \in \mathbb{Z}\}. \qquad (\dagger)$$

To prove this, let A be the right hand side of (†). One proves the following:

1. A is a subring of $\mathbb{R}$
2. Any subalgebra of $\mathbb{R}$ containing $\sqrt{2}$ and $\sqrt{3}$ must contain A.

Both of these are straightforward algebraic exercises.

Example 2.1.11. The subgroup of $(\mathbb{R}, +, 0, -)$ generated by π is $\{n\pi : n \in \mathbb{Z}\}$.

Example 2.1.12. The subring of $\mathbb{R}$ generated by $\varnothing$ is the smallest subring of $\mathbb{R}$, which is $\mathbb{Z}$. Indeed, $\mathbb{Z}$ is a subring of $\mathbb{R}$, and if A is any other subring of $\mathbb{R}$, one can show that

$$n \in \mathbb{Z} \implies \pm n \in A$$

by induction on n.

Equivalently, $\mathbb{Z} = \{t^{\mathbb{R}} : t \text{ is a closed term}\}$. That is $\mathbb{Z}$ is the set of real numbers built up from the ring operations with no parameters, like so:

There are some close links between generators and homomorphisms:

Theorem 2.1.13. *Let A be generated by $S \subseteq A$. Suppose two homomorphisms $\alpha_1, \alpha_2 : A \to B$ have the same restriction to S. Then $\alpha_1 = \alpha_2$.*

Proof. Any element of A has the form $t(\bar{a})$ for some term $t(x_1, \ldots, x_n)$ and some $\bar{a} \in S^n$. As homomorphisms preserve terms (Theorem 1.4.9),

$$\alpha_1(t(\bar{a})) = t(\alpha_1(\bar{a})) = t(\alpha_2(\bar{a})) = \alpha_2(t(\bar{a})). \qquad \square$$

Theorem 2.1.14. *Let A be generated by $S \subseteq A$. Let $\alpha : A \to B$ be a homomorphism. Then the image $\alpha(A)$ is $\langle \alpha(S) \rangle_B$.*

Proof.

$$\begin{aligned} \alpha(A) = \alpha(\langle S \rangle) &= \{\alpha(t^A(\bar{b})) : t \text{ is a term and } \bar{b} \in S^n\} \\ &= \{t^B(\alpha(\bar{b})) : t \text{ is a term and } \bar{b} \in S^n\} \\ &= \{t^B(\bar{b}) : t \text{ is a term and } \bar{b} \in \alpha(S)^n\} \\ &= \langle \alpha(S) \rangle_B. \end{aligned} \qquad \square$$

2.2 Products

Binary products

Recall that if A and B are sets, the *Cartesian* or *direct product* is the set

$$A \times B = \{(x, y) : x \in A \text{ and } y \in B\}.$$

The terminology "product" reflects the fact that $|A \times B| = |A| \cdot |B|$. For example, if A has 3 elements and B has 5 elements, then $A \times B$ has 15 elements, the product of 3 and 5.

Definition 2.2.1. Let A, B be two $\mathcal{L}$-algebras. The *product algebra* $A \times B$ is the $\mathcal{L}$-algebra with underlying set $A \times B$ and

$$f^{A\times B}((a_1, b_1), \dots, (a_k, b_k)) := (f^A(a_1, \dots, a_k), f^B(b_1, \dots, b_k)).$$

for each k-ary function symbol $f \in \mathcal{L}$.

The products in Definition 2.2.1 are called *binary products* because there are 2 factors A and B. Later we will consider k-ary products for other values of k, including infinite k.

Example 2.2.2. The direct product of the rings $\mathbb{R}$ and $\mathbb{Z}$ is the structure $(\mathbb{R} \times \mathbb{Z}, +, \cdot, -, 0, 1)$, where the operations are defined as follows:

$$\begin{aligned}(x_1, y_1) + (x_2, y_2) &:= (x_1 + x_2, y_1 + y_2)\\ (x_1, y_1) \cdot (x_2, y_2) &:= (x_1x_2, y_1y_2)\\ -(x, y) &:= (-x, -y)\\ 1 &:= (1, 1)\\ 0 &:= (0, 0).\end{aligned}$$

In other words, all the operations are componentwise.[1]

Any equational class is closed under binary products. For example, the product of two rings is a ring. This will take a little work to show.

Remark 2.2.3. Let A_1, A_2 be two $\mathcal{L}$-algebras. For $i = 1, 2$, let $\pi_i : A_1 \times A_2 \to A_i$ be the projection map $\pi_i(x_1, x_2) = x_i$. Then each π_i is a homomorphism. For example,

$$\begin{aligned}\pi_1(f^{A_1\times A_2}((a_1, b_1), \dots, (a_k, b_k))) &= f^{A_1}(a_1, \dots, a_k)\\ &= f^{A_1}(\pi_1(a_1, b_1), \dots, \pi_1(a_k, b_k)).\end{aligned}$$

Theorem 2.2.4. *Let A_1, A_2 be $\mathcal{L}$-algebras.*

1. *If φ is an equation and $A_i \models \varphi$ for $i = 1, 2$, then $A_1 \times A_2 \models \varphi$.*
2. *If $\mathcal{K}$ is an equational class and $A_1, A_2 \in \mathcal{K}$, then $A_1 \times A_2 \in \mathcal{K}$.*

[1] The operation + is essentially vector addition. In contrast, $\cdot$ is not a natural operation on vectors, except in settings like machine learning and NumPy.

Proof. Part (2) follows formally from (1). For (1), suppose $A_i \models t = s$ for $i = 1, 2$. Let $P = A_1 \times A_2$. We claim $P \models t = s$. Otherwise there are $a_1, \ldots, a_k \in P$ such that $t^P(\bar{a}) \neq s^P(\bar{a})$. Then there is $i \in \{1, 2\}$ such that

$$\pi_i(t^P(\bar{a})) \neq \pi_i(s^P(\bar{a})).$$

As π_i is a homomorphism, we can rewrite the two sides as follows:

$$t^{A_i}(\pi_i(\bar{a})) \neq s^{A_i}(\pi_i(\bar{a})).$$

Then $A_i \not\models t = s$, a contradiction. □

Example 2.2.5. The product of two groups is a group. The product of two rings is a ring.

Again, Theorem 2.2.4 can be used to see that certain classes are not varieties.

Example 2.2.6. The ring $\mathbb{R}$ is a field, but $\mathbb{R} \times \mathbb{R}$ is not, because the zero law (Theorem 1.4.16) fails:

$$\begin{aligned}(0,1) &\neq (0,0)\\ (1,0) &\neq (0,0)\\ (0,1) \cdot (1,0) &= (0,0).\end{aligned}$$

Therefore fields are not an equational class. Unlike the argument in Example 2.1.6, this argument is resilient under adding new symbols to the language, like how we made groups into an equational class by adding a symbol for the inverse map.

One could still try to salvage fields as an equational class by using a completely different set of operations. This doesn't work either. We will see later that if n is finite, then there is a field of size n if and only if n is a prime power. In particular, there are fields of size 2 and 3, but no field of size 6. Regardless of which operations we use, products cannot possibly work.

Perhaps we need to add some extra elements to fields, such as the element ∞. This *still* doesn't work. Suppose we had some way of representing a field with n elements as an algebra with $n + 1$ elements. The field of size 2 would give an algebra of size 3. Taking a product of this algebra with itself three times, we would get an algebra of size $3^3 = 27$, which would need to correspond to a field of size 26. But there is no field of size 26.[2]

Infinite products

Let I be a set.

Definition 2.2.7. An *I-tuple* is a function with domain I. If a is an I-tuple, we write $a(i)$ as $\pi_i(a)$. The notation $(a_i : i \in I)$ means the function $i \mapsto a_i$.

For example, $(2n : n \in \omega)$ is the ω-tuple corresponding to the function $f(n) = 2n$. Although I-tuples are officially functions, we think of them as distinct kinds of object, and use notation to hide the identification.

When $I = \{1, 2, \ldots, n\}$, we identify n-tuples and I-tuples, so that

$$(a_1, a_2, \ldots, a_n) = (a_i : i \in \{1, \ldots, n\}).$$

Likewise, we think of ω-tuples as tuples of length ω, i.e., sequences, so that

$$(a_1, a_2, a_3, \ldots) = (a_i : i \in \omega).$$

Definition 2.2.8. Let $\{A_i\}_{i\in I}$ be a family of sets. The *direct product* $\prod_{i\in I} A_i$ is the set of I-tuples $(a_i : i \in I)$ such that $a_i \in A_i$ for each $i \in I$.

For example, when $I = \{1, 2\}$,

$$\prod_{i\in\{1,2\}} A_i = \{(a_1, a_2) : a_1 \in A_1,\ a_2 \in A_2\} = A_1 \times A_2.$$

Similarly,

$$\prod_{i\in\{1,2,\ldots,n\}} A_i = A_1 \times A_2 \times \cdots \times A_n.$$

Consequently, $\prod_{i\in I} A_i$ generalizes binary direct products $A_1 \times A_2$.

Remark 2.2.9. Suppose A_i doesn't depend on i, so that $A_i = A$ for some fixed set A as i varies. Then $\prod_{i\in I} A$ is the set of functions from I to A. This set is also written A^I, and is called a *power* of A.

[2] Likewise, supposed we tried adding *two* elements, for ∞ and `NaN`. The field of size 2 would give an algebra of size 4. Taking the product of this algebra with itself three times we would get an algebra of size $4^3 = 64$, corresponding to a non-existent field of size 62.

Definition 2.2.10. Let I be a set and let A_i be an $\mathcal{L}$-algebra for each $i \in I$. We make $\prod_{i\in I} A_i$ into an $\mathcal{L}$-algebra by interpreting each k-ary function symbol f as

$$f(a_1, \ldots, a_k) = (f^{A_i}(\pi_i(a_1), \ldots, \pi_i(a_k)) : i \in I).$$

For example, if each A_i is a ring, then addition is defined by

$$a + b := (\pi_i(a) + \pi_i(b) : i \in I)$$

or equivalently

$$(a_i :\in I) + (b_i : i \in I) = (a_i + b_i : i \in I).$$

To be even more specific, when $I = \omega$ this says

$$\begin{aligned} &(a_1, a_2, a_3, \ldots) \\ +&(b_1, b_2, b_3, \ldots) \\ =&(a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots) \end{aligned}$$

As in the case of binary products, the operations are carried out componentwise. In fact Definition 2.2.10 generalizes Definition 2.2.1, which is the special case when $I = \{1, 2\}$.

Remark 2.2.11. The structure on $\prod_{i\in I} A_i$ is chosen to make π_i a homomorphism:

$$\pi_i(f(a_1, \ldots, a_k)) = f^{A_i}(\pi_i(a_1), \ldots, \pi_i(a_k)).$$

Theorem 2.2.12. *Let A_i be an $\mathcal{L}$-algebra for each $i \in I$.*

1. *If φ is an equation and $A_i \models \varphi$ for each $i \in I$, then $\prod_{i\in I} A_i \models \varphi$.*

2. *If $\mathcal{K}$ is an equational class and $A_i \in \mathcal{K}$ for all $i \in I$, then $\prod_{i\in I} A_i \in \mathcal{K}$.*

Proof. The proof of Theorem 2.2.4 works here. □

Example 2.2.13 (Powers)**.** If I is a set and A is an $\mathcal{L}$-algebra, the power $A^I := \prod_{i\in I} A$ is the set of functions $I \to A$, with all the operations defined pointwise. For example, the ring $\mathbb{R}^{\mathbb{R}}$ is the set of functions $f : \mathbb{R} \to \mathbb{R}$, with ring operations defined like so:

$$\begin{aligned} (f+g)(x) &:= f(x) + g(x) \\ (f \cdot g)(x) &:= f(x)g(x) \\ (-f)(x) &:= -f(x) \\ 0(x) &:= 0 \\ 1(x) &:= 1 \end{aligned}$$

We can get more examples of rings by taking certain subrings of $\mathbb{R}^{\mathbb{R}}$. For example, the set of differential functions (in calculus) is a subring. One subring of interest to us is the ring $\mathbb{R}[x]$ of *polynomials*, functions of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

for constants $a_0, \ldots, a_n \in \mathbb{R}$. We will say more about the ring $\mathbb{R}[x]$ later.

Example 2.2.14. Recall the boolean algebras $\{\textsc{False}, \textsc{True}\}$ and $\mathfrak{P}(S)$ from Example 1.3.16. It turns out that

$$\mathfrak{P}(S) \cong \{\textsc{False}, \textsc{True}\}^S. \tag{$*$}$$

The right hand side $\{\textsc{False}, \textsc{True}\}^S$ is the set of truth-valued functions on S, with operations defined pointwise. For example,

$$(f \wedge g)(x) = f(x) \wedge g(x) = (f(x) \text{ } \textsc{And} \text{ } g(x)).$$

We can identify a truth-valued function $f : S \to \{\textsc{False}, \textsc{True}\}$ with the set $\{x \in S : f(x)\}$, and then the pointwise And corresponds to intersections:

$$\{x \in S : f(x) \text{ and } g(x)\} = \{x \in S : f(x)\} \cap \{x \in S : g(x)\}.$$

Similarly, pointwise Or corresponds to unions, and so on, giving the isomorphism of $(*)$.

Applying Theorem 2.2.12 to $(*)$, we see that any equation satisfied by the algebra $\{\textsc{False}, \textsc{True}\}$ must also be satisfied by $\mathfrak{P}(S)$. For example, the logical identity

$$x \text{ and } (y \text{ or } z) \iff (x \text{ and } y) \text{ or } (x \text{ and } z)$$

corresponds to the set-theoretic fact

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z).$$

If I recall correctly, the observation that truth values and sets are governed by the same equations goes back to Boole, which is why boolean algebras are named in his honor.

2.3 Descending functions along surjections

Often in mathematics we want to define a function $f : A \to B$, where $A = \{\pi(x) : x \in A'\}$ for some function $\pi : A' \to A$. Since every element of A has the form $\pi(x)$, to specify f we only need to specify $f(\pi(x))$ for $x \in A'$. The following theorem gives the precise criterion that $f(\pi(x))$ needs to satisfy in order for $f(-)$ to be well-defined.

Theorem 2.3.1. *Let $\pi : A' \to A$ be a surjection. Let $f' : A' \to B$ be a function such that*

$$\pi(x) = \pi(y) \implies f'(x) = f'(y). \qquad (*)$$

Then there is a unique function $f : A \to B$ such that $f(\pi(x)) = f'(x)$, i.e., the following diagram commutes:

$$\begin{tikzcd}
A' \arrow[d, "\pi"'] \arrow[dr, "f'"] & \\
A \arrow[r, dashed, "f"'] & B.
\end{tikzcd}$$

Proof. For $z \in A$, let $S_z = \{f'(x) : x \in A',\ \pi(x) = z\}$. There is at least one $x \in A'$ with $\pi(x) = z$ because π is surjective, so S_z is non-empty. If $x_1, x_2 \in A'$ satisfy $\pi(x_i) = z$ for $i = 1, 2$, then $f(x_1) = f(x_2)$ by $(*)$. Therefore S_z has a unique element. Let $f(z)$ be the unique element of S_z.

If $x \in A'$ and $z = \pi(x)$, then $f'(x) \in S_z = \{f(z)\}$, so $f'(x) = f(z) = f(\pi(x))$. This proves existence of f. For uniqueness, suppose $f'' : A \to B$ is another function satisfying $f''(\pi(x)) = f'(x)$. For any $z \in A$, there is $x \in A'$ with $\pi(x) = z$, and then

$$f''(z) = f''(\pi(x)) = f'(x) = f(\pi(x)) = f(z),$$

so $f'' = f$. □

Example 2.3.2. Let $\mathcal{K}$ be the class of $\mathcal{L}$-algebras. If $X, Y \in \mathcal{K}$ are isomorphic, then $|X| = |Y|$. Therefore, there is a map from the class $\mathcal{K}/{\cong}$ of isomorphism classes to the class Card of cardinals sending the isomorphism class of X to the cardinality $|X|$. Ignoring the difference between sets and classes, this is an instance of Theorem 2.3.1:

$$\begin{tikzcd}
\mathcal{K} \arrow[d] \arrow[dr] & \\
\mathcal{K}/{\cong} \arrow[r, dashed] & \text{Card.}
\end{tikzcd}$$

The surjectivity of $\mathcal{K} \to \mathcal{K}/{\cong}$ holds because every isomorphism class is the isomorphism class of some algebra. The condition $(*)$ in Theorem 2.3.1 holds because

$$[X]_{\cong} = [Y]_{\cong} \iff X \cong Y \implies |X| = |Y|.$$

The conclusion of Theorem 2.3.1 says that the map $f : \mathcal{K}/{\cong} \to \text{Card}$ satisfies

$$f([X]_{\cong}) = |X|,$$

so that f sends the isomorphism class of X to the cardinality of X.

2.4 Congruences and quotients

Congruences

Recall that equivalence relations on A are subsets of $A \times A$.

Definition 2.4.1. Let A be an $\mathcal{L}$-algebra. A *congruence* on A is an equivalence relation E on A that is also a subalgebra of $A \times A$.

Unwinding the definition, an equivalence relation $\sim$ on A is a congruence iff

$$(a_1 \sim b_1 \text{ and } a_2 \sim b_2 \text{ and} \ldots \text{and } a_k \sim b_k) \implies f(a_1, \ldots, a_k) \sim f(b_1, \ldots, b_k)$$

for any k-ary function symbol $f \in \mathcal{L}$. For example, an equivalence relation $\sim$ on a group $(G, \cdot, 1, (-)^{-1})$ is a congruence if

$$(a_1 \sim b_1 \text{ and } a_2 \sim b_2) \implies a_1 a_2 \sim b_1 b_2$$
$$a \sim b \implies a^{-1} \sim b^{-1}$$
$$1 \sim 1.$$

The next lemma gives a slightly different criterion for being a congruence, which is sometimes easier to check.

Theorem 2.4.2. *Let $\sim$ be an equivalence relation on an $\mathcal{L}$-algebra A. Then $\sim$ is a congruence iff the following holds: for any k-ary function symbol $f \in \mathcal{L}$ and any $1 \leq i \leq k$,*

$$a_i \sim a_i' \implies f(a_1, \ldots, a_k) \sim f(a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_k). \tag{$*$}$$

Proof. First suppose $\sim$ is a congruence, and $a_i \sim a_i'$. For $j \neq i$ define $a_j' := a_j$. Then $a_j \sim a_j'$ because $\sim$ is reflexive. As $a_j \sim a_j'$ for *all* $j \leq k$, we see that

$$f(a_1, \ldots, a_k) \sim f(a_1', \ldots, a_k') = f(a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_k).$$

Conversely, suppose $(*)$ holds. Suppose $a_i \sim b_i$ for $i = 1, \ldots, k$. Then $(*)$ gives

$$\begin{aligned} &f(a_1, a_2, a_3, \ldots, a_k) \\ \sim &f(b_1, a_2, a_3, \ldots, a_k) \\ \sim &f(b_1, b_2, a_3, \ldots, a_k) \\ \sim &\cdots \\ \sim &f(b_1, b_2, \ldots, b_k). \end{aligned}$$ □

For example, a relation $\sim$ on a group G is a congruence iff

$$\begin{aligned} a \sim a' &\implies ab \sim a'b \\ b \sim b' &\implies ab \sim ab' \\ a \sim b &\implies a^{-1} \sim b^{-1}. \end{aligned}$$

Congruences are a little abstract, but can be understood in terms of more concrete objects in the case of rings and groups.

Definition 2.4.3. Let R be a ring. An *ideal* is a subset $I \subseteq R$ such that

1. $0 \in I$.
2. $x, y \in I \implies x + y \in I$.
3. $(x \in R \text{ and } y \in I) \implies xy \in I$.

Remark 2.4.4. The even numbers $2\mathbb{Z}$ are an ideal in the ring $\mathbb{Z}$. More generally, if R is any ring and $a \in R$, then the set $aR := \{ax : x \in R\}$ is an ideal. Such ideals are called *principal ideals.*

Theorem 2.4.5. *Let R be a ring.*

1. *If I is an ideal, define $x \equiv_I y$ to mean $x - y \in I$. Then $\equiv_I$ is a congruence.*
2. *This gives a bijection between congruences on R and ideals on R.*

Proof. First, note that if $\sim$ is a congruence, then

$$x \sim y \iff x - y \sim 0$$

for any $x, y \in R$. Indeed,

$$\begin{aligned} x \sim y &\implies x - y \sim y - y = 0 \\ x - y \sim 0 &\implies x = (x - y) + y \sim 0 + y = y. \end{aligned}$$

Therefore $\sim$ must have the form

$$x \sim y \iff x - y \in I$$

for some set $I \subseteq R$, namely $I = \{z \in R : z \sim 0\}$. It remains to characterize which sets I yield congruences.

1. Reflexivity says that $x - x \in I$ for any x. This holds iff $0 \in I$.
2. Symmetry says that $x - y \in I \iff y - x \in I$. This holds iff I is closed under negation.
3. Transitivity says that if $x - y \in I$ and $y - z \in I$, then $x - z \in I$. This holds iff I is closed under addition.
4. Compatibility with $+$ says that if $x - y \in I$, then $(x + a) - (y + a) \in I$. This condition holds for any I.
5. Compatibility with $\cdot$ says that if $x - y \in I$, then $(ax) - (ay) \in I$. This condition holds iff I is closed under multiplication by R.

In summary, I yields a congruence if and only if the following four properties hold:

- $0 \in I$
- $x \in I \implies -x \in I$
- $x, y \in I \implies x + y \in I$
- $a \in R,\ x \in I \implies ax \in I.$

The second condition is an instance of the fourth (take $a = -1$), so it can be removed. The remaining three conditions are the definition of "ideal." □

Remark 2.4.6. The relation $x \equiv_I y$ is called "congruence modulo I", and is usually written like $x \equiv y \pmod{I}$. When I is a principal ideal aR, it is usually written $x \equiv y \pmod{a}$.

Example 2.4.7. In the ring $\mathbb{Z}$, $x \equiv y \pmod 2$ holds iff $x - y$ is even. There are two equivalence classes, the even numbers and odd numbers.

Definition 2.4.8. Let G be a group. A *normal subgroup* is a subgroup $N \subseteq G$ such that

$$(x \in N \text{ and } y \in G) \implies yxy^{-1} \in N. \tag{†}$$

When G is abelian, $yxy^{-1} = xyy^{-1} = x$, so (†) says

$$(x \in N \text{ and } y \in G) \implies x \in N,$$

which is trivial. Therefore for abelian groups, a normal subgroup is the same thing as a subgroup. But for non-abelian groups, the two concepts are usually different.

Lemma 2.4.9. *Let G be a group.*

1. *If N is a normal subgroup, define $x \equiv_N y$ to mean $xy^{-1} \in N$. Then $\equiv_N$ is a congruence.*
2. *This gives a bijection between congruences on G and normal subgroups of G.*

Proof. Similar to Lemma 2.4.5. Compatibility with $(-)^{-1}$ can be ignored thanks to the following:

Claim. If $\approx$ is a monoid congruence (on $(G, \cdot, 1)$), then $\approx$ is a group congruence.

Indeed, if $x \approx y$ then

$$x^{-1} = x^{-1}yy^{-1} \approx x^{-1}xy^{-1} = y^{-1}. \qquad \square$$

Remark 2.4.10.

1. The relation $x \equiv_N y$ is called "congruence modulo N", and is usually written like $x \equiv y \pmod{N}$.
2. In group theory, the kernel of a homomorphism $f : G \to H$ is the *subgroup* $\{x \in G : f(x) = 1\}$. This is the normal subgroup corresponding to the kernel in the sense of Definition 2.6.2.

Quotients

If X is a set and E is an equivalence relation on X, let X/E denote the quotient, the set $\{[a]_E : a \in X\}$, where $[a]_E$ is the E-equivalence class $[a]_E = \{b \in X : a \; E \; b\}$. Recall that $[a]_E = [b]_E \iff a \; E \; b$. We omit the subscript when E is clear from context.

Theorem 2.4.11 (Quotients)**.** *Let A be an $\mathcal{L}$-algebra and E be a congruence on A. Then there is a unique $\mathcal{L}$-algebra with underlying set A/E such that $A \to A/E$ is a homomorphism, meaning that*

$$f^{A/E}([a_1], \ldots, [a_k]) = [f^A(a_1, \ldots, a_k)] \tag{$\dagger$}$$

for any k-ary function symbol in $\mathcal{L}$.

Proof. The equation ($\dagger$) is essentially an instance of Theorem 2.3.1:

$$\begin{tikzcd}
A^k \arrow[d] \arrow[dr] & \\
(A/E)^k \arrow[r, dashed] & A/E,
\end{tikzcd}$$

where the vertical arrow is $(x_1, \ldots, x_k) \mapsto ([x_1], \ldots, [x_k])$, the diagonal arrow is $\bar{x} \mapsto [f^A(\bar{x})]$, and the dashed arrow is the map $f^{A/E} : (A/E)^k \to A/E$ we are trying to define.

By Theorem 2.3.1, the function $f^{A/E} : (A/E)^k \to A/E$ is uniquely determined by (†), as long as

$$([a_1], \dots, [a_k]) = ([b_1], \dots, [b_k]) \implies [f^A(\bar{a})] = [f^A(\bar{b})],$$

or equivalently,

$$(a_i \; E \; b_i \text{ for } i = 1, \dots, k) \implies (f^A(\bar{a}) \; E \; f^A(\bar{b})).$$

This holds because E is a congruence. □

Definition 2.4.12. If A is an $\mathcal{L}$-algebra and E is a congruence, then A/E is called the *quotient algebra* of A by E.

Remark 2.4.13. In group theory and ring theory, if A is a group or ring, and B is a normal subgroup or ideal, then A/B means $A/\equiv_B$ where $\equiv_B$ is the congruence associated with B. In these cases, one can show that $|A| = |A/B| \cdot |B|$. In particular, when A is finite, one can show that $|A/B| = |A|/|B|$, which explains the term "quotient." (For more on this, see Theorems 2.4.18 and 2.4.19 below.)

Example 2.4.14. Let A be $\mathbb{Z}/2\mathbb{Z}$, that is, the quotient of the ring $\mathbb{Z}$ by the equivalence relation $x \equiv_2 y \iff x - y \in 2\mathbb{Z}$. There are two equivalence classes, Even and Odd, with $[x] =$ Even for $x \in 2\mathbb{Z}$, and $[x] =$ Odd for $x \notin 2\mathbb{Z}$. Addition on A is defined so that

$$[x] +^A [y] = [x + y].$$

If x and y are even, then $x + y$ is even, so Even + Even = Even. Similarly, we can complete the tables of addition and multiplication as follows:

+	Even	Odd
Even	Even	Odd
Odd	Odd	Even

·	Even	Odd
Even	Even	Even
Odd	Even	Odd

Note that this isn't just a ring—it's a field.

Like subalgebras and products, quotients preserve equations:

Theorem 2.4.15. *Let A be an $\mathcal{L}$-algebra and E be a congruence on A.*

1. *If A satisfies an equation φ, then A/E satisfies φ.*
2. *If $\mathcal{K} = \mathrm{Mod}(\Sigma)$ is an equational class, then $A \in \mathcal{K} \implies A/E \in \mathcal{K}$.*

Proof. By construction, there is a surjective homomorphism $A \to A/E$. Then $A \models \varphi \implies A/E \models \varphi$ (Lemma 1.4.10). □

If E is an equivalence relation on A, a *set of representatives* for E is a set $S \subseteq A$ containing exactly one element from each E-equivalence class. The next theorem gives a more concrete way to understand quotient structures.

Theorem 2.4.16. *Let A be an $\mathcal{L}$-algebra and E be a congruence. Let S be a set of representatives for E. Let $\rho : A \to S$ be the map sending $x \in A$ to the unique $y \in S \cap [x]_E$. For each k-ary function symbol $f \in \mathcal{L}$, define*

$$f^S(x_1, \ldots, x_k) = \rho(f^A(x_1, \ldots, x_k)).$$

This makes S into an $\mathcal{L}$-algebra isomorphic to A/E.

Proof. The construction certainly makes S into an $\mathcal{L}$-algebra. Define $\alpha : S \to A/E$ by $\alpha(x) = [x]$. We claim that α is an isomorphism.

1. α is a homomorphism: if f is a k-ary function symbol, then

   $$\alpha(f^S(x_1, \ldots, x_k)) = [\rho(f^A(x_1, \ldots, x_k))]$$

   But $\rho(y)\ E\ y$ for any $y \in A$, so $[\rho(y)] = [y]$. Therefore

   $$[\rho(f^A(x_1, \ldots, x_k))] = [f^A(x_1, \ldots, x_k)].$$

   By construction of the quotient,

   $$[f^A(x_1, \ldots, x_k)] = f^{A/E}([x_1], \ldots, [x_k]) = f^{A/E}(\alpha(x_1), \ldots, \alpha(x_k)).$$

   Putting everything together,

   $$\alpha(f^S(x_1, \ldots, x_k)) = f^{A/E}(\alpha(x_1), \ldots, \alpha(x_k)).$$

2. α is a bijection: clear by choice of S. □

Example 2.4.17. In the ring $\mathbb{Z}$, $\{0, 1\}$ is a set of representatives for $\equiv_2$, and so the quotient ring $\mathbb{Z}/{\equiv_2}$ is isomorphic to the ring

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$\diamondsuit$ The terminology "quotient"

Theorem 2.4.18. *Let R be a ring and I be an ideal. Let $[a]_I$ denote the equivalence class of $a \in R$ modulo I.*

1. *For any $a \in R$, the size of $[a]_I$ equals the size of I.*
2. *$|R| = |R/I| \cdot |I|$.*
3. *If R is finite, then $|R/I| = |R|/|I|$.*

Proof. 1. Note that $x \equiv 0 \pmod{I} \iff x \in I$, so $[0]_I = I$. There is a well-defined map

$$\begin{aligned} [0]_I &\to [a]_I \\ x &\mapsto x + a \end{aligned}$$

because $x \equiv 0 \pmod{I} \implies a + x \equiv a \pmod{I}$. Similarly, there is a well-defined map

$$\begin{aligned} [a]_I &\to [0]_I \\ x &\mapsto x - a. \end{aligned}$$

These two maps are inverses of each other, so they are bijections and $|[a]_I| = |[0]_I| = |I|$.

2. The ring R is a disjoint union of equivalence classes. Each equivalence class has cardinality $|I|$ by part (1), and the number of equivalence classes is $|R/I|$, because R/I is the set of equivalence classes.

3. Clear. □

In ring theory, $[a]_I$ is usually written $a + I$.

Theorem 2.4.19. *Let G be a group and let N be a normal subgroup. Let $[a]_N$ denote the equivalence class of $a \in G$ modulo N.*

1. *For any $a \in G$, the size of $[a]_N$ equals the size of N.*
2. *$|G| = |G/N| \cdot |N|$.*
3. *If G is finite, then $|G/N| = |G|/|N|$.*

Proof. Like Theorem 2.4.18, using the bijections

$$\begin{aligned}[1]_N &\to [a]_N \\ x &\mapsto xa\end{aligned}$$

and

$$\begin{aligned}[a]_N &\to [1]_N \\ x &\mapsto xa^{-1}\end{aligned}$$ □

2.5 Application: finite fields

The rings we have seen so far are subrings of $\mathbb{C}$, like $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$. All of the are infinite. In this section, we use the machinery of quotients to construct examples of finite rings and fields. These finite rings and fields play importat roles in number theory, cryptography, and error correcting codes.

Work in the ring of integers $\mathbb{Z}$. Recall the relation $x \equiv_n y$ or $x \equiv y \pmod{n}$, meaning that $x - y \in n\mathbb{Z}$. This relation is called *congruence modulo* n.

Lemma 2.5.1. *If* $n > 0$*, then* $\{0, 1, \ldots, n-1\}$ *is a system of representatives for* $\equiv_n$*. That is, for every* $x \in \mathbb{Z}$ *there is a unique* $y \in \{0, \ldots, n-1\}$ *with* $x \equiv y \pmod{n}$*.*

Proof. An exercise, by induction on x. □

For example, every integer x is congruent modulo 10 to exactly one value y in the set $\{0, 1, 2, \ldots, 9\}$. If x is positive, then y is the final digit in the base 10 representation of x. In general, if x and n are positive integers, then the unique $y \in \{0, 1, \ldots, n-1\}$ such that $x \equiv y \pmod{n}$ is the remainder of dividing x by n. In computer science, this operation is often written $x \bmod n$. We will encounter it later in Section 3.9.

Lemma 2.5.2. *If* $0 \neq n \in \mathbb{Z}$*, and* $x \in \mathbb{Z}$*, there is* $y \in \mathbb{Z}$ *with*

$$\begin{gathered} x \equiv y \pmod{n} \\ |y| < |n|. \end{gathered}$$

Proof. Since $n\mathbb{Z} = (-n)\mathbb{Z}$, we may assume $n > 0$ by replacing n with $-n$ if necessary. Then there is some $y \in \{0, 1, 2, \dots, n-1\}$ with $x \equiv y \pmod{n}$ by Lemma 2.5.1. □

Recall that a *principal ideal* in a ring R is an ideal of the form $aR = \{ax : x \in R\}$.

Theorem 2.5.3. *Every ideal $I \subseteq \mathbb{Z}$ is a principal ideal $I = n\mathbb{Z}$ for some $n \geq 0$.*

Proof. Note that $\{0\} \subseteq I$. If $I = \{0\}$, take $n = 0$. Otherwise, take $n \in I \setminus \{0\}$ minimizing $|n|$. Multiplying n by -1 if necessary, we may assume $n \geq 0$. Then $n\mathbb{Z} \subseteq I$ because I is an ideal. We claim $n\mathbb{Z} = I$. Otherwise, take $a \in I \setminus n\mathbb{Z}$. By Lemma 2.5.2 there is $b \in \mathbb{Z}$ with

$$\begin{gathered} b \equiv a \pmod{n} \\ |b| < |n|. \end{gathered}$$

Then $b - a \in n\mathbb{Z} \subseteq I$, and $a \in I$, so $b \in I$ because I is closed under addition. If $b \neq 0$ then b contradicts the choice of n. If $b = 0$, then $a \equiv b = 0 \pmod{n}$, so $a \in n\mathbb{Z}$, contradicting the choice of a. □

Remark 2.5.4. If $n > 0$, then $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $R = (\{0, 1, \dots, n-1\}, +^R, \cdot^R)$, where $x +^R y$ is the unique $z \in R$ with $x + y \equiv z \pmod{n}$, and $x \cdot^R y$ is the unique $w \in R$ with $xy \equiv w \pmod{n}$. This follows by Theorem 2.4.16 applied to the system of representatives in Lemma 2.5.1. In particular, $\mathbb{Z}/n\mathbb{Z}$ is finite, of size n.

Using the notation from computer science,

$$\begin{gathered} x +^R y = (x + y) \bmod n \\ x \cdot^R y = (xy) \bmod n. \end{gathered}$$

For example, here is the table of multiplication and addition for $\mathbb{Z}/5\mathbb{Z}$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Note that this is not just a ring but a field ($1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$). We will see shortly that $\mathbb{Z}/n\mathbb{Z}$ is a field whenever n is a prime number. We first prove a couple general facts about rings.

Lemma 2.5.5. *Let I, J be ideals in a ring R. Let $I + J := \{x + y : x \in I,\ y \in J\}$. Then $I + J$ is an ideal containing I and J.*

Proof. To show that $I + J$ is an ideal, there are three things to check:

1. $0 \in I + J$: take $x = 0 \in I$ and $y = 0 \in J$.
2. $I + J$ is closed under addition: if $x, x' \in I$ and $y, y' \in J$, then $(x + y) + (x' + y') = (x + x') + (y + y') \in I + J$.
3. $I + J$ is closed under multiplication by R: if $x \in I, y \in J$, and $a \in R$, then $a(x + y) = (ax) + (ay) \in I + J$.

Finally, if $x \in I$ then $x + 0 \in I + J$ because $0 \in J$. This shows $I \subseteq I + J$, and $J \subseteq I + J$ follows similarly. □

An ideal $I \subseteq R$ is *proper* if $1 \notin I$. If $1 \in I$, then $x = x1 \in I$ for every $x \in R$, and so $I = R$. Thus there is exactly one improper ideal, namely R itself. A *maximal ideal* is a maximal proper ideal. Using Zorn's lemma, one can show that every proper ideal is contained in a maximal proper ideal, though we will not use this fact.

Theorem 2.5.6. *If I is a maximal ideal, then R/I is a field.*

Proof. Let $[a] \in R/I$ denote the image of $a \in R$. First we show that $1 \neq 0$ in R/I. The fact that $1 \notin I$ means that $1 \not\equiv 0 \pmod{I}$, so $[1] \neq [0]$. Next we show that any $[a] \neq 0$ has a multiplicative inverse. By Lemma 2.5.5, $aR + I$ is an ideal containing aR and I. The fact that $[a] \neq 0$ means that $a = a - 0 \notin I$. Therefore $aR + I \supsetneq I$, as $a \in aR \subseteq aR + I$. By maximality of I, $aR + I$ is improper, so $1 \in aR + I$. Therefore there are $x \in R$ and $y \in I$ with $1 = ax + y$. Then $ax - 1 = y \in I$, so that $ax \equiv 1 \pmod{I}$ and $[a][x] = [ax] = [1]$. Then $[x]$ is the multiplicative inverse of $[a]$. □

Theorem 2.5.7. *If p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field.*

Proof. It suffices to show that the ideal $p\mathbb{Z}$ is maximal. If not, take a larger proper ideal $I \supsetneq p\mathbb{Z}$. By Theorem 2.5.3, $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Then $p \in p\mathbb{Z} \subseteq n\mathbb{Z}$, so p is a multiple of n. In other words, $p = nm$ for some $m \in \mathbb{Z}$. As p is prime, one of n or m is ± 1.

- If $n = \pm 1$, then $n\mathbb{Z}$ is improper, a contradiction.
- If $m = \pm 1$, then $n = \pm p$, and $n\mathbb{Z} = p\mathbb{Z}$, a contradiction. □

On the other hand, if n is a composite number ab, then $\mathbb{Z}/n\mathbb{Z}$ is not a field. To see this, note that a and b are not multiples of n, but $ab = n$ is a multiple of n. Thus

$$\begin{aligned} a &\not\equiv 0 \pmod{n} \\ b &\not\equiv 0 \pmod{n} \\ ab &\equiv 0 \pmod{n}. \end{aligned}$$

In the quotient $\mathbb{Z}/n\mathbb{Z}$, it follows that $[a] \neq 0$ and $[b] \neq 0$, but $[a][b] = [ab] = 0$, contradicting Theorem 1.4.16 if $\mathbb{Z}/n\mathbb{Z}$ is a field.

As for $n = 1$, the quotient $\mathbb{Z}/n\mathbb{Z}$ is the *trivial ring* with only one element, which fails to be a field because of the requirement that $0 \neq 1$ in fields. We will see later in Lemma 2.7.9 that $\mathbb{Z}/0\mathbb{Z}$ is isomorphic to $\mathbb{Z}$, so it is not a field. In summary, the only quotients of $\mathbb{Z}$ that are fields are $\mathbb{Z}/p\mathbb{Z}$ for prime p.

2.6 The fundamental theorem on homomorphisms

In this section, we prove the *fundamental theorem of homomorphisms* (Theorem 2.6.7), which analyzes the structure of homomorphisms in terms of quotients and subalgebras. This theorem shows that any homomorphism is built out of three components:

1. A homomorphism of the form $A \to A/E$ where A is an algebra and A/E is a quotient.
2. An isomorphism.
3. An inclusion homomorphism $A \to B$ where A is a subalgebra of B.

We will see some applications of this theorem in Section 2.7 and much later in Chapter 9.

Theorem 2.6.1 (Images). *Let $\alpha : A \to B$ be a homomorphism of $\mathcal{L}$-algebras. Then the image* $\mathrm{im}(\alpha) = \alpha(A) = \{\alpha(x) : x \in A\}$ *is a subalgebra of B.*

Proof. Suppose $f \in \mathcal{L}$ is a k-ary function symbol, and $b_1, \ldots, b_k \in \mathrm{im}(\alpha)$. Each b_i can be written as $\alpha(a_i)$ for some $a_i \in A$. Then

$$f(b_1, \ldots, b_k) = f(\alpha(a_1), \ldots, \alpha(a_k)) = \alpha(f(a_1, \ldots, a_k)) \in \mathrm{im}(\alpha). \qquad \square$$

Conversely, if A is a subalgebra of B, then A is the image of a homomorphism, namely the inclusion $A \hookrightarrow B$ which is a homomorphism by Theorem 2.1.3. Thus the subalgebras of B are precisely those sets which are images of homomorphisms into B. Next, we do something similar with congruences.

Definition 2.6.2. Let $\alpha : A \to B$ be a homomorphism of $\mathcal{L}$-algebras. The *kernel* of α is the equivalence relation

$$a \sim b \iff \alpha(a) = \alpha(b).$$

We write the kernel as $\ker(\alpha)$.

Theorem 2.6.3. *If $\alpha : A \to B$ is a homomorphism of $\mathcal{L}$-algebras, then the kernel is a congruence on A.*

Proof. Let $E = \ker(\alpha)$. Let $f \in \mathcal{L}$ be a k-ary function symbol. If $a_i \mathrel{E} b_i$ for $i = 1, \ldots, k$, then $\alpha(a_i) = \alpha(b_i)$ for each i. As α is a homomorphism,

$$\alpha(f(\bar{a})) = f(\alpha(\bar{a})) = f(\alpha(\bar{b})) = \alpha(f(\bar{b})).$$

Therefore $f(\bar{a}) \mathrel{E} f(\bar{b})$. □

Conversely, every congruence E on A is the kernel of some homomorphism out of A, namely the quotient homomorphism $A \to A/E$. Thus the congruences on A are precisely those relations which are kernels of homomorphisms out of A.

Remark 2.6.4. In ring theory, the kernel of a homomorphism $f : R \to S$ is the *ideal* $\{x \in R : f(x) = 0\}$. This is the ideal corresponding to the kernel in the sense of Definition 2.6.2.

Likewise, in group theory the kernel of a homomorphism $f : G \to H$ is $\{x \in G : f(x) = 1\}$, which is the normal subgroup corresponding to the kernel congruence.

Lemma 2.6.5. *Let A, B, C be algebras. Let $\alpha : A \to B$ be a surjective homomorphism and $\beta : B \to C$ be a function such that $\beta \circ \alpha : A \to C$ is a homomorphism. Then β is a homomorphism.*

Proof. Let f be a k-ary function symbol. If $\bar{b} \in B^k$, then $\bar{b} = \alpha(\bar{a})$ for some $\bar{a} \in A^k$. Then

$$\beta(f(\bar{b})) = \beta(f(\alpha(\bar{a}))) = \beta(\alpha(f(\bar{a})) = f(\beta(\alpha(\bar{a})) = f(\beta(\bar{b}))$$

because α and $\beta \circ \alpha$ are homomorphisms. Therefore β is a homomorphism. □

Theorem 2.6.6 (Universal property of quotients)**.** *Let A be an algebra and E be a congruence on A. If $\alpha : A \to B$ is a homomorphism and $E \subseteq \ker(\alpha)$, then there is a unique homomorphism $\beta : A/E \to B$ such that $\alpha(x) = \beta([x])$, or equivalently, the following diagram commutes:*

$$\begin{tikzcd}
A \arrow[d] \arrow[dr, "\alpha"] & \\
A/E \arrow[r, dashed, "\beta"'] & B
\end{tikzcd}$$

Proof. The condition $E \subseteq \ker(\alpha)$ means that

$$[x]_E = [y]_E \implies \alpha(x) = \alpha(y).$$

By Theorem 2.3.1 there is a unique *function* $\beta : A/E \to B$ such that $\alpha(x) = \beta([x])$. We need β to be a homomorphism. The composition $A \to A/E \to B$ is the homomorphism α, and $A \to A/E$ is a surjective homomorphism, so $\beta : A/E \to B$ is a homomorphism by Lemma 2.6.5. □

Theorem 2.6.7 (Fundamental theorem on homomorphisms)**.** *Let $\alpha : A \to B$ be a homomorphism of $\mathcal{L}$-algebras. Let E be the kernel (a congruence on A) and let* $\operatorname{im}(\alpha)$ *be the image (a subalgebra of B). There is an isomorphism $\beta : A/E \to \operatorname{im}(\alpha)$, and α is the composition of the following three homomorphisms:*

$$A \to A/E \xrightarrow{\beta} \operatorname{im}(\alpha) \xrightarrow{\subseteq} B$$

Proof. We can regard $\alpha : A \to B$ as a surjective homomorphism $\alpha' : A \to \operatorname{im}(\alpha)$. Then $\ker(\alpha') = \ker(\alpha) \supseteq E$, so Theorem 2.6.6 gives a homomorphism

$\beta : A/E \to \operatorname{im}(\alpha)$ making the diagram commute:

$$\begin{tikzcd}
A \arrow[rrr, "\alpha"] \arrow[dr] \arrow[drr, "\alpha'"] & & & B. \\
& A/E \arrow[r, dashed, "\beta"'] & \operatorname{im}(\alpha) \arrow[ur, hook] &
\end{tikzcd}$$

Then β is an isomorphism:

- β is surjective because any element of $\operatorname{im}(\alpha)$ has the form $\alpha(a) = \beta([a])$ for some $a \in A$.

- β is injective because for $a, b \in A$,

$$\beta([a]) = \beta([b]) \iff \alpha(a) = \alpha(b) \iff a \mathrel{E} b \iff [a] = [b]. \qquad \square$$

In the case of surjective homomorphisms, Theorem 2.6.7 says the following:

Corollary 2.6.8. *If $\alpha : A \to B$ is a surjective homomorphism, then there is an isomorphism $A/\ker(\alpha) \to B$.*

This gives some abstract intuition or motivation for quotients: the quotient A/E is the unique algebra, up to isomorphism, such that there is a surjective homomorphism $\alpha : A \to A/E$ with kernel E.

2.7 Application: characteristic of fields

Using the fundamental theorem on homomorphisms, we can define the *characteristic* of a ring or field. This is an important invariant, especially for fields, as we will see later in Chapter 9 and Theorem 14.2.10.

If R is a ring and $n \in \mathbb{Z}$, let n^R be the interpretation of n in R, that is,

$$n^R = \begin{cases} (\underbrace{1 + \cdots + 1}_{n \text{ times}})^R & \text{if } n > 0 \\ 0^R & \text{if } n = 0 \\ (-(\underbrace{1 + \cdots + 1}_{n \text{ times}}))^R & \text{if } n < 0 \end{cases}$$

For example, $n^{\mathbb{Z}} = n$.

Lemma 2.7.1. *The map $\alpha : n \mapsto n^R$ is the unique homomorphism from $\mathbb{Z}$ to R.*

Proof. The fact that α is a homomorphism is an exercise in induction and the ring axioms. If $\beta : \mathbb{Z} \to R$ is another homomorphism, then $\beta(n) = \alpha(n)$ by Theorem 1.4.9. For example,

$$\beta(3) = \beta(1+1+1) = (1+1+1)^R = \alpha(3).$$

Alternatively, uniqueness follows because a homomorphism is determined by what it does on a set of generators (Theorem 2.1.13), and $\mathbb{Z}$ is generated by the empty set. □

The subring of R generated by the empty set, written $\langle\varnothing\rangle_R$, can be described abstractly as the smallest subring of R, or explicitly as the set of things of the form t^R for t a closed term.

Lemma 2.7.2. *The image* $\operatorname{im}(\alpha)$ *equals* $\langle\varnothing\rangle_R$.

This follows from Theorem 2.1.14, but we give another proof.

Proof. The image $\operatorname{im}(\alpha)$ is a subring, so $\operatorname{im}(\alpha) \supseteq \langle\varnothing\rangle_R$. On the other hand, $\alpha(n) = n^R$ is clearly t^R for some closed term t, so $\alpha(n) \in \langle\varnothing\rangle_R$. Thus $\operatorname{im}(\alpha) \subseteq \langle\varnothing\rangle_R$. □

We summarize the situation below:

Theorem 2.7.3. *If R is a ring, then there is a unique homomorphism $\alpha : \mathbb{Z} \to R$ given by $\alpha(n) = n^R$, and the image* $\operatorname{im}(\alpha)$ *is the minimal subring $\langle\varnothing\rangle_R$.*

Definition 2.7.4. The *characteristic* of R, written $\operatorname{char}(R)$, is the unique $n \in \mathbb{N}$ such that the kernel of $\mathbb{Z} \to R$ is the principal ideal $n\mathbb{Z}$.

Here, we are using the kernel ideal $\ker(\alpha) = \{x : \alpha(x) = 0\}$, rather than the kernel congruence $\ker(\alpha) = \{(x, y) : \alpha(x) = \alpha(y)\}$; see Remark 2.6.4. The fact that the kernel is a principal ideal comes from Theorem 2.5.3.

Theorem 2.7.5. *If R has characteristic n, then the minimal subring $\langle\varnothing\rangle_R$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.*

Proof. By Theorem 2.7.3, $\langle \varnothing \rangle_R$ is the image of the unique homomorphism $\alpha : \mathbb{Z} \to R$. By the fundamental theorem on homomorphisms, $\langle \varnothing \rangle_R = \mathrm{im}(\alpha) \cong \mathbb{Z}/\ker(\alpha) = \mathbb{Z}/n\mathbb{Z}$, where $n = \mathrm{char}(R)$. □

Example 2.7.6. Consider the ring $R = \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$. The unique homomorphism $\mathbb{Z} \to \mathbb{R}$ is

$$\begin{aligned} \alpha : \mathbb{Z} &\to \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \\ x &\mapsto ([x]_{10}, [x]_{11}), \end{aligned}$$

where $[x]_n$ denotes the image of x in $\mathbb{Z}/n\mathbb{Z}$, i.e., the $\equiv_n$-class of x. The kernel of α is

$$\begin{aligned} \ker(\alpha) &= \{x \in \mathbb{Z} : \alpha(x) = 0\} \\ &= \{x \in \mathbb{Z} : [x]_{10} = 0 \text{ and } [x]_{11} = 0\} \\ &= \{x \in \mathbb{Z} : x \equiv_{10} 0 \text{ and } x \equiv_{11} 0\} \\ &= \{x \in \mathbb{Z} : x \in 10\mathbb{Z} \text{ and } x \in 11\mathbb{Z}\}. \end{aligned}$$

A number if a multiple of both 10 and 11 iff it is a multiple of 110, so $\ker(\alpha) = 110\mathbb{Z}$ and $\mathrm{char}(R) = 110$. By Theorem 2.7.5, the minimal subring of R is isomorphic to $\mathbb{Z}/110\mathbb{Z}$. But $\mathbb{Z}/110\mathbb{Z}$ has the same size as $R = (\mathbb{Z}/10) \times (\mathbb{Z}/11)$, and so

$$\mathbb{Z}/110\mathbb{Z} \cong \langle \varnothing \rangle_R = R = \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}.$$

More generally, $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ whenever n and m are coprime. For example,

$$\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Combined with the above, this shows

$$\mathbb{Z}/110\mathbb{Z} \cong \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}.$$

More generally, if $n_1, \ldots, n_k$ are coprime positive integers and $N = n_1 \cdots n_k$, then

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}, \qquad (*)$$

a fact known as the *Chinese remainder theorem.*

What this means concretely is that for $x \in \mathbb{Z}$, the value of x modulo N has the same information as the values of x modulo n_1, n_2, …, n_k. For example, $[x]_{110}$ has the same information as $([x]_2, [x]_5, [x]_{11})$.

Theorem 2.7.7. *If K is a field, then* $\operatorname{char}(K) \in \{0, 2, 3, 5, 7, 11, \ldots\}$.

Proof. If $n = \operatorname{char}(K)$, and $\alpha : \mathbb{Z} \to R$ is the unique homomorphism, then $\ker(\alpha) = n\mathbb{Z}$. We must rule out the following cases:

- $n = 1$. Then $1 \in 1\mathbb{Z} = \ker(\alpha)$, so $1^K = \alpha(1) = 0^K$, and K is not a field.
- n is a composite number ab, for some integers $a, b > 1$. Then $a, b \notin n\mathbb{Z}$ and $n \in n\mathbb{Z}$, so $a, b \notin \ker(\alpha)$ but $ab = n \in \ker(\alpha)$. This means that

$$\begin{aligned} \alpha(a) &\neq 0 \\ \alpha(b) &\neq 0 \\ \alpha(a)\alpha(b) = \alpha(ab) &= 0, \end{aligned}$$

  contradicting the zero law (Theorem 1.4.16). □

Conversely, each of the values $0, 2, 3, 5, 7, \ldots$ occurs as the characteristic of some field:

Theorem 2.7.8. *If $p \in \{0, 2, 3, 5, 7, \ldots\}$, then there is a field of characteristic p.*

Proof. The field $\mathbb{R}$ has characteristic 0. If $p > 0$, the kernel of $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is $p\mathbb{Z}$, so the field $\mathbb{Z}/p\mathbb{Z}$ has characteristic p. □

Lastly, let's spell out what the minimal subring of a field is in terms of the characteristic.

Lemma 2.7.9. *Let R be a ring. Then $R/0R \cong R$.*

Proof. By the fundamental theorem on homomorphisms (Corollary 2.6.8) applied to the surjective homomorphism $\mathrm{id}_R : R \to R$, we have $R \cong R/I$, where $I = \ker(\mathrm{id}_R) = \{x \in R : \mathrm{id}(x) = 0\} = \{0\} = 0R$. □

(We saw an instance of Lemma 2.7.9 earlier—the ring S in Example 1.4.8 was exactly $\mathbb{R}/0\mathbb{R}$.)

Theorem 2.7.10. *If K is a field, then the minimal subring $\langle\varnothing\rangle_K$ is isomorphic to $\mathbb{Z}$ if* $\operatorname{char}(K) = 0$, *and $\mathbb{Z}/p\mathbb{Z}$ if* $\operatorname{char}(K) = p > 0$.

Theorem 2.7.11. *Let $L \supseteq K$ be an extension of fields. Then* $\operatorname{char}(L) = \operatorname{char}(K)$.

Proof. Let $\alpha : \mathbb{Z} \to K$ be the unique homomorphism from $\mathbb{Z}$ to K. Then α is also the unique homomorphism from $\mathbb{Z}$ to L. The kernel of α is the same whether we regard α as a homomorphism to K or to L. □

2.8 Term algebras and free algebras

Let Σ be an equational theory. We have seen a number of ways to construct new models of Σ, such as taking subalgebras, products, and quotients of existing models. Another important source of models is *free algebras*, which are in some sense the "most general" or "generic" models of Σ. Free algebras are built out of the more primitive notion of *term algebras*.

Let $\bar{x}$ be a tuple of variables, possibly infinite. Let $T(\bar{x})$ be the set of terms in the variables $\bar{x}$. We make $T(\bar{x})$ into an algebra by setting

$$f^{T(\bar{x})}(t_1, \ldots, t_k) = f(t_1, \ldots, t_k).$$

The resulting algebra is called the *term algebra*.

Example 2.8.1. In the language of rings, the term algebra $T(x, y, z)$ has elements like

$$x + (y + z),\ 0,\ 0 \cdot y,\ (-y) + y.$$

If we "add" the first two of these elements, we get the element $(x+(y+z))+0$. Note that the term algebra is not itself a ring. For example, $x + (y + z)$ and $(x + y) + z$ are distinct elements of $T(x, y, z)$, because they are not equal as terms (i.e., as strings of symbols). Thus $T(x, y, z)$ fails to satisfy the associative law.

Theorem 2.8.2. *If A is an algebra and $\bar{a}$ is a tuple in A of the same length as $\bar{x}$, then the evaluation map*

$$\begin{aligned} \eta &: T(\bar{x}) \to A \\ \eta(t(\bar{x})) &= t^A(\bar{a}) \end{aligned}$$

is a homomorphism $T(\bar{x}) \to A$.

Proof. Suppose f is a k-ary function symbol, and $t_1(\bar{x}), \ldots, t_k(\bar{x}) \in T(\bar{x})$. Then

$$\eta(f^{T(\bar{x})}(t_1(\bar{x}), \ldots, t_k(\bar{x}))) = \eta(f(t_1(\bar{x}), \ldots, t_k(\bar{x})))$$
$$= f^A(t_1^A(\bar{a}), \ldots, t_k^A(\bar{a})) = f^A(\eta(t_1(\bar{x})), \ldots, \eta(t_k(\bar{x}))). \qquad \square$$

Fix an equational class $\mathcal{K}$. Let $\mathrm{Eq}(\mathcal{K})$ denote the set of equations φ such that every $A \in \mathcal{K}$ satisfies φ.

Definition 2.8.3. If t, s are two terms, then $t \equiv_{\mathcal{K}} s$ if the equation $t = s$ holds for all $A \in \mathcal{K}$. In other words, $t \equiv_{\mathcal{K}} s$ means that $(t = s) \in \mathrm{Eq}(\mathcal{K})$.

Example 2.8.4. For example, if $\mathcal{K}$ is the class of rings, then $0 \cdot x \equiv_{\mathcal{K}} 0$ because the equation $0x = 0$ holds in any ring (Corollary 1.4.14).

Theorem 2.8.5. *If $\bar{x}$ is a tuple of variables, then $\equiv_{\mathcal{K}}$ is a congruence on the term algebra $T(\bar{x})$.*

Proof. It is easy to see that $\equiv_{\mathcal{K}}$ is an equivalence relation. We show that $\equiv_{\mathcal{K}}$ is a congruence. Suppose $t_1, \ldots, t_k$ and $s_1, \ldots, s_k$ are terms in $T(\bar{x})$ with $t_i \equiv_{\mathcal{K}} s_i$ for each i, and f is a k-ary function symbol. Then for any $A \in \mathcal{K}$ and tuple $\bar{a}$ in A,

$$t_i^A(\bar{a}) = s_i^A(\bar{a}) \text{ for } i = 1, \ldots, k,$$

and so

$$f(t_1(\bar{a}), \ldots, t_k(\bar{a}))^A = f(s_1(\bar{a}), \ldots, s_k(\bar{a}))^A.$$

It follows that

$$f(t_1(\bar{x}), \ldots, t_k(\bar{x})) \equiv_{\mathcal{K}} f(s_1(\bar{x}), \ldots, s_k(\bar{x})). \qquad \square$$

Definition 2.8.6. The *($\mathcal{K}$-)free algebra* on the variables $\bar{x}$, written $F_{\mathcal{K}}(\bar{x})$ or $F(\bar{x})$, is the quotient $T(\bar{x})/{\equiv_{\mathcal{K}}}$.

Theorem 2.8.7. $F_{\mathcal{K}}(\bar{x}) \in \mathcal{K}$.

Proof. Let $t(y_1, \ldots, y_k) = s(y_1, \ldots, y_k)$ be any of the axioms defining $\mathcal{K}$. For any terms $u_1, \ldots, u_k \in T(\bar{x})$, any $A \in \mathcal{K}$, and any $\bar{a}$ in A, we have

$$t(u_1(\bar{a}), \ldots, u_k(\bar{a})) = s(u_1(\bar{a}), \ldots, u_k(\bar{a}))$$

because $A \models t = s$. Therefore

$$\begin{gathered} t(u_1(\bar{x}), \ldots, u_k(\bar{x})) \equiv_{\mathcal{K}} s(u_1(\bar{x}), \ldots, u_k(\bar{x})) \\ [t(u_1(\bar{x}), \ldots, u_k(\bar{x}))] = [s(u_1(\bar{x}), \ldots, u_k(\bar{x}))] \text{ in } F(\bar{x}) \\ t([u_1(\bar{x})], \ldots, [u_k(\bar{x})]) = s([u_1(\bar{x})], \ldots, [u_k(\bar{x})]) \text{ in } F(\bar{x}) \end{gathered}$$

Thus $F(\bar{x}) \models t = s$. $\square$

Example 2.8.8. Suppose $\mathcal{K}$ is the class of monoids. The free monoid $F(x, y, z)$ has elements like $(xy)z$, $x(yz)$, and xy. The first two are equal, because $(xy)z \equiv_{\mathcal{K}} x(yz)$. The third element is not equal to the first two, because the equation $(xy)z = xy$ fails in at least one monoid, such as $(\mathbb{R}, \cdot, 1)$.

Because $F(x, y, z)$ is a monoid, we can forget the parentheses, and write each element (other than 1) as a string of x, y, and z, like

$$xyz,\ xyzzy,\ yyyxyyy,\ z, \ldots$$

If $\{x, y, z\}^*$ denotes the set of finite strings in the alphabet $\{x, y, z\}$, then one can make $\{x, y, z\}^*$ into a monoid by letting $w \cdot v$ be the concatenation of w and v, and 1 be the empty string. One can show that $\{x, y, z\}^* \cong F(x, y, z)$.

Example 2.8.9. Suppose $\mathcal{K}$ is the class of rings. The free ring $F(x)$ has elements like $x + 0$, $x^2 + x$, and so on. One can show that each element of $F(x)$ can be written in a unique way as a polynomial

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

with integer coefficients $a_0, \ldots, a_n$. Consequently, $F(x)$ is isomorphic to the ring $\mathbb{Z}[x]$ of polynomials with integer coefficients. We will say more about rings of polynomials in Section 9.1.

More generally, the free ring $F(x_1, \ldots, x_n)$ is isomorphic to the ring $\mathbb{Z}[x_1, \ldots, x_n]$ of polynomials in the variables $x_1, \ldots, x_n$ with coefficients in $\mathbb{Z}$. Going in the other direction, the free ring $F()$ turns out to be isomorphic to $\mathbb{Z}$.

Fact 2.8.10. *If $\mathcal{K}$ is the class of boolean algebras (Example 1.3.16), then the free boolea algebra $F(x_1, \ldots, x_n)$ is isomorphic to the set of all n-ary boolean functions*

$$\{\textsc{False}, \textsc{True}\}^n \to \{\textsc{False}, \textsc{True}\}$$

with the operations $\wedge, \vee, \ldots$ defined pointwise, like

$$(f \wedge g)(\bar{x}) = f(\bar{x}) \wedge g(\bar{x}).$$

In other words, $F(x_1, \ldots, x_n)$ is isomorphic to the power $\{\textsc{False}, \textsc{True}\}^I$ where $I = \{\textsc{False}, \textsc{True}\}^n$. (See examples 2.2.13 and 2.2.14 for powers.)

The next theorem is an analogue of Theorem 2.8.2 for free algebras instead of term algebras.

Theorem 2.8.11 (Universal mapping property)**.** *For any $A \in \mathcal{K}$ and tuple $\bar{a}$ in A (of the same length as $\bar{x}$), there is a homomorphism $\alpha : F(\bar{x}) \to A$ sending $[t(\bar{x})]$ to $t(\bar{a})$.*

Proof. Let $\beta : T(\bar{x}) \to A$ be the evaluation map $t(\bar{x}) \mapsto t(\bar{a})$. Note that

$$t \equiv_{\mathcal{K}} s \implies t(\bar{a}) = s(\bar{a}) \iff \beta(t) = \beta(s).$$

Therefore $(\equiv_{\mathcal{K}}) \subseteq \ker(\beta)$. By the universal property of quotients (Theorem 2.6.6), there is a homomorphism $\alpha : F(\bar{x}) \to A$ making the diagram commute

$$\begin{tikzcd}
T(\bar{x}) \arrow[d] \arrow[dr, "\beta"] & \\
F(\bar{x}) \arrow[r, dashed, "\alpha"'] & A.
\end{tikzcd}$$

Thus $\alpha([t(\bar{x})]) = \beta(t(\bar{x})) = t(\bar{a})$.

□

Example 2.8.12. For example, if we are working with rings, then $F(x)$ is the polynomial ring $\mathbb{Z}[x]$, and Theorem 2.8.11 says that for any ring A and element $a \in A$, the evaluation map

$$\begin{aligned} \mathbb{Z}[x] &\to A \\ P(x) &\mapsto P(a) \end{aligned}$$

is a homomorphism.

Similarly, there is a homomorphism from $F()$ to A sending t to t^A. In fact, $F()$ is $\mathbb{Z}$ and this is merely the homomorphism $\mathbb{Z} \to A$ of Theorem 2.7.3.

Corollary 2.8.13. *If $A \in \mathcal{K}$, then there is a surjective homomorphism $\alpha : F(\bar{x}) \to A$ for some $\bar{x}$.*

Proof. Let $\bar{a} = (a_i : i \in I)$ be a tuple (probably infinite) enumerating all of A. Let $\bar{x} = (x_i : i \in I)$ be a tuple of variables of the same length. Let $\alpha : F(\bar{x}) \to A$ be the homomorphism sending $[t(\bar{x})]$ to $t^A(\bar{a})$. Letting $t(\bar{x}) = x_i$, we see that $\alpha([x_i]) = a_i$, so α is surjective. □

In light of Corollary 2.6.8, this means that any algebra in $\mathcal{K}$ is a quotient of a free algebra, up to isomorphism. For example, any ring is a quotient of a free ring. This will play an important role in the next section.

2.9 Birkhoff's HSP theorem

If $\mathcal{K}$ is an equational class, and $A \in \mathcal{K}$, then any subalgebra or quotient of A is in $\mathcal{K}$, and anything isomorphic to A is in $\mathcal{K}$. Moreover, any product of algebras in $\mathcal{K}$ is in $\mathcal{K}$. (See Theorems 2.1.3, 2.4.15, 1.4.11, and 2.2.12.) In Examples 2.1.6 and 2.2.6 we used these facts to see that the class of fields is *not* an equational class. Birkhoff's HSP theorem—the goal of this section—says that this is the *only* obstruction to being an equational class: if a class of algebras $\mathcal{K}$ respects subalgebras, quotients, products, and isomorphisms, then $\mathcal{K}$ is an equational class, axiomatized by some set of equations.

Lemma 2.9.1. *Let $\alpha_i : A \to B_i$ be a homomorphism of $\mathcal{L}$-algebras for $i \in I$. Let $\alpha : A \to \prod_{i \in I} B_i$ be the map $\alpha(a) = (\alpha_i(a) : i \in I)$. Then α is a homomorphism.*

Proof. Let π_j be the jth coordinate projection from $\prod_{i \in I} B_i$ to B_j. If f is a k-ary function symbol and $a_1, \ldots, a_k \in A$, we must show

$$\alpha(f(\bar{a})) \overset{?}{=} f(\alpha(\bar{a})).$$

Both sides are in $\prod_{i \in I} B_i$. If the two sides disagree, then there is $i \in I$ such that

$$\pi_i(\alpha(f(\bar{a}))) \neq \pi_i(f(\alpha(\bar{a}))).$$

As π_i is a homomorphism (Remark 2.2.11), we can change the right hand side:

$$\pi_i(\alpha(f(\bar{a}))) \neq f(\pi_i(\alpha(\bar{a}))).$$

Now $\pi_i \circ \alpha = \alpha_i$ by definition of α, so

$$\alpha_i(f(\bar{a})) \neq f(\alpha_i(\bar{a})).$$

This contradicts the fact that α_i is a homomorphism. □

Let $\mathcal{K}$ be a class of $\mathcal{L}$-algebras.

1. $\mathcal{K}$ is *closed under isomorphisms* if for any $A \in \mathcal{K}$ and $B \cong A$, $B \in \mathcal{K}$.

2. $\mathcal{K}$ is *closed under subalgebras* if for any $A \in \mathcal{K}$ and subalgebra $B \subseteq A$, $B \in \mathcal{K}$.

3. $\mathcal{K}$ is *closed under products* if for any family $\{A_i\}_{i \in I}$ with $A_i \in \mathcal{K}$, the product $\prod_{i \in I} A_i$ is in $\mathcal{K}$.

4. $\mathcal{K}$ is *closed under quotients* if for any $A \in \mathcal{K}$ and congruence E on A, $A/E \in \mathcal{K}$.

Theorem 2.9.2 (Birkhoff's HSP theorem)**.** *Let $\mathcal{K}$ be a class of algebras. Then $\mathcal{K}$ is an equational class if and only if $\mathcal{K}$ is closed under isomorphisms, subalgebras, products, and quotients.*

Proof. Equational classes are closed under isomorphisms (Theorem 1.4.11), subalgebras (Theorem 2.1.3), products (Theorem 2.2.12), and quotients (Theorem 2.4.15).

Conversely, suppose $\mathcal{K}$ is closed under isomorphisms, subalgebras, products, and quotients. Let Σ be $\mathrm{Eq}(\mathcal{K})$, the set of equations holding on $\mathcal{K}$. If $A \in \mathcal{K}$, then $A \models \Sigma$, and so $\mathcal{K} \subseteq \mathrm{Mod}(\Sigma) =: \overline{\mathcal{K}}$.

Claim. If $\bar{x}$ is a tuple of variables, then the $\overline{\mathcal{K}}$-free algebra $F_{\overline{\mathcal{K}}}(\bar{x})$ is in $\mathcal{K}$.

Proof. Let $\{(a_i, b_i)\}_{i \in I}$ enumerate all the pairs of distinct elements of $F = F_{\overline{\mathcal{K}}}(\bar{x})$. For each i, we can write $a_i = [t_i(\bar{x})]$ and $b_i = [s_i(\bar{x})]$ for terms $t_i, s_i \in T(\bar{x})$. The fact that $a_i \neq b_i$ means that $t_i(\bar{x}) \not\equiv_{\overline{\mathcal{K}}} s_i(\bar{x})$. Thus $(t_i = s_i) \notin \Sigma = \mathrm{Eq}(\mathcal{K})$, so there is $A_i \in \mathcal{K}$ with $A_i \not\models t_i = s_i$. Then there is $\bar{a}_i \in A_i$ with $t_i^A(\bar{a}_i) \neq s_i^A(\bar{a}_i)$. As $A_i \in \mathcal{K} \subseteq \overline{\mathcal{K}}$, there is a homomorphism $\beta_i : F(\bar{x}) \to A_i$ sending $[t(\bar{x})]$ to $t^{A_i}(\bar{a}_i)$ (see Theorem 2.8.11). Then

$$\beta_i(a_i) = \beta_i([t_i(\bar{x})]) = t_i^{A_i}(\bar{a}_i) \neq s_i^{A_i}(\bar{a}_i) = \beta_i([s_i(\bar{x})]) = \beta_i(b_i).$$

Thus, for every $i \in I$,

$$\beta_i(a_i) \neq \beta_i(b_i). \tag{$*$}$$

By Lemma 2.9.1, there is a homomorphism $\beta : F(\bar{x}) \to \prod_{i \in I} A_i$ with $\beta(x) = (\beta_i(x) : i \in I)$. Note that $\prod_{i \in I} A_i \in \mathcal{K}$ because $\mathcal{K}$ is closed under products. We claim that β is injective. Indeed, if $a, b \in F(\bar{x})$ and $a \neq b$, then $(a, b) = (a_i, b_i)$ for some $i \in I$. Then $\beta_i(a) = \beta_i(a_i) \neq \beta_i(b_i) = \beta_i(b)$, so $\beta(a)$ and $\beta(b)$ differ at the ith coordinate.

Then β is an isomorphism from $F(\bar{x})$ to $\mathrm{im}(\beta)$. As $\mathrm{im}(\beta)$ is a subalgebra of $\prod_{i \in I} A_i \in \mathcal{K}$, we have $\mathrm{im}(\beta) \in \mathcal{K}$ and then $F(\bar{x}) \in \mathcal{K}$. $\square_{\text{Claim}}$

Now if $A \in \overline{\mathcal{K}}$ then there is a surjective homomorphism $F(\bar{x}) \to A$ for some $\overline{\mathcal{K}}$-free algebra $F(\bar{x})$ (Corollary 2.8.13). By the fundamental theorem on homomorphisms (Corollary 2.6.8), A is isomorphic to a quotient of $F(\bar{x})$. By the claim, $F(\bar{x}) \in \mathcal{K}$, and thus $A \in \mathcal{K}$.

This shows that $\overline{\mathcal{K}} \subseteq \mathcal{K}$. As $\mathcal{K} \subseteq \overline{\mathcal{K}}$, the class $\mathcal{K}$ equals the equational class $\overline{\mathcal{K}}$. $\square$

Using the HSP theorem, one can prove the following:

Theorem 2.9.3. *If $\mathcal{K}$ is any class of $\mathcal{L}$-algebras, then there is a smallest equational class $\overline{\mathcal{K}}$ containing $\mathcal{K}$.*

In fact, $\overline{\mathcal{K}}$ is just the intersection of all equational classes containing $\mathcal{K}$. The class $\overline{\mathcal{K}}$ is called the equational class *generated by* $\mathcal{K}$. Then, it turns out that one can characterize groups, rings, and boolean algebras as follows.

Fact 2.9.4. *The equational class of rings is generated by the ring $\mathbb{R}$.*

Fact 2.9.5. *The equational class of boolean algebras is generated by the two-element boolean algebra $\{\textsc{False}, \textsc{True}\}$.*

Recall the group $\mathrm{Perm}(S)$ of permutations on a set S from Example 1.1.8.

Fact 2.9.6. *The equational class of groups is generated by the class of groups of the form $\mathrm{Perm}(S)$.*

These facts help motivate the definitions of groups, rings, and boolean algebras, which may seem arbitrary at first glance.

Facts 2.9.4–2.9.6 can also be used to show that the axioms of groups, rings, and boolean algebras are "complete" with respect to equations. For example, suppose Σ is the set of ring axioms, and φ is some equation in the language of rings. Then one of two things happens:

1. The equational class $\mathrm{Mod}(\Sigma \cup \{\varphi\})$ equals $\mathrm{Mod}(\Sigma)$, and so any ring satisfies φ. Then φ is a redundant axiom, a logical consequence of Σ.

2. The equational class $\mathrm{Mod}(\Sigma \cup \{\varphi\})$ is strictly smaller than the class of rings $\mathrm{Mod}(\Sigma)$, so it does *not* contain $\mathbb{R}$ by Fact 2.9.4. Then the equation φ is not satisfied by $\mathbb{R}$.

Therefore, every equation satisfied by $\mathbb{R}$ is a logical consequence of the ring axioms. Similarly, every equation satisfied by $\{\textsc{False}, \textsc{True}\}$ is a logical consequence of the boolean algebra axioms.

Remark 2.9.7. The letters "HSP" stand for Homomorphic image, Subalgebra, and Product. A class $\mathcal{K}$ is *closed under homomorphic images* if whenever $\alpha : A \to B$ is a homomorphism of $\mathcal{L}$-algebras (not necessarily in $\mathcal{K}$) and $A \in \mathcal{K}$, then $\mathrm{im}(\alpha) \in \mathcal{K}$. Using the fundamental homomorphism theorem (Theorem 2.6.7), one can see that $\mathcal{K}$ is closed under homomorphic images if and only if $\mathcal{K}$ is closed under quotients and closed under isomorphisms. Thus Theorem 2.9.2 says that $\mathcal{K}$ is an equational class if and only if $\mathcal{K}$ is closed under **h**omomorphic images, **s**ubalgebras, and **p**roducts.

Remark 2.9.8. Let $\mathcal{K}$ be any class of $\mathcal{L}$-algebras. Define the operations H, S, P as follows:

1. $H(\mathcal{K})$ is the class of homomorphic images of algebras in $\mathcal{K}$.
2. $S(\mathcal{K})$ is the class of subalgebras of algebras in $\mathcal{K}$.
3. $P(\mathcal{K})$ is the class of products of algebras in $\mathcal{K}$.

Theorem 2.9.2 is actually a corollary of the full HSP theorem, which says the following

Fact 2.9.9. *If $\mathcal{K}$ is any class of algebras, then the smallest equational class containing $\mathcal{K}$ is $H(S(P(\mathcal{K})))$.*

The proof is similar to the proof of Theorem 2.9.2, but slightly more complicated.

2.10 ♢ The sizes of finite fields I

Lemma 2.10.1. *If $f : G \to H$ is a homomorphism of finite groups, then $|\operatorname{im}(f)|$ divides $|G|$.*

Proof. If $N = \ker(G)$, then $\operatorname{im}(f) \cong G/\ker(G)$ by the fundamental homomorphism theorem (Theorem 2.6.7). Then $|\operatorname{im}(f)| = |G/\ker(G)| = |G|/|\ker(G)|$ by Theorem 2.4.19. So $|G|$ is $|\operatorname{im}(f)|$ times $|\ker(G)|$, and $|\operatorname{im}(f)|$ is a factor of $|G|$. □

Lemma 2.10.2. *Let K be a field, let F be a subfield, and let $a_1, \ldots, a_n$ be elements of K. Then there is a group homomorphism $f : (F, +)^n \to (K, +)$ whose image contains $\{a_1, \ldots, a_n\}$.*

Proof. Define $f(x_1, \ldots, x_n) = \sum_{i=1}^n x_i a_i$. It is easy to see that $f(\bar{x} + \bar{y}) = f(\bar{x}) + f(\bar{y})$, so f is a group homomorphism (by Theorem 1.4.13). Then $f(1, 0, 0, \ldots, 0) = a_1$, $f(0, 1, 0, \ldots, 0) = a_2$, and so on, so $\{a_1, \ldots, a_n\} \subseteq \operatorname{im}(f)$. □

Theorem 2.10.3. *Let K be a finite field. Let p be the characteristic of K. Then $|K| = p^n$ for some n.*

Proof. Let F be the minimal subfield of K. By Theorem 2.7.10, $F \cong \mathbb{Z}/p\mathbb{Z}$, so F has size p. Let $a_1, \ldots, a_m$ be a list of the elements of K. By Lemma 2.10.2, there is a group homomorphism $(F, +)^n \to (K, +)$ whose image contains $\{a_1, \ldots, a_n\} = K$. Then the image is all of K, and so $|K|$ divides $|F^n| = |F|^n = p^n$ by Lemma 2.10.1. The only divisors of p^n are $1, p, p^2, \ldots, p^n$, so $|K|$ must be a power of p. □

Later we will see that for every prime power p^n, there is a unique field of size p^n, up to isomorphism.

2.11 ♢ Why we can have nice things

Finite fields like $\mathbb{Z}/p\mathbb{Z}$ play an important role in electronic communication, specifically in cryptography and error-correcting codes.

Public key cryptography

Suppose Alice wants to buy something online from Bob the merchant. Typically, Alice needs to send a payment code or credit card number to Bob. Unfortunately, Eve is able to eavesdrop on any messages between Alice and Bob. How can Alice prevent Eve from intercepting her payment code and stealing her money?

The typical solution is to use cryptography. Alice and Bob use a secret code to encode their messages. Eve cannot decode the messages, and cannot get Alice's payment information.

It would be impractical to devise a new secret code for every online payment, so it is customary to use codes based on keys. The algorithm for encoding and decoding information is public knowledge, but it depends on an extra piece of information called a *key*. The key might be something like a random 256-bit string. If Alice and Bob both have the key and Eve does not, then Alice and Bob can exchange messages and Eve will not be able to read them. (There are too many possible keys for Eve to try all of them.)

This creates a new problem: how can Alice and Bob arrange to share a secret key? There are millions of online merchants and billions of online customers; it would be impractical to set up a new secret key between every possible pair of customer and merchant. This is called the *key distribution problem.*

Public key cryptography offers a solution to this problem. In public key cryptography, the algorithms for coding and decoding messages use two different keys. The key to encode messages is called the *public key*, and the key to decode messages is called the *secret key.* Moreover, there is no easy way to calculate the secret key from the public key.

Here is how this could be applied in the scenario above. Bob creates a pair (p, s) where p is the public key and s is the corresponding secret key. He publicly advertises the public key p, but keeps the secret key s secret. Anyone who wants to send a message to Bob can encode it using the public key p, and send it to Bob. Bob receives the message and decodes it using s. The point is that anyone can encode messages, but only Bob can decode them.

This helps solve the key distribution problem. If we have n people who want to communicate, then we only need n public keys and n secret keys, which is much better than $\binom{n}{2} = \frac{n(n-1)}{2}$ keys with a traditional approach.

But how could we design a code where the key to encode and the key to decode are unrelated? The magic ingredient is finite fields.

Lemma 2.11.1. *Let $(G, \cdot)$ be a finite abelian group, written multiplicatively. If $n = |G|$, then every $x \in G$ satisfies $x^n = 1$.*

Proof. Let $b_1, \dots, b_n$ be a list of the elements of G. Fix $a \in G$. The map $x \mapsto ax$ is a permutation of G, because the map $x \mapsto a^{-1}x$ is an inverse. Therefore $ab_1, ab_2, \dots, ab_n$ is a list of the elements of G. In other words, the two lists

$$(b_1, b_2, b_3, \dots, b_n)$$
$$(ab_1, ab_2, ab_3, \dots, ab_n)$$

are permutations of each other. Therefore

$$b_1 b_2 b_3 \cdots b_n = (ab_1)(ab_2) \cdots (ab_n) = a^n b_1 b_2 \cdots b_n.$$

Canceling $b_1 b_2 \cdots b_n$ from both sides, we see that $1 = a^n$. □

Lemma 2.11.1 also holds for non-abelian groups, by a different proof which can be found in any book on group theory.

Theorem 2.11.2 (Fermat's Little Theorem)**.** *If p is a prime number and a is an integer such that $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Let K be the field $\mathbb{Z}/p\mathbb{Z}$. The set $K^\times$ of non-zero elements of K forms a group with respect to the multiplication operation. (This holds in any field.) This group has size $p-1$, so $x^{p-1} = 1$ for any $x \in K^\times$. Taking $x = [a]$, we get that $[a]^{p-1} = [a^{p-1}] = 1$, meaning $a^{p-1} \equiv 1 \pmod{p}$. □

Corollary 2.11.3. *Let p be a prime number, a be an integer, and n be a positive integer. If $n \equiv 1 \pmod{p-1}$, then $a^n \equiv a \pmod{p}$.*

Proof. If $a \equiv 0 \pmod{p}$, then $a^n \equiv 0 \equiv a \pmod{p}$. Suppose $a \not\equiv 0 \pmod{p}$. Write n as $1 + (p-1)k$. Then

$$a^n = a^{1+(p-1)k} = a \cdot (a^{p-1})^k \equiv a \cdot 1^k = a \pmod{p}.$$ □

Lemma 2.11.4. *Let p, q be two prime numbers and e, s be two positive integers. Suppose $es \equiv 1 \pmod{(p-1)(q-1)}$. Then for any integer x,*

$$x^{es} \equiv x \pmod{pq}.$$

Proof. As $es \equiv 1 \pmod{(p-1)(q-1)}$, we have $es \equiv 1 \pmod{(p-1)}$, and so $x^{es} \equiv x \pmod{p}$. Similarly, $x^{es} \equiv x \pmod{q}$. Then p and q both divide $x^{es} - x$, so $x^{es} - x$ is a multiple of pq. □

One of the most popular public key cryptography systems is called *RSA*, and works as follows. Bob chooses two very large prime numbers p and q, and a random integer e such that e has a multiplicative inverse s modulo $(p-1)(q-1)$. He publishes $N = pq$ and e, keeping s secret. If Alice wants to send a message to Bob, she converts the message into a number $x < N$, and calculates

$$y = (x^e \bmod N),$$

the remainder when x^e is divided by N. Then Bob takes y and calculates $x' = (y^s \bmod N)$. Then

$$\begin{aligned} x' &\equiv y^s \pmod{N} \\ y &\equiv x^e \pmod{N}, \end{aligned}$$

and so

$$x' \equiv y^s \equiv (x^e)^s = x^{es} \equiv x \pmod{N}.$$

Then $x' = x$, and Bob has recovered Alice's message x.

The reason this works is that there are fast algorithms to do the following:

- Find big prime numbers.

- Calculate multiplicative inverses of a modulo N, even when a and N are big.

- Calculate $a^b \bmod N$, even when a, b, N are very big.

On the other hand, there is *not* a known fast algorithm to calculate the prime factors p and q from N. This prevents Eve from taking N, calculating $(p-1)(q-1)$, and calculating s as the inverse of e modulo $(p-1)(q-1)$.

Remark 2.11.5. Another approach to public key cryptography is the *Diffie-Hellman system*, which attacks the key distribution problem more directly. The Diffie-Hellman protocol allows Alice and Bob to exchange public messages and agree on a shared secret key that the eavesdropper Eve cannot calculate. First, Alice and Bob agreen on some big integer N and some invertible element $g \in \mathbb{Z}/N\mathbb{Z}$. Alice and Bob choose secret integers a and b, respectively. They calculate g^a and g^b, and publicly post their results. Alice takes g^b and calculates $(g^b)^a = g^{ab}$. Bob takes g^a and calculates $(g^a)^b = g^{ab}$. Now both Alice and Bob have the value g^{ab}. But there is no known method for Eve to take the two values g^a and g^b and calculate g^{ab}. Thus Alice and Bob have agreed on a secret key g^{ab} and Eve doesn't know it.

Error-correcting codes

It is often necessary to send digital information across noisy channels. Here are some examples:

- If you send digital information by radio (like Wi-Fi, Bluetooth, or mobile phone data), there is random "noise" coming from other people's radio, the sun, cosmic rays, etc.

- If you put information on an optical disc (like a CD or DVD), then the disc might get scratched, destroying whatever information is under the scratch.

- If you put information in a bar code or QR code, then the camera might be out of focus, or part of the code might wear off.

In all these cases, we are trying to send a digital message, but something is randomly flipping bits in the message.

This is not much of an issue when sending sound or video using analog signals. The sound becomes slightly noisy; the video becomes fuzzy or gray. But for digital information, noise is a much bigger problem. Flipping a random bit in a computer program *might* completely break the program. Flipping a random bit in a cryptographically encoded message *will* destroy the message. Even sound and video cannot tolerate noise when encoded digitally.[3]

Error-correcting codes solve this problem. An error correcting code is a method for encoding and decoding messages, such that if we encode a message, make a few small changes, and then decode, we get the original message back.

Fix some finite set A and integer n. Think of A as an alphabet and A^n as a set of strings of length n. If $w, v \in A^n$, then the *Hamming distance* from w to v is the number of $i \in n$ such that $w(i) \neq v(i)$. For example, the Hamming distance from 01001 to 11000 is 2.

Fix an integer e. Suppose $\Sigma \subseteq A^n$ is some set such that for any distinct $w, v \in \Sigma$, the Hamming distance $d(w, v)$ is at least $2e + 1$. For $v \in A^n$, let $f(v)$ be an element of $w \in \Sigma$ minimizing the Hamming distance $d(w, v)$, breaking ties arbitrarily.

Lemma 2.11.6. *Suppose $w \in \Sigma$ and $d(v, w) \leq e$. Then $f(v) = w$.*

Proof. Let $w' = f(v) \in \Sigma$. Then $d(v, w') \leq d(v, w) \leq e$. By the triangle inequality,

$$d(w, w') \leq d(w, v) + d(v, w') \leq e + e < 2e + 1.$$

This contradicts the assumption on Σ, unless $w' = w$. □

Then Σ is essentially an error correcting code capable of correcting $\leq e$ errors. Elements of Σ are called *codewords.* The person sending the message chooses one of the codewords w. The random noise modifies w to produce a new string v with $d(v, w) \leq e$. The person decoding the message can recover w as $f(v)$; this works by the Lemma.

[3] Suppose the signal takes values in the range $[0, 10^6]$. With analog encoding, the effect of noise might be to add a small random number to the signal, e.g., changing 218459 to 218482. With digital encoding, the effect of noise might be to change a random digit, changing 218459 to 278459, which is a much bigger effect.

For example, if $A = \{0, 1\}$ and $n = 7$, then there is an inefficient error-correcting code given by

$$\Sigma = \{0000000, 1111111\}.$$

The distance between the two codewords is $7 = 2 \cdot 3 + 1$, so this code can correct up to 3 errors. (The decoding operation $f(v)$ is a majority vote.) However, there are only two codewords, so we can only send one bit of information via the scheme. In other words, this error-correcting code encodes 1 bit of information as 7 bits, which is quite inefficient.

Finite fields can be used to create more efficient error correcting codes.

Theorem 2.11.7. *Let K be a finite field. Let $a_1, \ldots, a_n$ be distinct elements of K. Let $\Sigma \subseteq K^n$ be the set of strings of the form*

$$(P(a_1), \ldots, P(a_n))$$

where $P(x)$ is a polynomial $c_d x^d + c_{d-1} x^{d-1} + \cdots + c_1 x + c_0$ of degree at most d. Then any distinct $v, w \in \Sigma$ have $d(v, w) \geq n - d$, so we can correct up to $\lfloor (n - d - 1)/2 \rfloor$ errors.

Proof. Suppose v and w come from polynomials P and Q. If $d(v, w) < n - d$, then v and w differ at fewer than $n - d$ values, so they agree at more than d values. Thus $\{x \in K : P(x) = Q(x)\}$ has at least $d + 1$ values. That is, the polynomial $P - Q$ has at least $d + 1$ roots. A polynomial of degree $\leq d$ cannot have more than d roots unless it is identically zero[4]. Then $P - Q$ is the zero polynomial, so $P = Q$, and $v = w$. □

The resulting error correcting codes are called *Reed-Solomon codes*, and are used in CDs, DVDs, QR codes, and space probes. Reed-Solomon codes are the reason why people can put small images in the middle of QR codes without breaking them.

Remark 2.11.8. Rather than using the finite fields $\mathbb{Z}/p\mathbb{Z}$ of size $2, 3, 5, 7, \ldots$, Reed-Solomon codes usually use the finite fields of size $2, 4, 8, 16, \ldots$, since this is better suited for binary information. We will see the construction of these fields later (TODO).

[4] We will prove this in Theorem 9.1.6 below.

Chapter 3

First-order logic

We now begin the study of model theory proper. Model theory can be seen as a generalization of universal algebra, where equations are replaced by *first-order sentences*. First-order sentences are more general than equations in two ways. First, we can use logical operations like $\wedge$ (and), $\vee$ (or), $\neg$ (not), $\exists$ (there exists), and $\forall$ (for all). This lets us express things like the last axiom of fields:

$$(\neg(0 = 1)) \wedge \forall x\ (x = 0 \vee \exists y : x \cdot y = 1)$$

Second, first-order logic allows not just function symbols, but also *relation symbols* like $\leq$. This allows for things like the axioms of partial orders:

$$\forall x\ (x \leq x)$$
$$\forall x\ \forall y\ (x \leq y \wedge y \leq x \to x = y)$$
$$\forall x\ \forall y\ \forall z\ (x \leq y \wedge y \leq z \to x \leq z).$$

We can also mix function symbols and relation symbols, as in the ordered field $(\mathbb{R}, +, \cdot, -, 0, 1, \leq)$.

The following analogies hold between universal algebra and model theory:

Universal algebra	Model theory
Equations	(First-order) sentences
Algebras	Structures
Equational theories	Theories
Equational classes	Elementary classes

For example, a theory is a set of sentences, and an elementary class is a class of structures defined by a theory.

While first-order logic is much more expressive than the equational logic of universal algebra, there are still limits to its expressive power. We will see many of these in future chapters, especially Chapter 5. In the present chapter we will already see that the linear orders $(\mathbb{R}, \leq)$ and $(\mathbb{Q}, \leq)$ satisfy exactly the same first-order sentences (Corollary 3.7.11). One says that $(\mathbb{R}, \leq)$ and $(\mathbb{Q}, \leq)$ are *elementarily equivalent*.

The greater expressive power of first-order logic comes at a cost. Tools like subalgebras, products, and quotients no longer work properly.[1] Additionally, the notion of homomorphism is not very useful. Consequently, the basic tools of model theory are fairly different from universal algebra, in spite of the formal analogies between the two subjects.

This chapter is a review of these basic tools. In Sections 3.1–3.3, we define the basic concepts of model theory, namely languages, structures, terms, formulas, satisfaction, theories, models, and elementary classes. In Sections 3.4–3.5 and Section 3.8, we define some of the fundamental tools of model theory—the notions of elementary equivalence, (elementary) embeddings, (elementary) substructures, definable sets and definable functions.

Section 3.6 is about *complete theories*. As discussed in the introduction, complete theories are an important part of model theory's motivations in mathematical logic. We give an example of a complete theory in Section 3.7, and an example of an incomplete theory in Section 3.9.

3.1 Languages, structures, formulas, and satisfaction

We first need to expand our earlier notion of "language" (Definition 1.3.1) to include relation symbols like $\leq$.

Definition 3.1.1. A *language* $\mathcal{L}$ consists of a set of *function symbols*, a set of *relation symbols*, and a function assigning to each function or relation symbol X an integer $n_X \in \mathbb{N}$ called the *arity* of X. A symbol X is said to be *k-ary* if $n_X = k$. Nullary function symbols are called *constant symbols*.

Example 3.1.2. The *language of posets* or *language of orders* contains one binary relation symbol $\leq$. The *language of monoids* contains one binary

[1] The closest thing to these operations is *ultraproducts*, which will be discussed in Chapter 6.

function symbol $\cdot$ and one constant symbol 1. The language of ordered rings contains two binary function symbols $+, \cdot$, one unary function symbol $-$, two constant symbols $0, 1$, and one binary relation symbol $\leq$.

Let M be a set. For $n \geq 0$, an *n-ary relation* on M is a subset $R \subseteq M^n$. If $a_1, \ldots, a_n \in M$, then "$R(a_1, \ldots, a_n)$" means "$(a_1, \ldots, a_n) \in R$". We think of R as an n-ary function $M^n \to \{\textsc{False}, \textsc{True}\}$.

Definition 3.1.3. Let $\mathcal{L}$ be a language. An *$\mathcal{L}$-structure* $\mathcal{M}$ consists of the following:

1. A set M, called the *underlying set* of $\mathcal{M}$.
2. A map assigning an n-ary operation $f^{\mathcal{M}} : M^n \to M$ to each n-ary function symbol f.
3. A map assigning an n-ary relation $R^{\mathcal{M}} \subseteq M^n$ to each n-ary relation symbol R.

This is really just like the definition of $\mathcal{L}$-algebras (Definition 1.3.3). The reason for the switch in terminology from "algebras" in universal algebra to "structures" in model theory is historical or cultural—algebraists prefer the term "algebra" and logicians prefer the term "structure."

Usually we don't distinguish between a structure $\mathcal{M}$ and its underlying set M, writing both as M.

Example 3.1.4. If $\mathcal{L}$ is the language of posets, then an $\mathcal{L}$-structure is essentially a pair $(M, \leq^M)$ where M is a set and $\leq^M$ is a binary relation on M.

Definition 3.1.5. Let $\mathcal{L}^+$ be a language and $\mathcal{L}^-$ be a sublanguage. For any $\mathcal{L}^+$-structure M, we can form an $\mathcal{L}^-$-structure from M by forgetting about the symbols in $\mathcal{L}^+ \setminus \mathcal{L}^-$. The resulting structure $M \upharpoonright \mathcal{L}^-$ is called a *reduct* of M. Conversely, M is an *expansion* of $M \upharpoonright \mathcal{L}^-$.

We won't use expansions and reducts until later chapters, but it is helpful to fix the terminology now.

Example 3.1.6. Suppose $\mathcal{L}^+$ is the language of rings $\{+, \cdot, -, 0, 1\}$ and $\mathcal{L}^-$ is the language of abelian groups $\{+, -, 0\}$. If M is the field $(\mathbb{R}, +, \cdot, -, 0, 1)$, then the reduct $\mathbb{R} \upharpoonright \mathcal{L}^-$ is the abelian group $(\mathbb{R}, +, -, 0)$. Therefore $(\mathbb{R}, +, \cdot, -, 0, 1)$ is an expansion of $(\mathbb{R}, +, -, 0)$.

Fix a language $\mathcal{L}$ and a class $\mathcal{V} = \{x, y, z, \ldots\}$ of *variable symbols* disjoint from the symbols in $\mathcal{L}$.

Definition 3.1.7. An $\mathcal{L}$-*term* is a string generated by the following rules:

- If x is a variable symbol, then x is a term.
- If f is an n-ary function symbol in $\mathcal{L}$, and $t_1, \ldots, t_n$ are $\mathcal{L}$-terms, then $f(t_1, \ldots, t_n)$ is an $\mathcal{L}$-term.

Definition 3.1.7 is identical to our earlier definition of terms (Definition 1.3.5. Note that $\mathcal{L}$-terms only use the function symbols and constant symbols of $\mathcal{L}$, and not the relation symbols. If $\mathcal{L}$ is a *relational language*—a language with only relation symbols, then the only terms are variable symbols. This happens in the language of posets, for example.

Next we turn to *formulas*, expressions like $x \le y + z$. Conceptually, the difference between terms and formulas is that terms are expressions that take values in the model, while formulas are truth-valued expressions.

Definition 3.1.8. An $\mathcal{L}$-*formula* is a string generated by the following rules:

1. If R is a k-ary relation symbol in $\mathcal{L}$ and $t_1, \ldots, t_k$ are $\mathcal{L}$-terms, then $R(t_1, \ldots, t_k)$ is an $\mathcal{L}$-formula.
2. If t and s are $\mathcal{L}$-terms, then $(t = s)$ is an $\mathcal{L}$-formula.
3. If φ and ψ are $\mathcal{L}$-formulas, then so are $\varphi \wedge \psi$, $\varphi \vee \psi$, and $\neg\varphi$. These should be understood as "φ and ψ", "φ or ψ", and "not φ", respectively.
4. $\top$ and $\bot$ are $\mathcal{L}$-formulas. These should be understood as the constant values True and False, respectively.
5. If φ is an $\mathcal{L}$-formula and x is a variable symbol, then the following are $\mathcal{L}$-formulas:

$$\exists x \ (\varphi) \in \mathcal{F}$$
$$\forall x \ (\varphi) \in \mathcal{F}.$$

   These should be understood as "there is an x such that φ" and "for all x, φ", respectively.

The set of *atomic $\mathcal{L}$-formulas* is the subset generated by (1)–(2), while the set of *quantifier-free $\mathcal{L}$-formulas* is generated by (1)–(4).

Example 3.1.9. Here are some formulas in the language of ordered rings $\{+, \cdot, -, 0, 1, \leq\}$:

$$\begin{gathered}
x \leq y \\
x \leq y \ \wedge \ \neg(x = y) \\
x + y = y + x \\
\forall x \ \forall y \ (x + y = y + x) \qquad (*) \\
\exists y \ (y \cdot y = x) \\
\forall x \ (x \leq 0 \ \vee \ \exists y \ (y \cdot y = x)). \qquad (\dagger)
\end{gathered}$$

The first and the third are atomic, and the first three are quantifier-free.

If x is a variable symbol and α is a term or formula, an occurrence of x in α is *bound* if it occurs inside a quantifier $\exists x \ (\ldots)$ or $\forall x \ (\ldots)$, and *free* otherwise. The *free variables* of α are the variables with free occurrences in α. For example, in the formula

$$\exists y \ (y \cdot y = x),$$

y is bound and x is free. A *closed term* is a term with no free variables (i.e., no variables). A *sentence* is a formula with no free variables. For example, of the formulas listed above, $(*)$ and $(\dagger)$ are sentences, while the others are not.

Remark 3.1.10. In previous chapters, we played fast and loose with implicit universal quantifiers, writing $M \models x + y = y + x$ when we really meant

$$M \models \forall x \ \forall y \ (x + y = y + x).$$

From now on, we will be more careful about this, avoiding notation like $M \models x + y = y + x$.

We write “let $\varphi(x_1, \ldots, x_n)$ be a formula” to mean that $\varphi(x_1, \ldots, x_n)$ is a formula whose free variables are contained in $\{x_1, \ldots, x_n\}$. We use the same convention for terms. If $\varphi(x_1, \ldots, x_n)$ is a formula and $t_1, \ldots, t_n$ are terms, then $\varphi(t_1, \ldots, t_n)$ denotes the result of replacing the free occurrences of x_i with t_i in φ.

Example 3.1.11. If $\varphi(x)$ is the formula $\exists y\ (y^2 = x)$, then $\varphi(x+z)$ is the formula $\exists y\ (y^2 = x+z)$.

Let M be an $\mathcal{L}$-structure and A be a subset of M. The language $\mathcal{L}(A)$ is obtained by adding each element of A as a new constant symbol. We regard M as an $\mathcal{L}(A)$-structure by interpreting each new constant symbol as the corresponding element of A, so that $c^M = c$ for $a \in A$. For now, we are mostly interested in the case $A = M$.

If t is a closed $\mathcal{L}(M)$-term, define the interpretation t^M recursively as follows:

$$f(t_1, \ldots, t_k)^M = f^M(t_1^M, \ldots, t_k^M).$$

If $t(x_1, \ldots, x_n)$ is an $\mathcal{L}$-term or $\mathcal{L}(M)$-term, then the interpretation t^M is the function $M^n \to M$ defined by

$$t^M(a_1, \ldots, a_n) = (t(a_1, \ldots, a_n))^M.$$

So far, this is exactly how we defined things in Section 1.3. Next we turn to formulas and sentences. If φ is an $\mathcal{L}(M)$-sentence, we define $M \models \varphi$ recursively:

$$\begin{gathered}
M \models t = s \iff t^M = s^M \\
M \models R(t_1, \ldots, t_k) \iff (t_1^M, \ldots, t_k^M) \in R^M \\
M \models \varphi \vee \psi \iff (M \models \varphi \text{ or } M \models \psi) \\
M \models \varphi \wedge \psi \iff (M \models \varphi \text{ and } M \models \psi) \\
M \models \neg\varphi \iff M \not\models \varphi \\
M \models \top \text{ is always true} \\
M \models \bot \text{ is always false} \\
M \models \exists x\ \varphi(x) \iff \exists a \in M : M \models \varphi(a) \\
M \models \forall x\ \varphi(x) \iff \forall a \in M : M \models \varphi(a).
\end{gathered}$$

If $M \models \varphi$, we say that M *satisfies* φ, or φ is *true* in M.

Example 3.1.12. Let $(M, +^M, 0^M, -^M)$ be a structure in the language of abelian groups. Then the following are equivalent:

$$\begin{gathered}
M \models \forall x\ \forall y : (x + y = y + x) \\
\forall a \in M\ \ (M \models \forall y : a + y = y + a) \\
\forall a, b \in M\ \ (M \models a + b = b + a) \\
\forall a, b \in M\ (a +^M b = b +^M a).
\end{gathered}$$

That is, M satisfies the sentence $\forall x\ \forall y : x+y=y+x$ if and only if $(M, +^M)$ is commutative.

Similarly, $M \models \forall x\ \exists y : x+y=0$ if and only if

$$\forall a \in M\ \exists b \in M : a +^M b = 0^M.$$

In general, the meaning of "$M \models \varphi$" is obtained by replacing each quantifier with a quantifier over M, and each symbol in the language with its interpretation in M.

3.2 Theories and elementary classes

Fix a language $\mathcal{L}$. An *$\mathcal{L}$-theory* is a set T of $\mathcal{L}$-sentences. Elements of T are called *axioms*. An $\mathcal{L}$-structure M *satisfies* T, or is a *model* of T, written $M \models T$, if

$$M \models \varphi \text{ for every } \varphi \in T.$$

The set of models of T is written $\mathrm{Mod}(T)$. An *elementary class* is a class of the form $\mathrm{Mod}(T)$.

Example 3.2.1. Let $\mathcal{L}$ be the language of rings. The *theory of rings T_{rings}* has the following axioms:

$$\begin{gathered}\forall x\ \forall y\ (x+y=y+x)\\ \forall x\ \forall y\ \forall z\ (x+(y+z)=(x+y)+z)\\ \cdots\end{gathered}$$

Models of T_{rings} are exactly rings. Therefore the class of rings is an elementary class. The *theory of fields T_{fields}* is T_{rings} plus the following two axioms:

$$\begin{gathered}\neg(0=1)\\ \forall x\ (x=0 \vee \exists y\ (x \cdot y = 1)).\end{gathered}$$

Models of T_{fields} are fields. Therefore the class of fields is an elementary class. This shows that first-order sentences are more expressive than pure equations, since we saw earlier that fields are not an *equational* class (Examples 2.1.6 and 2.2.6).

3.3 Common abbreviations

The following abbreviations are standard:

Abbreviation	Meaning
$\varphi \to \psi$	$\neg\varphi \vee \psi$
$\varphi \leftarrow \psi$	$\psi \to \varphi$
$\varphi \leftrightarrow \psi$	$(\varphi \to \psi) \wedge (\psi \to \varphi)$
$t \neq s$	$\neg t = s$
$\bigwedge_{i=1}^{n} \varphi_i$	$\varphi_1 \wedge \cdots \wedge \varphi_n$ [or $\top$ if $n = 0$]
$\bigvee_{i=1}^{n} \varphi_i$	$\varphi_i \vee \cdots \vee \varphi_n$ [or $\bot$ if $n = 0$]
$\exists^{\geq n}\varphi(x)$	$\exists y_1, \ldots, y_n \left(\bigwedge_{i=1}^{n} \varphi(y_i) \wedge \bigwedge_{1 \leq i < j \leq n}(y_i \neq y_j)\right)$
$\exists^{=n}\varphi(x)$	$\exists^{\geq n} x\ \varphi(x) \wedge \neg\exists^{\geq n+1} x\ \varphi(x)$
$\exists! x\ \varphi(x)$	$\exists^{=1} x\ \varphi(x)$.

Additionally, if $\mathcal{L}$ contains a symbol $\leq$, then

$$t \geq s \text{ means } s \leq t$$
$$t < s \text{ means } t \leq s \wedge t \neq s$$
$$t > s \text{ means } s < t.$$

Example 3.3.1. Let $\mathcal{L} = \{\leq\}$ be the language of posets. The *theory of posets*, whose models are posets, has the following axioms:

$$\forall x(x \leq x)$$
$$\forall x, y, z(x \leq y \wedge y \leq z \to x \leq z)$$
$$\forall x, y(x \leq y \wedge y \leq x \to x = y).$$

The *theory of linear orders* adds one more axiom:

$$\forall x, y(x \leq y \vee y \leq x).$$

3.4 Elementary equivalence and embeddings

The *complete theory* of an $\mathcal{L}$-structure M is the set

$$\mathrm{Th}(M) := \{\varphi : \varphi \text{ is an } \mathcal{L}\text{-sentence and } M \models \varphi\}.$$

Two $\mathcal{L}$-structures M and N are *elementarily equivalent*, written $M \equiv N$, if $\text{Th}(M) = \text{Th}(N)$, meaning that $M \models \varphi \iff N \models \varphi$ for every $\mathcal{L}$-sentence φ. The relation $M \equiv N$ is very strong, because sentences are very expressive. For example, none of the rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are elementarily equivalent with each other, because they are distinguished by the sentences

$$(\exists x)\ x + x = 1$$
$$(\exists x)\ x^2 = 1 + 1$$
$$(\exists x)\ x^2 = -1.$$

In contrast, one can show that these four rings satisfy exactly the same equations.

In light of this, it's not obvious how to find any examples where $M \equiv N$. One trivial case where M and N are elementarily equivalent is when M and N are isomorphic—see Corollary 3.4.7 below. Later in this chapter, we will see a more complicated example, namely $(\mathbb{Q}, \leq) \equiv (\mathbb{R}, \leq)$ (Example 3.7.12(1)). In fact, we will see in Chapter 5 that for any infinite structure M, the elementary equivalence class of M is very big. More precisely, we will see that M is elementarily equivalent to a structure of size κ for almost any cardinal κ (see Corollary 5.4.7).

Definition 3.4.1. Let M, N be $\mathcal{L}$-structures. A function $\alpha : M \to N$ is an *embedding* if α is injective, and α strictly preserves the function and relation symbols:

$$\alpha(f^M(b_1, \ldots, b_n)) = f^N(\alpha(b_1), \ldots, \alpha(b_n))$$
$$R^M(b_1, \ldots, b_n) \iff R^N(\alpha(b_1), \ldots, \alpha(b_n)).$$

An *isomorphism* is a bijective embedding. Two structures M and N are *isomorphic*, written $M \cong N$, if there is an isomorphism from M to N.

Embeddings are a little like homomorphisms in universal algebra (Definition 1.4.1). If $\mathcal{L}$ is a functional language, then an embedding is the same thing as an injective homomorphism.

The analogue of Theorem 1.4.6 holds for embeddings. More precisely:

1. The composition of two embeddings is an embedding.

2. The identity map is an isomorphism.

3. The inverse of an isomorphism is an isomorphism.

Consequently, $\cong$ is an equivalence relation.

Theorem 3.4.2. *Let $f : M \to N$ be an embedding and $a_1, \ldots, a_n$ be in M.*

1. *If $t(x_1, \ldots, x_n)$ is a term, then*
$$f(t^M(a_1, \ldots, a_n)) = t^N(f(a_1), \ldots, f(a_n)).$$

2. *If $\varphi(x_1, \ldots, x_n)$ is a quantifier-free formula, then*
$$M \models \varphi(a_1, \ldots, a_n) \iff N \models \varphi(f(a_1), \ldots, f(a_n)).$$

3. *If f is an isomorphism and $\varphi(x_1, \ldots, x_n)$ is any formula, then*
$$M \models \varphi(a_1, \ldots, a_n) \iff N \models \varphi(f(a_1), \ldots, f(a_n)).$$

Proof. By induction on the complexity of t or φ, like in Theorem 1.4.9. (In fact, part (1) is an instance of Theorem 1.4.9.) □

Example 3.4.3. Consider $\mathbb{Z}$ and $\mathbb{R}$ as ordered rings, and let $\alpha : \mathbb{Z} \to \mathbb{R}$ be the inclusion embedding $\alpha(x) = x$. If $\varphi(x)$ is the formula $x \geq 0$, then α preserves φ:
$$\mathbb{Z} \models \varphi(n) \iff \mathbb{R} \models \varphi(n) \text{ for } n \in \mathbb{Z}.$$
In contrast, if $\psi(x)$ is the formula $\exists y\ (y^2 = x)$, then α does not preserve ψ:
$$\mathbb{Z} \not\models \psi(2) \text{ but } \mathbb{R} \models \psi(2).$$

In fact, embeddings are characterized by the fact that they preserve quantifier-free formulas:

Remark 3.4.4. If $\alpha : M \to N$ is a function, then the following are equivalent:

1. α is an embedding.

2. α preserves quantifier-free formulas.

3. α preserves atomic formulas.

4. α preserves formulas of the form

$$\begin{gathered} x_1 = x_2 \\ R(x_1, \dots, x_k) \\ f(x_1, \dots, x_k) = x_{k+1} \end{gathered}$$

Indeed, (1) $\implies$ (2) is Theorem 3.4.2, (2) $\implies$ (3) $\implies$ (4) is trivial, and (4) $\iff$ (1) is essentially the definition of "embedding."

Definition 3.4.5. A function $\alpha : M \to N$ is an *elementary embedding* if α preserves all $\mathcal{L}$-formulas $\varphi(x_1, \dots, x_n)$, in the sense that

$$M \models \varphi(b_1, \dots, b_n) \iff N \models \varphi(\alpha(b_1), \dots, \alpha(b_n)). \qquad (*)$$

Remark 3.4.6.

1. Any elementary embedding is an embedding, by Remark 3.4.4

2. Theorem 3.4.2(3) says that isomorphisms are elementary embeddings.

3. If $\alpha : M \to N$ is an elementary embedding, then $M \equiv N$. To see this, take $n = 0$ in $(*)$, so that φ is a sentence. Then $(*)$ says that $M \models \varphi \iff N \models \varphi$.

As promised, isomorphic structures are elementarily equivalent:

Corollary 3.4.7. *If $M \cong N$, then $M \equiv N$.*

This generalizes Theorem 1.4.11 from equations to sentences.

Remark 3.4.8. Later, we will see a weak converse to Remark 3.4.6(3): if $M_1 \equiv M_2$, then M_1 and M_2 are connected by a chain of two elementary embeddings

$$\begin{tikzcd} M_1 \arrow[dr] & & M_2 \arrow[dl] \\ & N & \end{tikzcd}$$

for some structure N, a fact called *elementary amalgamation* (Theorem 5.2.5).

The next theorem shows that the elementary equivalence class of a structure M is itself an elementary class.

Theorem 3.4.9. *A structure N is a model of* $\mathrm{Th}(M)$ *if and only if* $N \equiv M$.

Proof. Note that $N \models \mathrm{Th}(M)$ iff $\mathrm{Th}(N) \supseteq \mathrm{Th}(M)$. (More generally, $N \models T$ iff $\mathrm{Th}(N) \supseteq T$.) So we must rule out the case that $\mathrm{Th}(N) \supsetneq \mathrm{Th}(M)$. Suppose $\varphi \in \mathrm{Th}(N) \setminus \mathrm{Th}(M)$. Then $N \models \varphi$ and $M \not\models \varphi$, implying that $N \not\models \neg\varphi$ and $M \models \neg\varphi$. Then $(\neg\varphi) \in \mathrm{Th}(M) \setminus \mathrm{Th}(N)$, contradicting the fact that $\mathrm{Th}(N) \supseteq \mathrm{Th}(M)$. □

3.5 Substructures and extensions

Let M be an $\mathcal{L}$-structure.

Definition 3.5.1. A *substructure* of M is a subset $A \subseteq M$ such that for any k-ary function symbol f in $\mathcal{L}$,

$$a_1, \ldots, a_k \in A \implies f^M(a_1, \ldots, a_k) \in A.$$

If A is a substructure of M, we regard A as an $\mathcal{L}$-structure by defining f^A and R^A to be the restrictions of f^M and R^M to A. In this way, substructures are structures, not just sets.

If M is an $\mathcal{L}$-structure, an *extension* of M is an $\mathcal{L}$-structure N such that M is a substructure of N.

Definition 3.5.2. If A is a subset of M, then $\langle A \rangle_M$ denotes the smallest substructure of M containing A, which is

$$\{t^M(\bar{b}) : t(x_1, \ldots, x_n) \text{ is an } \mathcal{L}\text{-term and } \bar{b} \in A^n\}$$

The substructure $\langle A \rangle_M$ is called the substructure *generated* by A. We say that M is *finitely generated* if $M = \langle A \rangle$ for some finite $A \subseteq M$.

Remark 3.5.3. If the language $\mathcal{L}$ has no function symbols or constant symbols, then every subset of M is a substructure, and so $\langle A \rangle_M = A$.

Remark 3.5.4. If A is a substructure of M, then the inclusion $A \hookrightarrow M$ is an embedding. Therefore

$$A \models \varphi(\bar{a}) \iff M \models \varphi(\bar{a})$$

for *quantifier-free* formulas φ and tuples $\bar{a}$ in A.

Definition 3.5.5. Let M and N be $\mathcal{L}$-structures. We say that M is an *elementary substructure* of N, written $M \preceq N$, or that N is an *elementary extension* of M, written $N \succeq M$, if M is a substructure of N and the inclusion $M \to N$ is an elementary embedding, meaning that

$$M \models \varphi(a_1, \ldots, a_n) \iff N \models \varphi(a_1, \ldots, a_n) \tag{$*$}$$

for $\mathcal{L}$-formulas φ and $\bar{a} \in M^n$.

Equation $(*)$ says that M and N satisfy the same $\mathcal{L}(M)$-sentences.

Example 3.5.6. The ring $(\mathbb{Q}, +, \cdot, -, 0, 1)$ is a substructure of the ring $(\mathbb{R}, +, \cdot, -, 0, 1)$, but not an elementary substructure, because

$$\mathbb{R} \models \exists y\ y^2 = 2$$
$$\mathbb{Q} \not\models \exists y\ y^2 = 2.$$

Example 3.5.7. The linear order $(2\mathbb{Z}, \leq)$ is a substructure of $(\mathbb{Z}, \leq)$, and $2\mathbb{Z} \equiv \mathbb{Z}$ because of the isomorphism $x \mapsto x/2$. However, $2\mathbb{Z} \not\preceq \mathbb{Z}$, because

$$\mathbb{Z} \models \exists x\ (0 < x \wedge x < 2)$$
$$2\mathbb{Z} \not\models \exists x\ (0 < x \wedge x < 2).$$

It's hard to give concrete examples of elementary substructures and elementary extensions at this point, but we will see later in this chapter that $(\mathbb{Q}, \leq) \preceq (\mathbb{R}, \leq)$ (Theorem 3.7.13).

Theorem 3.5.8. *Let f be an embedding from M to N.*

1. *The image* $\operatorname{im}(f)$ *is a substructure of N, and $M \to$* $\operatorname{im}(f)$ *is an isomorphism.*

2. *If f is an elementary embedding, then* $\operatorname{im}(f) \preceq N$.

Proof. 1. Straightforward. The fact that $\operatorname{im}(f)$ is a substructure is like the analogous fact for homomorphisms (Theorem 2.6.1).

2. If $M' = \operatorname{im}(f)$, then the inclusion $M' \hookrightarrow N$ is the composition of two elementary maps:
$$M' \xrightarrow{\cong} M \xrightarrow{f} N. \qquad \square$$

3.6 Complete theories

We write $T \vdash \varphi$ if φ is provable from T, and $T \models \varphi$ if every model of T satisfies φ.

Fact 3.6.1 (Soundness and completeness theorem)**.** *If T is a theory and φ is a sentence, then*

$$T \vdash \varphi \iff T \models \varphi.$$

Fact 3.6.1 is one of the fundamental theorems of mathematical logic. Its proof can be found in any textbook on mathematical logic, and we will sketch a proof in Section 4.5. What Fact 3.6.1 is really saying is that the definition of provability ($\vdash$) is correct—φ is formally provable from the axioms in T if and only if it *should* be provable, based on the models of T. For example, if T_{fields} is the theory of fields, then φ is provable from T_{fields} if and only if every field satisfies φ.

The "soundness" part of Fact 3.6.1 is the direction:

$$T \vdash \varphi \implies T \models \varphi.$$

This says that the individual rules of the proof calculus are true: if φ is provable from T and M satisfies T, then M satisfies φ. The "completeness" part of Fact 3.6.1 is the harder direction:

$$T \models \varphi \implies T \vdash \varphi. \tag{$*$}$$

This says that the proof calculus is not missing any rules. In fact, if we add any new rules, getting a new provability relation $\vdash'$, then one of two things must happen:

1. $\vdash'$ is the same as $\vdash$, and the new rules are redundant.
2. $\vdash'$ is strictly bigger than $\vdash$. By ($*$), $\vdash'$ is strictly bigger than $\models$, which means that $\vdash'$ is no longer sound. Therefore, the new rules are incorrect.

The difficulty in proving ($*$) is that it requires constructing models. Indeed, the contrapositive to ($*$) is the statement

$$T \nvdash \varphi \implies T \not\models \varphi.$$

This says that if φ is *not* provable from T, then there is a model $M \models T$ such that $M \not\models \varphi$. Equivalently, one must construct a model of $T \cup \{\neg\varphi\}$. We will discuss some of the techniques to do this in Chapter 4.

For now, we will apply Fact 3.6.1 to the study of consistent and complete theories. A theory T is *inconsistent* if the following equivalent conditions hold:

1. $T \vdash \bot$.
2. $T \vdash \varphi$ for all φ.
3. $T \vdash \varphi$ and $T \vdash \neg\varphi$ for some φ.

Otherwise, T is *consistent.* Note that $T \models \bot$ if and only if T has no models, because no structure M satisfies $\bot$. Therefore the completeness theorem implies the following:

Theorem 3.6.2. *T is consistent if and only if T has a model.*

A theory T is *complete* if T is consistent and for any sentence φ,

$$T \vdash \varphi \text{ or } T \vdash \neg\varphi.$$

Theorem 3.6.3. *If T is complete and $M \models T$, then for any sentence φ,*

$$M \models \varphi \iff T \vdash \varphi.$$

Proof. As $M \models T$ and T is complete,

$$T \vdash \varphi \implies M \models \varphi$$
$$T \nvdash \varphi \implies T \vdash \neg\varphi \implies M \models \neg\varphi \implies M \not\models \varphi. \qquad \square$$

Theorem 3.6.4. *Let T be a theory. Then T is complete if and only if any two models $M_1, M_2 \models T$ are elementarily equivalent.*

Proof. First suppose T is complete. If M_1, M_2 are two models, then $\mathrm{Th}(M_1) = \{\varphi : T \vdash \varphi\} = \mathrm{Th}(M_2)$ by Theorem 3.6.3, and so $M_1 \equiv M_2$.

Conversely suppose T is incomplete, with $T \nvdash \varphi$ and $T \nvdash \neg\varphi$. By the completeness theorem, there are models $M_1, M_2 \models T$ with $M_1 \models \neg\varphi$ and $M_2 \models \varphi$. Then $M_1 \not\equiv M_2$. □

Once we have developed techniques to show that two structures are elementarily equivalent, Theorem 3.6.4 will be a very useful method to prove completeness.

The significance of complete theories is that if $M \models T$ and T is complete, then T determines exactly which sentences M satisfies (Theorem 3.6.3). In fact, in many cases, one even gets an algorithm to tell whether M satisfies a given sentence. Suppose the language $\mathcal{L}$ is countable.

Fact 3.6.5. *If T is finite or more generally if T is computably enumerable, then the set $\overline{T} = \{\varphi : T \vdash \varphi\}$ is computably enumerable.*

For the definitions of computable and computably enumerable sets, see any book on mathematical logic or computability theory.[2] We will not use these notions in an essential way, except to state some corollaries.

Theorem 3.6.6. *If T is complete and computably enumerable and M is a model of T, then* $\mathrm{Th}(M)$ *is computable—there is an algorithm which takes an $\mathcal{L}$-sentence φ and determines whether $M \models \varphi$.*

Proof. By Theorem 3.6.3, $\mathrm{Th}(M) = \overline{T}$, which is computably enumerable by Fact 3.6.5. However,

$$\varphi \notin \mathrm{Th}(M) \iff \neg\varphi \in \mathrm{Th}(M),$$

and so $\mathrm{Th}(M)$ is also co-c.e. As $\mathrm{Th}(M)$ is both c.e. and co-c.e., it is computable.

More informally, we can determine whether M satisfies φ via the following algorithm. Begin enumerating the infinite list of logical consequences of T. At some point, φ or $\neg\varphi$ will show up in this list. At this point, we know whether $M \models \varphi$ or $M \models \neg\varphi$, so we can terminate the algorithm and output the answer. □

3.7 Completeness via back-and-forth systems

Let M, N be two $\mathcal{L}$-structures.

Definition 3.7.1. A *partial elementary map* from M to N is a bijection $f : A \to B$ where A and B are subsets of M and N, respectively, and f preserves all $\mathcal{L}$-formulas, in the sense that

$$M \models \varphi(a_1, \ldots, a_n) \iff N \models \varphi(f(a_1), \ldots, f(a_n))$$

for $n \geq 0$, $\varphi(x_1, \ldots, x_n)$ an $\mathcal{L}$-formula, and $a_1, \ldots, a_n \in A$.

[2] Note that "computable", "computably enumerable", and "computability theory" are also called "recursive", "recursively enumerable", and "recursion theory".

Remark 3.7.2. Taking $n = 0$, we see that if f is a partial elementary map from M to N, then $M \equiv N$.

Conversely, $\varnothing : \varnothing \to \varnothing$ is a partial elementary map from M to N *if and only if* $M \equiv N$.

Remark 3.7.3. An elementary embedding from M to N is the same thing as a partial elementary map f from M to N with $\mathrm{dom}(f) = M$.

Definition 3.7.4. A *partial isomorphism* from M to N is an isomorphism $f : A \to B$ where A is a substructure of M and B is a substructure of N.

By Theorem 3.4.2, partial isomorphisms preserve quantifier-free formulas: if $f : A \to B$ is a partial isomorphism and $\bar{a} \in A^n$ and $\varphi(\bar{x})$ is quantifier-free, then

$$M \models \varphi(\bar{a}) \iff A \models \varphi(\bar{a}) \iff B \models \varphi(f(\bar{a})) \iff N \models \varphi(f(\bar{a})).$$

Definition 3.7.5. A *back-and-forth system* between M and N is a family $\mathcal{F}$ of partial isomorphisms satisfying the following conditions:

1. Forward: if $f : A \to B$ is in $\mathcal{F}$, and $a' \in M$, then there is $f' : A' \to B'$ in $\mathcal{F}$ such that f' extends f and $a' \in A'$.
2. Backward: if $f : A \to B$ is in $\mathcal{F}$, and $b' \in N$, then there is $f' : A' \to B'$ in $\mathcal{F}$ such that f' extends f and $b' \in B'$.

Theorem 3.7.6. *If $\mathcal{F}$ is a back-and-forth system, then every $f \in \mathcal{F}$ is a partial elementary map from M to N.*

Proof. We show by induction on the complexity of $\varphi(x_1, \ldots, x_n)$ that if $f : A \to B$ is in $\mathcal{F}$ and $a_1, \ldots, a_n \in A$, then

$$M \models \varphi(a_1, \ldots, a_n) \iff N \models \varphi(f(a_1), \ldots, f(a_n)). \tag{†}$$

We may assume that φ is defined without the use of $\forall$, since $\forall$ can be defined in terms of $\exists$ and $\neg$:

$$\forall x\ \psi(\bar{x}) \iff \neg\exists x\ \neg\psi(\bar{x}).$$

The case of atomic formulas holds because f is a partial isomorphism. The case of boolean operations is straightforward. It remains to consider the case where $\varphi(\bar{x})$ is $\exists y : \psi(\bar{x}, y)$. By symmetry, we only need to prove the $(\Rightarrow)$

direction of (†). Suppose $M \models \exists y : \psi(\bar{a}, y)$. Take some $a' \in M$ such that $M \models \psi(\bar{a}, a')$. By the "forward" condition, there is $g \in \mathcal{F}$ extending f with $a' \in \mathrm{dom}(g)$. By induction, $M \models \psi(\bar{a}, a') \implies N \models \psi(g(\bar{a}), g(a'))$, and then $N \models \varphi(g(\bar{a}))$. But $g(\bar{a}) = f(\bar{a})$, so $N \models \varphi(f(\bar{a}))$ as desired. □

Corollary 3.7.7. *Let M, N be two structures. If there is a non-empty back-and-forth system between M and N, then $M \equiv N$.*

Definition 3.7.8. A linear order $(M, \leq)$ is *dense* if for any $x < y$ there is z with $x < z < y$.

Definition 3.7.9. DLO is the theory of non-empty dense linear orders without endpoints. That is, $(M, \leq) \models$ DLO if $(M, \leq)$ is a non-empty dense linear order without a greatest or least element.

Theorem 3.7.10. *Let M and N be models of* DLO *and let $\mathcal{F}$ be the class of finite partial isomorphisms $f : A \to B$ between M and N. Then $\mathcal{F}$ is a back-and-forth system.*

Proof. We prove the forward condition; the backward condition follows by symmetry. Fix a finite partial isomorphism $f : A \to B$ and an element $a' \in M$. We must extend f to a larger finite partial isomorphism f' containing a'. Enumerate the elements of A:

$$A = \{a_1, \ldots, a_n\}$$
$$a_1 < a_2 < \cdots < a_n$$

Let $b_i = f(a_i)$. Then

$$B = \{b_1, \ldots, b_n\}$$
$$b_1 < b_2 < \cdots < b_n.$$

There are five cases.

1. $n = 0$, so that A, B are empty. Take any $b' \in N$. (N is non-empty.) Then $f' : \{a'\} \to \{b'\}$ extends f and is defined at a'.

2. $a' = a_i \in A$. Then we can take $f' = f$.

3. $a' < a_1$. Take $b' \in N$ with $b' < b_1$. (N has no minimum.) Then there is a partial isomorphism
$$f' : \{a', a_1, \ldots, a_n\} \to \{b', b_1, \ldots, b_n\}$$
extending f and sending a' to b'.

4. $a' > a_n$. This case is similar to the previous case.

5. $a_i < a' < a_{i+1}$ for some i. Take $b' \in N$ with $b_i < b' < b_{i+1}$. (N is densely ordered.) Then there is a partial isomorphism

$$f' : \{a_1, \dots, a_i, a', a_{i+1}, \dots, a_n\} \to \{b_1, \dots, b_i, b', b_{i+1}, \dots, b_n\}$$

extending f and sending a' to b'. □

Corollary 3.7.11. *1. The theory* DLO *is complete—any two models M, N are elementarily equivalent.*

2. If $M \models$ DLO*, then* Th(M) *is decidable.*

Example 3.7.12. 1. $(\mathbb{Q}, \leq) \equiv (\mathbb{R}, \leq)$.

2. The complete theory of $(\mathbb{Q}, \leq)$ is decidable.

We can also use the back-and-forth system to finally give a concrete example of an elementary substructure:

Theorem 3.7.13. $(\mathbb{Q}, \leq)$ *is an elementary substructure of* $(\mathbb{R}, \leq)$*.*

Proof. Let $\varphi(\bar{x})$ be a formula and $\bar{a}$ be a tuple in $\mathbb{Q}$. Let $S = \{a_1, \dots, a_n\}$. Then $\mathrm{id}_S : S \to S$ is a finite partial isomorphism from $\mathbb{Q}$ to $\mathbb{R}$. By Theorems 3.7.10 and 3.7.6, id_S is a partial elementary map from $\mathbb{Q}$ to $\mathbb{R}$. Therefore

$$\mathbb{Q} \models \varphi(\bar{a}) \iff \mathbb{R} \models \varphi(\mathrm{id}_S(\bar{a})) \iff \mathbb{R} \models \varphi(\bar{a}).$$ □

On the other hand, the ordered ring $\mathbb{Q}$ is not an elementary substructure of the ordered ring $\mathbb{R}$ (Example 3.5.6).

3.8 Definable sets and functions

Fix a language $\mathcal{L}$ and an $\mathcal{L}$-structure M. If $\varphi(x_1, \dots, x_n)$ is an $\mathcal{L}$-formula, then $\varphi(M^n)$ or $\varphi(M)$ denotes the set *defined by* φ:

$$\varphi(M^n) := \{\bar{a} \in M^n : M \models \varphi(\bar{a})\}.$$

More generally, if $\varphi(x_1, \dots, x_n; y_1, \dots, y_m)$ is an $\mathcal{L}$-formula and $\bar{b} \in M^m$, then $\varphi(M^n, \bar{b})$ or $\varphi(M, \bar{b})$ denotes the set defined by $\varphi(\bar{x}, \bar{b})$:

$$\varphi(M^n, \bar{b}) := \{\bar{a} \in M^n : M \models \varphi(\bar{a}, \bar{b})\}.$$

Sets of this form are called *definable sets.*

Example 3.8.1. In the language of ordered rings, if $\varphi(x, y)$ is the formula $x^2 + y^2 \leq 1$, then $\varphi(\mathbb{R}^2)$ is $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\}$, the closed unit disk. If $\psi(x, y; z)$ is the formula $x^2 + y^2 \leq z^2$, then $\varphi(\mathbb{R}^2; r)$ is the closed disk of radius r.

A set $D \subseteq M^n$ is A-*definable* or *definable over* A if $D = \varphi(M^n, \bar{b})$ with $\bar{b} \in A^m$. That is, an A-definable set is a set defined by an $\mathcal{L}(A)$-formula. Definable sets are the same thing as M-definable sets. A *0-definable set* is a $\varnothing$-definable set (a set defined by an $\mathcal{L}$-formula). If D, E are definable sets, a function $f : D \to E$ is *definable* if the graph $\Gamma(f) = \{(x, y) \in D \times E : f(x) = y\}$ is a definable set. A-definable functions are defined similarly.

Example 3.8.2. In the ordered field $\mathbb{R}$, the function $f(x) = x^2$ is definable, defined by the formula $y = x^2$:

$$\{(x, x^2) : x \in \mathbb{R}\} = \{(x, y) \in \mathbb{R}^2 : y = x^2\}.$$

Similarly, the square root function $f(x) = \sqrt{x}$ is defined by the formula $y \geq 0 \ \wedge \ y^2 = x$. As a more complicated example, the function

$$f : \mathbb{R} \to \mathbb{R}$$
$$f(x) = \sqrt[3]{x} + x$$

is definable, defined by the formula

$$\exists z \ (z^3 = x \ \wedge \ y = z + x).$$

Remark 3.8.3. If $t(x_1, \ldots, x_n)$ is an $\mathcal{L}(M)$-term, then the function $t^M : M^n \to M$ is definable, defined by the formula $t(\bar{x}) = y$.

Theorem 3.8.4. *If $f : X \to Y$ and $g : Y \to Z$ are definable, then $g \circ f : X \to Z$ is definable.*

Proof. Let $\varphi(\bar{x}, \bar{y})$ be an $\mathcal{L}(M)$-formula defining f, meaning that

$$f(\bar{a}) = \bar{b} \iff M \models \varphi(\bar{a}, \bar{b}).$$

Similarly, let $\psi(\bar{y}, \bar{z})$ define g. Let $\theta(\bar{x}, \bar{z})$ be

$$\exists \bar{y} \ (\varphi(\bar{x}, \bar{y}) \ \wedge \ \psi(\bar{y}, \bar{z})).$$

Then θ defines $g \circ f$:

$$\begin{aligned} M \models \theta(\bar{a}, \bar{c}) &\iff \exists \bar{b} \ \big(M \models \varphi(\bar{a}, \bar{b}) \text{ and } M \models \psi(\bar{b}, \bar{c})\big) \\ &\iff \exists \bar{b} \ (f(\bar{a}) = \bar{b} \text{ and } g(\bar{b}) = \bar{c}) \\ &\iff g(f(\bar{a})) = \bar{c}. \end{aligned}$$

□

3.9 Incompleteness of Peano Arithmetic

Consider $\mathbb{N}$ as an $\mathcal{L}$-structure $(\mathbb{N}, +, \cdot, 0, 1)$, where $\mathcal{L}$ is the language $\{+, \cdot, 0, 1\}$. *Peano Arithmetic* (PA) consists of the following axioms:

$$\begin{gathered}
\forall x : x + 1 \neq 0 \\
\forall x : (x = 0 \vee (\exists y : x = y + 1)) \\
\forall x, y : (x + 1 = y + 1 \to x = y) \\
\forall x : x + 0 = x \\
\forall x, y : x + (y + 1) = (x + y) + 1 \\
\forall x : x \cdot 0 = 0 \\
\forall x, y : x \cdot (y + 1) = (x \cdot y) + x
\end{gathered}$$

as well as the infinite set of axioms $\{Ind_\varphi : \varphi(x, y_1, \ldots, y_n) \text{ an } \mathcal{L}\text{-formula}\}$, where Ind_φ is the induction axiom

$$\forall \bar{y} \left(\varphi(0, \bar{y}) \wedge (\forall x\ \varphi(x, \bar{y}) \to \varphi(x + 1, \bar{y})) \to \forall x\ \varphi(x, \bar{y})\right).$$

For example, $(\mathbb{N}, +, \cdot, 0, 1) \models \text{PA}$.

Remark 3.9.1. The induction schema says that if $D \subseteq M^1$ is a definable set such that $0 \in D$ and $x \in D \implies x + 1 \in D$, then D contains every $x \in M$.

We are going to show that Peano Arithmetic is incomplete. This incompleteness is traditionally deduced as a form of Gödel's incompleteness theorem, but we will give a different proof.[3] Specifically, we will show that $\text{Th}(\mathbb{N})$, the *true theory of arithmetic* is undecidable. That is, there is no algorithm to determine whether a given $\mathcal{L}$-sentence φ is satisfied by $\mathbb{N}$. To do this, we show that progressively more complicated sets and functions are definable in $\mathbb{N}$, until we can reduce the halting problem to $\text{Th}(\mathbb{N})$.

Work in the structure $\mathbb{N}$.

[3] Gödel's incompleteness theorem is less a single theorem and more a "theorem schema" for proving that many different theories are incomplete. Gödel's original theorem was about the type theory in Russell and Whitehead's book *Principia Mathematica*, but the same argument could be applied to Peano Arithmetic, ZFC set theory, or any other sufficiently expressive theory. In modern introductions to mathematical logic, Gödel's incompleteness theorem is often stated for Peano Arithmetic. In contrast, our proof of the incompleteness of PA does *not* generalize to ZFC.

Remark 3.9.2. The relation $x \leq y$ is definable, defined by

$$\exists z : z + x = y.$$

Remark 3.9.3. The function $|x - y|$ is definable.

Proof. $|x - y| = z$ if and only if $x = y + z \vee y = x + z$. □

Definition 3.9.4. If $n > 0$ and $a \in \mathbb{N}$, then $a \bmod n$ denotes the unique $x \in \{0, 1, \ldots, n-1\}$ such that $x \equiv a \pmod{n}$.

The binary operator $x \bmod y$ is common in programming languages, where it is usually written `x % y` or `x mod y`.

Lemma 3.9.5. *The function $x \bmod y$ is definable.*

Proof. $(x \bmod y) = z$ if and only if

$$z + 1 \leq y \wedge (\exists k : k \cdot y + z = x).$$ □

The core of the argument is the following mysterious function, which goes back to Gödel.

Definition 3.9.6. For $a, b, x \in \mathbb{N}$, $\beta(a, b, x) = (a \bmod ((x + 1)b + 1))$.

The significance of the β function is that it lets us define *arbitrary finite sequences* in a uniform fashion, as described by the next lemma:

Lemma 3.9.7. *For any finite sequence $c_0, c_1, \ldots, c_n \in \mathbb{N}$, there are $a, b \in \mathbb{N}$ such that $c_i = \beta(a, b, i)$ for $0 \leq i \leq n$.*

Proof. Take $m > \max(c_0, \ldots, c_n, n)$, and let $b = m! = 1 \cdot 2 \cdot 3 \cdot 4 \cdots m$.
Claim. The numbers $\{b + 1, 2b + 1, 3b + 1, \ldots, (n + 1)b + 1\}$ are pairwise coprime.

Proof. Suppose a prime number p divides both $ib + 1$ and $jb + 1$ for some $1 \leq i < j \leq n + 1$. Then p divides the difference $(j - i)b$, and one of two things happens:

- p divides b.
- p divides $j - i$. Then $p \leq j - i \leq n \leq m$, so p divides $m! = b$.

Either way, p divides b, and so

$$0 \equiv ib + 1 \equiv i0 + 1 = 1 \pmod{p},$$

a contradiction. $\square_{\text{Claim}}$

By the Chinese remainder theorem (see Example 2.7.6), there is an a such that

$$a \equiv c_i \pmod{(i+1)b+1}$$

for each $0 \leq i \leq n$. But $c_i \leq m \leq b < (i+1)b + 1$, and so

$$c_i = (a \bmod ((i+1)b+1)) = \beta(a, b, i). \qquad \square$$

The next theorem shows how one can use the function β.

Theorem 3.9.8. *Let $f(n)$ be the nth Fibonacci number* $(1, 1, 2, 3, 5, 8, 13, \ldots)$

$$\begin{aligned} f(0) &= f(1) = 1 \\ f(n+2) &= f(n) + f(n+1) \end{aligned}$$

Then the function $f : \mathbb{N} \to \mathbb{N}$ is definable.

Proof. For fixed n and k, the following are equivalent:

1. $f(n) = k$.

2. There are $c_0, \ldots, c_n$ such that the following hold:

$$\begin{aligned} c_0 &= 1 \\ c_1 &= 1 \\ c_i &= c_{i-1} + c_{i-2} \text{ for all } 2 \leq i \leq n. \end{aligned}$$

3. There are a and b such that the following hold:

$$\begin{aligned} \beta(a, b, 0) &= 1 \\ \beta(a, b, 1) &= 1 \\ \beta(a, b, i) &= \beta(a, b, i-1) + \beta(a, b, i-2) \text{ for all } 2 \leq i \leq n. \end{aligned}$$

Indeed, (2) and (3) are equivalent by Lemma 3.9.7. Condition (3) is easily expressed by a formula. $\square$

Theorem 3.9.9. *If $f : \mathbb{N}^k \to \mathbb{N}$ is computable, then f is definable.*

Proof sketch. The only hard thing to check is primitive recursion, which is handled by the method of Theorem 3.9.8. We leave the details as an exercise to the reader. □

Corollary 3.9.10. *If $S \subseteq \mathbb{N}^k$ is computable, then S is definable.*

Theorem 3.9.11. Th($\mathbb{N}$) *is incomputable.*

Proof. Fix a reasonable enumeration of Turing machines. Let $S \subseteq \mathbb{N}^2$ be the set of pairs (n, k) such that the nth Turing machine halts within k steps. By Corollary 3.9.10, S is definable, defined by an $\mathcal{L}(\mathbb{N})$-formula $\varphi(x, y, n_1, n_2, \ldots)$. Replacing n_i with $\underbrace{1 + 1 + \cdots + 1}_{n_i \text{ times}}$, we see that S is $\varnothing$-definable, defined by an $\mathcal{L}$-formula $\varphi(x, y)$. Then for any $n \in \mathbb{N}$,

$$\mathbb{N} \models \exists y \; \varphi(\underbrace{1 + 1 + \cdots +}_{n \text{ times}}, y) \iff (\text{the } n\text{th Turing machine halts}).$$

Therefore the halting problem reduces to Th($\mathbb{N}$). □

PA is computably axiomatized, so Theorems 3.6.6 and 3.9.11 yield the following:

Corollary 3.9.12. *Peano arithmetic is incomplete.*

Then Theorem 3.6.4 gives the following:

Corollary 3.9.13. *There is a model $M \models$ PA with $M \not\equiv \mathbb{N}$.*

3.9.1 ♢ Undecidability of $\mathbb{Z}$ and $\mathbb{Q}$

We have just seen that Th($\mathbb{N}$) is undecidable, and therefore $\mathbb{N}$ cannot have a complete axiomatization. The same thing holds in the ring $\mathbb{Z}$ and the field $\mathbb{Q}$.

Fact 3.9.14 (Lagrange four square theorem)**.** *If $x \in \mathbb{N}$, then $x = y_1^2 + y_2^2 + y_3^2 + y_4^2$ for some integers y_1, y_2, y_3, y_4.*

For example $7 = 1^2 + 2^2 + 1^2 + 1^2$.

Corollary 3.9.15. *In the ring $\mathbb{Z}$, the set $\mathbb{N}$ is definable.*

Proof. It is defined by the formula

$$\exists y_1, y_2, y_3, y_4 : x = y_1^2 + y_2^2 + y_3^2 + y_4^2. \qquad \square$$

Corollary 3.9.16. *If $f : \mathbb{N}^k \to \mathbb{N}$ is computable, then f is definable in the ring $\mathbb{Z}$.*

Proof. By Corollary 3.9.10, f is definable in the structure $\mathbb{N}$. Once $\mathbb{N}$ is definable, we can use the definition of f in the structure $\mathbb{N}$ to define f in $\mathbb{Z}$. More precisely, we need to "relativize" the definition to the subset $\mathbb{N}$, replacing

$$\exists x : (\ldots) \text{ with } \exists x : x \in \mathbb{N} \wedge (\ldots)$$
$$\forall x : (\ldots) \text{ with } \forall x : x \in \mathbb{N} \to (\ldots),$$

where "$x \in \mathbb{N}$" is an abbreviation for the formula defining $\mathbb{N}$. □

Then the proof of Theorem 3.9.11 applies to give the following:

Theorem 3.9.17. *The complete theory of the ring $\mathbb{Z}$ is undecidable.*

Using deeper number-theoretic facts, Julia Robinson proved

Fact 3.9.18 (Robinson)**.** *The set $\mathbb{Z}$ is definable in the field $\mathbb{Q}$.*

By the above arguments, we then conclude

Theorem 3.9.19. *The complete theory of the field $\mathbb{Q}$ is undecidable.*

In contrast, we will see later that the complete theory of $\mathbb{C}$ is decidable (Corollary 9.4.8). The complete theory of $\mathbb{R}$ is also decidable, though the proof is too complicated to discuss in this course.

3.10 ♢ Examples of first-order theories

We have seen several examples of first-order theories, such as the theories of rings, fields, posets, and linear orders (Examples 3.2.1,3.3.1), as well as the complete theory DLO and the incomplete theory PA (Sections 3.7 and 3.9). Equational theories provide another source of examples—see the examples in Sections 1.3 and 1.5. In this section, we list some additional important examples of first-order theories and elementary classes.

Examples from algebra: A number of classes from abstract algebra are elementary classes. We have already seen fields, and here are three more important examples.

- An *integral domain* is a commutative ring R satisfying the axiom

  $$\forall x, y : xy = 0 \to x = 0 \vee y = 0.$$

  For example, $\mathbb{Z}$ is an integral domain and so are fields (Theorem 1.4.16).

- An abelian group $(A, +)$ is *torsion-free* if

  $$\forall x : \underbrace{x + x + \cdots + x}_{n \text{ times}} = 0 \to x = 0$$

  for each $n > 0$. For example, $(\mathbb{Z}, +)$ and $(\mathbb{R}, +)$ are torsion-free, though the quotient $\mathbb{R}/\mathbb{Z}$ is not.

- A *local ring* is a ring R with a unique maximal ideal (see Theorem 2.5.6). It turns out that local rings are exactly the rings satisfying the axiom

  $$\forall x \; \exists y : xy = 1 \vee (1 - x)y = 1.$$

  This says that for any x, at least one of x and $1 - x$ has a multiplicative inverse. Local rings are important in algebraic geometry and number theory.

Integral domains form an elementary class, but not an equational class (see Example 2.2.6). The same holds for torsion-free groups and local rings. This shows the expressive power of first-order theories.[4]

Algebraically closed fields: A field $(K, +, \cdot)$ is *algebraically closed* if every polynomial equation has a solution: for any $n > 0$ and $a_0, a_1, a_2, \ldots, a_{n-1} \in K$, there is some $z \in K$ such that

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

[4] However, model theorists are not very interested in the theories of integral domains, torsion-free groups, and local rings, because these theories are far from being complete.

The field $\mathbb{C}$ of complex numbers is algebraically closed, a deep fact called the *fundamental theorem of algebra*. In contrast, $\mathbb{R}$ is not algebraically closed, as there is no z such that $z^2 + 0z + 1 = 0$.

The class of algebraically closed fields is elementary, defined by a theory called ACF whose axioms consist of the field axioms plus the following infinite list of axioms:

$$\begin{gathered} \forall x_0, x_1\ \exists y : y^2 + x_1 y + x_0 = 0 \\ \forall x_0, x_1, x_2,\ \exists y : y^3 + x_2 y^2 + x_1 y + x_0 = 0 \\ \cdots . \end{gathered}$$

We will say more about ACF in Chapter 9, where we will show that ACF is nearly complete (Corollary 9.4.5).

Ordered fields and real closed fields: An *ordered field* is a structure

$$(K, +, \cdot, -, 0, 1, \leq)$$

where $(K, +, \cdot, -, 0, 1)$ is a field, $\leq$ is a linear order on K, and the following conditions hold for $a, x, y \in K$:

$$\begin{gathered} x \leq y \implies a + x \leq a + y \\ (x \leq y \text{ and } a > 0) \implies ax \leq ay. \end{gathered}$$

For example, $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields with respect to the usual order. Ordered fields are defined by an obvious first-order theory in the language of ordered rings $\mathcal{L} = \{+, \cdot, -, 0, 1, \leq\}$.

An ordered field is *real closed* if it satisfies the intermediate value theorem for polynomials:

> If $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ and if $P(b) < 0 < P(c)$, then there is x between b and c such that $P(x) = 0$.

This holds in $\mathbb{R}$ by the usual intermediate value theorem in real analysis, so $\mathbb{R}$ is real closed. In contrast, it fails in $\mathbb{Q}$ since for $P(x) = x^2 - 2$, we have

$$P(0) = -2 < 0 < P(2) = 2,$$

but there is no rational x with $P(x) = 0$.

Real closed fields are the models of a first-order theory called RCF. It is an interesting exercise to write down the axioms of RCF. Using quantifier elimination (see Chapter 8), one can prove that RCF is complete. The proof is similar to the case of ACF in Chapter 9, but more complicated. Because of the completeness of RCF, we can also "define" real closed fields to be fields that are elementarily equivalent to $\mathbb{R}$.

True arithmetic: The *true theory of arithmetic* is $\mathrm{Th}(\mathbb{N})$, where $\mathbb{N}$ is the ring-like structure $(\mathbb{N}, +, \cdot, 0, 1, \leq)$. By Theorem 3.4.9, the models of $\mathrm{Th}(\mathbb{N})$ are exactly the structures M that are elementarily equivalent to $\mathbb{N}$. Any model of true arithmetic is a model of Peano Arithmetic, but the converse does not hold (Corollary 3.9.13). Unlike ACF, RCF, and PA, $\mathrm{Th}(\mathbb{N})$ does not have an explicit axiomatization. In fact, $\mathrm{Th}(\mathbb{N})$ cannot have a computable axiomatization by Theorem 3.9.11.

Graphs and random graphs: In combinatorics, a *graph* consists of a set V of *vertices*, a set E of *edges*, and a map assigning to each edge e an unordered pair $\{v_1, v_2\}$ of vertices called the *ends* of e. Graphs are useful for understanding networks. For example, we could define a graph where the vertices are cities and the edges are highways between the cities. Or we could define a graph where the vertices are users of a social media platform, and there is an edge from v to w if and only if v and w are friends.

Two vertices v, w are *adjacent* if they are the ends of some edge. A *loop* is a edge e whose two ends are equal. Two edges e_1, e_2 are *parallel* if they have the same ends. A *simple graph* is a graph without loops or parallel edges. Model theorists usually assume that graphs are simple. We represent a (simple) graph (V, E) as a structure (V, R) where V is the set of vertices, and $R \subseteq V \times V$ is the adjacency relation.

Then the *language of graphs* is the language $\{R\}$ with one binary relation, and the *theory of graphs* says that R is irreflexive and symmetric:

$$\forall x, y : x \; R \; y \to y \; R \; x$$
$$\forall x : \neg x \; R \; x.$$

If φ is a sentence in the language of graphs, let $P_n(\varphi)$ be the probability that φ is satisfied by a random graph on the vertex set $\{1, 2, 3, \ldots, n\}$.

Fact 3.10.1 (Zero-one law for graphs)**.** *There is a complete theory T_{rand} in the language of graphs such that for any sentence φ,*

$$\lim_{n\to\infty} P_n(\varphi) = \begin{cases} 1 & \text{if } T_{rand} \vdash \varphi \\ 0 & \text{if } T_{rand} \vdash \neg\varphi. \end{cases}$$

We give more details about this in Section 3.11. The theory T_{rand} is called the *theory of the random graph*, and has a number of important model-theoretic properties such as $\aleph_0$-categoricity (see Chapter 12) and "simplicity".

The theory of finite fields: If $\mathcal{K}$ is a class of $\mathcal{L}$-structures, then $\mathrm{Th}(\mathcal{K})$ is the set of $\mathcal{L}$-sentences φ such that every $M \in \mathcal{K}$ satisfies φ. When $\mathcal{K}$ is the class of finite fields, the theory $\mathrm{Th}(\mathcal{K})$ is called the *theory of finite fields*. It consists of all the sentences φ in the language of rings such that every finite field satisfies φ. For example, using the pigeonhole principle, one can show that the map $f(x) = (x + 1)x$ is never surjective on a finite field, so the theory of finite fields contains the sentence

$$\exists y\ \forall x : (x + 1)x \neq y.$$

The terminology "theory of finite fields" may be misleading because there are other models besides the finite fields. These models are called *pseudo-finite fields*. In other words, a field K is pseudo-finite if K is infinite, but K satisfies every first-order sentence satisfied by finite fields. For example, the map $f(x) = (x + 1)x$ must be non-surjective on a pseudo-finite field. The fact that pseudo-finite fields exist can be shown using the Compactness Theorem (Theorem 4.4.5) in the next chapter.

The pseudo-finite fields are themselves the models of a theory, the *theory of pseudo-finite fields* (sometimes written PSF) whose axioms are the theory of finite fields plus axioms $\exists^{\geq n} x : \top$ for each n. Using deep facts from algebraic geometry and number theory, James Ax gave an explicit algebraic characterization of pseudo-finite fields[5]. Using this,

[5] If you know enough Galois theory, the characterization is as follows. A field K is pseudo-finite if the following properties hold. First, K should be perfect, meaning that $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p$ and the map $x \mapsto x^p$ is surjective. Second, K should have exactly one finite extension of degree n for each $n \geq 1$. Finally, if L/K is any field extension

Ax obtained complete axiomatizations of the theory of pseudo-finite fields as well as the theory of finite fields. For example, he found a list of axioms T_0 such that $T_0 \vdash \varphi$ if and only if φ is true on all finite fields. From this, it is easy to see that the theory of finite fields is decidable: there is an algorithm which takes a sentence φ and determines whether φ holds on all finite fields.[6] Aside from this application, the theory of pseudo-finite fields has some interesting model theoretic properties, such as being "geometric" (Chapter 14) and "simple" (like the random graph).

Ordered abelian groups: An *ordered abelian group* is a structure

$$(A, +, 0, -, \leq)$$

where $(A, +, 0, -)$ is an abelian group, $\leq$ is a linear order on A, and the following compatibility holds for any x, y, z:

$$x + z \leq y + z \iff x \leq y.$$

Examples of ordered abelian groups include $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}$. In model theory, two special classes of ordered abelian groups are of particular interest:

- A *divisible ordered abelian group* is an ordered abelian group that is non-trivial (with at least two elements) and divisible, meaning

  $$\forall x \; \exists y : \underbrace{y + y + \cdots + y}_{n \text{ times}} = x$$

  for each $n > 0$. Examples are $\mathbb{Q}$ and $\mathbb{R}$, but not $\mathbb{Z}$. The theory of divisible ordered abelian groups is often called DOAG or ODAG. Using the quantifier elimination techniques of Chapter 8, one can show that DOAG is complete, so that $\mathbb{R} \equiv \mathbb{Q}$ as ordered abelian groups.

such that K is relatively algebraically closed in L, then K should be existentially closed in L in the sense of Definition 10.2.1. The third condition is usually expressed differently, using algebraic geometry, by saying that any geometrically irreducible variety over K has a K-rational point.

[6] Run two processes in parallel. One process looks for a proof of φ from the axioms T_0. The other process looks for a finite field K with $K \not\models \varphi$. We are destined to eventually find one or the other, so this algorithm always terminates.

- *Presburger arithmetic* is the theory of ordered abelian groups A such that there is a smallest positive element, and such that A/nA has exactly n elements for each $n > 0$. For example, $\mathbb{Z}$ is a model of Presburger arithmetic. In fact, Presburger arithmetic is complete, so the models of Presburger arithmetic are exactly the ordered abelian groups that are elementarily equivalent to $\mathbb{Z}$.

  Sometimes Presburger arithmetic is defined by an alternate convention, to be the complete theory of $(\mathbb{N}, +, 0, 1, \leq)$ rather than the complete theory of $(\mathbb{Z}, +, 0, -, \leq)$. There is a way to translate between these two conventions. With the second convention, Presburger arithmetic can be defined by the axioms of Peano Arithmetic minus the axioms that mention multiplication. The surprising thing is that Presburger Arithmetic is complete, unlike Peano Arithmetic.

Valued fields: Let K be a field. A *valuation ring* on K is a subring $\mathcal{O}$ such that for every non-zero $x \in K$, at least one of x and $1/x$ is in $\mathcal{O}$. A *valued field* is a field with a valuation ring. Valued fields arise naturally in model theory via the following construction and its variants:

Example 3.10.2. Let K be an elementary extension of the ordered field $\mathbb{R}$. Define $\mathcal{O}$ to be the set of $x \in K$ that are "bounded" in the sense that $-y < x < y$ for some $y \in \mathbb{R}$. Then one can show that $\mathcal{O}$ is a valuation ring on K.

Valued fields are an elementary class, defined by the theory of fields plus the following axioms, where "$x \in \mathcal{O}$" is a new unary relation symbol:

$$0 \in \mathcal{O} \wedge 1 \in \mathcal{O}$$
$$\forall x, y : x \in \mathcal{O} \wedge y \in \mathcal{O} \to x + y \in \mathcal{O} \wedge xy \in \mathcal{O} \wedge -x \in \mathcal{O}$$
$$\forall x \; \exists y : x \in \mathcal{O} \vee (xy = 1 \wedge y \in \mathcal{O}).$$

The theory of algebraically closed valued fields, written ACVF, is an important example in model theory. ACVF shares many formal similarities with the theory RCF of real closed fields. For example, both are "geometric" theories (see Chapter 14), and both satisfy an important technical property called "NIP" or "dependence".

Another important source of valued fields comes from number theory. If x is a non-zero rational number and p is prime, then x can be written in the form $p^n \frac{a}{b}$ for some integers a, b not divisible by p. For example, taking $p = 2$,

$$\begin{aligned} 10 &= 2^1 \cdot \frac{5}{1} \\ 7/3 &= 2^0 \cdot \frac{7}{3} \\ 3/20 &= 2^{-2} \cdot \frac{3}{5}. \end{aligned}$$

The *p-adic absolute value* of x, written $|x|_p$, is defined to be

$$|x|_p = \begin{cases} 0 & \text{if } x = 0 \\ p^{-n} & \text{if } x = p^n \frac{a}{b} \text{ where } a, b \notin p\mathbb{Z} \end{cases}$$

In spite of its exotic definition, the p-adic absolute value on $\mathbb{Q}$ satisfies many of the same conditions as the usual absolute value on $\mathbb{R}$:

$$\begin{gathered} |x|_p \geq 0 \\ |x|_p = 0 \iff x = 0 \\ |xy|_p = |x|_p \cdot |y|_p \\ |x + y|_p \leq |x|_p + |y|_p. \end{gathered}$$

In fact, the p-adic absolute value satisfies the stronger statement $|x + y|_p \leq \max(|x|_p, |y|_p)$. Using this property, one can show that $\mathcal{O} = \{x \in \mathbb{Q} : |x|_p \leq 1\}$ is a valuation ring on $\mathbb{Q}$. This example is important in number theory, but less so in model theory due to the undecidability of the field $\mathbb{Q}$ (Section 3.9.1).

One can also mimic the construction of the real numbers via Cauchy sequences, replacing $|x|$ with $|x|_p$. A *p-adic Cauchy sequence* is a sequence $(x_0, x_1, x_2, \ldots) \in \mathbb{Q}^{\mathbb{N}}$ such that for every $\epsilon > 0$, there is $N < \omega$ such that for every $i, j > N$, $|x_i - x_j|_p < \epsilon$. If $\bar{x}, \bar{y}$ are p-adic Cauchy sequences, let $\bar{x} \sim \bar{y}$ mean that $\lim_{i \to \infty} |x_i - y_i|_p = 0$. Using the properties of $|x|_p$, one can show that

- The set of p-adic Cauchy sequences is a subring of $\mathbb{Q}^{\mathbb{N}}$.
- $\sim$ is a congruence on this subring.
- The quotient ring, written $\mathbb{Q}_p$, is a field.

- There is a well-defined p-adic absolute value $|-|_p : \mathbb{Q}_p \to \mathbb{R}$ defined by $|[\bar{x}]|_p = \lim_{i\to\infty} |x_i|_p$.

Note that if we carried out this construction using $|x|$ instead of $|x|_p$, we would get the field $\mathbb{R}$ rather than the field $\mathbb{Q}_p$.

The field $\mathbb{Q}_p$ is called the field of *p-adic numbers.* It is naturally a valued field with respect to the valuation ring $\{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. Analogies between $\mathbb{R}$ and $\mathbb{Q}_p$ are a major theme in number theory, and there are similar analogies in model theory. Just as $\mathbb{R}$ is completely axiomatized by the theory of real closed fields RCF, the field $\mathbb{Q}_p$ is completely axiomatized by the theory of *p-adically closed fields* pCF. Moreover, pCF has the same formal properties as RCF and ACVF: it is a geometric, NIP theory.

The true theory of real exponentiation: Let $\mathcal{L}_{\text{exp}}$ be the language of ordered rings plus a unary function symbol $\exp(-)$. Then $\mathbb{R}_{\text{exp}} := (\mathbb{R}, +, \cdot, 0, 1, -, \leq, \exp)$ is an $\mathcal{L}_{\text{exp}}$-structure in a natural way. The *true theory of real exponentiation* is the complete theory of $\mathbb{R}_{\text{exp}}$. Like true arithmetic $\text{Th}(\mathbb{N})$, there is no known axiomatization of this theory. Unlike $\text{Th}(\mathbb{N})$, there *might* be—Macintyre and Wilkie showed that $\text{Th}(\mathbb{R}_{\text{exp}})$ is decidable assuming something called Schanuel's conjecture.

Moreover, regardless of whether $\text{Th}(\mathbb{R}_{\text{exp}})$ is decidable, it is known to have a number of nice properties, especially with regard to definable sets. By work of Wilkie, we know that every definable set in $\mathbb{R}_{\text{exp}}$ has finitely many connected components, and every definable function is piecewise continuous and piecewise differentiable. The same properties hold in any model $M \models \text{Th}(\mathbb{R}_{\text{exp}})$, i.e., $M \equiv \mathbb{R}_{\text{exp}}$. It turns out that all these properties can be deduced from a fundamental notion called o-minimality:

Definition 3.10.3. An *o-minimal structure* is a structure $(M, \leq, \ldots)$ where $\leq$ is a linear order on M, and every definable set in one variable $D \subseteq M$ is a finite union of points $\{a\}$ and open intervals $(b, c) := \{x \in M : b < x < c\}$.

An *o-minimal theory* is a theory whose models are o-minimal. It turns out (this is hard to prove) that every o-minimal structure M is a model of an o-minimal theory, namely $\text{Th}(M)$. A deep theorem of Wilkie shows that $\mathbb{R}_{\mathrm{exp}}$ is o-minimal as a structure, and so $\mathrm{Th}(\mathbb{R}_{\mathrm{exp}})$ is o-minimal as a theory. Other examples of o-minimal theories include dense linear orders (DLO), real closed fields (RCF), and divisible ordered abelian groups (DOAG).

Zermelo-Fraenkel set theory: The *language of set theory* is the language $\{\in\}$ with one binary relation $\in$. *Zermelo set theory*, sometimes called Z^-, consists of the following axioms:

1. Extensionality: if x and y have the same elements, then $x = y$. This can be expressed by the sentence

$$\forall x, y : ((\forall z : z \in x \leftrightarrow z \in y) \rightarrow x = y)\,.$$

Temporarily being lazy about the outer universal quantifiers, we can write this more compactly as

$$(\forall z : z \in x \leftrightarrow z \in y) \rightarrow x = y.$$

For notational simplicity, we continue to use implicit universal quantification in listing the other Zermelo axioms.

2. The empty set: there is a set (namely $\varnothing$) with no elements. Formally,

$$\exists x\ \forall y : y \notin x.$$

3. Pair sets: for any x and y there is a set (namely $\{x, y\}$) with only the elements x and y. Formally,

$$\exists p\ \forall z : (z \in p \leftrightarrow z = x \vee z = y).$$

4. Separation: for any formula $\varphi(z)$ possibly with parameters, and any set x, there is a set (namely $\{x \in a : \varphi(x)\}$) whose elements are the values satisfying φ. Like the induction axiom in PA, this requires an axiom schema:

$$\exists x'\ \forall z : z \in x' \leftrightarrow (z \in x \wedge \varphi(z, \bar{y}))$$

where $\varphi(z, \bar{y})$ is any $\mathcal{L}$-formula. Note that x and $\bar{y}$ are implicitly universally quantified.

Like the induction axiom in PA, the separation axiom can be helpfully understood in terms of definable sets. If $(M, \in^M)$ is the structure, the separation axiom says that for any definable set $D \subseteq M$ and any $x \in M$, there is an $x' \in M$ such that x' " = " $x \cap D$, or more precisely,

$$\forall z \ (z \in^M x' \iff z \in^M x \wedge z \in D).$$

5. Powersets: for any x there is a set (namely $\mathfrak{P}(x)$) whose elements are exactly the subsets of x. Formally,

$$\exists p \ \forall z : (z \in p \leftrightarrow z \subseteq x),$$

where $z \subseteq x$ is the formula $\forall y : y \in z \to y \in x$.

6. Unionsets: for any x there is a set (namely $\bigcup x$) whose elements are exactly the elements of the elemets of x. Formally

$$\exists u \ \forall z : (z \in u \leftrightarrow \exists y : z \in y \in x).$$

7. The axiom of choice: If x is a set whose elements are non-empty and disjoint from each other, then there is a set y containing exactly one element from each set x. We leave the formal statement of this as an exercise.
8. The axiom of infinity: there is a set Z such that $\varnothing \in Z$ and $x \in Z \implies \{x\} \in Z$. Again, we leave the formal statement of this as an exercise.

An important variant of Z is Zermelo-Fraenkel set theory (ZFC), which adds the *axiom of replacement* and *axiom of foundation*. The axiom of replacement is an axiom schema like the axiom of separation. Essentially, it says that if $x \in (M, \in)$ and $f : x \to M$ is a definable function, then M contains the direct image $f[x] = \{f(y) : y \in x\}$. The axiom of foundation can be understood as something like an induction axiom. In one form, it says that if $D \subseteq M$ is definable and non-empty, then there is an element $x \in D$ such that no $y \in x$ satisfies $y \in D$. This is like the induction axiom in PA, which says that if $D \subseteq M$ is definable and non-empty, then there is $x \in D$ such that no $y < x$ satisfies $y \in D$.

Remark 3.10.4. By convention, ZFC is the foundation for mathematics—the ZFC axioms are the axioms that mathematicians are allowed to use in proofs. Whether this is reasonable is an important philosophical question. Another alternative is ZFC minus the axiom of infinity, or even ZFC with the negation of the axiom of infinity. The resulting system is equivalent on some level to Peano Arithmetic.

Remark 3.10.5. Most of the theories on this list have models. However, it is "unknown" whether there are models of ZFC. By Gödel's completeness theorem, this is equivalent to the statement $Con(\text{ZFC})$ saying that ZFC is consistent. By Gödel's *incompleteness* theorem, $\text{ZFC} \vdash Con(\text{ZFC})$ if and only if ZFC is *in*consistent. Thus, we don't expect ZFC to prove that models of ZFC exist, and if it *does* prove that models of ZFC exist, then ZFC is inconsistent.

This isn't to say that models of ZFC are unimportant. In fact, there are many set-theoretic hypotheses which imply that models of ZFC exist, such as all large cardinal hypotheses—statements like "inaccessible cardinals exist," "weakly compact cardinals exist," "measurable cardinals exist" and so on. So models of set theory play an important role in set theory, in spite of the fact that ZFC alone does not prove their existence.

3.11 ◇ The theory of the random graph

Recall from the previous section that we regard graphs as models of the theory

$$\forall x, y : x \; R \; y \to y \; R \; x$$
$$\forall x : \neg x \; R \; x$$

in the language with one binary relation symbol R.

Definition 3.11.1. A graph (V, R) is *random* if for any finite subsets $S_1, S_2 \subseteq_f V$ with $S_1 \cap S_2 = \varnothing$, there is an element $x \in V \setminus (S_1 \cup S_2)$ such that x is adjacent to every element of S_1 and not adjacent to any element of S_2.

Random graphs are models of a theory T_{rand} consisting of the theory of graphs plus the following axiom schema where n, m range over $\mathbb{N}$:

$$\forall y_1, \ldots, y_n, z_1, \ldots, z_m \left(\bigwedge_{i=1}^{n} \bigwedge_{j=1}^{m} y_i \neq z_j \right) \to$$
$$\exists x \left(\bigwedge_{i=1}^{n} x \, R \, y_i \wedge \bigwedge_{j=1}^{m} (x \neq z_i \wedge \neg x \, R \, z_i) \right).$$

Here, $\{y_1, \ldots, y_n\}$ and $\{z_1, \ldots, z_m\}$ correspond to the two sets S_1 and S_2.

If φ is a sentence in the language of graphs, let $P_n(\varphi)$ denote the probability that φ holds on a random graph on the vertex set $\{1, 2, \ldots, n\}$. The terminology "random graph" comes from the following fact.

Fact 3.11.2. *If φ is one of the axioms of T_{rand}, then $\lim_{n\to\infty} P_n(\varphi) = 1$.*

So the axioms of T_{rand} are true for "random" finite graphs. Fact 3.11.2 is not deep—it's an easy exercise in probability. Another easy exercise in probability then shows the following:

Fact 3.11.3. *If $\{\varphi_1, \ldots, \varphi_m\}$ is a finite subset of T_{rand}, then*

$$\lim_{n\to\infty} P_n \left(\bigwedge_{i=1}^{m} \varphi_i \right) = 1.$$

As a corollary, at least one finite graph satisfies $\bigwedge_{i=1}^{m} \varphi_i$. Thus, ay finite subset of T_{rand} has a model. This property is called *finite satisfiability.* In the next chapter, we will prove the *Compactness Theorem* (Theorem 4.4.5), which says that finitely satisfiable theories have models. Thus T_{rand} is consistent, having at least one model.[7]

The theory T_{rand} of the random graph is complete. This can be proven using back-and-forth systems, just like the case of DLO (Corollary 3.7.11). Specifically,

Lemma 3.11.4. *If $M_1, M_2 \models T_{rand}$, then the class of finite partial isomorphisms between M_1 and M_2 is a back-and-forth system. Therefore $M_1 \equiv M_2$.*

[7] This can also be seen via a different method: if one takes a random graph on the infinite vertex set $\mathbb{N}$, then it satisfies all the axioms of T_{rand} with probability 1, and is therefore a model with probability 1. This approach requires more measure theory, to make precise the notion of a random graph on an infinite vertex set.

Proof. Suppose we have $f : A \to B$ a finite partial isomorphism from M_1 to M_2, and an element $a \in M_1$. We need to find a larger finite partial isomosphism $f' : A' \to B'$ with $a \in A'$. We may assume $a \notin A$. Split A into $A^+ = \{x \in A : x \ R \ a\}$ and $A^- = \{x \in A : x \ R \ a\}$. Let B^+ and B^- be the image of A^+ and A^- under f. By the axioms of random graphs, there is $b \in M_2 \setminus B$ such that b is adjacent to every point in B^+ and not adjacent to any point in B^-. Then $f' = f \cup \{(a, b)\}$ is a finite partial isomorphism. □

This has an interesting corollary in combinatorics, the *zero-one law* for graphs:

Theorem 3.11.5 (Zero-one law). *If φ is any sentence in the language of graphs, then $\lim_{n\to\infty} P_n(\varphi)$ exists and is 0 or 1.*

Proof sketch. In fact,

$$\lim_{n\to\infty} P_n(\varphi) = \begin{cases} 1 & \text{if } T_{rand} \vdash \varphi \\ 0 & \text{if } T_{rand} \vdash \neg\varphi. \end{cases}$$

Because of the completeness of T_{rand}, either $T_{rand} \vdash \varphi$ or $T_{rand} \vdash \neg\varphi$. Replacing φ with $\neg\varphi$, we may assume $T_{rand} \vdash \varphi$. The proof of φ from T_{rand} uses only finitely many sentences $\{\psi_1, \ldots, \psi_m\} \subseteq_f T_{rand}$. Then any graph which satisfies $\{\psi_1, \ldots, \psi_m\}$ also satisfies φ. By Fact 3.11.3,

$$\lim_{n\to\infty} P_n(\varphi) \geq \lim_{n\to\infty} P_n\left(\bigwedge_{i=1}^{m} \psi_i\right) = 1,$$

and so $\lim_{n\to\infty} P_n(\varphi) = 1$ as claimed. □

Chapter 4

The compactness theorem

The *compactness theorem* is the fundamental tool of model theory. It says the following:

Theorem (Compactness theorem)**.** *Let T be a theory. Suppose every finite subset $T_0 \subseteq_f T$ has a model. Then T has a model.*

The reason for the name "compactness" will be made clear in Chapter 7 when we discuss topologies.

As we will see, the compactness theorem is a powerful method for constructing models. In the next chapter, we will use it to prove the Löwenheim-Skolem theorem (Theorem 5.4.5), and in Chapter 8 we will use it to realize types. For now, we focus on proving the compactness theorem. In the current chapter we give the proof using *Henkin's method*, and we will later see a different proof using *ultraproducts* (Theorem 6.2.14).

The core idea of Henkin's method is similar to the construction of free algebras in Section 2.8: given a theory T we want to take the "free" model of T, the model in which equations and relations only hold if T forces them to hold, and every element is named by a term. Unfortunately, this "free" model of T usually doesn't exist, *unless* T has two unusual properties—*completeness* and the *witness property* (Section 4.3). However, it turns out that if T is a theory which "should" have a model, then we can modify T to get a theory with the two desired properties. All we need to do is apply the following operations ad nauseam:

1. If T doesn't disprove φ, add φ to T.

2. If T proves $\exists x\ \varphi(x)$, add a new constant symbol c to the language and add the sentence $\varphi(c)$ into T.

This process is discussed in Section 4.4.

4.1 A temporary convention

When we defined formulas (Definition 3.1.8), we chose the following logical operators to be fundamental:

$$\wedge, \vee, \top, \bot, \exists, \forall, \neg.$$

In contrast, notions like $\leftrightarrow$ and $\exists!$ are defined in terms the fundamental operators (see Section 3.3). For example, $\varphi \to \psi$ is an abbreviation for $\neg\varphi \vee \psi$.

In this chapter, we temporarily switch conventions, regarding

$$\wedge, \top, \exists, \neg,$$

as fundamental logical operators, and $\vee, \forall, \bot$ as derived notions like $\leftrightarrow$ or $\exists!$. Specifically:

$$\begin{gathered}\varphi \vee \psi := \neg(\neg\varphi \wedge \neg\psi) \\ \bot := \neg\top \\ \exists x\ \varphi(x) := \neg\forall x\ \neg\varphi(x).\end{gathered}$$

This convention simplifies the proofs of the compactness and completeness theorems, without impacting the conclusions of these theorems.

4.2 Premodels

In model theory, we usually treat $=$ as a logical symbol, on the same level as $\wedge$, $\vee$, or $\exists$, rather than a symbol in the language like $\leq$ or $+$. In contrast, proof theorists usually treat $=$ as a part of the language, and regard the properties of equality, like

$$\begin{gathered}\forall x : x = x \\ \forall x, y : x = y \to (\varphi(x) \leftrightarrow \varphi(y))\end{gathered}$$

as axioms that should be included in the theory, rather than fundamental laws of logic. If we were to adopt this point of view, a “model” of the theory of abelian groups would be a structure $(G, +, 0, -, \approx)$ satisfying axioms like

$$\begin{gathered} \forall x : x \approx x \\ \forall x, y : x \approx y \to y \approx x \\ \forall x, y : x + y \approx y + x \\ \forall x, y, z : x \approx y \to x + z \approx y + z \end{gathered}$$

and so on. We will call the resulting objects *premodels* of the theory of groups. This section is about premodels more generally. However, we are mainly interested in premodels because they can be used to build models (Corollary 4.2.5), and not because of the philosophy of equality.

Definition 4.2.1. A *$\mathcal{L}$-prestructure* is a pair $(M, \approx)$ where M is an $\mathcal{L}$-structure and $\approx$ is an equivalence relation on M such that the following hold:

1. If f is a k-ary function symbol and $a_i \approx b_i$ for $i = 1, \dots, k$, then
$$f(a_1, \dots, a_k) \approx f(b_1, \dots, b_k).$$

2. If R is a k-ary relation symbol and $a_i \approx b_i$ for $i = 1, \dots, k$, then
$$R(a_1, \dots, a_k) \iff R(b_1, \dots, b_k).$$

The first condition says that $\approx$ is a congruence with respect to the function symbols. Thus, when $\mathcal{L}$ is a functional language, an $\mathcal{L}$-prestructure is just an $\mathcal{L}$-algebra with a congruence. As in the case of congruences on algebras, we can form quotient structures:

Definition 4.2.2. If $(M, \approx)$ is an $\mathcal{L}$-prestructure, then $M/\approx$ is the following $\mathcal{L}$-structure:

1. The underlying set is $M/\approx = \{[a] : a \in M\}$, where $[a] = \{b \in M : b \approx a\}$.

2. If f is a k-ary function symbol, then
$$f([a_1], \dots, [a_k]) = [f(a_1, \dots, a_k)]$$

3. If R is a k-ary relation symbol, then

$$R([a_1],\dots,[a_n]) \iff R(a_1,\dots,a_n).$$

This is well-defined by definition of prestructure (using Theorem 2.3.1).

If M is an $\mathcal{L}$-prestructure, if $\varphi(x_1,\dots,x_n)$ is an $\mathcal{L}$-sentence, and $a_1,\dots,a_n \in M$, then we define $M \models \varphi(a_1,\dots,a_n)$ exactly as for ordinary structures, except that

$$M \models t(\bar{a}) = s(\bar{a}) \iff t^M(\bar{a}) \approx s^M(\bar{a}).$$

In other words, we treat the symbol "=" as a non-logical symbol whose interpretation is $\approx$.

Definition 4.2.3. A *premodel* of T is an $\mathcal{L}$-prestructure satisfying T.

Theorem 4.2.4. *If $(M,\approx)$ is an $\mathcal{L}$-prestructure, then*

$$M \models \varphi(a_1,\dots,a_n) \iff (M/\approx) \models \varphi([a_1],\dots,[a_n]).$$

Proof. By induction on the complexity of φ. For example, if $\varphi(x_1,\dots,x_n)$ is $\exists y : \psi(\bar{x},y)$, then

$$\begin{aligned} M \models \varphi(a_1,\dots,a_n) &\iff \exists b \in M : M \models \psi(\bar{a},b) \\ &\iff \exists b \in M : (M/\approx) \models \psi([a_1],\dots,[a_n],[b]) \\ &\iff \exists c \in (M/\approx) : (M/\approx) \models \psi([a_1],\dots,[a_n],c) \\ &\iff (M/\approx) \models \varphi([a_1],\dots,[a_n]), \end{aligned}$$

as every element of $M/\approx$ has the form $[b]$ for some $b \in M/\approx$. □

Corollary 4.2.5. *If $(M,\approx)$ is a premodel of T, then $M/\approx$ is a model of T.*

Example 4.2.6. Let $\equiv_3$ denote congruence modulo 3 on $\mathbb{Z}$. Then $(\mathbb{Z},+,\cdot,-,0,1,\equiv_3$ $)$ is a prefield—a premodel of the theory of fields—because the quotient $\mathbb{Z}/\equiv_3 = \mathbb{Z}/3\mathbb{Z}$ is a field (Theorem 2.5.7). Note that $(\mathbb{Z},\equiv_3)$ really does satisfy the field axioms, when = is interpreted as $\equiv_3$. For example, the field axiom

$$\forall x : x \neq 0 \to \exists y : xy = 1$$

holds in $(\mathbb{Z},\equiv_3)$ because

$$\forall x : x \not\equiv_3 0 \to \exists y : xy \equiv_3 1.$$

This says that if x is an integer that is not a multiple of 3, then there is an integer y such that $xy \equiv 1 \pmod 3$.

Similarly,

$$\begin{gathered}\forall x, y : x + y \equiv_3 y + x \\ 0 \not\equiv_3 1\end{gathered}$$

and so on.

Example 4.2.7. Let F be the set of formal symbols $\frac{n}{m}$ where n and m are integers with $m \neq 0$. Because we are considering formal symbols, $\frac{2}{4} \neq \frac{1}{2}$. In fact,

$$\frac{a}{b} = \frac{c}{d} \iff (a, b) = (c, d).$$

But define $\approx$ to be the expected notion of equality:

$$\frac{a}{b} \approx \frac{c}{d} \iff ad = bc.$$

Also define operations on fractions following the usual rules:

$$\begin{gathered}\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \\ \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \\ -\left(\frac{a}{b}\right) = \frac{-a}{b} \\ 0 = \frac{0}{1} \\ 1 = \frac{1}{1}.\end{gathered}$$

Then $(F, +, \cdot, -, 0, 1, \approx)$ is a prefield, because all the field axioms hold up to $\approx$. For example,

$$\begin{gathered}\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} \approx \frac{a}{b} + \left(\frac{b}{c} + \frac{e}{f}\right) \\ \frac{a}{b} + \frac{-a}{b} \approx \frac{0}{1} \\ \frac{a}{b} \not\approx \frac{0}{1} \implies \frac{b}{a} \cdot \frac{a}{b} \approx \frac{1}{1}\end{gathered}$$

and so on. On the other hand, $(F, +, \cdot, -, 0, 1)$ isn't even a ring, because $\frac{1}{2} + \frac{-1}{2} = \frac{0}{4} \neq \frac{0}{1}$, so the equation $x + (-x) = 0$ doesn't hold.

The quotient structure $F/{\approx}$ is exactly the field $\mathbb{Q}$ of rational numbers. When one builds the real numbers from scratch in set theory, this is precisely how one builds $\mathbb{Q}$ from $\mathbb{Z}$.

4.3 The witness property

(Recall from Section 1.3 that a *closed term* is a term with no variables, like $1 + 0 \cdot (-1)$.)

Definition 4.3.1. Let T be an $\mathcal{L}$-theory.

- T is *satisfiable* if T has a model.
- T is *finitely satisfiable* if every $T_0 \subseteq_f T$ is satisfiable.
- T is *complete* if for every $\mathcal{L}$-sentence φ, $\varphi \in T$ or $\neg\varphi \in T$.
- T has the *witness property* if whenever $(\exists x\ \varphi(x)) \in T$, there is a closed term t such that $\varphi(t) \in T$.

Warning 4.3.2. The definition of "complete" we are using here is that $T \ni \varphi$ or $T \ni \neg\varphi$ for any φ, which is slightly different from definition of "complete" in §3.6, which said that $T \vdash \varphi$ or $T \vdash \neg\varphi$ for any φ.

Here are some examples of theories with and without the witness property:

1. Consider the ring $\mathbb{Z} = (\mathbb{Z}, +, \cdot, 0, 1, -)$. One can show that the complete theory $\mathrm{Th}(\mathbb{Z})$ has the witness property. For example, when $\varphi(x)$ is the formula $x + 1 + 1 = 0$, we have

$$\mathbb{Z} \models \exists x : x + 1 + 1 = 0.$$

The witness property says that there is some closed term t such that $\varphi(t)$ holds, i.e.,

$$\mathbb{Z} \models t + 1 + 1 = 0.$$

Taking $t = -(1 + 1)$ works, because

$$\mathbb{Z} \models (-(1 + 1)) + 1 + 1 = 0.$$

More generally, Th($\mathbb{Z}$) has the witness property because whenever $\mathbb{Z} \models \exists x : \psi(x)$, there must be an integer n such that $\mathbb{Z} \models \psi(n)$, and then we can write n as a closed term since we have the symbols $0, 1, +, -$ available.

2. If we remove the negation sign, the complete theory of $(\mathbb{Z}, +, \cdot, 0, 1)$ does *not* have the witness property, because of the formula $\varphi(x)$ from the previous point. There's no way to write -2 as a closed term.

3. If we use one of the obvious axiomatizations, then the theory of fields T_{fields} has the witness property vacuously, because it has no axioms of the form $\exists x\ \varphi(x)$. There is nothing to check.

4. The theory DLO does not have the witness property, arguably. One of the axioms says that the structure is non-empty: $\exists x : x = x$ or $\exists x : \top$. If DLO had the witness property, there would need to be a closed term t such that the sentence $t = t$ or $\top$ is in DLO. But there are no closed terms in the language of orders, because there are no constant symbols or function symbols.

The goal of this section is to show that if a theory T is finitely satisfiable, complete, and has the witness property, then T can be converted into a model of T in a canonical fashion (Theorem 4.3.5). We first need a couple lemmas. Recall from §3.6 that the notation $T \models \varphi$ means that every model of T satisfies φ.

Lemma 4.3.3. *Suppose an $\mathcal{L}$-theory T is finitely satisfiable and complete, $T_0 \subseteq_f T$, and $T_0 \models \varphi$. Then $\varphi \in T$.*

Proof. Otherwise, $\neg\varphi \in T$. Then $T_0 \cup \{\neg\varphi\}$ shows T is *not* finitely satisfiable. □

Lemma 4.3.4. *Suppose an $\mathcal{L}$-theory T is finitely satisfiable and complete and has the witness property. Let φ, ψ be sentences and $\theta(x)$ be a formula.*

1. $\neg\varphi \in T \iff \varphi \notin T$.

2. $\varphi \wedge \psi \in T \iff (\varphi \in T$ *and* $\psi \in T)$

3. $\top \in T$.

4. $(\exists x\ \theta(x)) \in T$ *if and only if there is a closed term t such that $\theta(t) \in T$.*

Proof.

1. Either $\varphi \in T$ or $\neg\varphi \in T$ by completeness. If both φ and $\neg\varphi$ are in T, then T is not finitely satisfiable.

2. Both directions hold by Lemma 4.3.3, because
$$\{\varphi, \psi\} \models \varphi \wedge \psi$$
$$\varphi \wedge \psi \models \varphi \text{ and } \varphi \wedge \psi \models \psi.$$

3. Lemma 4.3.3 again.

4. The $\Leftarrow$ direction holds by Lemma 4.3.3, and the $\Rightarrow$ direction holds because T has the witness property. □

Theorem 4.3.5. *Let T be finitely satisfiable and complete, with the witness property. Then T has a model.*

Proof. By Corollary 4.2.5, it suffices to build a premodel $(M, \approx) \models T$. The underlying set of M will be the set of closed $\mathcal{L}$-terms. If f is a k-ary function symbol and $t_1, \ldots, t_k \in M$, let $f^M(t_1, \ldots, t_k) = f(t_1, \ldots, t_k)$. (The functional part of M is essentially a term algebra, like in Section 2.8.) If R is a k-ary function symbol and $t_1, \ldots, t_k \in M$, let $R^M(t_1, \ldots, t_k)$ hold iff $R(t_1, \ldots, t_k) \in T$. Finally, let $t \approx s$ hold iff $(t = s) \in T$.

Claim. The relation $\approx$ is transitive.

Proof. Suppose $\{s = t, t = u\} \subseteq T$. Note that $\{s = t, t = u\} \models \{s = u\}$. (Any structure which satisfies $s = t$ and $t = u$ must also satisfy $s = u$.) By Lemma 4.3.3, $(s = u) \in T$. $\square_{\text{Claim}}$

Similar arguments show that $\approx$ is symmetric, reflexive, and respects the function and relation symbols. Thus M is an $\mathcal{L}$-prestructure.

Claim. If φ is an $\mathcal{L}$-sentence, then $M \models \varphi \iff \varphi \in T$.

Proof. Proceed by induction on φ:

1. If φ is an atomic formula, then $M \models \varphi \iff \varphi \in T$ by choice of the $\mathcal{L}$-structure:

   (a) $M \models R(t_1, \ldots, t_k) \iff R(t_1, \ldots, t_k) \in T$ by choice of R^M.

   (b) $M \models t = s \iff (t = s) \in T$ by choice of $\approx$.

(c) $M \models f(t_1, \ldots, t_k) = s \iff (f(t_1, \ldots, t_k) = s) \in T$ by choice of f^M.

2. The logical operators $\neg, \top, \wedge, \exists$ work correctly by Lemma 4.3.4 and induction. For example,

$$\begin{aligned} M \models \exists x\ \varphi(x) &\iff \exists t \in M : M \models \varphi(t) \\ &\iff \exists t \in M : \varphi(t) \in T \qquad \text{by induction} \\ &\iff (\exists x\ \varphi(x)) \in T \qquad \text{by Lemma 4.3.4(4).} \qquad \square_{\text{Claim}} \end{aligned}$$

By the Claim, M is a premodel of T. By Corollary 4.2.5, the quotient $M/{\approx}$ is a model of T. □

Remark 4.3.6. The construction of the model $M/{\approx}$ in Theorem 4.3.5 is formally related to the construction of free algebras in Theorems 2.8.5 and 2.8.7. In both constructions, we take a term algebra modulo the relation where $t \approx s$ iff $T \vdash t = s$.

Definition 4.3.7. Suppose T is finitely satisfiable and complete and has the witness property. The *canonical model* of T is the model constructed in the proof of Theorem 4.3.5.

The canonical model of T is characterized up to isomorphism by the fact that every element $a \in M$ is named by a closed term t, in the sense that $a = t^M$.

When we talk about ultraproducts in Chapter 6, we will need the following refinement of the witness property.

Definition 4.3.8. Let $\mathcal{C}$ be a collection of closed $\mathcal{L}$-terms. An $\mathcal{L}$-theory *has the witness property over* $\mathcal{C}$ if whenever $(\exists x\ \varphi(x)) \in T$, there is a term $t \in \mathcal{C}$ such that $\varphi(t) \in T$.

Theorem 4.3.9. *Let T be a finitely satisfiable, complete theory with the witness property over $\mathcal{C}$, and let M be the canonical model of T. Then every element of M is named by a term in $\mathcal{C}$.*

Proof. Fix $a \in M$. Then $a = t^M$ for some term t. The $\mathcal{L}$-sentence

$$\exists x\ x = t$$

holds in any $\mathcal{L}$-structure, so it must be in T by Lemma 4.3.3. By the witness property over $\mathcal{C}$, there is $t' \in \mathcal{C}$ such that $(t' = t) \in T$. Then $M \models t' = t$, so $a = t^M = (t')^M$, and a is named by a term in $\mathcal{C}$. □

4.4 Compactness via Henkin's method

We are almost ready to prove the compactness theorem: if T is finitely satisfiable then T has a model. We have seen in Theorem 4.3.5 that if T has the two additional properties of completeness and the witness property, then T has a model. In this section, we see how to get from an arbitrary finitely satisfiable theory T to one with these additional properties by adding new statements to T. This will take infinitely many steps, so it helps to know that a union of a chain of finitely satisfiable theories is finitely satisfiable:

Theorem 4.4.1. *Let I be a linear order and $\{T_i\}_{i \in I}$ be a chain of finitely satisfiable theories, meaning that $i < i' \implies T_i \subseteq T_{i'}$. Then the union $T = \bigcup_{i \in I} T_i$ is finitely satisfiable.*

Proof. Suppose $T_0 \subseteq_f T$. Let $T_0 = \{\varphi_1, \ldots, \varphi_n\}$. For each $j \leq n$, we have $\varphi_j \in T = \bigcup_i T_i$, so there is some $i_j \in I$ with $\varphi_j \in T_{i_j}$. Let $\ell = \max(i_1, \ldots, i_n) \in I$. Then for each $j \leq n$, we have $\varphi_j \in T_{i_j} \subseteq T_\ell$. Thus $T_0 \subseteq_f T_\ell$, and T_0 is satisfiable because T_ℓ is finitely satisfiable. □

First, let's see how to turn a finitely satisfiable theory into a complete theory by adding sentences:

Lemma 4.4.2. *If T is a finitely satisfiable $\mathcal{L}$-theory, then there is a complete, finitely satisfiable $\mathcal{L}$-theory $T' \supseteq T$.*

Proof. By Zorn's lemma and Theorem 4.4.1 there is a $T' \supseteq T$ which is maximal among finitely satisfiable $\mathcal{L}$-theories. We claim T' is complete. Otherwise there is a sentence φ with $\varphi \notin T'$ and $\neg\varphi \notin T'$. By maximality, $T' \cup \{\varphi\}$ is not finitely satisfiable, so there is $T_1 \subseteq_f T$ with $T_1 \models \neg\varphi$. Similarly, $\neg\varphi \notin T'$ implies that there is $T_2 \subseteq_f T$ with $T_2 \models \varphi$. Then $T_1 \cup T_2$ is not satisfiable, a contradiction. □

Next, we need to add the witness property. This time, we will need to change the language, by adding new constant symbols.

Lemma 4.4.3. *Let T be a finitely satisfiable $\mathcal{L}$-theory containing a sentence $\exists x\ \varphi(x)$. Let $\mathcal{L}' = \mathcal{L} \cup \{c\}$ where c is a new constant symbol. Then $T \cup \{\varphi(c)\}$ is a finitely satisfiable $\mathcal{L}'$-theory.*

Proof. Otherwise, $T_0 \cup \{\varphi(c)\}$ is unsatisfiable for some $T_0 \subseteq_f T$. Take $M \models T_0 \cup \{\exists x\ \varphi(x)\}$ and take $b \in M$ such that $M \models \varphi(b)$. Expand the $\mathcal{L}$-structure M to an $\mathcal{L}'$-structure by interpreting c as b. Then $M \models T_0 \cup \{\varphi(c)\}$, contradicting the choice of T_0. □

Note that Lemma 4.4.3 moves us one step closer to the witness property: if $\exists x\ \varphi(x) \in T$ then the witness property requires a constant or term t such that $\varphi(t) \in T$, and this is exactly what Lemma 4.4.3 adds to T.

By applying Lemma 4.4.3 infinitely many times, we can get a larger theory $T' \supseteq T$ with the witness property. In fact, we may as well get the witness property and completeness at the same time:

Lemma 4.4.4. *Let T be a finitely satisfiable $\mathcal{L}$-theory. There is a language $\mathcal{L}' \supseteq \mathcal{L}$ and an $\mathcal{L}'$-theory $T' \supseteq T$ that is finitely satisfiable and complete, and has the witness property.*

Proof. Build increasing chains

$$\begin{gathered}\mathcal{L}_0 \subseteq \mathcal{L}_1 \subseteq \cdots \\ T_0 \subseteq T_1 \subseteq \cdots\end{gathered}$$

where T_i is a finitely satisfiable $\mathcal{L}_i$-theory as follows:

1. $\mathcal{L}_0 = \mathcal{L}$ and $T_0 = T$.

2. If $n > 0$ and n is odd, then $\mathcal{L}_n = \mathcal{L}_{n-1}$ and T_n is a completion of T_{n-1} from Lemma 4.4.2.

3. If $n > 0$ and n is even, let $\{\varphi_i(x) : i \in I\}$ enumerate the $\mathcal{L}_{n-1}$-formulas such that $(\exists x\ \varphi(x)) \in T_{n-1}$. Let $\mathcal{L}_n = \mathcal{L}_{n-1} \cup \{c_i : i \in I\}$ where the c_i are new constant symbols. Let $T_n = T_{n-1} \cup \{\varphi_i(c_i) : i \in I\}$. Then T_n is finitely satisfiable by Lemma 4.4.3.

Finally, take $\mathcal{L}' = \bigcup_n \mathcal{L}_n$ and $T' = \bigcup_n T_n$. Then T' is finitely satisfiable because each T_i is, T' is complete because of the odd-numbered steps, and T' has the witness property because of the even-numbered steps. □

Theorem 4.4.5 (Compactness)**.** *If T is finitely satisfiable, then T has a model.*

Proof. By Lemma 4.4.4, there is a language $\mathcal{L}' \supseteq \mathcal{L}$ and an $\mathcal{L}'$-theory $T' \supseteq T$ such that T' is finitely satisfiable and complete and has the witness property. By Theorem 4.3.5 there is an $\mathcal{L}'$-structure M satisfying T', and therefore T. □

Since this has all been so abstract, let's give a simple application of the compactness theorem:

Theorem 4.4.6. *Consider* $\mathbb{R}$ *as an ordered field* $(\mathbb{R}, +, \cdot, -, 0, 1, \leq)$*. There is* $M \equiv \mathbb{R}$ *with* $M \not\cong \mathbb{R}$*.*

Proof. Let $\mathcal{L}$ be the language of ordered rings, and let $T = \mathrm{Th}(\mathbb{R})$. Let $\mathcal{L}' = \mathcal{L} \cup \{c\}$ where c is a new constant symbol. For $n \in \mathbb{N}$, let

$$T_n = T \cup \{c > 0, c > 1, c > 2, \ldots, c > n\},$$

where $2, 3, \ldots$ mean $1 + 1, 1 + 1 + 1, \ldots$. Each T_n is satisfiable—in fact $(\mathbb{R}, +, \cdot, -, 0, 1, \leq, n + 1)$ is a model (interpreting the constant symbol c as $n + 1$). By Theorem 4.4.1, the union

$$T' = \bigcup_{n=1}^{\infty} T_n = T \cup \{c > 0, c > 1, c > 2, \ldots\}$$

is finitely satisfiable. By the compactness theorem, it has a model

$$(M, +, \cdot, -, 0, 1, \leq, c) \models T'.$$

Then $(M, +, \cdot, -, 0, 1, \leq) \models T = \mathrm{Th}(\mathbb{R})$, so $M \equiv \mathbb{R}$ by Theorem 3.4.9. On the other hand, $M \models c > n$ for each $n \in \mathbb{N}$, and so the element c^M is greater than $1, 2, 3, \ldots$. Therefore M is not isomorphic to $\mathbb{R}$. □

In the next chapter, we will use more sophisticated versions of this argument to show that any infinite structure has arbitrarily big elementary extensions (Theorem 5.4.9).

4.5 ♢ The proof of the completeness theorem

Recall the soundness and completeness theorems (Fact 3.6.1):

$$T \models \varphi \iff T \vdash \varphi.$$

Here, $T \models \varphi$ means that every model of T satisfies φ and $T \vdash \varphi$ means that φ is provable from T. The ⇐ direction is Soundness, which is relatively easy to prove, and the ⇒ direction is Completeness, which is more subtle.

The completeness theorem is closely related to the compactness theorem. Traditionally, the compactness theorem was deduced as a corollary of the completeness theorem as follows:

Proof. Suppose T is finitely satisfiable but T has no models. Then every model of T satisfies $\bot$, so $T \models \bot$. By the completeness theorem, $T \vdash \bot$: there is a proof of $\bot$ from T. The proof uses only finitely many axioms in T, so $T_0 \vdash \bot$ for some finite subset $T_0 \subseteq_f T$. Then T_0 is not satisfiable (by Soundness), contradicting finite satisfiability. □

However, the proof of the completeness theorem can be modified slightly to prove the compactness theorem. This proof of compactness, which is the one in Sections 4.3–4.4, is much more direct than the proof via completeness, because we avoid any discussion of provability.

In this section, we explain how to undo the modifications, and get back the original proof of the completeness theorem.

In order to prove the completeness theorem, we need a precise definition of the provability relation $T \vdash \varphi$. There are many equivalent definitions, all of which are slightly complicated. We give one definition in Section 4.6 below. Regardless of how provability is defined, it has the following essential properties.

Fact 4.5.1. *Say that a theory T is* inconsistent *if $T \vdash \bot$, and* consistent *otherwise.*

1. *$T \vdash \varphi$ if and only if $T \cup \{\neg\varphi\}$ is inconsistent.*

2. *If T is consistent, then any subset $T_0 \subseteq T$ is consistent.*

3. *If every finite subset $T_0 \subseteq_f T$ is consistent, then T is consistent.*

4. *If T is consistent, then $\{\varphi, \neg\varphi\} \not\subseteq T$.*

5. *If T is consistent, then $T \cup \{\varphi\}$ is consistent or $T \cup \{\neg\varphi\}$ is consistent.*

6. *If T is consistent and $(\exists x \varphi(x)) \in T$, then $T \cup \{\varphi(c)\}$ is consistent, where c is a new constant symbol added to the language.*

7. *The following things hold:*

$$\begin{gathered}\varphi, \psi \vdash \varphi \wedge \psi \\ \varphi \wedge \psi \vdash \varphi \\ \varphi \wedge \psi \vdash \psi \\ \varnothing \vdash \top \\ \theta(t) \vdash \exists x \theta(x) \\ \varnothing \vdash t = t \\ t = s \vdash s = t \\ t_1 = t_2,\ t_2 = t_3 \vdash t_1 = t_3.\end{gathered}$$

One can then prove the following:

Theorem 4.5.2 (Completeness theorem, first form)**.** *If T is consistent, then T is satisfiable.*

Proof. One mimics the proof of the compactness theorem in §4.3–4.4, replacing "finitely satisfiable" with "consistent" and the relation $T \models \varphi$ with $T \vdash \varphi$. In more detail, here are the steps, with some comments on the proofs.

- Lemma 4.3.3: If T is consistent and complete, $T_0 \subseteq T$, and $T_0 \vdash \varphi$, then $\varphi \in T$.
  - *Proof:* Otherwise T contains the inconsistent theory $T_0 \cup \{\neg\varphi\}$.
- Lemma 4.3.4: If T is consistent, complete, and has the witness property, then
  1. $\neg\varphi \in T \iff \varphi \notin T$.
  2. $\varphi \wedge \psi \in T \iff (\varphi \in T$ and $\psi \in T)$.
  3. $\top \in T$.
  4. $(\exists x\ \theta(x)) \in T$ iff there is a closed term t with $\theta(t) \in T$.
- Theorem 4.3.5: If T is consistent, complete, and has the witness property, then T has a model.
- Theorem 4.4.1: A union of a chain of consistent theories is consistent.

- Lemma 4.4.2: If T is consistent, then there is a complete consistent $T' \supseteq T$.
    - *Proof:* If T is maximal among consistent theories, then one of $T \cup \{\varphi\}$ or $T \cup \{\neg\varphi\}$ is consistent, so $\varphi \in T$ or $\neg\varphi \in T$ by maximality.
- Lemma 4.4.3: If T is consistent and contains $\exists x\ \varphi(x)$, then we can add $\varphi(c)$ to T without losing consistency.
    - *Proof:* This is part of Fact 4.5.1.
- Lemma 4.4.4: If T is a consistent $\mathcal{L}$-theory, then there is a larger language $\mathcal{L}' \supseteq \mathcal{L}$ and a larger $\mathcal{L}'$-theory $T' \supseteq T$ such that T' is consistent, complete, and has the witness property.
- Lemma 4.4.5: If T is consistent, then T has a model.

All of the proofs go through with minor changes, using the properties listed in Fact 4.5.1. □

Finally, one can deduce the full completeness theorem as follows:

Theorem 4.5.3 (Completeness theorem, second form)**.** *If $T \models \varphi$, then $T \vdash \varphi$.*

Proof. Suppose $T \nvdash \varphi$. Then $T \cup \{\neg\varphi\}$ is consistent, so it has a model M. Then $M \models T$ but $M \not\models \varphi$, so $T \not\models \varphi$, a contradiction. □

4.6 ♠ A proof calculus

There are many equivalent ways to define the provability relation $T \vdash \varphi$. In this appendix, we present one of these definitions, chosen with the following goals in mind:

1. $\vdash$ should be defined by a small set of rules.
2. The rules should resemble the structure of informal proofs.
3. The rules should make Henkin's method work smoothly.

4. Equality (=) needs to be treated as a fundamental symbol, unlike in proof theory where it is treated as part of the signature.

Recall our convention in this chapter that the only fundamental logical operations are $\top, \wedge, \exists$, and $\neg$, and that $\bot, \vee, \forall$ are abbreviations. With this convention, the provability relation $\vdash$ can be defined as follows:

Definition 4.6.1. The class of triples $(\mathcal{L}, T, \varphi)$ where $\mathcal{L}$ is a language, T is an $\mathcal{L}$-theory, φ is an $\mathcal{L}$-sentence, and $T \vdash \varphi$, is generated by the following rules:

(Assumption) If $\varphi \in T$ then $T \vdash \varphi$.

($\top$) $T \vdash \top$.

($\wedge_1$) If $T \vdash \varphi$ and $T \vdash \psi$ then $T \vdash \varphi \wedge \psi$.

($\wedge_2$) If $T \vdash \varphi \wedge \psi$, then $T \vdash \varphi$ and $T \vdash \psi$.

($\neg_1$) If $T \vdash \varphi$ and $T \vdash \neg\varphi$, then $T \vdash \psi$.

($\neg_2$) If $T \cup \{\varphi\} \vdash \psi$ and $T \cup \{\neg\varphi\} \vdash \psi$, then $T \vdash \psi$.

($\exists_1$) If t is a closed term and $T \vdash \theta(t)$, then $T \vdash \exists x : \theta(x)$.

($\exists_2$) Let $\mathcal{L}' = \mathcal{L} \cup \{c\}$ where c is a new constant symbol. If $T \cup \{\theta(c)\} \vdash \psi$, then $T \cup \{\exists x : \theta(x)\} \vdash \psi$.

($=_1$) $T \vdash t = t$.

($=_2$) If $T \vdash t = s$ and $T \vdash \theta(t)$, then $T \vdash \theta(s)$.

Here T is an $\mathcal{L}$-theory, φ, ψ are $\mathcal{L}$-sentences, t, s are closed $\mathcal{L}$-terms, and $\theta(x)$ is an $\mathcal{L}$-formula in one variable.

Usually we omit braces to the left of the symbol $\vdash$, writing $T, \varphi \vdash \psi$ rather than $T \cup \{\varphi\} \vdash \psi$.

While Definition 4.6.1 may look mysterious, each rule is actually describing a well-known proof strategy:

(Assumption) We can use assumptions in proofs.

($\top$) The statement $\top$ is always true.

($\wedge_1$) To prove $\varphi \wedge \psi$, prove φ and prove ψ.

($\wedge_2$) From $\varphi \wedge \psi$, conclude φ. From $\varphi \wedge \psi$, conclude ψ.

($\neg_1$) The principle of explosion: if we have proven φ and $\neg\varphi$, then we can prove anything.

($\neg_2$) If we're trying to prove ψ, we can break into cases depending on whether some other sentence φ is true or false.

($\exists_1$) From $\theta(t)$, conclude $\exists x \theta(x)$.

($\exists_2$) To use an assumption of the form $\exists x : \theta(x)$, say "Fix some c such that $\theta(c)$" and proceed with the assumption $\theta(c)$.

($=_1$) The statement $t = t$ is true.

($=_2$) If $t = s$ and $\theta(t)$ is true, then $\theta(s)$ is true since we can replace t with s.

The following examples show how to use Definition 4.6.1, and how to translate informal proofs into formal proofs.

Example 4.6.2. Let $\mathcal{L} = \{R, a\}$ where $R(-)$ is a unary relation symbol and a is a constant symbol. We claim that

$$\neg\exists x : R(x) \vdash \neg R(a).$$

We first give an informal proof:

Proof. Break into two cases.

1. $R(a)$ is false. Then $\neg R(a)$ is true, as desired.

2. $R(a)$ is true. Then $\exists x : R(x)$ is true. With the assumption $\neg\exists x : R(x)$, we get a contradiction, and so $\neg R(a)$ holds.

Either way, $\neg R(a)$ holds as claimed. □

This can be converted into the following formal proof:

Step	Assumptions	$\vdash$	Claim	Why?
1	$\neg\exists xR(x),\ \neg R(a)$	$\vdash$	$\neg R(a)$	(ASSUMPTION)
2	$\neg\exists xR(x),\ R(a)$	$\vdash$	$R(a)$	(ASSUMPTION)
3	$\neg\exists xR(x),\ R(a)$	$\vdash$	$\exists xR(x)$	($\exists_1$) and Step 2
4	$\neg\exists xR(x),\ R(a)$	$\vdash$	$\neg\exists xR(x)$	(ASSUMPTION)
5	$\neg\exists xR(x),\ R(a)$	$\vdash$	$\neg R(a)$	($\neg_1$) and Steps 3 and 4.
6	$\neg\exists xR(x)$	$\vdash$	$\neg R(a)$	($\neg_2$) and Steps 1 and 5.

Step 1 is the first case of the proof, Steps 2–5 are the second case, and Step 6 combines the two cases.

Example 4.6.3. Let $\mathcal{L} = \{a, b, c\}$ where a, b, c are constant symbols. Then $a = b,\ b = c \vdash a = c$:

Step	Assumptions	$\vdash$	Claim	Why?
1	$a = b,\ b = c$	$\vdash$	$a = b$	(ASSUMPTION)
2	$a = b,\ b = c$	$\vdash$	$a = a$	($=_1$)
3	$a = b,\ b = c$	$\vdash$	$b = a$	Steps 1 and 2 plus ($=_2$) with the formula $x = a$.
4	$a = b,\ b = c$	$\vdash$	$b = c$	(ASSUMPTION)
5	$a = b,\ b = c$	$\vdash$	$a = c$	Steps 3 and 4 plus ($=_2$) with the formula $x = c$.

Example 4.6.4. Here is a slightly more complicated proof, illustrating rule ($\exists_2$). Let $\mathcal{L} = \{P, R\}$ where P and R are unary relation symbols. We claim

$$\exists xR(x),\ \neg\exists xP(x) \vdash \exists x(R(x) \wedge \neg P(x)).$$

First we give an informal proof:

Proof. Suppose $\exists xR(x)$ and $\neg\exists P(x)$. Fix some c such that $R(c)$. Break into cases:

1. $P(c)$ is true. Then $\exists xP(x)$ is true. This contradicts the assumption that $\neg\exists xP(x)$. Therefore $\neg P(c)$.

2. $P(c)$ is false. Then $\neg P(c)$.

Either way, $\neg P(c)$ holds. Also, $R(c)$ holds by assumption. Therefore $R(c) \wedge \neg P(c)$ holds. Consequently $\exists x(R(x) \wedge \neg P(x))$ holds. □

This translates to the following formal proof:

Step	Language	Assumptions	$\vdash$	Claim	Why?
1	$\mathcal{L} \cup \{c\}$	$R(c),\ \neg\exists x P(x),\ P(c)$	$\vdash$	$P(c)$	(Assumption)
2	$\mathcal{L} \cup \{c\}$	$R(c),\ \neg\exists x P(x),\ P(c)$	$\vdash$	$\exists x P(x)$	$(\exists_1)$, Step 1
3	$\mathcal{L} \cup \{c\}$	$R(c),\ \neg\exists x P(x),\ P(c)$	$\vdash$	$\neg\exists x P(x)$	(Assumption)
4	$\mathcal{L} \cup \{c\}$	$R(c),\ \neg\exists x P(x),\ P(c)$	$\vdash$	$\neg P(c)$	$(\neg_1)$, Steps 2–3
5	$\mathcal{L} \cup \{c\}$	$R(c),\ \neg\exists x P(x),\ \neg P(c)$	$\vdash$	$\neg P(c)$	(Assumption)
6	$\mathcal{L} \cup \{c\}$	$R(c),\ \neg\exists x P(x)$	$\vdash$	$\neg P(c)$	$(\neg_2)$, Steps 4–5
7	$\mathcal{L} \cup \{c\}$	$R(c),\ \neg\exists x P(x)$	$\vdash$	$R(c)$	(Assumption)
8	$\mathcal{L} \cup \{c\}$	$R(c),\ \neg\exists x P(x)$	$\vdash$	$R(c) \wedge \neg P(c)$	$(\wedge_1)$, Steps 6–7
9	$\mathcal{L} \cup \{c\}$	$R(c),\ \neg\exists x P(x)$	$\vdash$	$\exists x(R(x) \wedge \neg P(x))$	$(\exists_1)$, Step 8
10	$\mathcal{L}$	$\exists x R(x),\ \neg\exists x P(x)$	$\vdash$	$\exists x(R(x) \wedge \neg P(x))$	$(\exists_2)$, Step 9

Note that a general proof of $T \vdash \varphi$ is a finite list

Language	Claim
$\mathcal{L}_1$	$T_1 \vdash \varphi_1$
$\mathcal{L}_2$	$T_2 \vdash \varphi_2$
$\vdots$	$\vdots$
$\mathcal{L}_{n-1}$	$T_{n-1} \vdash \varphi_{n-1}$
$\mathcal{L}$	$T \vdash \varphi$

where each row is obtained from previous rows using the rules of Definition 4.6.1. We may as well assume that the proof contains no unnecessary rows, so that each row is used by one of the later rows. Then by working backwards from the last row, one can verify the following conditions:

- Each language $\mathcal{L}_i$ has the form $\mathcal{L} \cup \{c_1, \ldots, c_m\}$, where the c_i are new constant symbols added via the $(\exists_2)$ rule.

- Each theory T_i has the form $T \cup \{\psi_1, \ldots, \psi_m\}$, where the ψ_i are new assumptions added via the $(\neg_2)$ and $(\exists_2)$ rules.

This shows that proofs are finitary in nature—each line in the proof consists of a finite amount of data layered on top of the fixed sets $\mathcal{L}$ and T which are constant throughout the proof. (This is the key to proving Fact 3.6.5 on the computable nature of proofs.)

From this description, and by looking carefully at the rules, we can see the following about how the proof depends on T:

1. If we have a proof of $T \vdash \varphi$ and $T' \supseteq T$, then we can replace T with T' in each line[1], getting a proof that $T' \vdash \varphi$.

2. If we have a proof that $T \vdash \varphi$, then there is a finite subset $T_0 \subseteq_f T$ such that we can replace T with T_0 in each line[2] and get a proof that $T_0 \vdash \varphi$.

To summarize:

Fact 4.6.5. *The provability relation $\vdash$ has the following properties:*

(Monotonicity) *If $T \vdash \varphi$ and $T' \supseteq T$, then $T' \vdash \varphi$.*

(Finite Character) *If $T \vdash \varphi$ then there is a finite subset $T_0 \subseteq T$ such that $T_0 \vdash \varphi$.*

Fact 4.6.5 can also be proven more directly, and more abstractly, by the following strategy:

1. Let $T \vdash^M \varphi$ mean that for every $T' \supseteq T$, we have $T' \vdash \varphi$. One can verify that $\vdash^M$ satisfies all the rules generating $\vdash$ in Definition 4.6.1. As $\vdash$ is the smallest relation satisfying these rules, we must have $T \vdash \varphi \implies T \vdash^M \varphi$, which is Monotonicity.

2. Let $T \vdash^f \varphi$ mean that there is a finite subset $T_0 \subseteq_f T$ such that $T_0 \vdash \varphi$. Using Monotonicity, one can verify that $\vdash^f$ satisfies all the rules generating $\vdash$ in Definition 4.6.1. Thus $T \vdash \varphi \implies T \vdash^f \varphi$, which is Finite Character.

Interestingly, the same proof strategy can be used to prove the Soundness theorem:

3. Recall that $T \models \varphi$ means that every model of T satisfies φ. One can verify that $\models$ satisfies all the rules generating $\vdash$ in Definition 4.6.1. Thus $T \vdash \varphi \implies T \models \varphi$.

With monotonicity and finite character established, we can verify the other properties needed in the proof of the completeness theorem.

Recall that T is inconsistent if $T \vdash \bot$, but $\bot$ is an abbreviation for $\neg\top$ due to our conventions.

[1] More precisely, replace $T \cup \{\psi_1, \dots, \psi_m\} \vdash \cdots$ with $T' \cup \{\psi_1, \dots, \psi_m\} \vdash \cdots$.

[2] More precisely, replace $T \cup \{\psi_1, \dots, \psi_m\} \vdash \cdots$ with $T_0 \cup \{\psi_1, \dots, \psi_m\} \vdash \cdots$.

Theorem 4.6.6. *$T \vdash \varphi$ if and only if $T, \neg\varphi \vdash \bot$.*

Proof. First suppose $T \vdash \varphi$. Then

$$\begin{aligned} T, \neg\varphi &\vdash \varphi && \text{by Monotonicity} \\ T, \neg\varphi &\vdash \neg\varphi && \text{by the (A}\textsc{ssumption}\text{) rule} \\ T, \neg\varphi &\vdash \bot && \text{by the } (\neg_1) \text{ rule.} \end{aligned}$$

Conversely, suppose $T, \neg\varphi \vdash \bot$. Then

$$\begin{aligned} T, \neg\varphi &\vdash \neg\top && \\ T, \neg\varphi &\vdash \top && \text{by the } (\top) \text{ rule} \\ T, \neg\varphi &\vdash \varphi && \text{by the } (\neg_1) \text{ rule} \\ T, \varphi &\vdash \varphi && \text{by the (A}\textsc{ssumption}\text{) rule} \\ T &\vdash \varphi && \text{by the } (\neg_2) \text{ rule.} \end{aligned}$$

□

Theorem 4.6.7. *If every finite $T_0 \subseteq_f T$ is consistent, then T is consistent.*

Proof. If T is inconsistent, then $T \vdash \bot$. By Finite Character, there is a finite $T_0 \subseteq_f T$ such that $T_0 \vdash \bot$, i.e., T_0 is inconsistent. □

Theorem 4.6.8. *If T is consistent then $T \cup \{\varphi\}$ or $T \cup \{\neg\varphi\}$ is consistent.*

Proof. Otherwise,

$$\begin{gathered} T, \varphi \vdash \bot \\ T, \neg\varphi \vdash \bot, \end{gathered}$$

and so $T \vdash \bot$ by the rule $(\neg_2)$. □

Theorem 4.6.9. *If $\{\varphi, \neg\varphi\} \subseteq T$, then T is inconsistent.*

Proof.

$$\begin{aligned} T &\vdash \varphi && \text{by the (A}\textsc{ssumption}\text{) rule} \\ T &\vdash \neg\varphi && \text{by the (A}\textsc{ssumption}\text{) rule} \\ T &\vdash \bot && \text{by the } (\neg_1) \text{ rule.} \end{aligned}$$

□

Theorem 4.6.10. *Suppose T is consistent and $\exists x \theta(x) \in T$. Let c be a new constant symbol. Then $T \cup \{\theta(c)\}$ is consistent.*

Proof. Otherwise,

$$\begin{gathered} T, \theta(c) \vdash \bot \\ T, \exists x \theta(x) \vdash \bot \end{gathered}$$

by the $(\exists_2)$ rule. But $T \vdash \exists x \theta(x)$ by the (Assumption) rule, so $T \vdash \bot$ by Lemma 4.6.11 below. □

Lemma 4.6.11. *If $T \vdash \varphi$ and $T, \varphi \vdash \psi$, then $T \vdash \psi$.*

Proof.

$$\begin{aligned} T, \neg\varphi &\vdash \varphi && \text{by Monotonicity} \\ T, \neg\varphi &\vdash \neg\varphi && \text{by the (Assumption) rule} \\ T, \neg\varphi &\vdash \psi && \text{by the } (\neg_1) \text{ rule} \\ T, \varphi &\vdash \psi && \text{by assumption} \\ T &\vdash \psi && \text{by the } (\neg_2) \text{ rule.} \end{aligned}$$

□

Theorem 4.6.12. *The following things hold:*

$$\begin{gathered} \varphi, \psi \vdash \varphi \wedge \psi \\ \varphi \wedge \psi \vdash \varphi \\ \varphi \wedge \psi \vdash \psi \\ \varnothing \vdash \top \\ \theta(t) \vdash \exists x \theta(x) \\ \varnothing \vdash t = t \\ t = s \vdash s = t \\ t_1 = t_2,\ t_2 = t_3 \vdash t_1 = t_3. \end{gathered}$$

Proof. The proofs are straightforward using the rules in Definition 4.6.1, except perhaps the last two lines, which follow by the method of Example 4.6.3. □

Chapter 5

Categoricity

With the compactness theorem proved, we now turn towards applications. The key result of this chapter is the *Löwenheim-Skolem theorem*, which in one form says the following:

Theorem. *Let T be a theory in a countable language. Suppose T has an infinite model M. Then for any infinite cardinal κ, T has a model M_κ of size κ.*

On one hand, this gives us a source of new models. For example, it tells us that there are fields of size κ for any infinite κ, because there is at least one infinite field ($\mathbb{R}$).

On the other hand, the Löwenheim-Skolem theorem shows the limits of what can be expressed using first-order logic. In particular, first-order sentences have no way of saying anything about infinite cardinalities—there is no way to say "M is countable" or "M is uncountable," because any theory with a countable infinite model will have uncountable models, any theory with an uncountable model will have a countable infinite model.

We apply the Löwenheim-Skolem theorem to the notion of categoricity. A theory T is *absolutely categorical* if it has exactly one model, up to isomorphism. Absolutely categorical theories are complete, because any two models are elementarily equivalent. Unfortunately, the Löwenheim-Skolem theorem makes it nearly impossible to be absolutely categorical (see Theorem 5.5.2).

However, the more refined notion of *κ-categoricity* works well. If κ is an infinite cardinal, then a theory T is *κ-categorical* if it has exactly one model of size κ. Using the Löwenheim-Skolem theorem, one can show that

κ-categorical theories are complete, modulo a few small issues (see Theorem 5.6.2). Several important theories turn out to be κ-categorical for various values of κ.

In the process of studying categoricity, we will also meet some important technical tools. The *diagram* of a structure M is a theory whose models are essentially the extensions of M (the structures extending M). There is also a related theory called the *elementary diagram* of M, whose models are essentially the elementary extensions of M. Diagrams are a common tool in applications of the compactness theorem. Using elementary diagrams, we also prove a fact called *elementary amalgamation*, which says that if $M_1 \equiv M_2$, then up to isomorphism the two structures M_1 and M_2 are both elementary substructures of a third structure M_3. We will see later in Chapter 11 that for any structure M one can in fact make a big elementary extension $\mathbb{M} \succeq M$ such that $\mathbb{M}$ is an elementary extension of every "small" $N \equiv M$.

5.1 A useful fact around finite satisfiability

Let T be a set of sentences. Suppose T is closed under finite conjunctions, in the sense that

$$\varphi_1, \ldots, \varphi_n \in T \implies \bigwedge_{i=1}^{n} \varphi_i \in T.$$

Then T is finitely satisfiable if and only if every $\varphi \in T$ is satisfiable, because any finite subset $\{\varphi_1, \ldots, \varphi_n\} \subseteq T$ is equivalent to a single formula $\bigwedge_{i=1}^{n} \varphi_i$ in T.

More generally, suppose T_1, T_2 are two sets of sentences, and T_1 is closed under finite conjunctions. Then the following are equivalent:

- $T_1 \cup T_2$ is finitely satisfiable.
- For every $\varphi \in T_1$ and finite subset $T_2' \subseteq_f T_2$, the theory $\{\varphi\} \cup \{T_2'\}$ is satisfiable.

We will use this fact implicitly in what follows.

Example 5.1.1. Where would we find a theory that is closed under finite conjunctions? One example is $\mathrm{Th}(M)$, the complete theory of M (Section 3.4). This theory is closed under finite conjunctions because if $M \models \varphi$ and $M \models \psi$, then $M \models \varphi \wedge \psi$. Most theories that are closed under finite conjunctions come from variants of $\mathrm{Th}(M)$. For example, one might look at the set of quantifier-free sentences that are satisfied by M, or the set of $\mathcal{L}_0$-sentences for some sublanguage $\mathcal{L}_0 \subseteq \mathcal{L}$.

5.2 Diagrams and elementary amalgamation

Let M be an $\mathcal{L}$-structure and A be a subset of M. The language $\mathcal{L}(A)$ is obtained by adding each element of A as a new constant symbol. We regard M as an $\mathcal{L}(A)$-structure by interpreting each new constant symbol as the corresponding element of A:

$$a^M = a.$$

The point of the language $\mathcal{L}(A)$ is that it lets us mention elements of A in our formulas and sentences.

Example 5.2.1. Let $\mathcal{L}$ be the language of rings $\{+, \cdot, -, 0, 1\}$. Then $M = \mathbb{R}$ is naturally an $\mathcal{L}$-structure. Take $A = \mathbb{Q}$. The language $\mathcal{L}(\mathbb{Q})$ is obtained by adding a new constant symbol for each rational number. Here are some $\mathcal{L}(\mathbb{Q})$-formulas:

$$\exists y : y \cdot y = 0.5 + x$$
$$\forall x : x \cdot x \neq 1/3.$$

The second formula is also an $\mathcal{L}(\mathbb{Q})$-sentence. This $\mathcal{L}(\mathbb{Q})$-sentence is false in $\mathbb{R}$, because $\sqrt{1/3} \in \mathbb{R}$, but true in the substructure $\mathbb{Q}$, because $\pm\sqrt{1/3} \notin \mathbb{Q}$.

Remark 5.2.2. If $\varphi(\bar{x}, \bar{y})$ is an $\mathcal{L}$-formula and $\bar{a}$ is a tuple in A, then $\varphi(\bar{a}, \bar{y})$ is an $\mathcal{L}(A)$-formula, and all $\mathcal{L}(A)$-formulas arise this way. For example, the formula

$$\exists y : y \cdot y = 0.5 + x$$

can be understood as $\varphi(0.5, x)$, where $\varphi(z, x)$ is

$$\exists y : y \cdot y = z + x.$$

If $\varphi(\bar{x})$ is an $\mathcal{L}$-formula and $\bar{a}$ is a tuple in A, then $\varphi(\bar{a})$ is an $\mathcal{L}(A)$-sentence, and all $\mathcal{L}(A)$-sentences arise this way.

Definition 5.2.3. The *elementary diagram* of M, written $\mathrm{eldiag}(M)$, is the set of $\mathcal{L}(M)$-sentences φ such that $M \models \varphi$. The *diagram* of M is the set of atomic and negated atomic formulas in $\mathrm{eldiag}(M)$.

Example 5.2.4. The diagram of the ring $\mathbb{Z}$ consists of sentences like $1+1 = 2$, $1+2 = 3$, $2+1 = 3$, $3 \cdot 5 = 15$, and so on[1]. One can thinks of $\mathrm{diag}(\mathbb{Z})$ as a description of the multiplication and addition tables of $\mathbb{Z}$.

The elementary diagram of $\mathbb{Z}$ is much more complicated, containing both the diagram of $\mathbb{Z}$ and the full complete theory $\mathrm{Th}(\mathbb{Z})$.

By Remark 5.2.2, we could equivalently define $\mathrm{eldiag}(M)$ as

$$\{\varphi(\bar{c}) : \varphi(\bar{x}) \text{ is an } \mathcal{L}\text{-formula, } \bar{c} \in M^n, \text{ and } M \models \varphi(\bar{c}).\}$$

Thus $\mathrm{eldiag}(M)$ contains all information about satisfaction of formulas in the structure M. Likewise, $\mathrm{diag}(M)$ has a similar definition restricting $\varphi(\bar{x})$ to atomic $\mathcal{L}$-formulas.

How should we understand models of $\mathrm{diag}(M)$ and $\mathrm{eldiag}(M)$? A model of $\mathrm{diag}(M)$ consists of an $\mathcal{L}$-structure N and a map

$$\begin{aligned} M &\to N \\ a &\mapsto a^N \end{aligned}$$

such that for any atomic $\mathcal{L}$-formula $\varphi(x_1, \ldots, x_n)$ and any $\bar{a} \in M^n$,

$$\begin{aligned} M \models \varphi(a_1, \ldots, a_n) &\implies N \models \varphi(a_1^N, \ldots, a_n^N) \\ M \models \neg\varphi(a_1, \ldots, a_n) &\implies N \models \neg\varphi(a_1^N, \ldots, a_n^N). \end{aligned}$$

This precisely means that $a \mapsto a^N$ is an embedding (see Remark 3.4.4). Therefore, a model of $\mathrm{diag}(M)$ is the same thing as an $\mathcal{L}$-structure N with an embedding $f : M \to N$. In particular, if N is an extension of M, then N is a model of $\mathrm{diag}(M)$ in a natural way, interpreting $a \in M$ as $a \in N$. Every model of $\mathrm{diag}(M)$ is isomorphic as an $\mathcal{L}(M)$-structure to an extension of M.

Similarly, a model of $\mathrm{eldiag}(M)$ is the same thing as an $\mathcal{L}$-structure N with an elementary embedding $f : M \to N$. Any elementary extension of M is a model of $\mathrm{eldiag}(M)$, and every model of $\mathrm{eldiag}(M)$ is isomorphic as an $\mathcal{L}(M)$-structure to an elementary extension of M.

[1] It also contains more complicated sentences like $2 \cdot (2+3) = 5+7$.

To summarize, models of diag(M) are essentially extensions of M, and models of eldiag(M) are essentially elementary extensions of M.

We will see several applications of (elementary) diagrams in this chapter in the next. Here is a first example.

Theorem 5.2.5 (Elementary amalgamation)**.** *If M_1 and M_2 are elementarily equivalent, then there is a structure N and elementary embeddings $M_1 \to N$ and $M_2 \to N$.*

We first prove a lemma. Recall the notion of *expansion* from Definition 3.1.5: an expansion of M is a structure with the same underlying set as M, but with additional functions and relations on top of the ones in M.

Lemma 5.2.6. *If $M_1 \equiv M_2$ and $\varphi \in$ eldiag(M_2), then there is an $\mathcal{L}(M_2)$-structure N expanding the $\mathcal{L}$-structure M_1 such that $N \models \varphi$.*

Proof. Write φ as $\psi(\bar{c})$ for some $\mathcal{L}$-formula $\psi(\bar{x})$ and tuple $\bar{c}$ in M_2 (Remark 5.2.2). The fact that $M_2 \models \psi(\bar{c})$ implies that $M_2 \models \exists \bar{x}\ \psi(\bar{x})$ and then $M_1 \models \exists \bar{x}\ \psi(\bar{x})$ as $M_1 \equiv M_2$. Take $\bar{a}$ in M_1 such that $M_1 \models \psi(\bar{a})$. Expand M_1 to an $\mathcal{L}(M_2)$-structure N by interpreting the symbols $c_1, \ldots, c_n$ as $a_1, \ldots, a_n$, respectively.[2] Then $N \models \psi(\bar{c})$ because $\bar{c}^N = \bar{a}$ and $M_1 \models \psi(\bar{a})$. □

Now we prove Theorem 5.2.5.

Proof. It suffices to show that eldiag$(M_1) \cup$ eldiag(M_2) is consistent. Otherwise, by the Compactness Theorem, there is an $\mathcal{L}(M_2)$-sentence $\varphi \in$ eldiag(M_2) such that eldiag$(M_1) \cup \{\varphi(\bar{c})\}$ is inconsistent. But $M_1 \models$ eldiag(M_1), and Lemma 5.2.6 gives an expansion of M_1 satisfying $\{\varphi(\bar{c})\}$, and so eldiag$(M_1) \cup \{\varphi(\bar{c})\}$ is consistent. □

5.3 The Tarski-Vaught criterion

The Tarski-Vaught criterion is an important tool for testing whether a given subset of M is an elementary substructure of M. In the next section, we will use it to find small elementary substructures.

[2] ♠ This only works if the symbols $c_1, \ldots, c_n$ are pairwise distinct. At the start of the proof, we should have arranged for $\bar{c}$ to not contain any element more than once. However, this is easy to ensure. For example, let $\{c_1, \ldots, c_n\}$ be a list of the constant symbols appearing in φ *without repeats*. Then φ has the form $\psi(c_1, \ldots, c_n)$.

Theorem 5.3.1. *Let M be a structure and A be a subset. Then $A \preceq M$ iff the following holds: for every non-empty A-definable $D \subseteq M$, we have $D \cap A \neq \varnothing$.*

This condition is called the *Tarski-Vaught criterion.*

Proof. First suppose $A \preceq M$. Suppose D is A-definable and non-empty. Write D as $\varphi(M, \bar{a})$ for some $\mathcal{L}(A)$-formula $\varphi(x, \bar{a})$. Then

$$M \models \exists x : \varphi(x, \bar{a}) \implies A \models \exists x : \varphi(x, \bar{a})$$

so there is $b \in A$ with $A \models \varphi(b, \bar{a})$, which implies $M \models \varphi(b, \bar{a})$ as $A \preceq M$. Then $b \in A$ and $b \in D = \varphi(M, \bar{a})$.

Conversely, suppose the Tarski-Vaught criterion holds. First we show that A is a substructure. Suppose f is a k-ary function symbol and $a_1, \ldots, a_k \in A$. The set $\{f(\bar{a})\}$ is non-empty and A-definable, so A intersects it, meaning that $f(\bar{a}) \in A$.

Next we show that for any $\mathcal{L}$-formula $\varphi(\bar{x})$ and any $\bar{a} \in A$,

$$M \models \varphi(\bar{a}) \iff A \models \varphi(\bar{a}). \tag{$*$}$$

We may assume φ makes no use of $\wedge$, $\forall$, $\top$, $\bot$. Proceed by induction on the complexity of φ. If φ is atomic or more generally quantifier-free, then $(*)$ holds because A is a substructure.

If φ is $\psi \vee \theta$, then

$$\begin{aligned} M \models \varphi(\bar{a}) &\iff M \models \psi(\bar{a}) \text{ or } M \models \theta(\bar{a}) \\ &\iff A \models \psi(\bar{a}) \text{ or } A \models \theta(\bar{a}) \\ &\iff A \models \varphi(\bar{a}) \end{aligned}$$

by induction. Finally, if $\varphi(\bar{x})$ is $\exists y : \psi(\bar{x}, y)$, then

$$\begin{aligned} M \models \varphi(\bar{a}) &\iff \exists b \in M : M \models \psi(\bar{a}, b) \\ &\overset{\text{TV}}{\iff} \exists b \in A : M \models \psi(\bar{a}, b) \\ &\overset{\text{ind}}{\iff} \exists b \in A : A \models \psi(\bar{a}, b) \\ &\iff A \models \varphi(\bar{a}). \end{aligned}$$

The second line uses the Tarski-Vaught criterion, and the third line uses induction. □

Remark 5.3.2. There is a subtle connection between the Tarski-Vaught criterion and the witness property. Specifically, the $\mathcal{L}(A)$-theory of M

$$\mathrm{Th}_A(M) := \{\varphi(\bar{a}) : \varphi(\bar{x}) \text{ is an } \mathcal{L}\text{-formula, } \bar{a} \in A^n,\ M \models \varphi(\bar{a})\}$$

has the witness property over A (Definition 4.3.8) if and only if A satisfies the Tarski-Vaught criterion. In both cases, we are saying that if $M \models \exists x\ \varphi(\bar{a}, x)$, then there is $b \in A$ such that $M \models \varphi(\bar{a}, b)$.

When $\mathrm{Th}_A(M)$ has the witness property, the canonical model (Definition 4.3.7) is essentially A. The canonical model A satisfies $\mathrm{Th}_A(M)$ by Claim 4.3 in the proof of Theorem 4.3.5, and $A \models \mathrm{Th}_A(M)$ means the same thing as $A \preceq M$. So, on some level, the proof of Claim 4.3 is the same as the proof of Theorem 5.3.1.

5.4 The Löwenheim-Skolem theorem

In this section, we prove the *Löwenheim-Skolem theorem*, which in one form says that if M is an infinite structure and κ is an infinite cardinal, then there is $N \equiv M$ with $|N| = \kappa$. Moreover, there are two refined versions of this theorem:

1. Downward Löwenheim-Skolem: if $\kappa \leq |M|$, we can take $N \preceq M$.

2. Upward Löwenheim-Skolem: if $\kappa \geq |M|$, we can take $N \succeq M$.

Strictly speaking, the statements above are only true when the language $\mathcal{L}$ is countable. For general languages, we need to keep track of the "size" of $\mathcal{L}$, defined as follows:

Definition 5.4.1. If $\mathcal{L}$ is a language, the *size* of $\mathcal{L}$, written $|\mathcal{L}|$, is $\aleph_0$ plus the number of symbols in $\mathcal{L}$.

If $\bar{x}$ is a finite tuple of variables, then $|\mathcal{L}|$ is the number of $\mathcal{L}$-formulas $\varphi(\bar{x})$.

Remark 5.4.2. If M is a $\mathcal{L}$-structure and $A \subseteq M$, then the number of A-definable sets in M is at most $|A| + |\mathcal{L}|$.

Theorem 5.4.3 (Downward Löwenheim-Skolem theorem)**.** *Let M be an $\mathcal{L}$-structure.*

1. *If $A \subseteq M$, there is an elementary substructure $N \preceq M$ with $N \supseteq A$ and $|N| \leq |A| + |\mathcal{L}|$.*

2. *For any κ with $|\mathcal{L}| \leq \kappa \leq |M|$, there is $N \preceq M$ with $|N| = \kappa$.*

Proof. 1. Let $F : \mathfrak{P}(M) \setminus \{\varnothing\} \to M$ be a function such that $F(X) \in X$. Recursively define $A_0 \subseteq A_1 \subseteq \cdots$ by letting $A_0 = A$ and

$$A_{n+1} = A_n \cup \{F(X) : X \subseteq M \text{ is } A_n\text{-definable and non-empty}\}.$$

Let $N = \bigcup_{n=0}^{\infty} A_n$. Then $A = A_0 \subseteq N$. By induction on n, each A_n has size at most $|A| + |\mathcal{L}|$, and therefore $|N| \leq |A| + |\mathcal{L}|$. If X is N-definable and non-empty, then X is A_n-definable for some n, so $F(X) \in A_{n+1} \subseteq N$. Thus N intersects every N-definable set, and $N \preceq M$ by Tarski-Vaught.

2. Take a subset $A \subseteq M$ with $|A| = \kappa$, and take $N \preceq M$ as in part (1). Then $|N| \leq |A| + |\mathcal{L}| = \kappa + |\mathcal{L}| = \kappa$. On the other hand, $|N| \geq \kappa$ because $N \supseteq A$. □

Example 5.4.4. The fields $\mathbb{C}$ and $\mathbb{R}$ have countable elementary substructures. At this point it's not obvious what these elementary substructures could be. For example, $\mathbb{Q}$ isn't an elementary substructure of $\mathbb{R}$ or $\mathbb{C}$. Later, in Example 13.5.5 we will show that the set $\mathbb{Q}^{\text{alg}}$ of *algebraic numbers* is a countable elementary substructure of $\mathbb{C}$. Using deeper facts that are beyond the scope of this course, one can also show that $\mathbb{Q}^{\text{alg}} \cap \mathbb{R}$ is a countable elementary substructure of $\mathbb{R}$.

Theorem 5.4.5 (Löwenheim-Skolem theorem, first version)**.** *Let T be an $\mathcal{L}$-theory. Suppose T has an infinite model, or more generally that for every $n < \omega$, T has a model of size at least n. Then for any $\kappa \geq |\mathcal{L}|$, T has a model of size κ.*

Proof. Let $\mathcal{L}' = \mathcal{L} \cup \{c_\alpha : \alpha < \kappa\}$, where the c_α are new constant symbols. Let $\Sigma = \{(c_\alpha \neq c_\beta) : \alpha < \beta < \kappa\}$.

Claim. $T \cup \Sigma$ is finitely satisfiable.

Proof. Suppose $\Sigma_0 \subseteq_f \Sigma$. Let S be the finite set of $\alpha \in \kappa$ such that c_α appears in Σ_0. Take a model $M \models T$ with $|M| > |S|$. Expand M to an $\mathcal{L}'$-structure by interpreting the c_α for $\alpha \in S$ as distinct elements of M, and interpreting c_α for $\alpha \in \kappa \setminus S$ arbitrarily. Then $M \models T \cup \Sigma_0$. $\square_{\text{Claim}}$

By compactness, $T \cup \Sigma$ has a model M. Then the c_α^M are pairwise distinct, so $|M| \geq \kappa$. By downward Löwenheim-Skolem (Theorem 5.4.3), there is an elementary substructure $N \preceq M$ with $|N| = \kappa$. Then $N \equiv M$ and $M \models T$, so $N \models T$. □

Example 5.4.6. There is at least one infinite field, so Theorem 5.4.5 gives a field of size κ for any infinite κ.

Corollary 5.4.7 (Löwenheim-Skolem theorem, second version)**.** *Let M be an infinite $\mathcal{L}$-structure. For any $\kappa \geq |\mathcal{L}|$, there is $N \equiv M$ with $|N| = \kappa$.*

Proof. Apply Theorem 5.4.5 to the $\mathcal{L}$-theory $\mathrm{Th}(M)$. Models of $\mathrm{Th}(M)$ are elementarily equivalent to M (Theorem 3.4.9). □

Example 5.4.8. Earlier we saw that Peano Arithmetic has models which are not elementarily equivalent to $\mathbb{N}$ (Corollary 3.9.13). Using the Löwenheim-Skolem theorem, we can also produce models that are elementarily equivalent to $\mathbb{N}$ but not isomorphic to it. For example, Corollary 5.4.7 gives $M \equiv \mathbb{N}$ with $|M| > \aleph_0$. Then $M \models \mathrm{PA}$ but $M \ncong \mathbb{N}$.

Theorem 5.4.9 (Upward Löwenheim-Skolem theorem)**.** *If M is an infinite $\mathcal{L}$-structure and $\kappa \geq |M| + |\mathcal{L}|$, then there is an elementary extension $N \succeq M$ with $|N| = \kappa$.*

Proof. As $\kappa \geq |M| + |\mathcal{L}| = |\mathcal{L}(M)|$, we can apply the Löwenheim-Skolem theorem (Theorem 5.4.5) to the $\mathcal{L}(M)$-theory $\mathrm{eldiag}(M)$ to get a model $N \models \mathrm{eldiag}(M)$ with $|N| = \kappa$. Moving N by an isomorphism (see Section 5.8), we may assume $N \succeq M$. □

5.5 Absolute categoricity

Recall that T is complete if all its models are elementarily equivalent (Theorem 3.6.4). The easiest way this could be true is if T only has one model in the first place.

Definition 5.5.1. A theory T is *absolutely categorical* if there is a unique model of T, up to isomorphism.

Unfortunately, this is almost never possible:

Theorem 5.5.2. *If T is absolutely categorical, then the unique model M is finite.*

Proof. Take $\kappa > |M| + |\mathcal{L}|$. If M is infinite, then there is a model $N \models T$ with $|N| = \kappa$ by Theorem 5.4.5. Then M and N are two non-isomorphic models, contradicting categoricity. □

Conversely, if M is finite, then $\mathrm{Th}(M)$ is absolutely categorical; we sketch a proof in the rest of this section. Recall that models of $\mathrm{Th}(M)$ are the same thing as structures elementarily equivalent to M (Theorem 3.4.9).

Theorem 5.5.3. *If M is finite and $M \equiv N$, then $M \cong N$.*

Proof. By elementary amalgamation (Theorem 5.2.5) there are elementary embeddings $M \to M'$ and $N \to M'$ for some structure M'. Moving M and N by isomorphisms, we may assume $M \preceq M'$ and $N \preceq M'$. Let n be the size of M. By Lemma 5.5.4 below, $|M| = |M'| = |N| = n$. As M and N are subsets of M', we must have $M = M' = N$. □

Lemma 5.5.4. *Suppose $M \equiv N$. If $|M| = n < \infty$, then $|N| = n$. Consequently, M is finite iff N is finite.*

Proof. Suppose $|M| = n$. Let φ be the sentence $\exists^{=n}x \top$ (see Section 3.3). Then φ says that there are exactly n elements, so $M \models \varphi$. Therefore $N \models \varphi$ and $|N| = n$. □

5.6 κ-categoricity

We have seen that absolute categoricity isn't useful. The next best thing is *κ-categoricity.*

Definition 5.6.1. Let κ be an infinite cardinal. A theory T is *κ-categorical* if there is a unique model of cardinality κ.

Like absolute categoricity, κ-categoricity implies completeness:

Theorem 5.6.2 (Łoś-Vaught criterion)**.** *Suppose T is κ-categorical for some $\kappa \geq |\mathcal{L}|$.*

1. *Any two infinite models of T are elementarily equivalent.*

2. *If all models of T are infinite, then T is complete.*

Proof. 1. Given infinite models M_1, M_2, use Löwenheim-Skolem (Corollary 5.4.7) to get $N_i \equiv M_i$ with $|N_i| = \kappa$. By κ-categoricity, $N_1 \cong N_2$. Then $M_1 \equiv N_1 \equiv N_2 \equiv M_2$.

2. Clear. □

We will see several examples of κ-categorical theories throughout this course. Much later, we will see that the complete theory $\mathrm{Th}(\mathbb{C})$ of the field $(\mathbb{C}, +, \cdot)$ is $\aleph_1$-categorical. In the present section, we show that the complete theory of the linear order $(\mathbb{Q}, \leq)$ is $\aleph_0$-categorical.

Recall the notion of a back-and-forth system from Definition 3.7.5.

Lemma 5.6.3. *Let M, N be countable structures and let $\mathcal{F}$ be a back-and-forth system between M and N. If $f_0 \in \mathcal{F}$, then there is an isomorphism $f : M \to N$ extending f_0.*

Proof. Let $a_1, a_2, \ldots$ be an enumeration of M and $b_1, b_2, \ldots$ be an enumeration of N. Recursively build an increasing sequence of partial isomorphisms $f_i : A_i \to B_i$ in $\mathcal{F}$ as follows:

- For $i = 0$, let $f_0 : A_0 \to B_0$ be the given partial isomorphism.
- For $i = 2k - 1$, take f_i to be an extension of f_{i-1} with $a_k \in \mathrm{dom}(f_i)$. Such an f_i exists by the "forward" condition.
- For $i = 2k$, take f_i to be an extension of f_{i-1} with $b_k \in \mathrm{im}(f_i)$. Such an f_i exists by the "backward" condition.

Take $f = \bigcup_{i=0}^{\infty} f_i$. Then f is an isomorphism from M to N. □

Theorem 5.6.4. *Let M, N be countable structures. If there is a non-empty back-and-forth system between M and N, then $M \cong N$.*

Recall the theory DLO from Definition 3.7.9. Theorem 3.7.10 gives a non-empty back-and-forth system between any two models of DLO.

Corollary 5.6.5 (Cantor)**.** *DLO is $\aleph_0$-categorical: any two countable models of DLO are isomorphic.*

Any model of DLO is infinite, so the Łoś-Vaught criterion shows that DLO is complete, as we saw earlier (Corollary 3.7.11).

Theorem 5.6.6. *DLO is not κ-categorical for $\kappa > \aleph_0$.*

Proof. If A, B are linear orders, let $A \times B$ denote the lexicographic product, the set $A \times B$ with the lexicographic order

$$(a, b) < (a', b') \iff a < a' \text{ for } a \neq a'$$
$$(a, b) < (a, b') \iff b < b'.$$

Also, let A^* denote A with the reversed order.

Let $M = \kappa \times \mathbb{Q}$. It is straightforward to see that M and M^* are models of DLO, of size κ. We claim that $M \ncong M^*$. Note that for any $a \in M$,

$$|\{x \in M : x < a\}| < \kappa$$
$$|\{x \in M : x > a\}| = \kappa.$$

In M^*, the reverse properties hold, so $M \ncong M^*$, and DLO is not κ-categorical. □

Remark 5.6.7. If you know enough abstract algebra, there are some impressive applications of the Łoś-Vaught criterion (Theorem 5.6.2) to things like algebraically closed fields. For more on this, see Chapter 9 and Theorem 14.2.10.

But with our approach, Theorem 5.6.2 is never especially useful. The problem is that most methods to prove κ-categoricity in algebra are thinly veiled proofs of completeness, if you know enough model theory. For example, we just proved that DLO is $\aleph_0$-categorical using back-and-forth systems, but back-and-forth systems already prove completeness as we saw in Section 3.7. The only case where we will really apply Theorem 5.6.2 is vector spaces (Corollary 13.7.6).

5.7 ♢ The random graph revisited

Recall the theory of the random graph from Section 3.11. If M, N are two models, then the collection of finite partial isomorphisms from M to N is a back-and-forth system by Lemma 3.11.4. This family is always non-empty, because $\varnothing : \varnothing \to \varnothing$ is a finite partial isomorphism from M to N. By Theorem 5.6.4, $M \cong N$ when M and N are countable. In other words, the theory of the random graph is $\aleph_0$-categorical. The unique countable model is called the *Rado graph*, or sometimes the *Erős-Rényi graph*.

Suppose we take a random graph on the vertex set $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$. That is, for each pair (i, j) with $i < j < \omega$, we flip a fair coin and put an edge between i and j if the coin comes up heads. If φ is a first-order sentence, let $P(\varphi)$ be the probability that the resulting graph $(\mathbb{N}, R)$ satisfies φ. The following analog of Fact 3.11.2 holds:

Fact 5.7.1. *If φ is one of the axioms of random graphs, then $P(\varphi) = 1$.*

The theory of random graphs has only countably many axioms. Because of how infinite probability spaces work, it follows that a random graph $(\mathbb{N}, R)$ on the vertex set $\mathbb{N}$ will satisfy *all* the axioms of random graphs, with probability 1. Therefore, $(\mathbb{N}, R)$ will be isomorphic to the Rado graph with probability 1.

5.8 ♠ "Moving by an isomorphism"

In some places, such as the proof of the upward Löwenheim-Skolem theorem, we need the fact that any model of $\mathrm{eldiag}(M)$ can be converted into an elementary extension of M. Let's see in more detail how this works. The proof is a little confusing, but really nothing more than bookkeeping.

First, we need some set-theoretic nonsense:

Lemma 5.8.1. *If X is a set and κ is a cardinal, then there is a set Y with $|Y| = \kappa$ and $Y \cap X = \varnothing$.*

Proof. There are many ways to prove this. For example, let

$$S = \{x : \exists y \ (x, y) \in X\}.$$

Using the axiom of replacement in Zermelo-Fraenkel set theory, one can see that S is a set, rather than a proper class.[3] Because S is a set, we can find $x \notin S$. Take a set Y_0 with $|Y_0| = \kappa$. Let $Y = \{x\} \times Y_0 = \{(x, y) : y \in Y_0\}$. Then $|Y| = |Y_0| = \kappa$, and $Y \cap X = \varnothing$ by choice of x. □

Lemma 5.8.2. *Let $f : A \to B$ be a bijection. If $M \supseteq A$, then there is a bijection $g : M \to M'$ where $M' \supseteq B$ and g extends f.*

[3] This can also be seen from the plain Zermelo axioms using the unionset and separation axioms, assuming we are using Kuratowski ordered pairs.

Proof. Let $\kappa = |M \setminus A|$. Take some set W with $|W| = \kappa$ and $W \cap B = \varnothing$. Let $h : M \setminus A \to W$ be a bijection. Let $M' = W \cup B$. Then

$$g : M \to M'$$
$$g(x) = \begin{cases} f(x) & \text{if } x \in A \\ h(x) & \text{if } x \in M \setminus A \end{cases}$$

is a bijection from the disjoint union $M = A \sqcup (M \setminus A)$ to the disjoint union $M' = B \sqcup W$. □

The next lemma says that we can move structures along bijections:

Lemma 5.8.3. *Let $\mathcal{L}$ be a language and M be an $\mathcal{L}$-structure. Let M' be a set and $\alpha : M \to M'$ be a bijection. Then there is a way to regard M' as an $\mathcal{L}$-structure such that α becomes an isomorphism.*

Proof. If R is an n-ary relation symbol, define

$$R^{M'}(a_1, \ldots, a_n) \iff R^M(\alpha^{-1}(a_1), \ldots, \alpha^{-1}(a_n)). \tag{$*$}$$

If f is an n-ary function symbol, define

$$f^{M'}(a_1, \ldots, a_n) = \alpha(f^M(\alpha^{-1}(a_1), \ldots, \alpha^{-1}(a_n))).$$

Then

$$\alpha^{-1}(f^{M'}(a_1, \ldots, a_n)) = f^M(\alpha^{-1}(a_1), \ldots, \alpha^{-1}(a_n)). \tag{$\dagger$}$$

By $(*)$ and $(\dagger)$, α^{-1} is an isomorphism from M' to M, and then α is an isomorphism from M to M'. □

Using this, we can take an $\mathcal{L}$-structure and move it to make the constant symbols go to arbitrary values:

Lemma 5.8.4. *Let $\mathcal{L}$ be a language containing some constant symbols $\{c_i : i \in I\}$, among other things. Let M be an $\mathcal{L}$-structure such that $M \models c_i \neq c_j$ for $i \neq j$. Let $\{z_i : i \in I\}$ be some distinct values. Then there is an isomorphic $\mathcal{L}$-structure $M' \cong M$ such that $c_i^{M'} = z_i$ for each i.*

Proof. Let $A = \{c_i^M : i \in I\}$ and $B = \{z_i : i \in I\}$. By assumption,

$$i \neq j \implies c_i^M \neq c_j^M,$$

and so the map

$$\begin{aligned} I &\to A \\ i &\mapsto c_i^M \end{aligned}$$

is a bijection. Similarly, the map

$$\begin{aligned} I &\to B \\ i &\mapsto z_i \end{aligned}$$

is a bijection. Let $f : A \to B$ be the bijection sending c_i^M to z_i. By Lemma 5.8.2, there is a set $M' \supseteq B$ and a bijection $g : M \to M'$ extending f. By Lemma 5.8.3, we can make the set M' into an $\mathcal{L}$-structure in such a way that g is an isomorphism. Then

$$c_i^{M'} = g(c_i^M) = f(c_i^M) = z_i. \qquad \square$$

Finally, we apply this to diagrams. Recall that a model N of $\mathrm{diag}(M)$ is essentially an $\mathcal{L}$-structure N with an embedding $c \mapsto c^N$ from M to N. If $c^N = c$ for each c, then the embedding is an inclusion, and so N is an extension of M.

Theorem 5.8.5. *If N is a model of* $\mathrm{diag}(M)$*, then there is an isomorphic $\mathcal{L}(M)$-structure $N' \cong N$ such that N' is an extension of M.*

Proof. Apply Lemma 5.8.4 to find $N' \cong N$ such that $c^{N'} = c$ for each $c \in M$. The only things we need to check are that if c_1 and c_2 are distict elements of M, then

$$\begin{aligned} c_1^M &\neq c_2^M \\ c_1 &\neq c_2. \end{aligned}$$

The second line is trivial, and the first line holds because $c \mapsto c^M$ is an embeddign, hence injective. □

A similar statement holds for elementary diagrams:

Theorem 5.8.6. *If N is a model of* $\mathrm{eldiag}(M)$*, then there is an isomorphic $\mathcal{L}(M)$-structure $N' \cong N$ such that N' is an elementary extension of M.*

Chapter 6

Ultraproducts

In the context of universal algebra, we had a number of ways to take models of an equational theory T and produce new models, as discussed in Chapter 2. Is there anything like this in the more general setting of first-order logic? If T is a first-order theory, and we have some models of T, can we combine them to produce new models?

We have already seen a few vague constructions of this form. For example, the upward and downward Löwenheim-Skolem theorems let us take a model M and produce elementary extensions and elementary substructures of a chosen cardinality. But this is not a very close analogue to products, subalgebras, and quotients in universal algebra.

In this chapter, we introduce the *ultraproduct* construction, which gives a much more precise, controlled way to build new models of T from old models. Let I be a set and let M_i be a model of T for each $i \in I$. To define the ultraproduct, we need one additional piece of data, a mysterious object called an *ultrafilter on* I, which is best understood as a boolean algebra homomorphism $\mathfrak{P}(I) \to \{\textsc{False}, \textsc{True}\}$. Given an ultrafilter $\mathcal{U}$ on I, one can define the ultraproduct $\prod_{i\in I}^{/\mathcal{U}} M_i$, which is a new model of T. The first-order properties of $\prod_{i\in I}^{/\mathcal{U}} M_i$ are determined in a precise way by $\mathcal{U}$ and the first-order properties of the M_i, a fact called *Łoś's theorem* (Theorem 6.2.7). This can be used to produce models having desired properties. For example, we use it to give a new proof of the compactness theorem (see Theorem 6.2.14).

The actual construction of ultraproducts is a combination of products and quotients. In fact, when T is an equational class (in a functional language), the ultraproduct $\prod_{i\in I}^{/\mathcal{U}} M_i$ is literally a quotient of the product $\prod_{i\in I} M_i$. See

Remark 6.2.6.

There is also an analogue of Birkhoff's HSP theorem.

Theorem (Keisler, Shelah)**.** *Let $\mathcal{K}$ be a class of structures. Then $\mathcal{K}$ is an elementary class (axiomatized by a first-order theory) if and only if the following hold:*

1. *$\mathcal{K}$ is closed under isomorphisms.*
2. *$\mathcal{K}$ is closed under ultraproducts: if I is a set, $M_i \in \mathcal{K}$ for $i \in I$,and $\mathcal{U}$ is an ultrafilter on I, then the ultraproduct $\prod_{i\in I}^{/\mathcal{U}} M_i$ is in $\mathcal{K}$.*
3. *$\mathcal{K}$ is closed under "ultraroots": if I is a set, $\mathcal{U}$ is an ultrafilter on I, M is a structure, and the ultrapower $M^{\mathcal{U}} := \prod_{i\in I}^{/\mathcal{U}} M$ is in $\mathcal{K}$, then M itself is in $\mathcal{K}$.*

The proof of this theorem is sadly too technical to discuss here, but we do prove the following related result:

Theorem. *Let $\mathcal{K}$ be a class of structures. Then $\mathcal{K}$ is axiomatized by a universal theory if and only if $\mathcal{K}$ is closed under isomorphisms, substructures, and ultraproducts.*

Here, a *universal sentence* is a sentence of the form $\forall \bar{x}\ \varphi(\bar{x})$ with φ being quantifier-free, and a *universal theory* is a set of universal sentences. For example, equational theories are essentially universal theories.

6.1 Ultrafilters

Let I be a set.

Definition 6.1.1. A *filter* on I is a set $\mathcal{F} \subseteq \mathfrak{P}(I)$ satisfying the following:

1. If $X, Y \in \mathcal{F}$, then $X \cap Y \in \mathcal{F}$.
2. If $X \subseteq Y \subseteq I$ and $X \in \mathcal{F}$, then $Y \in \mathcal{F}$.
3. $I \in \mathcal{F}$.

A filter is *proper* if $\varnothing \notin \mathcal{F}$.

Example 6.1.2. Let I be a set. A subset $X \subseteq I$ is *cofinite* if the complement $I \backslash X$ is finite. The collection of cofinite sets forms a filter $\mathcal{F}$, called hte *Frechet filter.* The Frechet filter is proper whenever I is infinite.

Warning 6.1.3. Most authors define "filter" to mean "proper filter."

Definition 6.1.4. A family of sets $\mathcal{S} \subseteq \mathfrak{P}(I)$ has the *finite intersection property* (FIP) if for any $n \geq 0$ and $X_1, \ldots, X_n \in \mathcal{S}$, we have $\bigcap_{i=1}^n X_i \neq \varnothing$.

(When $n = 0$, $\bigcap_{i=1}^n X_i$ is defined to be I.)

Remark 6.1.5. If $\mathcal{F}$ is a proper filter, then $\mathcal{F}$ has the FIP, because $\varnothing \notin \mathcal{F}$, and $\mathcal{F}$ is closed under intersection.

Lemma 6.1.6. *If $\mathcal{S} \subseteq \mathfrak{P}(I)$ has the FIP, then there is a proper filter $\mathcal{F} \supseteq \mathcal{S}$.*

Proof. Let $\mathcal{F}$ be the set of $X \subseteq I$ such that there are $n \geq 0$ and $Y_1, \ldots, Y_n \in \mathcal{S}$ with $X \supseteq \bigcap_{i=1}^n Y_i$. Then $\mathcal{F}$ is a proper filter containing $\mathcal{S}$. □

Definition 6.1.7. An *ultrafilter* on I is a proper filter $\mathcal{U}$ such that for any $X \subseteq I$,

$$X \in \mathcal{U} \text{ or } I \setminus X \in \mathcal{U}.$$

Example 6.1.8. If $a \in I$, let $\mathcal{U}_a = \{X \subseteq I : a \in X\}$. Then $\mathcal{U}_a$ is an ultrafilter on I. Ultrafilters of this form are called *principal ultrafilters.* Non-principal ultrafilters are sometimes called *free ultrafilters.*

Lemma 6.1.9. *If $\mathcal{F}$ is a proper filter on I, then there is an ultrafilter $\mathcal{U} \supseteq \mathcal{F}$.*

Proof. By Zorn's lemma, there is a maximal proper filter $\mathcal{U} \supseteq \mathcal{F}$. We claim that $\mathcal{U}$ is an ultrafilter. Otherwise, there is $X \subseteq I$ with $X \notin \mathcal{U}$ and $I \backslash X \notin \mathcal{U}$. By maximality, $\mathcal{U} \cup \{X\}$ is not contained in a filter, and does not have FIP. Therefore there are $Y_1, \ldots, Y_n \in \mathcal{U}$ such that $X \cap \bigcap_{i=1}^n Y_i = \varnothing$. As $\mathcal{U}$ is a filter, $\mathcal{U}$ contains $Y := \bigcap_{i=1}^n Y_i$. Then $X \cap Y = \varnothing$, so $Y \subseteq I \setminus X$.

Applying the same argument to the complement of X, we get $Z \in \mathcal{U}$ with $Z \subseteq X$. Then $Y \cap Z \in \mathcal{U}$ because $\mathcal{U}$ is a filter. However, $Y \cap Z \subseteq (I \setminus X) \cap X = \varnothing$, so $\varnothing \in \mathcal{U}$ contradicting the fact that $\mathcal{U}$ is proper. □

Combining Lemmas 6.1.6 and 6.1.9, the following corollary is immediate.

Theorem 6.1.10. *If $\mathcal{S} \subseteq \mathfrak{P}(I)$ has the FIP, then $\mathcal{S}$ is contained in an ultrafilter $\mathcal{U}$ on I.*

Example 6.1.11. If I is infinite, and $\mathcal{F}$ is the Frechet filter on I (see Example 6.1.2), then $\mathcal{F}$ is proper so there is an ultrafilter $\mathcal{U}$ containing $\mathcal{F}$. We claim that $\mathcal{U}$ is non-principal (see Example 6.1.8). Otherwise, take $a \in I$ such that $\mathcal{U}$ is the principal ultrafilter $\mathcal{U}_a$. Then $I \setminus \{a\} \in \mathcal{F} \subseteq \mathcal{U}$, and $\{a\} \in \mathcal{U}_a = \mathcal{U}$, and so $\mathcal{U}$ contains the intersection

$$(I \setminus \{a\}) \cap \{a\} = \varnothing,$$

contradicting the fact that $\mathcal{U}$ is proper. Consequently, infinite sets have non-principal ultrafilters.

On the other hand, if I is finite, one can show that every ultrafilter on I is principal.

Theorem 6.1.12. *Let $\mathcal{U}$ be a subset of $\mathfrak{P}(I)$. Then $\mathcal{U}$ is an ultrafilter iff the following properties hold for $X, Y \subseteq I$:*

$$X \cap Y \in \mathcal{U} \iff (X \in \mathcal{U} \text{ and } Y \in \mathcal{U}) \tag{$\wedge$}$$

$$I \setminus X \in \mathcal{U} \iff X \notin \mathcal{U} \tag{$\neg$}$$

$$I \in \mathcal{U} \tag{1}$$

$$\varnothing \notin \mathcal{U} \tag{0}$$

$$X \cup Y \in \mathcal{U} \iff (X \in \mathcal{U} \text{ or } Y \in \mathcal{U}). \tag{$\vee$}$$

Proof. First suppose that $\mathcal{U}$ is an ultrafilter. The right-to-left direction of $(\wedge)$ holds by definition of "filter", and the left-to-right direction holds because $X \cap Y \subseteq X$ and $X \cap Y \subseteq Y$. Line $(\neg)$ says that $\mathcal{U}$ contains exactly one of X and $I \setminus X$. The definition of "ultrafilter" says that $\mathcal{U}$ contains at least one of X and $I \setminus X$. But if $\mathcal{U}$ contains *both* X and $I \setminus X$, then it contains their intersection $\varnothing$, contradicting properness. Lines (1) and (0) hold by definition of "proper filter." Finally, $(\vee)$ holds by $(\wedge)$, $(\neg)$, and de Morgan's laws:

$$\begin{aligned}
X \cup Y \in \mathcal{U} &\iff I \setminus (X \cup Y) \notin \mathcal{U} \\
&\iff (I \setminus X) \cap (I \setminus Y) \notin \mathcal{U} \\
&\iff \text{not}(I \setminus X \in \mathcal{U} \text{ and } I \setminus Y \in \mathcal{U}) \\
&\iff I \setminus X \notin \mathcal{U} \text{ or } I \setminus Y \notin \mathcal{U} \\
&\iff X \in \mathcal{U} \text{ or } Y \in \mathcal{U}.
\end{aligned}$$

Conversely, suppose the lines ($\wedge$), ($\neg$), (1), (0), and ($\vee$) hold for $\mathcal{U}$. We claim that $\mathcal{U}$ is an ultrafilter:

1. If $X, Y \in \mathcal{U}$, then $X \cap Y \in \mathcal{U}$ by ($\wedge$).
2. If $X \subseteq Y$ and $X \in \mathcal{U}$, then $Y = X \cup Y \in \mathcal{U}$ by ($\vee$).
3. $I \in \mathcal{U}$ by (1).
4. $\varnothing \notin \mathcal{U}$ by (0).
5. If $X \subseteq I$, then exactly one of X and $I \setminus X$ is in $\mathcal{U}$ by ($\neg$), and so $X \in \mathcal{U}$ or $I \setminus X \in \mathcal{U}$. □

Remark 6.1.13. If $\mathcal{U} \subseteq \mathfrak{P}(I)$ and $\mathbf{1}_{\mathcal{U}} : \mathfrak{P}(I) \to \{0, 1\}$ is the characteristic function of $\mathcal{U}$

$$\mathbf{1}_{\mathcal{U}}(X) = \begin{cases} 1 & X \in \mathcal{U} \\ 0 & X \notin \mathcal{U}, \end{cases}$$

then the conditions of Theorem 6.1.12 exactly say that $\mathbf{1}_{\mathcal{U}}$ is a boolean algebra homomorphism $\mathfrak{P}(I) \to \{0, 1\}$. For example, condition ($\wedge$) says that $\mathbf{1}_{\mathcal{U}}(X \cap Y) = \mathbf{1}_{\mathcal{U}}(X) \wedge \mathbf{1}_{\mathcal{U}}(Y)$. Consequently, ultrafilters on I correspond bijectively with boolean algebra homomorphisms $\mathfrak{P}(I) \to \{0, 1\}$.

♢ The intuition for ultrafilters

Let $\mathcal{U}$ be an ultrafilter on I. If $X \subseteq I$, we think of X being "big" if $X \in \mathcal{U}$ and "small" if $X \notin \mathcal{U}$. The following intuitive facts hold:

1. Every set $X \subseteq I$ is either big or small.
2. X is big iff the complement $I \setminus X$ is small.
3. If $X \subseteq Y$ and X is big, then Y is big.
4. If $X \subseteq Y$ and Y is small, then X is small.
5. If $X \cup Y$ is big, then X is big or Y is big.
6. If X and Y are small, then $X \cup Y$ is small.
7. If X and Y are big, then $X \cap Y$ is big.

8. $\varnothing$ is small.

9. I is big.

Each of these facts follows easily from either Theorem 6.1.12 or the definition of "ultrafilter".

If P_i is a statement for each $i \in I$, then we say that P_i holds for "most" i if

$$\{i \in I : P_i\} \in \mathcal{U},$$

that is, the set $\{i \in I : P_i\}$ is big. For example, if $\mathcal{U}$ is an ultrafilter on $I = \mathbb{N}$, then

"most $i \in \mathbb{N}$ are prime"

means that the set of prime numbers is big:

$$\{2, 3, 5, 7, \ldots\} \in \mathcal{U}.$$

Again, certain intuitive facts hold:

1. If P_i is true for every $i \in I$, then P_i is true for most $i \in I$.

2. If P_i is true for most $i \in I$, then P_i is true for some $i \in I$.

3. Exactly one of the following holds:

   - P_i is true for most $i \in I$.
   - P_i is false for most $i \in I$.

4. If P_i is true for most i and Q_i is true for most i, then $P_i \wedge Q_i$ is true for most i.

5. If P_i is true for most i, and $P_i \implies Q_i$ for all i, then Q_i is true for most i.

6. If $P_i \vee Q_i$ is true for most i, then P_i holds for most i or Q_i holds for most i (or both).

6.2 Ultraproducts via premodels

In this section, we give a simple description of ultraproducts using the "premodels" of Section 4.2. We leave some of the proofs to the following section, where we present ultraproducts via a slightly different approach that complicates the definitions but simplifies the proofs.

Let I be a set and let $\mathcal{U}$ be an ultrafilter on I. Let M_i be an $\mathcal{L}$-structure for each $i \in I$. For technical reasons, we must assume each M_i is non-empty. Let $P = \prod_{i \in I} M_i$ and let $\pi_i : P \to M_i$ be the ith coordinate projection. If f is a function symbol in $\mathcal{L}$, define f^P as if forming the product algebra (Definition 2.2.10), so that

$$f^P(c_1, \ldots, c_k) = (f^{M_i}(\pi_i(c_1), \ldots, \pi_i(c_k)) : i \in I).$$

If R is a relation symbol in $\mathcal{L}$, define

$$R^P(c_1, \ldots, c_k) \iff \{i \in I : M_i \models R(\pi_i(c_1), \ldots, \pi_i(c_k))\} \in \mathcal{U}.$$

Finally, if $c, d \in P$, define

$$c \approx d \iff \{i \in I : \pi_i(c) = \pi_i(d)\} \in \mathcal{U}.$$

Lemma 6.2.1. *The set P with the functions f^P and relations R^P and $\approx$ is an $\mathcal{L}$-prestructure (Definition 4.2.1).*

We will prove Lemma 6.2.1 in the next section.

Definition 6.2.2. The *ultraproduct* $\prod_{i \in I}^{/\mathcal{U}} M_i$ is the quotient structure $P/{\approx}$, as in Definition 4.2.2.

Definition 6.2.3. If M is an $\mathcal{L}$-structure and $\mathcal{U}$ is an ultrafilter on a set I, then the *ultrapower* $M^{\mathcal{U}}$ is the ultraproduct $\prod_{i \in I}^{/\mathcal{U}} M$, that is, the ultraproduct $\prod_{i \in I}^{\mathcal{U}} M_i$ where $M_i = M$ for all i.

Example 6.2.4. Consider $\mathbb{R}$ as a structure in the language of ordered rings $\mathcal{L} = \{+, \cdot, -, 0, 1, \leq\}$. Let $I = \mathbb{N}$ and let $\mathcal{U}$ be an ultrafilter on $\mathbb{N}$. The product $P = \prod_{i \in \mathbb{N}} \mathbb{R}$ is the power $\mathbb{R}^{\mathbb{N}}$, which can be identified with the set of ω-tuples in $\mathbb{R}$

$$(a_0, a_1, \ldots) \text{ where } a_0, a_1, \ldots \in \mathbb{R}.$$

The function symbols on $\mathbb{R}^{\mathbb{N}}$ are defined in the usual way, by coordinatewise operations:

$$\begin{aligned}(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) &= (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)\\ (a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) &= (a_0 b_0, a_1 b_1, a_2 b_2, \ldots)\\ -(a_0, a_1, a_2, \ldots) &= (-a_0, -a_1, -a_2, \ldots)\\ 0 &= (0, 0, 0, \ldots)\\ 1 &= (1, 1, 1, \ldots).\end{aligned}$$

The relations $\leq$ and $\approx$ are defined using $\mathcal{U}$:

$$\begin{aligned}\bar{a} \leq \bar{b} &\iff \{i \in I : a_i \leq b_i\} \in \mathcal{U}\\ \bar{a} \approx \bar{b} &\iff \{i \in I : a_i = b_i\} \in \mathcal{U}.\end{aligned}$$

Intuitively, $\bar{a} \approx \bar{b}$ if $a_i = b_i$ for "most" i.

Lemma 6.2.1 says that $(\mathbb{R}^{\mathbb{N}}, +, \cdot, -, 0, 1, \leq, \approx)$ is a premodel, and the ultrapower $\mathbb{R}^{\mathcal{U}}$ is defined to be the quotient structure $\mathbb{R}^{\mathbb{N}}/\approx$. Thus, elements of $\mathbb{R}^{\mathcal{U}}$ are $\approx$-equivalence classes $[\bar{a}]$ with $\bar{a} \in \mathbb{R}^{\mathbb{N}}$, and the functions and relations are defined by

$$\begin{aligned}[][\bar{a}] + [\bar{b}] = [\bar{a} + \bar{b}] &= [(a_0 + b_0, a_1 + b_1, \ldots)]\\ &\cdots\\ [\bar{a}] \leq [\bar{b}] &\iff \{i \in \mathbb{N} : a_i \leq b_i\} \in \mathcal{U}.\end{aligned}$$

Suppose we took $\mathcal{U}$ extending the Frechet filter, as in Example 6.1.11. Let $\omega = [(0, 1, 2, 3, \ldots)] \in \mathbb{R}^{\mathcal{U}}$. Then

$$1 + 1 = [(1 + 1, 1 + 1, \ldots)] \leq [(0, 1, 2, 3, \ldots)] = \omega$$

because $1 + 1 \leq i$ for "most" values of $i \in \mathbb{N}$. A similar argument shows that

$$\mathbb{R}^{\mathcal{U}} \models \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} \leq \omega$$

for each n. No element of $\mathbb{R}$ has this property, so $\mathbb{R}^{\mathcal{U}} \not\cong \mathbb{R}$. But we will see shortly that $\mathbb{R}^{\mathcal{U}} \equiv \mathbb{R}$.

Remark 6.2.5. The ring $\mathbb{R}^{\mathcal{U}}$ is important in non-standard analysis, where it is called the ring of *hyperreal numbers.*

Remark 6.2.6. When $\mathcal{L}$ is a functional language as in Chapters 1–2, ultraproducts can be easily defined in terms of product and quotient algebras. Specifically, the ultraproduct $\prod_{i \in I}^{/\mathcal{U}} M_i$ can be constructed by first forming the product algebra $P = \prod_{i \in I} M_i$ as in Definition 2.2.10, and then forming the quotient algebra $P/{\approx}$ as in Theorem 2.4.11, where $\approx$ is the congruence defined as follows:

$$\bar{a} \approx \bar{b} \iff \{i \in I : a_i = b_i\} \in \mathcal{U}.$$

When all the M_i are rings, the corresponding ideal $J \subseteq P$ is defined by

$$\begin{aligned} \bar{a} \in J &\iff \{i \in I : a_i = 0\} \in \mathcal{U} \\ &\iff \{i \in I : a_i \neq 0\} \notin \mathcal{U}. \end{aligned}$$

The second equivalence holds by Theorem 6.1.12. The set $\{i \in I : a_i \neq 0\}$ is the "support" of $\bar{a}$, so we can think of J as the set of tuples $\bar{a} \in P$ with "small support." Then the ultraproduct is the quotient ring P/J.

The key property of ultraproducts is the following fact

Theorem 6.2.7 (Łoś's theorem). *Let M be a ultraproduct $\prod_{i \in I}^{/\mathcal{U}} M_i$.*

1. *If φ is an $\mathcal{L}$-sentence, then*

$$M \models \varphi \iff \{i \in I : M_i \models \varphi\} \in \mathcal{U}.$$

2. *More generally, if $\varphi(x_1, \ldots, x_n)$ is an $\mathcal{L}$-sentence and $a_1, \ldots, a_n \in P$, then*

$$M \models \varphi([a_1], \ldots, [a_n]) \iff \{i \in I : M_i \models \varphi(\pi(a_1), \ldots, \pi(a_n))\} \in \mathcal{U}.$$

Again, we defer the proof to the next section. Note that (1) is the $n = 0$ case of (2).

Example 6.2.8. Part (2) of Łoś's theorem might be hard to parse, so here is a concrete example. Consider the ring $\mathbb{Z}$ and the ultrapower $\mathbb{Z}^{\mathcal{U}}$ for some ultrafilter $\mathcal{U}$ on $\mathbb{N}$. Let $\varphi(x, y)$ be the formula saying that x divides y:

$$\exists z : xz = y.$$

If $\bar{a}, \bar{b}$ are two tuples in $\mathbb{Z}^{\mathbb{N}}$, then Łoś's theorem says

$$\mathbb{Z}^{\mathcal{U}} \models \varphi([\bar{a}], [\bar{b}]) \iff \{i \in \mathbb{N} : \mathbb{Z} \models \varphi(a_i, b_i)\} \in \mathcal{U}.$$

That is, $[\bar{a}]$ divides $[\bar{b}]$ in the ring $\mathbb{Z}^{\mathcal{U}}$ if and only if a_i divides b_i in $\mathbb{Z}$ for "most" $i \in I$.

Example 6.2.9. Consider the ultrapower $\mathbb{R}^{\mathcal{U}}$ as in Example 6.2.4. Note that $M_i = \mathbb{R}$ for every i, and so

$$\{i \in \mathbb{N} : M_i \models \varphi\} = \begin{cases} \mathbb{N} & \text{if } \mathbb{R} \models \varphi \\ \varnothing & \text{if } \mathbb{R} \not\models \varphi. \end{cases}$$

Then Łoś's theorem says that $\mathbb{R}^{\mathcal{U}} \models \varphi \iff \mathbb{R} \models \varphi$.

For example, suppose φ is the sentence

$$\forall x\ \exists y\ (y^2 = x \vee y^2 = -x).$$

Note that $\mathbb{R}$ satisfies φ, but the power $\mathbb{R}^{\mathbb{N}}$ does *not* satisfy φ—take $x = (1, -1, 0, 0, 0, \ldots)$. Nevertheless, the ultraproduct $\mathbb{R}^{\mathcal{U}}$ satisfies φ. This can be seen directly, without using Łoś's theorem, as follows. Let $x = [(a_0, a_1, a_2, \ldots)]$ be given. Note that

$$\{i \in \mathbb{N} : a_i \geq 0\} \cup \{i \in \mathbb{N} : a_i \leq 0\} = \mathbb{N} \in \mathcal{U},$$

and so one of the two sets is in $\mathcal{U}$. There are two cases:

Case 1: $\{i \in \mathbb{N} : a_i \geq 0\} \in \mathcal{U}$. For $i \in \mathbb{N}$ let

$$b_i = \begin{cases} \sqrt{a_i} & \text{if } a_i \geq 0 \\ 0 & \text{if } a_i < 0, \end{cases}$$

and let $y = [\bar{b}] = [(b_0, b_1, b_2, \ldots)]$. Then $b_i^2 = a_i$ for "most" $i \in \mathbb{N}$, so $y^2 = x$.

Case 2: $\{i \in \mathbb{N} : a_i \leq 0\} \in \mathcal{U}$. Define

$$b_i = \begin{cases} 0 & \text{if } a_i > 0 \\ \sqrt{-a_i} & \text{if } a_i \leq 0 \end{cases}$$

and show similarly that $[\bar{b}]^2 = -x$.

Next we discuss some consequences of Łoś's theorem. First, we see that an ultraproduct of models of T is a model of T:

Theorem 6.2.10. *Let I be a set, $\mathcal{U}$ be an ultrafilter on I, M_i be an $\mathcal{L}$-structure for $i \in I$, and M be the ultraproduct $\prod_{i \in I}^{/\mathcal{U}} M_i$.*

1. *Let T be a theory. If $M_i \models T$ for all i, then $M \models T$.*

2. *Let $\mathcal{K}$ be an elementary class. If $M_i \in \mathcal{K}$ for all i, then $M \in \mathcal{K}$.*

Proof. (1) follows from Łoś's theorem: if $\varphi \in T$, then

$$\{i \in I : M_i \models \varphi\} = I \in \mathcal{U},$$

so $M \models \varphi$. (2) is a restatement of (1). □

Theorem 6.2.10 is analogous to the fact for *equational* theories that a product of models is a model (Theorem 2.2.12).

Example 6.2.11. An ultraproduct of fields is a field.

Next, we see that ultrapowers give elementary extensions.

Theorem 6.2.12. *Let $\Delta : M \to M^{\mathcal{U}}$ be the diagonal map sending $a \in M$ to the class of the tuple $(a : i \in I) \in M^I = \prod_{i \in I} M$. Then Δ is an elementary embedding.*

Proof. Fix a formula $\varphi(x_1, \ldots, x_n)$ and a tuple $\bar{a} = (a_1, \ldots, a_n) \in M^n$. Let $S = \{i \in I : M \models \varphi(a_1, \ldots, a_n)\}$. By Łoś's theorem,

$$M^{\mathcal{U}} \models \varphi(\Delta(a_1), \ldots, \Delta(a_n)) \iff S \in \mathcal{U}.$$

But

$$S = \begin{cases} I & \text{if } M \models \varphi(\bar{a}) \\ \varnothing & \text{if } M \not\models \varphi(\bar{a}). \end{cases}$$

Therefore $S \in \mathcal{U} \iff M \models \varphi(\bar{a})$, and

$$M^{\mathcal{U}} \models \varphi(\Delta(\bar{a})) \iff M \models \varphi(\bar{a}).$$ □

Consequently, we can regard $M^{\mathcal{U}}$ as an elementary extension of M, up to isomorphism.

Example 6.2.13. If $\mathcal{U}$ is a non-principal ultrafilter on $\mathbb{N}$, then the hyperreal numbers $\mathbb{R}^{\mathcal{U}}$ are an elementary extension of $\mathbb{R}$, via the elementary embedding

$$x \mapsto [(x, x, x, \ldots)]$$

The elementary extension is a proper elementary extension, because the hyperreal number $\omega = [(0, 1, 2, \ldots)]$ of Example 6.2.4 is greater than every finite natural number, hence does not equal any standard real number in $\mathbb{R}$.

Lastly, we use Łoś's theorem to give another proof of the compactness theorem (Theorem 4.4.5). If $\mathcal{K}$ is a class of $\mathcal{L}$-structures and T is an $\mathcal{L}$-theory, say that T is *finitely satisfiable in* $\mathcal{K}$ if for any finite subtheory $T_0 \subseteq_f T$ there is $M \in \mathcal{K}$ satisfying T_0.

Theorem 6.2.14. *If T is finitely satisfiable in $\mathcal{K}$, then there is an ultraproduct M of structures in $\mathcal{K}$ such that $M \models T$.*

Proof. Let $\{M_i\}_{i \in I}$ be a small collection of structures in $\mathcal{K}$ containing at least one representative from every elementary equivalence class. If φ is an $\mathcal{L}$-sentence, let $[\![\varphi]\!] = \{i \in I : M_i \models \varphi\}$. Let $\mathcal{F} = \{[\![\varphi]\!] : \varphi \in T\}$. We claim that $\mathcal{F}$ has the FIP. Indeed, if $\varphi_1, \ldots, \varphi_n \in T$ then there is some M_i satisfying $\bigwedge_{j=1}^n \varphi_j$, and then $i \in \bigcap_{j=1}^n [\![\varphi_j]\!]$.

Because $\mathcal{F}$ has the FIP, it is contained in an ultrafilter $\mathcal{U}$ on I (Theorem 6.1.10). Let $M = \prod_{i \in I}^{/\mathcal{U}} M_i$. Then for $\varphi \in T$ we have

$$\{i \in I : M_i \models \varphi\} = [\![\varphi]\!] \in \mathcal{F} \subseteq \mathcal{U},$$

and so $M \models \varphi$ by Łoś's theorem. □

Taking $\mathcal{K}$ to be the class of *all* structures, we get the compactness theorem.

6.3 Ultraproducts via the witness property

In this section, we give an alternative exposition of ultraproducts using the witness property (see Definition 4.3.1). With this approach, the definitions are a more opaque, but the proofs are simpler. We will see that two definitions of "ultraproduct" agree, while also proving Lemma 6.2.1 and Theorem 6.2.7.

As in the previous section, let I be a set and let $\mathcal{U}$ be an ultrafilter on I. Let M_i be a non-empty $\mathcal{L}$-structure for each $i \in I$. Let $P = \prod_{i \in I} M_i$ and let $\pi_i : P \to M_i$ be the ith coordinate projection.

Let $\mathcal{L}(P)$ be $\mathcal{L}$ with a new constant symbol added for each $a \in P$. Regard M_i as an $\mathcal{L}(P)$-structure by interpreting $a \in P$ as $\pi_i(a) \in M_i$.

For any $\mathcal{L}(P)$-sentence φ, let $[\![\varphi]\!] = \{i \in I : M_i \models \varphi\}$. Note the following:

$$[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$$
$$[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!]$$
$$[\![\neg\varphi]\!] = I \setminus [\![\varphi]\!]$$

Lemma 6.3.1. *Let T be the set of $\mathcal{L}(P)$-sentences φ such that $[\![\varphi]\!] \in \mathcal{U}$. Then T is finitely satisfiable and complete and has the witness property over P in the sense of Definition 4.3.8.*

Proof. For finite satisfiability, suppose $\varphi_1, \ldots, \varphi_n \in T$. If $S = [\![\bigwedge_{i=1}^n \varphi_i]\!] = \bigcap_{i=1}^n [\![\varphi_i]\!]$, then $S \in \mathcal{U}$ so $S \neq \varnothing$. Taking $i \in S$, we have $M_i \models \bigwedge_{i=1}^n \varphi_i$.

For completeness, note that $[\![\varphi]\!]$ and $[\![\neg\varphi]\!]$ are complementary, so one of them is in $\mathcal{U}$, and therefore one of φ and $\neg\varphi$ is in T.

For the witness property, suppose $\exists x\ \varphi(x)$ is in T, meaning that $S := [\![\exists x\ \varphi(x)]\!] \in \mathcal{U}$. Define $c = (c_i : i \in I) \in P$ as follows:

1. If $i \in S$, then $M_i \models \exists x \varphi(x)$. Choose $c_i \in M_i$ so that $M_i \models \varphi(c_i)$.
2. If $i \notin S$, take any $c_i \in M_i$.

Then $i \in S \implies M_i \models \varphi(c)$, so $[\![\varphi(c)]\!] \supseteq S$. It follows that $[\![\varphi(c)]\!] \in \mathcal{U}$ and $\varphi(c) \in T$. □

By Definition 4.3.7 and Theorem 4.3.9, we can talk about the canonical model of T—the unique model in which every element is named by an element of P.

Definition 6.3.2. The *ultraproduct* $\prod_{i \in I}^{/\mathcal{U}} M_i$ is the canonical model of T.

Theorem 6.3.3. *Let $P = \prod_{i \in I} M_i$, let $M = \prod_{i \in I}^{/\mathcal{U}} M_i$, and let $[c]$ be the element of M named by $c \in P$.*

1. *Every element of M has the form $[c]$ for some $c \in P$.*
2. *$[c] = [d]$ if and only if $\{i \in I : \pi_i(c) = \pi_i(d)\} \in \mathcal{U}$.*
3. *Let R be a k-ary relation symbol. Then*
$$R^M([c_1], \ldots, [c_k]) \iff \{i \in I : M_i \models R(\pi_i(c_1), \ldots, \pi_i(c_k))\} \in \mathcal{U}.$$
4. *If f is a k-ary function symbol, then*
$$f^M([c_1], \ldots, [c_k]) = [f^P(c_1, \ldots, c_k)],$$
where P is given the product structure so that
$$f^P(c_1, \ldots, c_k) = (f^{M_i}(\pi_i(c_1), \ldots, \pi_i(c_k)) : i \in I).$$

5. *If $\varphi(x_1, \ldots, x_n)$ is an $\mathcal{L}$-formula, then*

$$M \models \varphi([c_1], \ldots, [c_n]) \iff \{i \in I : M_i \models \varphi(\pi_i(c_1), \ldots, \pi_i(c_n))\} \in \mathcal{U}.$$

Proof. Part (1) is true by construction, as M is the canonical model of T. Part (5) is also true by construction:

$$\begin{aligned} M \models \varphi([c_1], \ldots, [c_n]) &\iff M \models \varphi(c_1, \ldots, c_n) \iff \varphi(c_1, \ldots, c_n) \in T \\ &\iff [\![\varphi(c_1, \ldots, c_n)]\!] \in \mathcal{U} \\ &\iff \{i \in I : M_i \models \varphi(\pi_i(c_1), \ldots, \pi_i(c_n))\} \in \mathcal{U}. \end{aligned}$$

Remember that a constant symbol $c \in P$ is interpreted as $[c]$ in M, and $\pi_i(c)$ in M_i.

Parts (2) and (3) follow by specializing part (5) to atomic formulas $x = y$ and $R(x_1, \ldots, x_k)$. It remains to prove part (4). Fix $c_1, \ldots, c_k \in P$ and let $d = f^P(c_1, \ldots, c_k)$. Then $\pi_i(d) = f^{M_i}(\pi_i(c_1), \ldots, \pi_i(c_k))$ for each $i \in I$. Then

$$\{i \in I : M_i \models \pi_i(d) = f(\pi_i(c_1), \ldots, \pi_i(c_k))\} = I \in \mathcal{U},$$

so by part (5), we have

$$M \models [d] = f([c_1], \ldots, [c_k]),$$

which means that $f^M([c_1], \ldots, [c_k]) = [d] = [f^P(c_1, \ldots, c_k)]$. □

From Theorem 6.3.3, one can see that the definition of "ultraproduct" in this section agrees with the definition in the previous section, and Lemma 6.2.1 and Theorem 6.2.7 hold.

In more detail, first verify Lemma 6.2.1 as follows:

1. Part (2) shows that the relation

$$c \approx d \iff \{i \in I : \pi_i(c) = \pi_i(d)\} \in \mathcal{U}$$

is an equivalence relation, since it is equivalent to $[c] = [d]$ in M.

2. Parts 2 and 4 show that $\approx$ is compatible with f^P, because if

$$c_i \approx d_i \text{ for } 1 \leq i \leq k,$$

then

$$\begin{gathered}
[c_i] = [d_i] \text{ for } 1 \leq i \leq k \\
f^M([c_1], \ldots, [c_k]) = f^M([d_1], \ldots, [d_k]) \\
[f^P(c_1, \ldots, c_k)] = [f^P(d_1, \ldots, d_k)] \\
f^P(c_1, \ldots, c_k) \approx f^P(d_1, \ldots, d_k).
\end{gathered}$$

3. Similarly, Parts 2 and 3 show that $\approx$ is compatible with R^P.

Define the quotient structure $P/\approx$ as in the previous section. Then parts (1)–(4) show that there is an isomorphism $P/\approx \to M$ sending the class of c in $P/\approx$ to the class of c in M. Consequently, the two definitions of "ultraproduct" agree, up to isomorphism. Finally, Łoś's theorem (Theorem 6.2.7) is a restatement of part (5) of Theorem 6.3.3.

Remark 6.3.4. One can also prove Lemma 6.2.1 and Theorem 6.2.7 directly from the definitions, but the proof is somewhat repetitive and tedious. I believe that the approach using the witness property helps clarify the underlying reason why everything works.

6.4 ♢ Pseudo-finite fields from ultraproducts

The *theory of finite fields* is the set T of sentences φ in the language of rings such that every finite field satisfies φ. For example, if K is a finite field then one can show that the map $f : K \to K$ given by

$$f(x) = x^3 - x = x(x-1)(x-2)$$

is not surjective, using the fact that $f(0) = f(1)$. Consequently, T contains the sentence

$$\exists x \; \forall y : y^3 - y \neq x. \tag{$*$}$$

The theory of finite fields was one of the examples listed in Section 3.10.

Now let $I = \{2, 3, 5, 7, \ldots\}$. Take an ultrafilter $\mathcal{U}$ on I extending the Frechet filter, and consider the ultraproduct

$$K = \prod_{p \in I}^{/\mathcal{U}} (\mathbb{Z}/p\mathbb{Z}).$$

Each $\mathbb{Z}/p\mathbb{Z}$ is a field (Theorem 2.5.7), so the ultraproduct K is also a field. Moreover, each $\mathbb{Z}/p\mathbb{Z}$ is a model of T, so $K \models T$. However, K is not finite. To see this, let φ_n be the sentence $\exists^{\geq n} x : \top$ saying that there are at least n distinct values. Then

$$\mathbb{Z}/p\mathbb{Z} \models \varphi_n \iff |\mathbb{Z}/p\mathbb{Z}| \geq n \iff p \geq n.$$

The set of primes $\geq n$ is in the Frechet filter, so it is "big" with respect to $\mathcal{U}$, and Łoś's theorem shows that the ultraproduct K satisfies φ_n. Thus $|K| \geq n$ for every finite n, and K is infinite.

In summary, K is an infinite model of the theory of finite fields. Such fields are called *pseudo-finite fields*. No common examples of fields are pseudo-finite. For example, $\mathbb{R}$ and $\mathbb{C}$ fail to satisfy the sentence $(*)$ above, and $\mathbb{Q}$ fails a more complicated sentence.

Remark 6.4.1. Up to elementary equivalence, all pseudo-finite fields arise as ultraproducts of finite fields. That is, if K is a pseudo-finite field, then $K \equiv \prod_{i \in I}^{/\mathcal{U}} F_i$ for some $I, \mathcal{U}$, and family of finite fields F_i. This can be seen by applying Theorem 6.2.14 to the complete theory $\mathrm{Th}(K)$ and the class of finite fields. If $\mathrm{Th}(K)$ fails to be finitely satisfiable in the class of finite fields, it must be because $K \models \varphi$ but no finite field satisfies φ. Then $\neg\varphi$ is part of the theory of finite fields, and so $K \models \neg\varphi$, contradicting pseudo-finiteness.

6.5 Characterizations of elementary classes

Lemma 6.5.1. *If M_1 and M_2 are elementarily equivalent, then there is an elementary embedding from M_2 to an ultrapower $M_1^{\mathcal{U}}$.*

Proof. In the proof of elementary amalgamation, we saw that $\mathrm{eldiag}(M_2)$ is finitely satisfiable in expansions of M_1 to $\mathcal{L}(M_2)$-structures (Lemma 5.2.6). By Theorem 6.2.14, there is an ultraproduct $N = \prod_{i \in I}^{/\mathcal{U}} N_i$ satisfying $\mathrm{eldiag}(M_2)$, where each N_i is an expansion of M_1 to an $\mathcal{L}(M_2)$-structure. The fact that $N \models \mathrm{eldiag}(M_2)$ gives an elementary embedding $M_2 \to N$. On the other hand, $N \restriction \mathcal{L}$ is

$$\prod_{i \in I}^{/\mathcal{U}} (N_i \restriction \mathcal{L}) = \prod_{i \in I}^{/\mathcal{U}} M_1 = M_1^{\mathcal{U}},$$

and we have the desired elementary embedding $M_2 \to M_1^{\mathcal{U}}$. □

Theorem 6.5.2. *A class $\mathcal{K}$ of $\mathcal{L}$-structures is elementary iff $\mathcal{K}$ is closed under ultraproducts, isomorphisms, and elementary substructures.*

Proof. Suppose $\mathcal{K}$ is closed under ultraproducts, isomorphisms, and elementary substructures.

Claim. $\mathcal{K}$ is closed under elementary equivalence: if $M \equiv N$ and $M \in \mathcal{K}$ then $N \in \mathcal{K}$.

Proof. By Lemma 6.5.1, there is an ultrapower $M^{\mathcal{U}}$ and an elementary embedding $f : N \to M^{\mathcal{U}}$. Then $N \cong \operatorname{im}(f) \preceq M^{\mathcal{U}}$, so

$$M \in \mathcal{K} \implies M^{\mathcal{U}} \in \mathcal{K} \implies \operatorname{im}(f) \in \mathcal{K} \implies N \in \mathcal{K}. \qquad \square_{\text{Claim}}$$

Let T be the set of all sentences φ such that every $N \in \mathcal{K}$ satisfies φ. Then $\mathcal{K} \subseteq \operatorname{Mod}(T)$. We claim that $\mathcal{K} = \operatorname{Mod}(T)$. Fix $M \in \operatorname{Mod}(T)$; we claim that $M \in \mathcal{K}$. Break into two cases:

1. $\operatorname{Th}(M)$ is finitely satisfiable in $\mathcal{K}$. By Theorem 6.2.14, there is a model $N \models \operatorname{Th}(M)$ such that N is an ultraproduct of structures in $\mathcal{K}$. By assumption, $N \in \mathcal{K}$. The fact that $N \models \operatorname{Th}(M)$ means that $N \equiv M$ (Theorem 3.4.9), and so $M \in \mathcal{K}$.

2. $\operatorname{Th}(M)$ is not finitely satisfiable in $\mathcal{K}$. Then there is $\varphi \in \operatorname{Th}(M)$ such that no $N \in \mathcal{K}$ satisfies φ. Then every $N \in \mathcal{K}$ satisfies $\neg\varphi$, so $\neg\varphi \in T$ and $M \models \neg\varphi$, contradicting the fact that $\varphi \in \operatorname{Th}(M)$. □

Fact 6.5.3 (Keisler-Shelah)**.** *If $M \equiv N$, then there is a set I and an ultrafilter $\mathcal{U}$ on I such that the ultraproducts $M^{\mathcal{U}}$ and $N^{\mathcal{U}}$ are isomorphic.*

Definition 6.5.4. A structure M is an *ultraroot* of a structure N if N is an ultrapower of M. A class $\mathcal{K}$ is *closed under ultraroots* if $M^{\mathcal{U}} \in \mathcal{K} \implies M \in \mathcal{K}$.

If M is an ultraroot of N, then $N \succeq M$, so $N \equiv M$. Therefore, elementary classes are closed under ultraroots.

Theorem 6.5.5. *A class $\mathcal{K}$ is elementary iff $\mathcal{K}$ is closed under ultraproducts, ultraroots, and isomorphisms.*

Proof. Suppose $\mathcal{K}$ is closed under ultraproducts, ultraroots, and isomorphisms. By the Keisler-Shelah theorem, $\mathcal{K}$ is closed under elementary equivalence. Then the proof of Theorem 6.5.2 applies. □

6.6 Universal classes

Lemma 6.6.1 (Lemma on constants)**.** *Let $\bar{c} = (c_1, \ldots, c_n)$ be a tuple of constant symbols not appearing in T. If $T \vdash \varphi(\bar{c})$, then $T \vdash \forall \bar{x}\ \varphi(\bar{x})$.*

Proof. Otherwise, there is $M \models T$ with $M \not\models \forall \bar{x}\ \varphi(\bar{x})$. Take $\bar{a} \in M$ with $M \models \neg\varphi(\bar{a})$. Interpreting $\bar{c}$ as $\bar{a}$, we get a model of $T \cup \{\neg\varphi(\bar{c})\}$, contradicting $T \vdash \varphi(\bar{c})$. □

A *universal formula* or *∀-formula* is one of the form $\forall \bar{y} : \varphi(\bar{x}, \bar{y})$ where φ is quantifier-free. A *universal theory* is a set of universal sentences.

Lemma 6.6.2. *If T is a universal theory, and $M \models T$, then any substructure of M is a model of T.*

Proof. Let ψ be a sentence in T. We can write ψ as $\forall \bar{x} : \varphi(\bar{x})$ where φ is quantifier-free. Let N be a substructure of M. If $\bar{a} \in N$, then

$$M \models \forall \bar{x} : \varphi(\bar{x}) \implies M \models \varphi(\bar{a}) \implies N \models \varphi(\bar{a}),$$

where the second implication holds because $\varphi(\bar{x})$ is quantifier-free (see Remark 3.5.4). As this holds for any $\bar{a} \in N$, we have $N \models \forall \bar{x} : \varphi(\bar{x})$. □

If T is a theory, then $T_\forall$ denotes the set of universal sentences φ such that $T \vdash \varphi$.

Theorem 6.6.3. *$M \models T_\forall$ if and only if M is a substructure of a model of T.*

Proof. First suppose M is a substructure of $N \models T$. Then $N \models T_\forall$, so $M \models T_\forall$ as $T_\forall$ is a universal theory.

Conversely, suppose $M \models T_\forall$. Break into two cases:

1. The $\mathcal{L}(M)$-theory $\operatorname{diag}(M) \cup T$ is consistent. Take a model N. Moving N by an isomorphism, we may assume that N is an extension of M, and $N \models T$. Then we are done.

2. $\operatorname{diag}(M) \cup T$ is inconsistent. By compactness, there is a finite tuple $\bar{a} \in M$ and a quantifier-free formula $\varphi(\bar{a}) = \bigwedge_{i=1}^{n} \varphi_i(\bar{a})$ with $\varphi_i(\bar{a}) \in \operatorname{diag}(M)$ such that $\{\varphi(\bar{a})\} \cup T$ is inconsistent. Then $T \vdash \neg\varphi(\bar{a})$, so $T \vdash \forall \bar{x}\ \neg\varphi(\bar{x})$ by the lemma on constants (Lemma 6.6.1). But then

$$(\forall \bar{x}\ \neg\varphi(\bar{x})) \in T_\forall,$$

so $M \models \forall \bar{x}\ \neg\varphi(\bar{x})$, contradicting the fact that $M \models \varphi(\bar{a})$. □

Theorem 6.6.4. *Let T be a theory. Then T is axiomatizable by universal sentences if and only if* $\mathrm{Mod}(T)$ *is closed under substructures.*

Proof. If T is axiomatizable by universal sentences, then $\mathrm{Mod}(T)$ is closed under substructures by Lemma 6.6.2.

Next suppose that $\mathrm{Mod}(T)$ is closed under substructures. We claim that $T_\forall$ axiomatizes T. Certainly $M \models T \implies M \models T_\forall$. Conversely, suppose $M \models T_\forall$. By Theorem 6.6.3 there is an extension $N \supseteq M$ with $N \models T$. By the assumption on T, $M \models T$. □

Theorem 6.6.5. *Let $\mathcal{K}$ be a class of structures. Then the following are equivalent:*

1. *$\mathcal{K}$ is axiomatized by a universal theory.*

2. *$\mathcal{K}$ is closed under isomorphism, substructures, and ultraproducts.*

Proof. (1) $\implies$ (2) is clear.

(2) $\implies$ (1): by Theorem 6.5.2, $\mathcal{K}$ is an elementary class. Then use Theorem 6.6.4. □

Chapter 7

Topologies

This chapter is a digression into point-set topology, which will play an important role in the chapters ahead. In Section 7.1, we review the basic definitions of topological spaces, continuity, compactness, and Hausdorffness; this section can be skipped if you have ever studied topology. Section 7.2 is about the specialized topic of *ultralimits*, a variant of limits which completes the analogy

metric spaces : limits of sequences :: topological spaces : ultralimits.

(If you've studied point set topology before, ultralimits are similar to nets or filters, though better behaved in some ways.) We use ultralimits to give unusual proofs of some basic facts about compact Hausdorff spaces.

We apply point-set topology to model theory in Section 7.3, where we build a topology on the set S of complete theories (in a fixed language $\mathcal{L}$). The compactness theorem can be seen as a statement that this topological space is compact, and ultraproducts correspond to ultralimits in this space. The construction of the topological space S works in a more general abstract setting, which we describe in Section 7.4. This abstract generalization will be used later when we consider spaces of types and quantifier-free types in the next chapter.

7.1 Topological spaces

Fix a set S.

Definition 7.1.1. A family of sets $\mathcal{F} \subseteq \mathfrak{P}(S)$ is *closed under infinite unions* if whenever I is a set and $X_i \in \mathcal{F}$ for all $i \in I$, we have $\bigcup_{i \in I} X_i \in \mathcal{F}$. We say that $\mathcal{F} \subseteq \mathfrak{P}(S)$ is *closed under finite unions* if this holds for finite I.

Remark 7.1.2. The definition of "*closed under (in)finite intersections*" is similar, with fine print. We understand $\bigcap_{i \in I} X_i$ to mean

$$\{x \in S : \forall i \in I \ x \in X_i\}$$

Consequently, when $I = \varnothing$, the intersection $\bigcap_{i \in I} X_i$ is defined to be S, and not the set-theoretic universe, for example.

Definition 7.1.3. A *metric space* is a set S and function $d : S^2 \to \mathbb{R}$ satisfying the axioms:

1. $d(x, y) \geq 0$
2. $d(x, y) = d(y, x)$
3. $d(x, y) = 0 \iff x = y$.
4. $d(x, z) \leq d(x, y) + d(y, z)$.

Example 7.1.4. $\mathbb{R}^2$ is a metric space with respect to the metric

$$d((x_1, y_1), (x_2, y_2)) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}.$$

Fix a metric space (S, d). An *open ball* is a set of the form

$$B_\epsilon(p) = \{x \in S : d(x, p) < \epsilon\}$$

for some $p \in S$ and $\epsilon > 0$. A set $X \subseteq S$ is *open* if for every $p \in X$, there is $\epsilon > 0$ such that $B_\epsilon(p) \subseteq X$.

Fact 7.1.5. *Let (S, d) be a metric space.*

1. *Every open ball is open.*
2. *The collection of open sets is closed under infinite unions and finite intersections.*

Definition 7.1.6. A *topology* on S is a family of sets τ closed under finite intersections and infinite unions. A *topological space* is a set S with a topology τ.

Fix a topological space (S, τ).

Definition 7.1.7. A set $X \subseteq S$ is *open* if $X \in \tau$ and *closed* if $S \setminus X$ is open.

Fact 7.1.8. *In a metric space, a set X is closed if and only if it "closed under limits" in the sense that:*

$$\left(b_1, b_2, \ldots \in X \text{ and } \lim_{i \to \infty} b_i = a\right) \implies a \in X.$$

Definition 7.1.9. A topological space S is *Hausdorff* if for any $a_1 \neq a_2$ in S, there are open sets $U_i \ni a_i$ with $U_1 \cap U_2 = \varnothing$.

Remark 7.1.10. Metric spaces are Hausdorff: if $a_1 \neq a_2$, then $B_\epsilon(a_1) \cap B_\epsilon(a_2) = \varnothing$ for $\epsilon = d(a_1, a_2)/3$.

Theorem 7.1.11. *If S is Hausdorff and $p \in S$, then $\{p\}$ is closed.*

Proof. For every $q \neq p$, take open sets U_q, V_q with $q \in U_q$, $p \in V_q$, and $U_q \cap V_q = \varnothing$. In particular, $q \in U_q$ and $p \notin U_q$ for each $q \neq p$. Then $S \setminus \{p\}$ is the open set $\bigcup_{q \neq p} U_q$. □

Definition 7.1.12. An *open cover* is a collection $\mathcal{C}$ of open sets with $\bigcup \mathcal{C} = S$. A *subcover* of $\mathcal{C}$ is another open cover $\mathcal{C}' \subseteq \mathcal{C}$.

Definition 7.1.13. A topological space S is *compact* if every open cover has a finite subcover.

Fact 7.1.14. *A metric space (S, d) is compact if and only if every sequence has a convergent subsequence: for any $a_1, a_2, a_3, \ldots \in S$, there is a subsequence*

$$a_{i_1}, a_{i_2}, a_{i_3}, \ldots$$

(with $i_1 < i_2 < \cdots$) such that $\lim_{n \to \infty} a_{i_n}$ exists.

Theorem 7.1.15. *If a topological space S is compact and $\mathcal{F}$ is a family of closed sets with the FIP, then $\bigcap \mathcal{F} \neq \varnothing$. Conversely, this property characterizes compactness.*

Proof. Let X_i be open for $i \in I$, and let Y_i be the complementary closed sets. We claim that the following are equivalent:

1. If $\bigcup_{i \in I} X_i = S$, then there is $I_0 \subseteq_f I$ with $\bigcup_{i \in I_0} X_i = S$.

2. If $\bigcap_{i \in I} Y_i = \varnothing$, then there is $I_0 \subseteq_f I$ with $\bigcap_{i \in I_0} Y_i = \varnothing$.

3. If $\bigcap_{i \in I_0} Y_i \neq \varnothing$ for every $I_0 \subseteq_f I$, then $\bigcap_{i \in I} Y_i \neq \varnothing$.

Indeed, (1) and (2) are equivalent by de Morgan's laws, and (2) and (3) are contrapositives. Finally, observe that (1) is the definition of compactness, and (3) says that if $\{Y_i\}_{i \in I}$ has FIP then $\bigcap_i Y_i \neq \varnothing$. □

Definition 7.1.16. Let S_1, S_2 be two topological spaces and $f : S_1 \to S_2$ be a function. Then f is *continuous* if for every open set $U \subseteq S_2$, the preimage $f^{-1}(U)$ is open in S_1.

Fact 7.1.17. *If S_1, S_2 are metric spaces, a function $f : S_1 \to S_2$ is continuous iff f "preserves limits", in the sense that*

$$\lim_{i \to \infty} b_i = a \implies \lim_{i \to \infty} f(b_i) = f(a).$$

Definition 7.1.18. A function $f : S_1 \to S_2$ is a *homeomorphism* if f is continuous, f is a bijection, and $f^{-1} : S_2 \to S_1$ is continuous. Two topological spaces S_1, S_2 are *homeomorphic* if there is a homeomorphism from S_1 to S_2.

7.2 Ultralimits

Definition 7.2.1. If I is a set, $a_i \in S$ for $i \in I$, $\mathcal{U}$ is an ultrafilter on I, and $b \in S$, then b is an *ultralimit* of the a_i, written

$$b = \lim_{i \to \mathcal{U}} a_i$$

if for every open set $N \ni b$,

$$\{i \in I : a_i \in N\} \in \mathcal{U}.$$

Fact 7.2.2. *If S is Hausdorff then ultralimits are unique: for any $I, \mathcal{U}, \{a_i\}_{i \in I}$, there is at most one b with $b = \lim_{i \to \mathcal{U}} a_i$. In fact, this property holds if and only if S is Hausdorff.*

Half-proof. Suppose S is Hausdorff, and

$$b = \lim_{i \to \mathcal{U}} a_i$$
$$c = \lim_{i \to \mathcal{U}} a_i.$$

If $b \neq c$, by Hausdorffness there are open sets $N_1 \ni b$ and $N_2 \ni c$ with $N_1 \cap N_2 = \varnothing$. By definition of ultralimit, the sets

$$\{i \in I : a_i \in N_1\}$$
$$\{i \in I : a_i \in N_2\}$$

are in the ultrafilter $\mathcal{U}$. But their intersection is empty, and $\varnothing \notin \mathcal{U}$, a contradiction. □

Fact 7.2.3. *If S is compact then ultralimits exist: for any I,$\mathcal{U}$, $\{a_i\}_{i \in I}$, there is at least one b with $b = \lim_{i \to \mathcal{U}} a_i$. In fact, this property holds if and only if S is compact.*

Half-proof. Suppose S is compact. Say an open set $N \subseteq S$ is *good* if $\{i \in I : a_i \in N\} \in \mathcal{U}$, and *bad* otherwise, i.e., if $\{i \in I : a_i \notin N\} \in \mathcal{U}$. A finite union of bad sets is bad, because $\mathcal{U}$ is closed under finite intersections. The set S is good. There are two cases:

- S is covered by bad open sets. Then compactness gives a finite subcover, so S is a finite union of bad sets and S is bad, a contradiction.
- S is not covered by bad open sets. Take $p \in S$ such that p is in no bad set. Then every open set $N \ni p$ is good, which means $p = \lim_{i \to \mathcal{U}} a_i$. □

Theorem 7.2.4. *A set $C \subseteq S$ is closed if and only if C is closed under ultralimits, in the sense that*

$$\Big(a_i \in C \textit{ for all } i \in I \textit{ and } b = \lim_{i \to \mathcal{U}} a_i\Big) \implies b \in C.$$

Proof. First suppose C is closed, and $a_i \in C$ for all $i \in I$. If $b \notin C$, then the complement $S \setminus C$ is an open set containing b, but $\{i \in I : a_i \in S \setminus C\} = \varnothing \notin \mathcal{U}$, contradicting the definition of ultralimits. Thus $b \in C$, and C is closed under ultralimits.

Conversely, suppose C is closed under ultralimits. Let U_0 be the union of open sets disjoint from C. It suffices to show that $C \cup U_0 = S$, as then C is the complement of the open set U_0. Fix $p \notin U_0$; we claim $p \in C$. Let

$$\mathcal{F} = \{C \cap U : U \text{ is open and } U \ni p\}.$$

Then $\mathcal{F}$ is closed under finite intersections, because a finite intersection of open sets is open. Moreover, $\varnothing \notin \mathcal{F}$, or else $C \cap U = \varnothing$ and U shows $p \in U_0$, a contradiction. Thus $\mathcal{F}$ has the FIP and is contained in an ultrafilter $\mathcal{U}$ on C. Then

$$p = \lim_{x \to \mathcal{U}} x$$

because for any open set U containing p,

$$\{x \in C : x \in U\} = C \cap U \in \mathcal{F} \subseteq \mathcal{U}.$$

By assumption on C, $p \in C$. □

Fact 7.2.5. *If S_1, S_2 are topological spaces and $f : S_1 \to S_2$ is continuous, then f preserves ultralimits, in the sense that*

$$b = \lim_{i \to \mathcal{U}} a_i \implies f(b) = \lim_{i \to \mathcal{U}} f(a_i).$$

In fact, this property holds if and only if f is continuous.

Half-proof. Suppose f is continuous and $b = \lim_{i \to \mathcal{U}} a_i$. If N is an open set containing $f(b)$, then $f^{-1}(N)$ is an open set containing b, and so

$$\{i \in I : f(a_i) \in N\} = \{i \in I : a_i \in f^{-1}(N)\} \in \mathcal{U}. \qquad \square$$

Theorem 7.2.6. *Let S_1, S_2 be compact Hausdorff spaces and let $f : S_1 \to S_2$ be continuous.*

1. *If $X \subseteq S_1$ is closed, then the image $f(X)$ is closed.*

2. *If f is a bijection, then f is a homeomorphism.*

Proof. 1. By Theorem 7.2.4, it suffices to show that $f(X)$ is closed under ultralimits. Suppose $a_i \in f(X)$ and $\lim_{i \to \mathcal{U}} a_i = b$. We must show $b \in f(X)$. Write a_i as $f(\alpha_i)$ for some $\alpha_i \in X$. Let

$$\beta = \lim_{i \to \mathcal{U}} \alpha_i.$$

The ultralimit exists as S_1 is compact (Fact 7.2.3). The ultralimit β is in X because X is closed (Theorem 7.2.4). Then

$$f(\beta) = \lim_{i \to \mathcal{U}} f(\alpha_i) = \lim_{i \to \mathcal{U}} a_i$$

because the continuous function f preserves ultralimits (Fact 7.2.5). As S_2 is Hausdorff, ultralimits are unique (Fact 7.2.2), and so $f(\beta) = b$. Then $\beta \in X \implies b = f(\beta) \in f(X)$.

2. Let X be a subset of S_1. Part (1) shows that

$$X \text{ is closed in } S_1 \implies f(X) \text{ is closed in } S_2.$$

The reverse direction holds by continuity. Thus f is a homeomorphism.

□

7.3 The space of complete theories

Fix a language $\mathcal{L}$. Let $S = \{\mathrm{Th}(M) : M \text{ is an } \mathcal{L}\text{-structure}\}$. For each $\mathcal{L}$-sentence φ, let

$$[\![\varphi]\!] = \{T \in S : \varphi \in T\} = \{\mathrm{Th}(M) : M \models \varphi\}.$$

Note that $M \models \varphi \wedge \psi \iff (M \models \varphi \text{ and } M \models \psi)$, and so

$$[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!].$$

Similarly,

$$\begin{gathered}[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!] \\ [\![\neg\varphi]\!] = S \setminus [\![\varphi]\!] \\ [\![\top]\!] = S \\ [\![\bot]\!] = \varnothing.\end{gathered}$$

Definition 7.3.1. A set $X \subseteq S$ is *clopen* if $S = [\![\varphi]\!]$ for some sentence φ, and *open* if $X = \bigcup_{i \in I} Y_i$ where each Y_i is clopen.

Theorem 7.3.2. *The collection of open sets is closed under infinite unions and finite intersections, so it defines a topology on S. Moreover, the topology is Hausdorff.*

Proof. Infinite unions are clear: an infinite union of infinite unions of clopen sets is an infinite union of clopen sets. For finite intersections, note that

$$\left(\bigcup_{i \in I} [\![\varphi_i]\!]\right) \cap \left(\bigcup_{j \in J} [\![\psi_j]\!]\right) = \bigcup_{(i,j) \in I \times J} ([\![\varphi_i]\!] \cap [\![\psi_j]\!]) = \bigcup_{(i,j) \in I \times J} [\![\varphi_i \wedge \psi_j]\!].$$

For Hausdorffness, suppose $T_1, T_2 \in S$ and $T_1 \neq T_2$. Then there is a sentence φ such that, say, $\varphi \in T_1$ and $\varphi \notin T_2$. This means $T_1 \in [\![\varphi]\!]$ and $T_2 \notin [\![\varphi]\!]$. Then $T_2 \in S \setminus [\![\varphi]\!] = [\![\neg\varphi]\!]$. The two open sets $[\![\varphi]\!]$ and $[\![\neg\varphi]\!]$ separate T_1 from T_2. □

Lemma 7.3.3. *Let X_i be clopen for each $i \in I$.*

1. *Suppose $\{X_i : i \in I\}$ has the FIP: for any $I_0 \subseteq_f I$, we have $\bigcap_{i \in I_0} X_i \neq \varnothing$. Then $\bigcap_{i \in I} X_i \neq \varnothing$.*

2. *If $S = \bigcup_{i \in I} X_i$, then there is finite $I_0 \subseteq_f I$ such that $S = \bigcup_{i \in I_0} X_i$.*

Proof. 1. Let $X_i = [\![\varphi_i]\!]$. For any $I_0 \subseteq I$, there is M with $\mathrm{Th}(M) \in \bigcap_{i \in I_0} [\![\varphi_i]\!]$, meaning that $M \models \{\varphi_i : i \in I_0\}$. By the compactness theorem, there is M satisfying $\{\varphi_i : i \in I\}$, and then $\mathrm{Th}(M) \in \bigcap_{i \in I} [\![\varphi_i]\!]$.

2. Let $Y_i = S \setminus X_i$. Apply part (1) to the family of clopen sets $\{Y_i\}_{i \in I}$. By assumption, $\bigcap_{i \in I} Y_i = \varnothing$, so there must be $I_0 \subseteq_f I$ such that $\bigcap_{i \in I_0} Y_i = \varnothing$, or equivalently, $\bigcup_{i \in I_0} X_i = S$. □

Theorem 7.3.4. *The topological space S is compact.*

Proof. Suppose $S = \bigcup_{i \in I} U_i$ for some open sets U_i. Let $\mathcal{F}$ be the family of clopen sets X such that $X \subseteq U_i$ for some i. Every open set is the union of its clopen subsets, so $U_i \subseteq \bigcup \mathcal{F}$ for each i. Then $S = \bigcup_{i \in I} U_i \subseteq \bigcup \mathcal{F}$. Applying Lemma 7.3.3(2) to the clopen cover $\mathcal{F}$, there is a finite subcover $S = \bigcup_{j=1}^{n} X_j$ with $X_j \in \mathcal{F}$. For each j, choose a $U_{i_j} \supseteq X_j$. Then $S = \bigcup_{j=1}^{n} X_j \subseteq \bigcup_{j=1}^{n} U_{i_j}$, and $\{U_{i_1}, \ldots, U_{i_n}\}$ is an open subcover of the original cover. □

If S is compact, then ultralimits should exist (Fact 7.2.3). In fact, ultralimits correspond exactly to ultraproducts:

Theorem 7.3.5. *Let M be an ultraproduct $\prod_{i \in I}^{/\mathcal{U}} M_i$. Then $\mathrm{Th}(M)$ is the ultralimit $\lim_{i \to \mathcal{U}} \mathrm{Th}(M_i)$ in the topological space S.*

Proof. Let N be an open set containing $\mathrm{Th}(M)$. Then there is a clopen set $[\![\varphi]\!]$ with $\mathrm{Th}(M) \in [\![\varphi]\!] \subseteq N_0$, because N_0 is a union of clopen sets. Then

$$\mathrm{Th}(M) \in [\![\varphi]\!] \implies M \models \varphi \implies \{i \in I : M_i \models \varphi\} \in \mathcal{U}$$

by Łoś's theorem (Theorem 6.2.7). If $M_i \models \varphi$, then $\mathrm{Th}(M_i) \in [\![\varphi]\!] \subseteq N$. Therefore

$$\{i \in I : \mathrm{Th}(M_i) \in N\} \in \mathcal{U}.$$ □

Recall that X is closed iff $S \setminus X$ is open.

Theorem 7.3.6. *A set $X \subseteq S$ is clopen if and only if X is both closed and open.*

Proof. If X is clopen, then X is open. The complement $S \setminus X$ is clopen, hence open, and so X is also closed.

Conversely, suppose X is closed and open. Then $X = \bigcup_{i \in I} Y_i$ and $S \setminus X = \bigcup_{j \in J} Z_j$ where the Y_i and Z_i are clopen sets. Note that $S = \bigcup_{i \in I} Y_i \cup \bigcup_{j \in J} Z_j$. By Lemma 7.3.3(2), there are finite $I_0 \subseteq_f I$ and $J_0 \subseteq_f J$ such that $S = \bigcup_{i \in I_0} Y_i \cup \bigcup_{j \in J_0} Z_j$. Then X is the clopen set $\bigcup_{i \in I_0} Y_i$. □

7.4 Stone spaces

Definition 7.4.1. In any topological space, a *clopen set* is a set that is both closed and open.

Definition 7.4.2. A *Stone space* is a compact, Hausdorff topological space in which every open set is a union of clopen sets.

Theorem 7.4.3. *Let S be a set. Let $\mathcal{B}$ be a boolean subalgebra of $\mathfrak{P}(S)$. Suppose the following two conditions hold:*

1. *If $a, b \in S$ are distinct, then there is $X \in \mathcal{B}$ with $a \in X$ and $b \notin X$, or $b \in X$ and $a \notin X$.*

2. *If $\{X_i\}_{i \in I}$ is a family of sets in $\mathcal{B}$ with the FIP, then $\bigcap_{i \in I} X_i \neq \varnothing$.*

Then there is a Stone space topology on S in which the clopen sets are exactly the elements of $\mathcal{B}$.

Proof. This follows by the arguments of Section 7.3. □

Theorem 7.4.4. *Let S_1, S_2 be Stone spaces and $f : S_1 \to S_2$ be a map. Suppose that for any clopen set X in S_2, the preimage $f^{-1}(X)$ is clopen in S_1. Then f is continuous.*

Proof. If U is open in S_2, then $U = \bigcup_{i \in I} X_i$ for some clopen sets X_i. Then $f^{-1}(U) = \bigcup_{i \in I} f^{-1}(X_i)$ which is open in S_1. □

Chapter 8

Types and quantifier elimination

This chapter introduces two important notions in model theory: *types* and *quantifier elimination*.

Types

Fix a model M. A *type* over M can be seen as an abstract description of a potential object, which might not exist in M, but does exist in a further elementary extension of M. A *partial 1-type* over M is a set $\Sigma(x)$ of formulas $\varphi(x)$ in one variable x, with parameters from M (i.e., $\mathcal{L}(M)$-formulas), satisfying the following two conditions, which turn out to be equivalent:

1. There is a element b in an elementary extension $N \succeq M$, and b satisfies all the formulas in $\Sigma(x)$.

2. $\Sigma(x)$ is *finitely satisfiable* in M: for any finite subset $\Sigma_0 \subseteq_f \Sigma$, there is an element of M satisfying each formula in Σ_0.

For example, in the ordered field $(\mathbb{R}, +, \cdot, -, 0, 1, \leq)$, the set of formulas

$$\Sigma(x) = \{0 \leq x,\ 1 \leq x,\ 2 \leq x,\ 3 \leq x,\ \ldots\}$$

is a partial type: any finite subset is realized by a big enough real number. But no real number satisfies all the formulas in $\Sigma(x)$. Nevertheless, using compactness, one can find an elementary extension $N \succeq \mathbb{R}$ containing an element satisfying $\Sigma(x)$. The fact that partial types can be realized encapsulates many compactness arguments.

Quantifier elimination

A theory T has *quantifier elimination* if for any formula φ, there is a quantifier-free formula φ' that is equivalent to φ in models of T. When quantifier elimination holds, there is a simple criterion for testing whether models of T are elementarily equivalent. This can sometimes be used to prove that T is complete, and when T is incomplete it can be used to find the completions of T. We will see an example of this in the next chapter when we consider the theory of algebraically closed fields. Quantifier elimination also helps one analyze the structure of definable sets (see Corollary 8.4.4 for an example in dense linear orders).

Fortunately, many theories have quantifier elimination. How do we prove that a given theory T has quantifier elimination? One way is to show that an element's type is determined by its *quantifier-free type* (Theorem 8.3.3). This is often used in conjunction with the *back-and-forth systems* of Definition 3.7.5. We will see one example of this method in the current chapter (Section 8.4), another example in the next chapter (Section 9.4), and a third example in Chapter 11 (Section 11.6) after stating the definitive criterion for quantifier elimination (Theorem 11.5.4).

8.1 Types

Definition 8.1.1. Let M be an $\mathcal{L}$-structure, let A be a subset, and let $\bar{b}$ be an n-tuple. The *type* of $\bar{b}$ over A, written $\mathrm{tp}(\bar{b}/A)$, is the set of $\mathcal{L}(A)$-formulas $\varphi(x_1, \ldots, x_n)$ such that $M \models \varphi(\bar{b})$. When $A = \varnothing$, we write $\mathrm{tp}(\bar{b}/A)$ as $\mathrm{tp}(\bar{b})$. We write $\mathrm{tp}(-)$ as $\mathrm{tp}^M(-)$ when we need to specify M.

Remark 8.1.2. Partial elementary maps preserve types: if f is a partial elementary map from M to N and $\bar{a}$ is a tuple in $\mathrm{dom}(f)$, then $\mathrm{tp}(\bar{a}) = \mathrm{tp}(f(\bar{a}))$. Indeed, for any formula $\varphi(\bar{x})$,

$$\varphi(\bar{x}) \in \mathrm{tp}(\bar{a}) \iff M \models \varphi(\bar{a}) \iff N \models \varphi(f(\bar{a})) \iff \varphi(\bar{x}) \in \mathrm{tp}(f(\bar{a})).$$

Remark 8.1.3. If $\bar{b}, \bar{c}$ are two n-tuples in the same structure M, then the following are equivalent:

1. $\mathrm{tp}(\bar{b}/A) = \mathrm{tp}(\bar{c}/A)$.

2. For every A-definable set D, $\bar{b} \in D \iff \bar{c} \in D$.

Indeed, (1) and (2) are equivalent to

3. For every $\mathcal{L}(A)$-formula $\varphi(\bar{x})$, $M \models \varphi(\bar{b}) \iff M \models \varphi(\bar{c})$.

Let M be an $\mathcal{L}$-structure and A be a set.

Definition 8.1.4. A *complete n-type* over A is something of the form $\mathrm{tp}^N(\bar{b}/A)$ for some $N \succeq M$ and n-tuple $\bar{b} \in N^n$. The set of complete n-types is written $S_n(A)$.

Lemma 8.1.5. *1. If $p \in S_n(A)$ and $\varphi(\bar{x})$ is an $\mathcal{L}(A)$-formula, then $\neg\varphi \in p \iff \varphi \notin p$.*

2. If $p, q \in S_n(A)$ and $p \subseteq q$, then $p = q$.

Proof. 1. If $p = \mathrm{tp}^N(\bar{b}/A)$ for some elementary extension $N \succeq M$ and $\bar{b} \in N^n$, then

$$\neg\varphi \in p \iff N \models \neg\varphi(\bar{b}) \iff N \not\models \varphi(\bar{b}) \iff \varphi \notin p.$$

2. Otherwise take $\varphi \in q \setminus p$. Then $\varphi \in q \implies \neg\varphi \notin q$, and $\varphi \notin p \implies \neg\varphi \in p$. Then $\neg\varphi \in p \setminus q$, contradicting $p \subseteq q$. □

Definition 8.1.6. Let $\Sigma(x_1, \ldots, x_n)$ be a set of $\mathcal{L}(A)$-formulas in the variables $x_1, \ldots, x_n$. Then $\bar{b} \in M^n$ *realizes* Σ if $\Sigma \subseteq \mathrm{tp}(\bar{b}/A)$. We say that $\Sigma(\bar{x})$ is *realized* in M if some $\bar{a} \in M^n$ realizes Σ, and *omitted* in M otherwise.

Remark 8.1.7. If $p \in S_n(A)$ is a complete type, then a tuple $\bar{b}$ realizes p if and only if $\mathrm{tp}(\bar{b}/A) = p$, by Lemma 8.1.5(2) applied to the complete types p and $\mathrm{tp}(\bar{b}/A)$.

Theorem 8.1.8. *Let $\Sigma(\bar{x})$ be a set of $\mathcal{L}(A)$-formulas in the variables $x_1, \ldots, x_n$. The following are equivalent:*

1. Every finite subset $\Sigma_0 \subseteq_f \Sigma$ is realized in M.

2. Σ is realized in an elementary extension of M.

Proof. Consider a third condition:

3. Every finite subset $\Sigma_0 \subseteq_f \Sigma$ is realized in an elementary extension of M.

We claim (3) $\implies$ (1) $\implies$ (2) $\implies$ (3). The direction (2) $\implies$ (3) is clear.

(3) $\implies$ (1): if $\Sigma_0 = \{\varphi_1, \ldots, \varphi_n\}$, and Σ_0 is realized in $N \succeq M$, then

$$N \models \exists \bar{x} \bigwedge_{i=1}^{n} \varphi_i(\bar{x}).$$

As $M \preceq N$, the same sentence holds in M, which means that Σ_0 is realized in M.

(1) $\implies$ (2): Let $\mathcal{L}' = \mathcal{L}(A) \cup \{c_1, \ldots, c_n\}$ where the c_i are new constant symbols. If $\Sigma_0 \subseteq_f \Sigma$, then the $\mathcal{L}'$-structure

$$\mathrm{eldiag}(M) \cup \{\varphi(\bar{c}) : \varphi \in \Sigma_0\}$$

is satisfied by the structure M with $\bar{c}$ interpreted as a realization of Σ_0. By compactness,

$$\mathrm{eldiag}(M) \cup \{\varphi(\bar{c}) : \varphi \in \Sigma\}$$

is satisfied by some $\mathcal{L}'$-structure N. The fact that $N \models \mathrm{eldiag}(M)$ means that, up to isomorphism, $N \succeq M$. Then the interpretation $\bar{c}^N$ of $\bar{c}$ in N is an n-tuple realizing $\Sigma(\bar{x})$, and so (2) holds. □

Definition 8.1.9. A *partial n-type* over A is a set $\Sigma(\bar{x})$ of $\mathcal{L}(A)$-formulas in the variables $x_1, \ldots, x_n$ satisfying the equivalent conditions of Theorem 8.1.8.

Remark 8.1.10. Condition (2) of Theorem 8.1.8 says that $\Sigma(\bar{x})$ is a partial type if and only if $\Sigma(\bar{x}) \subseteq \mathrm{tp}^N(\bar{b}/A)$ for some tuple $\bar{b}$ in an elementary extension $N \succeq M$. Equivalently, $\Sigma(\bar{x})$ is a partial type if and only if Σ is a subset of a complete type. In particular, complete types are partial types.

Theorem 8.1.11. *Let $p(\bar{x})$ be a set of $\mathcal{L}(A)$-formulas in $\bar{x}$. Then $p(\bar{x})$ is a complete type over A if and only if $p(\bar{x})$ is a maximal partial type over A.*

Proof. By Remark 8.1.10, every partial type is contained in a complete type. Therefore, any maximal partial type is a complete type.

Conversely, suppose p is a complete type, but not maximal. Take a larger partial type $\Sigma \supsetneq p$. Then $\Sigma \subseteq q$ for some complete type q, and we have $p \subsetneq \Sigma \subseteq q$, contradicting the incomparability of complete types (Lemma 8.1.5(2)). □

Types over a theory

Let T be an $\mathcal{L}$-theory.

Definition 8.1.12. A *complete n-type* over T is something of the form $\mathrm{tp}^M(\bar{a})$ for some $M \models T$ and n-tuple $\bar{a} \in M^n$. The set of complete n-types is written $S_n(T)$.

Lemma 8.1.13. *If $p, q \in S_n(T)$ and $p \subseteq q$, then $p = q$.*

Proof. Like Lemma 8.1.5. □

Theorem 8.1.14. *If $M \models T$ and $\bar{a} \in M^n$ realizes $p \in S_n(T)$, then $\mathrm{tp}(\bar{a}) = p$.*

Proof. Like Remark 8.1.7. □

Theorem 8.1.15. *Let $\Sigma(\bar{x})$ be a set of $\mathcal{L}$-formulas in the variables $x_1, \ldots, x_n$. The following are equivalent:*

1. *Every finite subset $\Sigma_0 \subseteq \Sigma$ is realized in a model of T.*

2. *Σ is realized in a model of T.*

Proof. Like Theorem 8.1.8, but more straightforward. □

Definition 8.1.16. A *partial n-type* over T is a set $\Sigma(\bar{x})$ of $\mathcal{L}$-formulas in the variables $x_1, \ldots, x_n$ satisfying the equivalent conditions of Theorem 8.1.15.

Remark 8.1.17. As in Remark 8.1.10, $\Sigma(\bar{x})$ is a partial type if and only if $\Sigma(\bar{x})$ is a subset of a complete type. In particular, complete types are partial types.

Theorem 8.1.18. *Let $p(\bar{x})$ be a set of $\mathcal{L}$-formulas in $\bar{x}$. Then $p(\bar{x})$ is a complete type over T if and only if $p(\bar{x})$ is a maximal partial type over T.*

Proof. Like Theorem 8.1.11 □

Lemma 8.1.19. *Let T be a* complete *theory, M be a model, and $\Sigma(\bar{x})$ be a set of $\mathcal{L}$-formulas in the variables $\bar{x}$.*

1. *If $\Sigma(\bar{x})$ is finite, then $\Sigma(\bar{x})$ is realized in a model of T if and only if $\Sigma(\bar{x})$ is realized in M.*

2. *$\Sigma(\bar{x})$ is a partial type over T if and only if $\Sigma(\bar{x})$ is a partial type over $\varnothing \subseteq M$.*

3. *$\Sigma(\bar{x})$ is a complete type over T if and only if $\Sigma(\bar{x})$ is a complete type over $\varnothing \subseteq M$.*

Proof. 1. If $N \models \exists \bar{x} \bigwedge_{\varphi \in \Sigma} \varphi(\bar{x})$ and $N \models T$ then $M \models \exists \bar{x} \bigwedge_{\varphi \in \Sigma} \varphi(\bar{x})$ because $M \equiv N$.

2. By part (1), $\Sigma(\bar{x})$ is finitely realized in models of T if and only if $\Sigma(\bar{x})$ is finitely realized in M.

3. The complete types over T are the maximal partial types over T, and similarly for types over $A = \varnothing$. Since the sets of partial types agree by part (2), the sets of maximal partial types agree. □

Corollary 8.1.20. *If T is a complete theory and M is a model, then $S_n(T) = S_n^M(\varnothing)$.*

Fact 8.1.21. *If $A \subseteq M$ and $T_{A,M}$ is the complete $\mathcal{L}(A)$-theory of M, then $S_n^M(A) = S_n(T_{A,M})$.*

8.2 The topology on type space

Let M be an $\mathcal{L}$-structure and A be a subset of M.

Theorem 8.2.1. *For each $\mathcal{L}(A)$-formula $\varphi(x_1, \ldots, x_n)$, let $[\![\varphi]\!] = \{p \in S_n(A) : \varphi \in p\}$. Then*

$$\begin{gathered}
[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!] \\
[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!] \\
[\![\neg\varphi]\!] = S_n(A) \setminus [\![\varphi]\!] \\
[\![\top]\!] = S_n(A) \qquad [\![\bot]\!] = \varnothing
\end{gathered}$$

Proof. This is a matter of unwinding definitions. For example, if $p \in S_n(A)$ is $\mathrm{tp}^N(\bar{b}/A)$, then

$$\begin{gathered}
p \in [\![\varphi \wedge \psi]\!] \iff \varphi \wedge \psi \in p \iff N \models \varphi(\bar{b}) \wedge \psi(\bar{b}) \\
\iff N \left(\models \varphi(\bar{b}) \text{ and } N \models \psi(\bar{b})\right) \iff \cdots \iff (p \in [\![\varphi]\!] \text{ and } p \in [\![\psi]\!]),
\end{gathered}$$

showing that $[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$. □

Theorem 8.2.2. *If φ, ψ are $\mathcal{L}(A)$-formulas, then*

$$\begin{aligned} [\![\varphi]\!] \subseteq [\![\psi]\!] &\iff \varphi(M) \subseteq \psi(M) \\ [\![\varphi]\!] = [\![\psi]\!] &\iff \varphi(M) = \psi(M). \end{aligned}$$

Proof. We prove the first line, which directly implies the second line. Unwinding the definitions, $[\![\varphi]\!] \subseteq [\![\psi]\!]$ means that for every $N \succeq M$ and $\bar{b} \in N$, if $N \models \varphi(\bar{b})$ then $N \models \psi(\bar{b})$. Equivalently, every $N \succeq M$ satisfies

$$N \models \forall \bar{x} \ (\varphi(\bar{x}) \to \psi(\bar{x})).$$

Similarly, $\varphi(M) \subseteq \psi(M)$ means

$$M \models \forall \bar{x} \ (\varphi(\bar{x}) \to \psi(\bar{x})).$$

The two conditions are equivalent because $N \succeq M$. □

Theorem 8.2.3. *The collection of sets $[\![\varphi]\!]$ form a basis for a topology making $S_n(A)$ into a Stone space, and the sets $[\![\varphi]\!]$ are exactly the clopen sets in this topology.*

Proof. We use Theorem 7.4.3. There are two things to check:

1. If $p, q \in S_n(A)$ are distinct, then there is a set $[\![\varphi]\!]$ distinguishing p and q. Indeed, take φ in $p \setminus q$.

2. If $\{[\![\varphi_i]\!]\}_{i \in I}$ has the FIP, then $\bigcap_i [\![\varphi_i]\!] \neq \varnothing$. Equivalently, if every finite subset of $\{\varphi_i : i \in I\}$ is contained in a complete type, then $\{\varphi_i : i \in I\}$ is contained in a complete type. This is clear by Theorem 8.1.8. □

Using Theorem 8.2.2 we see the following:

Corollary 8.2.4. *The boolean algebra of clopen sets in $S_n(A)$ is isomorphic to the boolean algebra of A-definable subsets of M^n via the isomorphism $[\![\varphi]\!] \mapsto \varphi(M^n)$.*

There is an analogous picture for type spaces of a theory. Let T be an $\mathcal{L}$-theory:

Theorem 8.2.5. *For each $\mathcal{L}$-formula $\varphi(x_1, \ldots, x_n)$, let $[\![\varphi]\!] = \{p \in S_n(T) : \varphi \in p\}$. Then*

$$[\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$$
$$[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!]$$
$$[\![\neg\varphi]\!] = S_n(T) \setminus [\![\varphi]\!]$$
$$[\![\top]\!] = S_n(T) \qquad [\![\bot]\!] = \varnothing$$

Moreover, $[\![\varphi]\!] = [\![\psi]\!]$ if and only if φ and ψ are equivalent modulo T, in the sense that

$$T \vdash \forall \bar{x}\ (\varphi(\bar{x}) \leftrightarrow \psi(\bar{x}))$$

or equivalently $\varphi(M) = \psi(M)$ for all $M \models T$.

Theorem 8.2.6. *The collection of sets $[\![\varphi]\!]$ is a basis for a topology making $S_n(T)$ a Stone space, and the clopen sets are exactly the sets $[\![\varphi]\!]$.*

8.3 Quantifier elimination

Definition 8.3.1. A theory T has *quantifier elimination* if for every formula $\varphi(\bar{x})$, there is a quantifier-free formula $\psi(\bar{x})$ that is equivalent to φ in models of T:

$$T \vdash \forall \bar{x}(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x})).$$

Definition 8.3.2. If $(a_1, \ldots, a_n)$ is a tuple in a structure M, then the *quantifier-free type* $\mathrm{qftp}(\bar{a})$ is the set of quantifier-free formulas $\varphi(x_1, \ldots, x_n)$ with $M \models \varphi(\bar{a})$.

For any theory T, let $S_n^{\mathrm{qfree}}(T)$ be the space of quantifier-free n-types, analogous to the space of complete n-types $S_n(T)$. Each quantifier-free formula $\varphi(x_1, \ldots, x_n)$ defines a set $[\![\varphi]\!]_{\mathrm{qfree}} \subseteq S_n^{\mathrm{qfree}}(T)$, and these sets form a basis for a topology making $S_n^{\mathrm{qfree}}(T)$ into a Stone space. Moreover, every clopen set in $S_n^{\mathrm{qfree}}(T)$ has the form $[\![\varphi]\!]_{\mathrm{qfree}}$ for some quantifier-free φ. The proofs are analogous to the case of $S_n(T)$ (Section 8.2). There is a restriction map

$$S_n(T) \to S_n^{\mathrm{qfree}}(T)$$

sending $\mathrm{tp}(\bar{a})$ to $\mathrm{qftp}(\bar{a})$. Note that

$$\mathrm{qftp}^M(\bar{a}) \in [\![\varphi]\!]_{\mathrm{qfree}} \iff M \models \varphi(\bar{a}) \iff \mathrm{tp}^M(\bar{a}) \in [\![\varphi]\!]$$

so the preimage of $[\![\varphi]\!]_{\text{qfree}}$ is $[\![\varphi]\!]$. Because preimages of clopen sets are clopen, the restriction map is continuous (Theorem 7.4.4).

Theorem 8.3.3. *The following are equivalent:*

1. *T has quantifier elimination.*
2. *For any $M, N \models T$ and $\bar{a} \in M^n$ and $\bar{b} \in N^n$,*

$$\mathrm{qftp}^M(\bar{a}) = \mathrm{qftp}^N(\bar{b}) \implies \mathrm{tp}^M(\bar{a}) = \mathrm{tp}^N(\bar{b}).$$

Proof. Consider a third condition:

3. For every n, the restriction map $S_n(T) \to S_n^{\text{qfree}}(T)$ is a homeomorphism.

We claim (1) $\implies$ (2) $\implies$ (3) $\implies$ (1).

(1) $\implies$ (2): Suppose that T has quantifier elimination and $\mathrm{qftp}^M(\bar{a}) = \mathrm{qftp}^N(\bar{b})$. For any formula $\varphi(\bar{x})$, there is an equivalent quantifier free-formula $\psi(\bar{x})$, and then

$$M \models \varphi(\bar{a}) \iff M \models \psi(\bar{a}) \iff N \models \psi(\bar{b}) \iff N \models \varphi(\bar{b}),$$

so that $\mathrm{tp}^M(\bar{a}) = \mathrm{tp}^N(\bar{b})$.

(2) $\implies$ (3): The restriction map is surjective, since $\mathrm{qftp}^M(\bar{a})$ lifts to $\mathrm{tp}^M(\bar{a})$. The restriction map is injective by (2). Then the restriction map is a continuous bijection between compact Hausdorff spaces, and therefore a homeomorphism (Theorem 7.2.6).

(3) $\implies$ (1): Let $\varphi(x_1, \ldots, x_n)$ be a formula. Then $[\![\varphi]\!] \subseteq S_n(T)$ is clopen. The image under the homeomorphism $S_n(T) \to S_n^{\text{qfree}}(T)$ is a clopen set, which must be $[\![\psi]\!]_{\text{qfree}} \subseteq S_n^{\text{qfree}}(T)$ for some quantifier-free formula ψ. Then

$$M \models \varphi(\bar{a}) \iff \mathrm{tp}(\bar{a}) \in [\![\varphi]\!] \iff \mathrm{qftp}(\bar{a}) \in [\![\psi]\!]_{\text{qfree}} \iff M \models \psi(\bar{a}),$$

so $T \vdash \varphi \leftrightarrow \psi$. □

Theorem 8.3.4. *Suppose M, N are $\mathcal{L}$-structures and $\bar{a} \in M^n$ and $\bar{b} \in N^n$. Then the following are equivalent:*

1. $\mathrm{qftp}(\bar{a}) = \mathrm{qftp}(\bar{b})$.
2. *There is an isomorphism $f : \langle \bar{a} \rangle_M \to \langle \bar{b} \rangle_N$ with $f(\bar{a}) = \bar{b}$.*

Proof. (1) $\Longrightarrow$ (2): Let $p = \mathrm{qftp}(\bar{a}) = \mathrm{qftp}(\bar{b})$. Note that every element of $\langle \bar{a} \rangle_M$ has the form $t^M(\bar{a})$ for some term t. Similarly, $\langle \bar{b} \rangle_M = \{t^N(\bar{b}) : t(\bar{x}) \text{ a term}\}$. Moreover,

$$t^M(\bar{a}) = s^M(\bar{a}) \iff (t(\bar{x}) = s(\bar{x})) \in p \iff t^N(\bar{b}) = s^N(\bar{b}),$$

Therefore there is a bijection $f : \langle \bar{a} \rangle_M \to \langle \bar{b} \rangle_N$ sending $t^M(\bar{a})$ to $t^N(\bar{b})$. If R is a k-ary relation symbol and $t_1, \ldots, t_k$ are terms in $\bar{x}$, then

$$R^M(t_1^M(\bar{a}), \ldots, t_k^M(\bar{a})) \iff R(t_1, \ldots, t_k) \in p \iff R^N(t_1^N(\bar{a}), \ldots, t_k^N(\bar{a})),$$

and so f preserves relation symbols. A similar argument shows f preserves function symbols.

(2) $\Longrightarrow$ (1): Let $A = \langle \bar{a} \rangle_M$ and $B = \langle \bar{b} \rangle_N$. Then

$$\mathrm{qftp}^M(\bar{a}) = \mathrm{qftp}^A(\bar{a}) = \mathrm{qftp}^B(\bar{b}) = \mathrm{qftp}^N(\bar{b})$$

by Theorem 3.4.2 applied to the embeddings $A \to M$, $B \to N$, and $A \overset{\cong}{\to} B$. □

Theorem 8.3.5. *Suppose T has quantifier elimination. If $M, N \models T$, then*

$$M \equiv N \iff \langle \varnothing \rangle_M \cong \langle \varnothing \rangle_N.$$

Proof. The left hand side says that $\mathrm{tp}^M() = \mathrm{tp}^N()$. Indeed, $\mathrm{tp}^M()$ is the set of formulas in 0 free variables (i.e., sentences) satisfied by the empty tuple (i.e., true in M), which is just $\mathrm{Th}(M)$.

Meanwhile, the right hand side of $(*)$ is equivalent to $\mathrm{qftp}^M() = \mathrm{qftp}^N()$ by Theorem 8.3.4. We don't have to worry about how the isomorphism acts on the generators, because there are no generators to check.

Finally, quantifier elimination gives

$$\mathrm{tp}^M() = \mathrm{tp}^N() \iff \mathrm{qftp}^M() = \mathrm{qftp}^N().$$ □

Theorem 8.3.6. *Suppose T has quantifier elimination and $M, N \models T$.*

1. *If $f : M \to N$ is an embedding, then f is an elementary embedding.*
2. *If M is a substructure of N, then M is an elementary substructure of N.*

Proof. Embeddings preserve quantifier-free formulas (Theorem 3.4.2(3)), and quantifier elimination allows us to replace any formula with an equivalent quantifier-free formula. □

8.4 Quantifier elimination in DLO

Theorem 8.4.1. *DLO has quantifier elimination.*

Proof. We use the criterion of Theorem 8.3.3. Suppose $M, N \models \text{DLO}$, $\bar{a} \in M^n$, $\bar{b} \in N^n$, and $\text{qftp}^M(\bar{a}) = \text{qftp}^N(\bar{b})$. We must show $\text{tp}^M(\bar{a}) \overset{?}{=} \text{tp}^N(\bar{b})$.

By Theorem 8.3.4, there is a partial isomorphism $f : \langle \bar{a} \rangle_M \to \langle \bar{b} \rangle_N$ with $f(\bar{a}) = \bar{b}$. As the language of orders is relational, all terms are trivial, and so $\text{dom}(f) = \langle \bar{a} \rangle_M = \{a_1, \ldots, a_n\}$. Then f is a finite partial isomorphism. By Theorem 3.7.10, the class of finite partial isomorphisms is a back-and-forth system, and so f is a partial elementary map by Theorem 3.7.6. Therefore $\text{tp}^M(\bar{a}) = \text{tp}^N(f(\bar{a})) = \text{tp}^N(\bar{b})$. □

If M, N are models of DLO, then $\langle \varnothing \rangle_M$ and $\langle \varnothing \rangle_N$ are both the empty order $\varnothing$, so $M \equiv N$. This gives another proof of the completeness of DLO.

Corollary 8.4.2. $\mathbb{Q}$ *and the open interval* $(0, 1) = \{x \in \mathbb{R} : 0 < x < 1\}$ *are elementary substructures of* $\mathbb{R}$.

Definition 8.4.3. If $(M, \leq) \models \text{DLO}$ and $a < b$ are two points in M, then we define

$$\begin{aligned} (a, b) &:= \{x \in M : a < x < b\} \\ (a, +\infty) &:= \{x \in M : a < x\} \\ (-\infty, a) &:= \{x \in M : x < a\} \\ (-\infty, +\infty) &:= M \end{aligned}$$

Sets of these forms are called *open intervals.*

Corollary 8.4.4. *If* $M \models \text{DLO}$ *and* $D \subseteq M^1$ *is definable, then* D *is a finite union of points and open intervals.*

Proof. Let $\mathcal{F}$ be the collection of sets $D \subseteq M$ such that D is a finite union of points and open intervals. It is an exercise to see that $\mathcal{F}$ is closed under boolean operations (it is a boolean subalgebra of $\mathfrak{P}(M)$). We must show that $D \in \mathcal{F}$. Write D as $\varphi(M, \bar{b})$ for some $\mathcal{L}$-formula $\varphi(x, \bar{y})$ and tuple of parameters $\bar{b}$. By quantifier-elimination, we may assume φ is quantifier-free. Then φ is a boolean combination of atomic formulas. As $\mathcal{F}$ is closed under boolean combinations, we may assume φ is atomic. Then $\varphi(x, \bar{b})$ has one of the following forms:

$$x \leq x,\ x \leq b_i,\ b_i \leq x,\ b_i \leq b_j,\ x = x,\ x = b_i,\ b_i = x,\ b_i = b_j.$$

Each of these formulas defines a set in $\mathcal{F}$. □

Chapter 9

Algebraically closed fields

We now turn to an important example—the theory ACF of *algebraically closed fields*. An algebraically closed field is a field in which every polynomial equation

$$a_n x^n + \cdots a_1 x + a_0 = 0$$

has a solution (except in the degenerate case where $a_0 \neq 0 = a_1 = a_2 = \cdots = a_n$). The field $\mathbb{C}$ is algebraically closed—a fact known as the "fundamental theorem of algebra". The class of algebraically closed fields is axiomatized by a theory ACF. For $p \in \{0, 2, 3, 5, 7, \ldots\}$, ACF_p is the theory of algebraically closed fields of characteristic p. For example, $\mathbb{C} \models \mathrm{ACF}_0$.

In the current chapter, we show that ACF has quantifier elimination (Theorem 9.4.4). From this, we see that two algebraically closed fields are elementarily equivalent if and only if they have the same characteristic (Corollary 9.4.5). As a consequence, each theory ACF_p is complete, including ACF_0 (Corollary 9.4.7). As $\mathbb{C}$ is a model of ACF_0, it follows that the structure $\mathbb{C}$ is decidable—there is an algorithm which determines whether a given sentence is true or false in $\mathbb{C}$ (Corollary 9.4.8).

We continue to use ACF as a running example in later chapters. In Chapter 10, we show that if K is algebraically closed, then any system of equations that has a solution in an extension of K already has a solution in K (Theorem 10.3.6), and we verify that algebraically closed fields of characteristic p actually exist for $p > 0$ (Corollary 10.3.5). In Chapter 13, we show that the set $\mathbb{Q}^{\mathrm{alg}}$ of *algebraic numbers* is an elementary substructure of $\mathbb{C}$ (Example 13.5.5). In Chapter 14, we show that the theories ACF_0 and ACF_p are κ-categorical for any $\kappa > \aleph_0$ (Corollary 14.2.7), and use this to classify algebraically closed fields (Theorem 14.2.10). We will also see that there is a good notion of "dimension" for definable sets in algebraically closed fields (Sections 14.5–14.6), a fact known to algebraic geometers.

9.1 Polynomial rings

Fact 9.1.1. *Let R be a ring and x be a symbol. There is a ring $R[x]$ extending R, generated by $R \cup \{x\}$, with the following properties:*

1. *Every element of $R[x]$ has the form $\sum_{i=0}^{n} a_i x^i$ for some $n \geq 0$ and $a_0, \ldots, a_n \in R$.*
2. *Two elements $\sum_{i=0}^{n} a_i x^i$ and $\sum_{i=0}^{n} b_i x^i$ are equal if and only if the tuples $\bar{a}$ and $\bar{b}$ are equal.*
3. *The sum of two elements is given by*
$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i.$$
4. *The product of two elements is given by*
$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0}^{n+m} c_k x^k, \text{ where } c_k = \sum_{\substack{0 \leq i \leq n \\ 0 \leq j \leq m \\ i+j=k}} a_i b_j.$$

Elements of $R[x]$ are called polynomials*.*

If $P(x)$ is a non-zero polynomial, then we can write
$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$
where $n \geq 0$ and $a_n \neq 0$. Then $a_n x^n$ is called the *leading term*, a_n is called the *leading coefficient*, and n is called the *degree* of $P(x)$. We write the degree of P as $\deg P$. The degree of the zero polynomial is defined to be $-\infty$. A nonzero polynomial is *monic* if the leading coefficient is 1.

Definition 9.1.2 (Evaluating polynomials)**.** If $P(x) \in R[x]$ has the form
$$P(x) = \sum_{i=0}^{n} a_i x^i$$

and if $b \in R$, then

$$P(b) := \sum_{i=0}^{n} a_i b^i.$$

Fact 9.1.3. *For fixed b, the map*

$$\begin{gathered} R[x] \to R \\ P(x) \mapsto P(b) \end{gathered}$$

is a ring homomorphism, meaning among other things that

$$\begin{gathered} (P+Q)(b) = P(b) + Q(b) \\ (PQ)(b) = P(b)Q(b) \end{gathered}$$

Lemma 9.1.4. *Let K be a field, and let $A(x), B(x) \in K[x]$ be polynomials with $B(x)$ non-zero. then there is $R(x) \in K[x]$ such that*

$$\begin{gathered} A(x) \equiv R(x) \pmod{B(x)} \\ \deg R(x) < \deg B(x). \end{gathered}$$

Proof. If bx^m is the leading term of $B(x)$, replace $B(x)$ with $b^{-1}B(x)$. Then we can assume $B(x)$ is monic. Proceed by induction on $\deg A(x)$. If $\deg A(x) < \deg B(x)$, take $R(x) = A(x)$. Otherwise, let

$$\begin{gathered} A(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots \\ B(x) = x^m + b_{m-1}x^{m-1} + \cdots \end{gathered}$$

where $m = \deg(B) \leq n = \deg(A)$. Let

$$\begin{gathered} A'(x) = A(x) - a_n x^{n-m} B(x) \\ = (a_n x^n + a_{n-1}x^{n-1} + \cdots) - (a_n x^n + a_n b_{m-1} x^{n-1} + \cdots + a_n b_0 x^{n-m}). \end{gathered}$$

Then $\deg A'(x) < n = \deg A(x)$, but $A(x) \equiv A'(x) \pmod{B(x)}$. By induction, $A'(x) \equiv R(x) \pmod{B(x)}$ for some suitable $R(x)$. □

Let K be a field.

Theorem 9.1.5. *Suppose $P(x) \in K[x]$ and $P(a) = 0$ for some $a \in K$. Then $P(x) = (x - a)Q(x)$ for some $Q(x) \in K[x]$.*

Proof. Apply the division lemma to $P(x)$ and $(x-a)$, to get $R(x) \in K[x]$ with

$$\begin{gathered} P(x) \equiv R(x) \pmod{x-a} \\ \deg R(x) < \deg(x-a) = 1. \end{gathered}$$

The first line means there is $Q(x) \in K[x]$ with

$$P(x) = (x-a)Q(x) + R(x). \tag{$*$}$$

The second line means $R(x) = c$ for some constant c. Substituting $x = a$ into $(*)$, we see

$$\begin{aligned} P(a) &= (a-a)Q(a) + c \\ 0 &= 0 + c. \end{aligned}$$

Then $c = 0$, so $R(x) = 0$ and $P(x) = (x-a)Q(x)$. □

A *root* of $P(x) \in K[x]$ is an element $a \in K$ with $P(a) = 0$. Note that a is a root of $P(x)Q(x)$ if and only if a is a root of $P(x)$ or a is a root of $Q(x)$, by the zero law (Theorem 1.4.16).

Theorem 9.1.6. *If $P(x)$ is a non-zero polynomial, then the number of roots of $P(x)$ in K is at most* $\deg P(x)$.

Proof. Let $d = \deg P(x)$. If $P(x)$ has no roots, then the claim holds. Otherwise, take some root a. Then $P(x) = (x-a)Q(x)$ for some polynomial $Q(x)$ of degree $d-1$. By induction on d, $Q(x)$ has at most $d-1$ roots. As $(x-a)$ has one root, $P(x)$ has at most $(d-1)+1 = d$ roots. □

Theorem 9.1.7. *If K is a field, every ideal $I \subseteq K[x]$ is a principal ideal $P(x)K[x]$ for some polynomial $P(x)$.*

Proof. Like the proof of the same fact in $\mathbb{Z}$ (Theorem 2.5.3), but using Lemma 9.1.4 instead of Lemma 2.5.2 and using $\deg P$ instead of $|n|$. □

Remark 9.1.8. In Theorem 9.1.7, scaling $P(x)$ by a non-zero constant, we may assume $P(x)$ is zero or monic. Then $P(x)$ is uniquely determined.

Definition 9.1.9. A non-constant polynomial $P(x)$ is *reducible* if $P(x)$ is a product of two non-constant polynomials, and *irreducible* otherwise.

Theorem 9.1.10. *If $P(x)$ is an irreducible polynomial in $K[x]$, then the quotient $K[x]/P(x)K[x]$ is a field.*

Proof. Like the proof that $\mathbb{Z}/p\mathbb{Z}$ is a field when p is prime (Theorem 2.5.7). □

9.2 The theory ACF

Definition 9.2.1. A field K is *algebraically closed* if every polynomial $P(x) \in K[x]$ with $\deg P > 0$ has a root. That is, for every $n > 0$ and $a_0, a_1, \dots, a_n \in K$ with $a_n \neq 0$, there is $x \in K$ with

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

Note that the class of algebraically closed fields is elementary, defined by a theory consisting of the field axioms plus an axiom schema

$$\forall a_1, \dots, a_n \left(a_n \neq 0 \to \exists x \ \sum_{i=0}^{n} a_i x^i = 0 \right) \text{ for } n > 0.$$

This theory is usually called *ACF*.

Fact 9.2.2 (Fundamental theorem of algebra)**.** *The field* $\mathbb{C} = \{x + yi : x, y \in \mathbb{R}\}$ *is algebraically closed.*

Theorem 9.2.3. *If K is algebraically closed, then K is infinite.*

Proof. If $K = \{a_1, \dots, a_n\}$, then $P(x) = 1 + \prod_{i=1}^{n}(x - a_i)$ has no root in K, so $K \not\models$ ACF. □

9.3 Algebraic and transcendental elements

Let L be a field and K be a subfield.

Definition 9.3.1. An element $a \in L$ is *algebraic* over K if $P(a) = 0$ for some non-zero polynomial $P(x) \in K[x]$. Otherwise, a is *transcendental* over K.

If $a \in L$, then $K[a]$ denotes the subring of L generated by $K \cup \{a\}$.

Theorem 9.3.2. *Fix $a \in L$. Let $I_{a/K} = \{P(x) \in K[x] : P(a) = 0\}$.*

1. *$I_{a/K}$ is an ideal in $K[x]$.*

2. *$K[x]/I_{a/K}$ is isomorphic to $K[a]$ via the isomorphism sending $P(x)$ to $P(a)$.*

3. *If a is transcendental over K, then $I_{a/K}$ is the zero ideal $0 \cdot K[x] = \{0\}$.*

4. *If a is algebraic over K, then $I_{a/K} = P(x) \cdot K[x]$ for some irreducible monic polynomial $P(x)$.*

Proof. Let $f : K[x] \to K[a]$ be the ring homomorphism $P(x) \mapsto P(a)$. Then $I_{a/K}$ is the kernel. The image $\mathrm{im}(f)$ is a subring of $K[a]$ containing $f(K) = K$ and $f(x) = a$, so it must be all of $K[a]$. By the fundamental theorem on homomorphisms, $K[x]/I_{a/K}$ is isomorphic to the image $K[a]$ via the map $P(x) \mapsto P(a)$.

By Theorem 9.1.7 and Remark 9.1.8, the ideal $I_{a/K}$ is $P(x) \cdot K[x]$, where $P(x)$ is zero or a monic polynomial. In the first case, $I_{a/K} = \{0\}$, which means precisely that a is transcendental. In the second case, $P(x) \in I_{a/K}$ implies that $P(a) = 0$, and so a is algebraic. Suppose for the sake of contradiction that $P(x)$ is reducible as $P(x) = Q_1(x)Q_2(x)$. Note that $\deg P > \deg Q_i$ for $i = 1, 2$, so $Q_i \notin P(x) \cdot K[x] = I_{a/K}$, and therefore $Q_i(a) \neq 0$ for $i = 1, 2$. But then $0 = P(a) = Q_1(a)Q_2(a) \neq 0$, a contradiction. □

Definition 9.3.3. If $a \in L$ is algebraic over K, then the *minimal polynomial* of a over K is the monic irreducible polynomial $P(x)$ appearing in Theorem 9.3.2(4).

Theorem 9.3.4. *If $P(x) \in K[x]$ is a monic irreducible polynomial and $a \in L$ is a root of $P(x)$, then $P(x)$ is the minimal polynomial of a.*

Proof. Let $P_0(x)$ be the actual minimal polynomial of a. Then

$$P(a) = 0 \implies P(x) \in I_{a/K} = P_0(x) \cdot K[x].$$

Thus $P(x)$ is a multiple of $P_0(x)$:

$$P(x) = P_0(x)Q(x).$$

As $P(x)$ is irreducible, this forces $Q(x) = 1$ and $P(x) = P_0(x)$. □

9.4 Quantifier elimination in ACF

Lemma 9.4.1. *Let M_1, M_2 be two fields. Let $f : R_1 \to R_2$ be a partial isomorphism. Then there is a larger partial isomorphism $g : K_1 \to K_2$ such that K_1 and K_2 are fields.*

Proof. Let $K_i = \{a/b : a, b \in R_i,\ b \neq 0\}$. Then K_i is a subfield of M_i. For example, K_i is closed under addition because

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

Let $g : K_1 \to K_2$ be defined by $g(a/b) = f(a)/f(b)$. This is well-defined because

$$\begin{aligned} \frac{a}{b} = \frac{a'}{b'} &\iff ab' = a'b \implies f(ab') = f(a'b) \\ &\iff f(a)f(b') = f(a')f(b) \iff \frac{f(a)}{f(b)} = \frac{f(a')}{f(b')}. \end{aligned}$$

It is an exercise in algebra to see that g is an isomorphism. For example, g preserves addition because

$$\begin{aligned} g\left(\frac{a}{b} + \frac{c}{d}\right) = g\left(\frac{ad + bc}{bd}\right) &= \frac{f(ad + bc)}{f(bd)} = \frac{f(a)f(d) + f(b)f(c)}{f(b)f(d)} \\ &= \frac{f(a)}{f(b)} + \frac{f(c)}{f(d)} = g\left(\frac{a}{b}\right) + g\left(\frac{c}{d}\right). \end{aligned}$$ □

Lemma 9.4.2. *Let M_1, M_2 be two uncountable algebraically closed fields extending a countable subfield K. For any $a \in M_1$, there is $b \in M_2$ and an isomorphism $f : K[a] \to K[b]$ sending a to b and fixing K.*

Proof. Recall the notation

$$I_{a/K} = \{P(x) \in K[x] : P(a) = 0\}$$

from Theorem 9.3.2.

Claim. There is $b \in M_2$ with $I_{a/K} = I_{b/K}$.

Proof. First suppose a is transcendental. There are countably many nonzero polynomials in $K[x]$, and each has finitely many roots (Theorem 9.1.6). Therefore only countable many $b \in M_2$ are algebraic over K. Take $b \in M_2$ transcendental over K. Then $I_{a/K} = \{0\} = I_{b/K}$ by Theorem 9.3.2.

Next suppose a is algebraic with minimal polynomial $P(x) \in K[x]$. As M_2 is algebraically closed, there is $b \in M_2$ with $P(b) = 0$. By Theorem 9.3.4, $P(x)$ is the minimal polynomial of b, and then

$$I_{a/K} = P(x) \cdot K[x] = I_{b/K}.$$ $\square_{\text{Claim}}$

Fix $b \in M_2$ as in the claim, and let $I = I_{a/K} = I_{b/K}$. By Theorem 9.3.2, we have isomorphisms

$$K[x]/I \to K[a]$$
$$K[x]/I \to K[b]$$

sending $P(x)$ to $P(a)$ and $P(b)$, respectively. The composition

$$K[a] \to K[x]/I \to K[b]$$

is the desired isomorphism. □

Lemma 9.4.3. *Let M_1, M_2 be two uncountable algebraically closed fields. Let $f : R_1 \to R_2$ be a finitely-generated partial isomorphism. For any $a \in M_1$, there is $b \in M_2$ and an isomorphism $R_1[a] \to R_2[b]$ extending f.*

Proof. By Lemma 9.4.1, the isomorphism $f : R_1 \to R_2$ extends to an isomorphism $f' : K_1 \to K_2$ where the K_i are fields. Moving M_2, we may assume $K_1 = K_2$ and f' is the identity map. Applying Lemma 9.4.2, there is an element $b \in M_2$ and an isomorphism $K_1[b] \to K_2[b]$ extending f'. This isomorphism restricts to an isomorphism $R_1[b] \to R_2[b]$ extending f. □

Theorem 9.4.4. *The theory ACF has quantifier elimination.*

Proof. We use the criterion of Theorem 8.3.3. Suppose $M, N \models \mathrm{ACF}$, $\bar{a} \in M^n$, $\bar{b} \in N^n$, and $\mathrm{qftp}^M(\bar{a}) = \mathrm{qftp}^N(\bar{b})$. We must show $\mathrm{tp}^M(\bar{a}) = \mathrm{tp}^N(\bar{b})$. Recall that M and N are infinite (Theorem 9.2.3). Replacing M, N with elementary extensions, we may assume M and N are uncountable. By Theorem 8.3.4, there is a partial isomorphism $f : \langle \bar{a} \rangle_M \to \langle \bar{b} \rangle_N$ with $f(\bar{a}) = \bar{b}$. Let $\mathcal{F}$ be the collection of finitely generated partial isomorphisms from M to N. Then $\mathcal{F}$ is a back-and-forth system: Lemma 9.4.3 gives the forward condition, and the backward condition holds by symmetry. By Theorem 3.7.6, the fact that $f \in \mathcal{F}$ implies that f is a partial elementary map, and so $\mathrm{tp}^M(\bar{a}) = \mathrm{tp}^N(\bar{b})$. □

Corollary 9.4.5. *If $M, N \models$ ACF, then $M \equiv N \iff \mathrm{char}(M) = \mathrm{char}(N)$.*

Proof. By quantifier elimination in ACF and Theorem 8.3.5, we have

$$M \equiv N \iff \langle \varnothing \rangle_M \cong \langle \varnothing \rangle_N.$$

By Theorem 2.7.5, the right hand side is equivalent to

$$\mathbb{Z}/n_M\mathbb{Z} \overset{?}{\cong} \mathbb{Z}/n_N\mathbb{Z}, \tag{$*$}$$

where $n_M = \text{char}(M)$ and $n_N = \text{char}(N)$. Clearly, $(*)$ holds if and only if $n_M = n_N$. □

Definition 9.4.6. For $p \in \{0, 2, 3, 5, 7, 11, 13, \ldots\}$, ACF_p is the theory of algebraically closed fields of characteristic p:

$$\text{ACF}_0 = \text{ACF} \cup \{\underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} \neq 0 : p = 2, 3, 5, 7, \ldots\}$$

$$\text{ACF}_p = \text{ACF} \cup \{\underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} = 0\} \text{ for } p > 0$$

For example, $\mathbb{C} \models \text{ACF}_0$. We will see later (Corollary 10.3.5) that ACF_p is consistent for each p.

Corollary 9.4.7. *Each theory* ACF_p *is complete.*

Corollary 9.4.8. $\text{Th}(\mathbb{C})$ *is decidable.*

Chapter 10

Existentially closed models

For a fixed theory T, a model M is *existentially closed* if "everything which could exist does exist," in a certain sense. More precisely, any quantifier free $\mathcal{L}(M)$-formula which is satisfied in an extension of M is already satisfied in M. For example, a field K is existentially closed if any system of equations which is satisfied in an extension of K is already satisfied in K. It turns out that the existentially closed fields are precisely the algebraically closed fields (Theorem 10.3.6), so "existentially closed" can be seen as a generalization of "algebraically closed from fields to other theories.

There are a couple important things to say about existentially closed models in general. First, under some technical assumptions on T, existentially closed models exist (Theorem 10.2.5). Second, if T has quantifier elimination, then all models of T are existentially closed.

10.1 Unions of chains of structures

Fix a language $\mathcal{L}$.

Definition 10.1.1. A *chain of $\mathcal{L}$-structures* is a family $\{M_i\}_{i \in I}$ where $(I, \leq)$ is a linear order, M_i is an $\mathcal{L}$-structure for $i \in I$, and M_i is a substructure of M_j for $i \leq j$.

If $\{M_i\}_{i \in I}$ is a chain of $\mathcal{L}$-structures, we can make $M = \bigcup_{i \in I} M_i$ into a $\mathcal{L}$-structure by defining

$$f^M(a_1, \ldots, a_n) = f^{M_i}(a_1, \ldots, a_n)$$
$$R^M(a_1, \ldots, a_n) \iff R^{M_i}(a_1, \ldots, a_n)$$

for any $i \in I$ large enough that $\{a_1, \ldots, a_n\} \subseteq M_i$. The choice of i doesn't matter—if j is another choice, then

$$f^{M_i}(\bar{a}) = f^{M_j}(\bar{a})$$
$$R^{M_i}(\bar{a}) \iff R^{M_j}(\bar{a})$$

because M_i is a substructure or extension of M_j.

Definition 10.1.2. A theory T is *inductive* if whenever $\{M_i\}_{i \in I}$ is a chain of models of T, the union $\bigcup_{i \in I} M_i$ is also a model of T.

Definition 10.1.3. An $\forall\exists$-*sentence* is one of the form $\forall \bar{x}\ \exists \bar{y}\ \varphi(\bar{x}, \bar{y})$, where φ is quantifier-free. An $\forall\exists$-*theory* is a set of $\forall\exists$-sentences.

Theorem 10.1.4. *If T is an $\forall\exists$-theory, then T is inductive.*

Proof. Suppose $\{M_i\}_{i \in I}$ is a chain of structures, and

$$M_i \models \forall \bar{x}\ \exists \bar{y}\ \varphi(\bar{x}, \bar{y}) \tag{$*$}$$

for all i, where φ is quantifier-free. Let $M = \bigcup_i M_i$. If $\bar{a} \in M^n$, then $\bar{a} \in M_i^n$ for large enough i. By $(*)$, there is $\bar{b} \in M_i^m$ with $M_i \models \varphi(\bar{a}, \bar{b})$. Then $M \models \varphi(\bar{a}, \bar{b})$ because φ is quantifier-free. We have shown

$$M \models \forall \bar{x}\ \exists \bar{y}\ \varphi(\bar{x}, \bar{y}).$$ □

Example 10.1.5. The theory of fields is an $\forall\exists$-theory, so it is inductive.

10.2 Existentially closed models

Definition 10.2.1. Let $M \subseteq N$ be structures. Then M is *existentially closed* in N, written $M \preceq_1 N$, if for any quantifier-free $\mathcal{L}(M)$-formula $\varphi(\bar{x})$,

$$N \models \exists \bar{x}\ \varphi(\bar{x}) \implies M \models \exists \bar{x}\ \varphi\bar{x}.$$

Remark 10.2.2. $M \preceq N \implies M \preceq_1 N$.

Fix a theory T. **“Model” will always mean model of T.**

Definition 10.2.3. A model $M \models T$ is *existentially closed* if for any larger model $N \models T$ with $N \supseteq M$, we have $M \preceq_1 N$.

Theorem 10.2.4. *If T has quantifier-elimination, then every model of T is existentially closed.*

Proof. Suppose $M \subseteq N$ are models of T. Then $M \preceq N$ by quantifier elimination (Theorem 8.3.6), and so $M \preceq_1 N$. □

Theorem 10.2.5. *If T is inductive, then any model M embeds into an existentially closed model $N \supseteq M$.*

Proof. If $M \models T$ and $\varphi(\bar{x})$ is a quantifier-free $\mathcal{L}(M)$-formula, say that $\varphi(\bar{x})$ is *realizable beyond* M if it is realized in some larger model $N \supseteq M$. We make two observations:

1. A model M is existentially closed iff every quantifier-free $\mathcal{L}(M)$-formula that is realizable beyond M is already realized in M.

2. If N extends M and a quantifier-free $\mathcal{L}(M)$-formula φ is realizable beyond N, then it is realizable beyond M—the extension of N where φ is realized is an extension of M.

Claim. For any model M, there is a larger model $M^* \supseteq M$ such that every quantifier-free $\mathcal{L}(M)$-formula that is realizable beyond M^* is realized in M^*.

Proof. Let $\{\varphi_\alpha\}_{\alpha<\kappa}$ enumerate all quantifier-free $\mathcal{L}(M)$-formulas. Build an increasing chain of models $\{M_\alpha\}_{\alpha<\kappa}$ as follows:

1. $M_0 = M$.

2. If φ_α is realizable beyond M_α, then $M_{\alpha+1}$ is an extension of M_α with a realization of φ_α. Otherwise take $M_{\alpha+1} = M_\alpha$.

3. If α is a limit ordinal, take $M_\alpha = \bigcup_{\beta<\alpha} M_\beta$. This is a model because the theory is inductive.

Let $M^* = \bigcup_{\alpha<\kappa} M_\alpha$. Again, this is a model because T is inductive. Suppose φ is a quantifier-free $\mathcal{L}(M)$-formula that is realizable beyond M^*. Then $\varphi = \varphi_\alpha$ for some α. By observation (2) above, φ_α is realizable beyond $M_\alpha \subseteq M^*$. Then φ_α is realized in $M_{\alpha+1}$ by construction. That is, $M_{\alpha+1} \models \varphi_\alpha(\bar{c})$ for some tuple $\bar{c}$ in $M_{\alpha+1}$. As M^* extends $M_{\alpha+1}$ and φ_α is quantifier-free, $M^* \models \varphi_\alpha(\bar{c})$. $\square_{\text{Claim}}$

Using the claim, build an increasing chain of length ω:

$$M = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$$

where $M_{i+1} = M_i^*$. Let $N = \bigcup_{n=0}^{\infty} M_n$. Again, $N \models T$ because T is inductive. We claim N is existentially closed. Take a quantifier-free $\mathcal{L}(N)$-formula φ that is realizable beyond N. Then φ is an $\mathcal{L}(M_i)$-formula for some $i < \omega$. By observation (2), φ is realizable beyond $M_{i+1} = M_i^*$, so φ is realized in M_{i+1}. Then φ is realized in N, and N is existentially closed by observation (1). □

10.3 Existentially closed fields

Lemma 10.3.1. *Let K, L be fields, and $\alpha : K \to L$ be a ring homomorphism. Then α is injective.*

Proof. Let $I = \ker(\alpha)$. We claim $I = \{0\}$. Otherwise take $a \in I \setminus \{0\}$. Then $1 = a^{-1}a \in I$, so $1^L = \alpha(1^K) = 0^L$, contradicting the definition of "field."

As $\ker(\alpha) = \{0\}$, it follows that

$$\alpha(x) = \alpha(y) \iff x - y \in \ker(\alpha) \iff x - y = 0 \iff x = y.$$

This means that α is injective. □

Lemma 10.3.2. *If K is a field and $P(x)$ is a polynomial of positive degree, then there is a larger field $L \supseteq K$ in which $P(x)$ has a root.*

Proof. Write $P(x)$ as a product $\prod_{i=1}^{n} Q_i(x)$ of irreducible factors. Replacing $P(x)$ with one of its irreducible factors, we may assume $P(x)$ is irreducible. Then $K[x]/P(x)K[x]$ is a field (Theorem 9.1.10). The composition

$$K \overset{\subseteq}{\to} K[x] \to K[x]/P(x)K[x]$$

is a homomorphism of fields, hence an embedding (Lemma 10.3.1). Up to isomorphism, $L := K[x]/P(x)K[x]$ is a field extending K. The fact that

$$P(x) \equiv 0 \pmod{P(x)} \text{ in } K[x]$$

means that

$$P(x) = 0 \text{ in } L$$

and so the element x is a root of P in L. □

An *existentially closed field* is a field that is existentially closed among the class of all fields.

Theorem 10.3.3. *If K is an existentially closed field, then K is algebraically closed.*

Proof. Let $P(x) \in K[x]$ be a polynomial of positive degree. By Lemma 10.3.2, the quantifier-free $\mathcal{L}(K)$-formula $P(x) = 0$ is realized in a field extending K. As K is existentially closed, it is realized in K, meaning that $P(x)$ has a root. □

Corollary 10.3.4. *If K is a field, then there is an algebraically closed field L extending K.*

Proof. The class of fields is inductive, so Theorem 10.2.5 applies. □

Corollary 10.3.5. *For every $p \in \{0, 2, 3, 5, 7, \ldots\}$, there are algebraically closed fields of characteristic p.*

Proof. Take a field K of characteristic p (Theorem 2.7.8) and an algebraically closed field $M \supseteq K$ by Corollary 10.3.4. Then $\operatorname{char}(M) = \operatorname{char}(K) = p$ because characteristic doesn't change in field extensions (Theorem 2.7.11). □

Theorem 10.3.6. *A field K is existentially closed if and only if it is algebraically closed.*

Proof. If K is existentially closed, then K is algebraically closed by Theorem 10.3.3. Conversely, suppose K is algebraically closed. We claim K is existentially closed. Let $L \supseteq K$ be an extension. By Corollary 10.3.4 there is an algebraically closed field $M \supseteq L \supseteq K$. Because ACF has quantifier elimination, algebraically closed fields are existentially closed *among algebraically closed fields*, and so $K \preceq_1 M$. But this implies $K \preceq_1 L$: if a quantifier-free $\mathcal{L}(K)$-formula φ is realized in L, then it is realized in M, hence realized in K. □

Chapter 11

Monster models

11.1 Pushing types along partial elementary maps

This chapter is about *monster models*, or more precisely, about *κ-saturated* and *strongly κ-homogeneous* models. The basic idea of saturated models is similar to existentially closed models:

Everything which could exist does exist.

For existentially closed models (Chapter 10), this meant

> If a *quantifier-free formula* $\varphi(x)$ over M is satisfied in an *extension* of M, then it is satisfied in M.

For monster models, we want something slightly different:

> If a *partial type* $\Sigma(x)$ over M is satisfied in an *elementary extension* of M, then it is satisfied in M.

As written above, this is usually impossible—the set of formulas $\{x \neq a : a \in M\}$ is satisfied in an elementary extension, but not satisfied in M. Instead, we only want to consider partial types that are "small." This leads to the notion of *κ-saturation* for a fixed cardinal κ. A structure M is κ-saturated if every type over a small subset of M is realized in M, where "small" means "size less than κ."

There is also a closely related notion called *strong κ-homogeneity*, which says that if two small tuples $\bar{a}, \bar{b}$ in M have the same type, then there is an isomorphism $\sigma : M \to M$ sending $\bar{a} \mapsto \bar{b}$. This means that M is highly symmetric.

Finally, a *monster model* is a model $\mathbb{M}$ that is κ-saturated and strongly κ-homogeneous for some very big cardinal κ. Monster models exist (Section 11.4), and have a number of favorable properties. For example, every small model occurs as an elementary substructure of the monster $\mathbb{M}$ (Theorem 11.2.4), definable sets satisfy a property like compactness in topology (Theorem 11.2.7), and we can detect the parameters needed to define a set by studying the symmetries of $\mathbb{M}$ (Theorem 11.3.8). Because of these good properties, it is common in more advanced model theory to always work within a monster model. We will follow this approach in later chapters.

As an application of monster models, we give a relatively simple criterion for quantifier elimination in Theorem 11.5.4, and use it to study the model theory of discrete linear orders in Section 11.6.

Theorem 11.1.1. *Let M, N be $\mathcal{L}$-structures and $f : A \to B$ be a partial elementary map from M to N. If $\Sigma(\bar{x})$ is a set of $\mathcal{L}(A)$-formulas, let $f_*\Sigma(\bar{x})$ be*

$$\{\varphi(\bar{x}, f(\bar{c})) : \bar{c} \in A,\ \varphi(\bar{x}, \bar{c}) \in \Sigma(\bar{x})\}.$$

1. *If $\Sigma(\bar{x})$ is finite, then $\Sigma(\bar{x})$ is realized in M if and only if $f_*\Sigma(\bar{x})$ is realized in N.*

2. *$\Sigma(\bar{x})$ is finitely realized in M if and only if $f_*\Sigma(\bar{x})$ is finitely realized in N.*

3. *f_* gives a bijection between partial types over A and partial types over B.*

4. *f_* gives a bijection between $S_n(A)$ and $S_n(B)$.*

Proof.

1. Write $\Sigma(\bar{x})$ as $\{\varphi_i(\bar{x}, \bar{c}_i) : 1 \leq i \leq n\}$. Then

$$M \models \exists \bar{x} \bigwedge_{i=1}^{n} \varphi_i(\bar{x}, \bar{c}_i) \iff N \models \exists \bar{x} \bigwedge_{i=1}^{n} \varphi_i(\bar{x}, f(\bar{c}_i)),$$

because f is a partial elementary map.

2. Clear from (1).

3. By (2), f_* is a map from partial types over A to partial types over B. The inverse map is $(f^{-1})_*$.

4. Clear from (3), since $S_n(A)$ and $S_n(B)$ are exactly the maximal partial types over A and B. □

Corollary 11.1.2. *If $A \subseteq M \preceq N$, then $S_n^M(A) = S_n^N(A)$.*

Proof. The identity map $\mathrm{id}_A : A \to A$ is a partial elementary map from M to N. □

11.2 κ-saturated models

Let κ be an infinite cardinal.

Definition 11.2.1. A structure M is *κ-saturated* if for every $A \subseteq M$ with $|A| < \kappa$ and every $p \in S_1(A)$, p is realized in M.

Fix $\mathcal{L}$-structures N, M, where M is κ-saturated.

Lemma 11.2.2. *Let $f : A \to B$ be a partial elementary map from N to M, with $|A| < \kappa$. For any $\alpha \in N$ there is $\beta \in M$ such that $f \cup \{(\alpha, \beta)\}$ is a partial elementary map.*

Proof. Let $p = \mathrm{tp}(\alpha/A) \in S_1(A)$. Let $f_*p = \{\varphi(x, f(\bar{a})) : \varphi(x, \bar{a}) \in p\}$. By Theorem 11.1.1, $f_*p \in S_1(B)$. As $|B| = |A| < \kappa$, there is $\beta \in M$ realizing f_*p. Then

$$N \models \varphi(\alpha, \bar{c}) \iff \varphi(x, \bar{c}) \in p(x)$$
$$\iff \varphi(x, f(\bar{c})) \in f_*p(x) \iff M \models \varphi(\beta, f(\bar{c}))$$

for any $\mathcal{L}$-formula α and tuple $\bar{c}$ in A, so $f \cup \{(\alpha, \beta)\}$ is a partial elementary map. □

Lemma 11.2.3. *Let $f : A \to B$ be a partial elementary map from N to M. Suppose $A \subseteq A' \subseteq N$, $|A| < \kappa$, and $|A'| \leq \kappa$. Then f can be extended to a partial elementary map $f : A' \to B'$.*

Proof. Write A' as $\{a_\alpha : \alpha < \kappa\}$. Recursively choose partial elementary maps f_α for $\alpha < \kappa$ as follows:

- $f_0 = f$.
- $f_{\alpha+1} = f_\alpha \cup \{(a_\alpha, b)\}$ for some $b \in M$.
- $f_\beta = \bigcup_{\alpha<\beta} f_\alpha$ if β is a limit ordinal.

The successor step $\alpha + 1$ works because $\operatorname{dom}(f_\alpha) \leq |A| + |\alpha| < \kappa$, so Lemma 11.2.2 applies.

Let $g = \bigcup_{\alpha<\kappa} f_\alpha$. Then g is a partial elementary map with domain A'. □

Theorem 11.2.4 (κ-universality). *If M is κ-saturated and $N \equiv M$ with $|N| \leq \kappa$, then there is an elementary embedding $g : N \to M$. In particular, N is isomorphic to an elementary substructure of M.*

Proof. Note that $\varnothing : \varnothing \to \varnothing$ is a partial elementary map from N to M. Use Lemma 11.2.3 to extend to a partial elementary map g with $\operatorname{dom}(g) = N$. Then g is an elementary embedding $N \to M$. □

Theorem 11.2.5. *Suppose M is κ-saturated and $A \subseteq M$ with $|A| < \kappa$. For any finite $n < \omega$ and $p \in S_n(A)$, p is realized in M.*

Proof. Take $N \succeq M$ containing a realization $\bar{b} = p$. Note that $\mathrm{id}_A : A \to A$ is a partial elementary map from N to M. By Lemma 11.2.3, we can extend it to a partial elementary map f with $\operatorname{dom}(f) = A \cup \{a_1, \ldots, a_n\}$. Then

$$\varphi(\bar{x}, \bar{b}) \in p(\bar{x}) \implies N \models \varphi(\bar{a}, \bar{b}) \iff M \models \varphi(f(\bar{a}), \bar{b})$$

for any formula φ and tuple $\bar{b}$ in A, and so $f(\bar{a}) \in M^n$ realizes p. □

Theorem 11.2.6. *Suppose M is κ-saturated, $A \subseteq M$ satisfies $|A| < \kappa$, and $\Sigma(\bar{x})$ is a partial type over A in at most κ variables. Then $\Sigma(\bar{x})$ is realized in M.*

Proof. Similar to Theorem 11.2.5. □

Theorem 11.2.7 (κ-compactness)**.** *Let M be κ-saturated.*

1. *Let $\Sigma(\bar{x})$ be a partial n-type over M. If $|\Sigma| < \kappa$, then $\Sigma(\bar{x})$ is realized in M.*
2. *Suppose $|I| < \kappa$ and X_i is a definable subset of M^n for each $i \in I$. If $\{X_i : i \in I\}$ has FIP, then $\bigcap_i X_i \neq \varnothing$.*

3. *Suppose $X \subseteq M^n$ is definable, $|I| < \kappa$, $Y_i \subseteq M^n$ is definable for $i \in I$, and $X \subseteq \bigcup_{i \in I} Y_i$. Then there is a finite $I_0 \subseteq_f I$ such that $X \subseteq \bigcup_{i \in I_0} Y_i$.*

Proof. 1. Let A be the set of parameters used in $\Sigma(\bar{x})$. Then $|A| < \kappa$, and $\Sigma(\bar{x})$ is a partial n-type over A. Take a complete n-type $p \in S_n(A)$ with $p \supseteq \Sigma(\bar{x})$. Then p is realized in M by Theorem 11.2.5.

2. Write X_i as $\varphi_i(M^n)$ for some $\mathcal{L}(M)$-formula φ_i. Let $\Sigma = \{\varphi_i : i \in I\}$. The FIP means that Σ is finitely realized in M, i.e., a partial type. Apply (1) to find a point realizing Σ, i.e., a point in $\bigcap_{i \in I} X_i$.

3. If there is no finite subcover, then the family

$$\{X\} \cup \{M^n \setminus Y_i : i \in I\}$$

has the FIP. By (2), there is a point $\bar{a} \in X \cap \bigcap_i (M^n \setminus Y_i)$. Then $\bar{a} \in X$ but $\bar{a} \notin \bigcup_i Y_i$, a contradiction. □

Corollary 11.2.8. *If M is κ-saturated and $D \subseteq M^n$ is definable, then one of two things happens:*

1. *D is finite.*
2. *$|D| \geq \kappa$.*

Proof. Otherwise, $\{\{p\} : p \in D\}$ is a small cover of D without a finite subcover, contradicting Theorem 11.2.7(3). □

11.3 Strongly κ-homogeneous models

If M is a structure, then $\mathrm{Aut}(M)$ denotes the set of automorphisms of M, i.e., isomorphisms from M to M. If $A \subseteq M$, then

$$\mathrm{Aut}(M/A) := \{\sigma \in \mathrm{Aut}(M) : \forall x \in A \ \sigma(x) = x\}$$

Definition 11.3.1. M is *strongly κ-homogeneous* if any partial elementary map f from M to M with $|\mathrm{dom}(f)| < \kappa$ can be extended to an automorphism $\sigma \in \mathrm{Aut}(M)$.

Theorem 11.3.2. *Suppose M is strongly κ-homogeneous. Suppose $\bar{a}, \bar{b} \in M^n$, $C \subseteq M$, and $|C| < \kappa$. Then the following are equivalent:*

1. $\mathrm{tp}(\bar{a}/C) = \mathrm{tp}(\bar{b}/C)$.

2. *There is* $\sigma \in \mathrm{Aut}(M/C)$ *with* $\sigma(\bar{a}) = \bar{b}$.

Proof. (1) $\implies$ (2): if $\mathrm{tp}(\bar{a}/C) = \mathrm{tp}(\bar{b}/C)$, then there is a partial elementary map

$$f : C \cup \{a_1, \ldots, a_n\} \to C \cup \{b_1, \ldots, b_n\}$$
$$f(x) = \begin{cases} x & \text{if } x \in C \\ b_i & \text{if } x = a_i \end{cases}$$

Then f extends to an automorphism $\sigma \in \mathrm{Aut}(M)$. Note that $\sigma \supseteq f \supseteq \mathrm{id}_C$, so $\sigma \in \mathrm{Aut}(M/C)$, and $\sigma(\bar{a}) = f(\bar{a}) = \bar{b}$.

(2) $\implies$ (1): isomorphisms preserve all formulas. □

Definition 11.3.3. $\bar{a} \equiv_C \bar{b}$ means $\mathrm{tp}(\bar{a}/C) = \mathrm{tp}(\bar{b}/C)$.

Informal Definition 11.3.4. A *monster model* is a structure that is κ-saturated and strongly κ-homogeneous for some cardinal κ bigger than any cardinals we care about. A set X is "small" or "large" depending on whether $|X| < \kappa$ or $|X| \geq \kappa$.

Work in a monster model $\mathbb{M}$. Fix a small set $A \subseteq \mathbb{M}$.

Definition 11.3.5. A set $X \subseteq \mathbb{M}^n$ is *A-invariant* if $\sigma(X) = X$ for all $\sigma \in \mathrm{Aut}(\mathbb{M}/A)$.

Theorem 11.3.6. *The following are equivalent for* $X \subseteq \mathbb{M}^n$*:*

1. *X is A-invariant.*

2. *If* $\bar{b}, \bar{c} \in \mathbb{M}^n$*, then*

$$\mathrm{tp}(\bar{b}/A) = \mathrm{tp}(\bar{c}/A) \implies (\bar{b} \in A \iff \bar{c} \in A).$$

3. *There is a subset* $X' \subseteq S_n(A)$ *such that*

$$X = \{\bar{b} \in \mathbb{M}^n : \mathrm{tp}(\bar{b}/A) \in X'\}.$$

Proof. Note that (1) means the following: if $\bar{a} \in \mathbb{M}^n$ and $\sigma \in \operatorname{Aut}(\mathbb{M}/C)$, then

$$\bar{a} \in X \iff \sigma(\bar{a}) \in X.$$

This is equivalent to (2) by Theorem 11.3.2. The equivalence of (2) and (3) is clear. □

Remark 11.3.7. An A-definable set $\varphi(\mathbb{M}^n)$ corresponds to the clopen set $[\![\varphi]\!] \subseteq S_n(A)$, so A-definable sets are A-invariant.

Theorem 11.3.8. *If $D \subseteq \mathbb{M}^n$ is definable and A-invariant, then D is A-definable.*

Proof. Note that D is B-definable for some small $B \supseteq A$. Let $f : S_n(B) \to S_n(A)$ be the restriction map sending $\operatorname{tp}(\bar{c}/B)$ to $\operatorname{tp}(\bar{c}/A)$. This map is surjective because every complete type over A extends to a complete type over B. Additionally, it is continuous by Theorem 7.4.4, because the preimage of the clopen set $[\![\varphi]\!] \subseteq S_n(A)$ is the clopen set $[\![\varphi]\!] \subseteq S_n(B)$. As X is A-invariant and B-invariant, there are sets $X_A \subseteq S_n(A)$ and $X_B \subseteq S_n(B)$ such that

$$\bar{c} \in X \iff \operatorname{tp}(\bar{c}/A) \in X_A$$
$$\bar{c} \in X \iff \operatorname{tp}(\bar{c}/B) \in X_B.$$

Then $X_B = f^{-1}(X_A)$. As f is surjective

$$X_A = f(X_B)$$
$$S_n(A) \setminus X_A = f(S_n(B) \setminus X_B).$$

Because X is B-definable the set $X_B \subseteq S_n(B)$ is clopen, and so X_B and $S_n(B) \setminus X_B$ are closed. The image of a closed set is closed (Theorem 7.2.6), so X_A and its complement are both closed. Then X_A is a clopen set $[\![\psi]\!]$, and X is the A-definable set $\psi(\mathbb{M}^n)$. □

11.4 Construction of monster models

A cardinal κ is *regular* if whenever $|I| < \kappa$ and $|X_i| < \kappa$ for every $i \in I$, we have $\left|\bigcup_{i \in I} X_i\right| < \kappa$. The cardinal $\aleph_0$ is regular, because a finite union of finite sets is finite. For any cardinal κ, the successor κ^+ is regular, because a union of at most κ-many sets of size at most κ has size at most $\kappa^2 = \kappa < \kappa^+$. Consequently, for any cardinal κ we can find a larger cardinal that is regular.

If κ is a regular cardinal and $A \subseteq \kappa$ with $|A| < \kappa$, then $\sup(A) < \kappa$. Otherwise, $\sup(A) = \kappa$, and then κ is a union $\bigcup_{\alpha \in A} \alpha$ where $|A| < \kappa$ and $|\alpha| < \kappa$ for each $\alpha \in \kappa$, contradicting regularity.

Lemma 11.4.1. *Let κ be a regular cardinal. Let $\{S_\alpha\}_{\alpha<\kappa}$ be an increasing chain of sets, indexed by κ. If $A \subseteq \bigcup_{\alpha<\kappa} S_\alpha$ and $|A| < \kappa$, then $A \subseteq S_\alpha$ for some $\alpha < \kappa$.*

Proof. Define $f : A \to \kappa$ by $f(x) = \min\{\alpha < \kappa : x \in S_\alpha\}$. Then $|f(A)| \leq |A| < \kappa$, so $\alpha := \sup f(A) < \kappa$. For any $x \in A$, we have $f(x) \in f(A)$ and so $f(x) \leq \alpha$. Then $x \in S_{f(x)} \subseteq S_\alpha$ for any $x \in A$, so $A \subseteq S_\alpha$. □

Definition 11.4.2. A chain of structures $\{M_i\}_{i \in I}$ is *elementary* if $M_i \preceq M_j$ for $i \leq j$.

Theorem 11.4.3 (Tarski-Vaught)**.** *Let $\{M_i\}_{i \in I}$ be an elementary chain of $\mathcal{L}$-structures. Let $M = \bigcup_{i \in I} M_i$. Then $M_i \preceq M$ for all $i \in I$.*

Proof sketch. For each i, note that $\mathrm{eldiag}(M_i)$ is finitely satisfiable, complete, and has the witness property. Therefore the union $\bigcup_i \mathrm{eldiag}(M_i)$ is finitely satisfiable, complete, and has the witness property. The canonical model is M. Then $M \succeq M_i$ because $M \models \mathrm{eldiag}(M_i)$. □

Lemma 11.4.4. *If M is a structure, there is $N \succeq M$ such that every type in $S_1(M)$ is realized in N.*

Proof. Let $\{p_i(x) : i \in I\}$ enumerate $S_1(M)$. Let $\bar{x} = (x_i : i \in I)$ be a tuple of variables, one for each $i \in I$. Let $\Sigma(\bar{x}) = \{p_i(x_i) : i \in i\}$. Then $\Sigma(\bar{x})$ is finitely satisfiable in M because each p_i is finitely satisfiable in M. Therefore, $\Sigma(\bar{x})$ is realized by some tuple $\bar{a} = (a_i : i \in I)$ in an elementary extension $N \succeq M$. The element a_i realizes p_i. □

Theorem 11.4.5. *If M is a structure and κ is a cardinal, there is a κ-saturated $N \succeq M$.*

Proof. Replacing κ with κ^+ if necessary, we may assume κ is regular. Build an elementary chain $\{M_\alpha\}_{\alpha<\kappa}$ by recursion on α:

- $M_0 = M$.
- $M_{\alpha+1}$ is an elementary extension of M_α realizing every complete 1-type over M_α (using Lemma 11.4.4).

- If α is a limit ordinal, take $M_\alpha = \bigcup_{\beta<\alpha} M_\beta$, using the Tarski-Vaught theorem on chains (Theorem 11.4.3).

Let $N = \bigcup_{\alpha<\kappa} M_\alpha$. Then $N \succeq M_0 = M$ by Tarski-Vaught again. If $A \subseteq N$ and $|A| < \kappa$, then $A \subseteq M_\alpha$ for some $\alpha < \kappa$ by Lemma 11.4.1. If $p \in S_1(A)$, then p is a partial type over M_α, so it extends to a complete type $p' \in S_1(M_\alpha)$, which is then realized by some $b \in M_{\alpha+1} \subseteq N$. Therefore N is κ-saturated. □

Lemma 11.4.6. *Let M be a structure and N be an $|M|^+$-saturated elementary extension. Let f be a partial elementary map from M to M.*

1. *There is a partial elementary map g from N to N extending f, with* $\mathrm{dom}(g) = M$.

2. *There is a partial elementary map h from N to N extending f, with* $\mathrm{im}(h) = M$.

Proof.

1. Let $\kappa = |M|^+$. Then N is κ-saturated and $|M| < \kappa$. Note that f is a partial elementary map from M to N. By Lemma 11.2.3, we can extend f to a partial elementary map g from M to N with $\mathrm{dom}(g) = M$.

2. This follows from (1) by symmetry. More precisely, apply part (1) to f^{-1} to get a partial elementary map g extending f^{-1} with $\mathrm{dom}(g) = M$. Then set $h = g^{-1}$, so that $\mathrm{im}(h) = \mathrm{dom}(g) = M$. □

Lemma 11.4.7. *For any M there is an elementary extension $N \succeq M$ with the following properties:*

1. *Every complete type over M is realized in N.*

2. *If f is a partial elementary map from M to M, then there is $\sigma \in$* $\mathrm{Aut}(N)$ *extending f.*

Proof. Build an elementary chain $\{M_i\}_{i<\omega}$ by recursion on i:

- $M_0 = M$.

- M_{i+1} is an $|M_i|^+$-saturated elementary extension of M_i. This is possible by Theorem 11.4.5.

Let $N = \bigcup_{i=0}^{\infty} M_i$. Then $M = M_0 \preceq N$ by the Tarski-Vaught theorem on chains (Theorem 11.4.3). Every complete type over M is already realized in M_1, hence in N.

Let $f : A \to B$ be a partial elementary map from M to M. Recursively build an increasing chain of partial elementary maps $\{f_i\}_{i<\omega}$ with $\mathrm{dom}(f_i), \mathrm{im}(f_i) \subseteq M_i$ as follows:

- $f_0 = f$.
- If $n > 0$, then $f_n : M_n \dashrightarrow M_n$ is a partial elementary map extending $f_{n-1} : M_{n-1} \dashrightarrow M_{n-1}$ with

$$\mathrm{dom}(f_n) = M_{n-1} \text{ if } n \text{ is odd}$$
$$\mathrm{im}(f_n) = M_{n-1} \text{ if } n \text{ is even.}$$

Take $\sigma = \bigcup_{n=0}^{\infty} f_n$. Then σ is a partial elementary map from N to N. The odd steps ensure $\mathrm{dom}(\sigma) \supseteq \bigcup_n M_n = N$, and the even steps ensure $\mathrm{im}(\sigma) \supseteq \bigcup_n M_n = N$. Thus $\mathrm{dom}(\sigma) = \mathrm{im}(\sigma) = N$, and $\sigma \in \mathrm{Aut}(N)$. □

Theorem 11.4.8. *If M is a structure and κ is a cardinal, then there is a κ-saturated, strongly κ-homogeneous elementary extension $N \succeq M$.*

Proof. Replacing κ with κ^+ if necessary, we may assume κ is regular. Build an elementary chain $\{M_\alpha\}_{\alpha<\kappa}$ by recursion on α as follows:

1. $M_0 = M$.
2. $M_{\alpha+1}$ is an elementary extension of M_α as in Lemma 11.4.7. In particular, every complete 1-type over M_α is realized in $M_{\alpha+1}$.
3. If α is a limit ordinal, then $M_\alpha = \bigcup_{\beta<\alpha} M_\beta$. This works by the Tarski-Vaught theorem on chains (Theorem 11.4.3).

Let $N = \bigcup_{\alpha<\kappa} M_\alpha$. As in the proof of Theorem 11.4.5, N is κ-saturated. We prove strong κ-homogeneity. Suppose f is a partial elementary map from N to N with $|\mathrm{dom}(f)| = |\mathrm{im}(f)| < \kappa$. By Lemma 11.4.1, there is $\alpha < \kappa$ with $\mathrm{dom}(f) \cup \mathrm{im}(f) \subseteq M_\alpha$. Then f is a partial elementary map from M_α to M_α. By Lemma 11.4.7, we can extend f to an automorphism $\sigma_{\alpha+1} \in \mathrm{Aut}(M_{\alpha+1})$. Build an increasing chain $\{\sigma_\beta\}_{\alpha<\beta<\kappa}$ with $\sigma_\beta \in \mathrm{Aut}(M_\beta)$ by repeatedly applying Lemma 11.4.7. Take $\sigma = \bigcup_{\alpha<\beta<\kappa} \sigma_\beta$. Then $\sigma \in \mathrm{Aut}(N)$, and $\sigma \supseteq \sigma_{\alpha+1} \supseteq f$. Therefore N is strongly κ-homogeneous. □

11.5 Saturation and back-and-forth

Theorem 11.5.1. *Let M and N be ω-saturated. For any $\bar{a} \in M^n$ and $\bar{b} \in N^n$ with $\operatorname{tp}(\bar{a}) = \operatorname{tp}(\bar{b})$, let $g_{\bar{a},\bar{b}}$ be the isomorphism from $\langle \bar{a} \rangle_M$ to $\langle \bar{b} \rangle_N$ sending $\bar{a}$ to $\bar{b}$ as in Theorem 8.3.4. Then the family $\mathcal{F} = \{g_{\bar{a},\bar{b}} : n \in \mathbb{N},\ \bar{a} \in M,\ \bar{b} \in N,\ \operatorname{tp}(\bar{a}) = \operatorname{tp}(\bar{b})\}$ is a back-and-forth system.*

Proof. We verify the "forward" condition; "backward" is similar. Fix some $g_{\bar{a},\bar{b}}$. Let a' be an element of M. By Lemma 11.2.2 we can extend the partial elementary map $\bar{a} \mapsto \bar{b}$ to a partial elementary map $(\bar{a}, a') \mapsto (\bar{b}, b')$. Then $\operatorname{tp}(\bar{a}, a') = \operatorname{tp}(\bar{b}, b')$, and $g_{\bar{a}a',\bar{b}b'}$ is the desired partial isomorphism in $\mathcal{F}$ extending $g_{\bar{a},\bar{b}}$ and containing a' in its domain. □

Corollary 11.5.2. *If M, N are countable and ω-saturated, and $M \equiv N$, then $M \cong N$.*

Proof. Let $\mathcal{F}$ be as in Theorem 11.5.1. By Theorem 5.6.4, it suffices to show that $\mathcal{F}$ is non-empty. We only need to find some $n \in \mathbb{N}$, some $\bar{a} \in M^n$, and $\bar{b} \in N^n$ with $\operatorname{tp}(\bar{a}) = \operatorname{tp}(\bar{b})$. Take $n = 0$, $\bar{a} = () \in M^0$, and $\bar{b} = () \in N^0$. Then $\operatorname{tp}(\bar{a}) = \operatorname{Th}(M) = \operatorname{Th}(N) = \operatorname{tp}(\bar{b})$. □

Corollary 11.5.3. *If M is countable and ω-saturated, then M is strongly ω-homogeneous.*

Proof. Let $f : A \to B$ be a partial elementary map from M to M, with A and B finite. Let $\bar{a}$ be a tuple enumerating A. Then $\bar{b} := f(\bar{a})$ enumerates B, and $\operatorname{tp}(\bar{a}) = \operatorname{tp}(\bar{b})$. We must find $\sigma \in \operatorname{Aut}(M)$ with $\sigma(\bar{a}) = \bar{b}$. If $\mathcal{F}$ is the back-and-forth system between M and M given by Theorem 11.5.1, then $g_{\bar{a},\bar{b}} \in \mathcal{F}$. By Lemma 5.6.3, there is an isomorphism $\sigma : M \to M$ extending $g_{\bar{a},\bar{b}}$. Then $\sigma(\bar{a}) = \bar{b}$. □

Theorem 11.5.4. *Let κ be an infinite cardinal. The following are equivalent:*

1. *T has quantifier elimination.*

2. *If M, N are κ-saturated structures, then the family $\mathcal{F}_0$ of* all *finitely generated partial isomorphisms from M to N is a back-and-forth system.*

Proof. (1) $\implies$ (2): Note that M, N are ω-saturated. If $\bar{a} \in M^n$ and $\bar{b} \in N^n$ and $\mathrm{qftp}(\bar{a}) = \mathrm{qftp}(\bar{b})$, let $g_{\bar{a},\bar{b}} : \langle \bar{a} \rangle_M \to \langle \bar{b} \rangle_N$ be the partial isomorphism sending $\bar{a}$ to $\bar{b}$ from Theorem 8.3.4. Then

$$\mathcal{F}_0 = \{g_{\bar{a},\bar{b}} : \mathrm{qftp}(\bar{a}) = \mathrm{qftp}(\bar{b})\}.$$

By quantifier elimination, this is

$$\mathcal{F}_0 = \{g_{\bar{a},\bar{b}} : \mathrm{tp}(\bar{a}) = \mathrm{tp}(\bar{b})\},$$

which is a back-and-forth system by Theorem 11.5.1.

(2) $\implies$ (1): By Theorem 8.3.3, it suffices to show that if $M, N \models T$, if $\bar{a} \in M^n$ and $\bar{b} \in N^n$, then

$$\mathrm{qftp}^M(\bar{a}) = \mathrm{qftp}^N(\bar{b}) \implies \mathrm{tp}^M(\bar{a}) = \mathrm{tp}^N(\bar{b}).$$

Replacing M and N by elementary extensions, we may assume M and N are κ-saturated. By (2), the family $\mathcal{F}_0$ of finitely generated partial isomorphisms from M to N is a back-and-forth system. Suppose $\mathrm{qftp}^M(\bar{a}) = \mathrm{qftp}^N(\bar{b})$. Then $\mathcal{F}$ contains the isomorphism $g_{\bar{a},\bar{b}} : \langle \bar{a} \rangle_M \to \langle \bar{b} \rangle_N$. By Theorem 3.7.6, $g_{\bar{a},\bar{b}}$ is a partial elementary map, so $\mathrm{tp}(\bar{a}) = \mathrm{tp}(\bar{b})$. □

11.6 Application: discrete linear orders with endpoints

Definition 11.6.1. Let x, y be elements in a linear order $(M, \leq)$. Then y is a *successor* of x, and x is a *predecessor* of y, written $x \lhd y$, if $x < y$ but there is no $z \in M$ with $x < z < y$.

Let T be the theory of linear orders $(M, \leq)$ such that the following hold:

1. $\min(M)$ and $\max(M)$ exist. In particular, M is non-empty.
2. Every $x \in M$ other than $\max(M)$ has a successor $y \rhd x$.
3. Every $x \in M$ other than $\min(M)$ has a predecessor $y \lhd x$.

Example 11.6.2. Any finite non-empty linear order is a model of T.

Definition 11.6.3. Suppose $M \models T$ and $x, y \in M$. The *distance* between x and y, written $d(x, y)$, is the element of $\mathbb{N} \cup \{\infty\}$ defined as follows:

1. If $x = y$, then $d(x, y) = 0$.

2. If $x < y$, then $d(x, y)$ is $1 + |\{z \in M : x < z < y\}|$.

3. If $x > y$, then $d(y, x) = d(x, y)$.

Note that we define $d(x, y)$ to be the symbol "∞" when $[x, y]$ is infinite, rather than distinguishing cardinalities.

Let $\mathcal{L}'$ be the base language of orders $\mathcal{L} = \{\leq\}$ plus two new constant symbols $\min, \max$ and a binary relation R_n for each $n < \infty$. Expand any model $M \models T$ to an $\mathcal{L}'$-structure by interpreting the new symbols as follows:

1. $\min^M = \min(M)$.

2. $\max^M = \max(M)$.

3. $R_n^M(x, y) \iff d(x, y) = n$.

The resulting $\mathcal{L}'$-structures are the models of some $\mathcal{L}'$-theory T'.

Remark 11.6.4. Let M, N be models of T'. Suppose

$$\begin{gathered}\min(M) = a_1 < a_2 < \cdots < a_n = \max(M)\\ \min(N) = b_1 < b_2 < \cdots < b_n = \max(N)\\ d(a_i, a_{i+1}) = d(b_i, b_{i+1}) \text{ for } 1 \leq i < n.\end{gathered}$$

Then there is a partial isomorphism

$$\begin{gathered}f : \{a_1, \ldots, a_n\} \to \{b_1, \ldots, b_n\}\\ f(a_i) = b_i.\end{gathered}$$

Moreover, all finite partial isomorphisms from M to N arise in this way.

Lemma 11.6.5. *Let M, N be $\aleph_1$-saturated models of T'. Let $\mathcal{F}$ be the collection of finite partial isomorphisms $f : A \to B$. Then $\mathcal{F}$ is a back-and-forth system.*

Proof. By symmetry we only need to prove the forward condition. Let $f : A \to B$ be a finite partial isomorphism and α be an element of M. We must find $f' \in \mathcal{F}$ extending f with $\alpha \in \mathrm{dom}(f')$. We may assume $\alpha \notin \mathrm{dom}(f)$; otherwise take $f' = f$. By Remark 11.6.4, f has the form

$$f : \{a_1, \ldots, a_n\} = \{b_1, \ldots, b_n\}$$
$$f(a_i) = b_i$$

where

$$\min(M) = a_1 < a_2 < \cdots < a_n = \max(M)$$
$$\min(N) = b_1 < b_2 < \cdots < b_n = \max(N)$$
$$d(a_i, a_{i+1}) = d(b_i, b_{i+1}) \text{ for } 1 \leq i < n.$$

There must be some i such that $a_i < \alpha < a_{i+1}$. (The cases $\alpha < a_1 = \min(M)$ and $\alpha > a_n = \max(M)$ are impossible.) By Remark 11.6.4, we must find β such that

$$b_i < \beta < b_{i+1}$$
$$d(b_i, \beta) = d(a_i, \alpha) =: x$$
$$d(\beta, b_{i+1}) = d(\alpha, a_{i+1}) =: y.$$

Note that $d(b_i, b_{i+1}) = d(a_i, a_{i+1}) = x + y$. There are four cases:

1. $x, y < \infty$. Take β between b_i and b_{i+1} with $d(b_i, \beta) = x$. Then $d(\beta, b_{i+1}) = (x + y) - x = y$ as desired.

2. $x < \infty = y$. Then $d(b_i, b_{i+1}) = \infty$. Take β between b_i and b_{i+1} with $d(b_i, \beta) = x$. Then $d(\beta, b_{i+1}) = \infty$.

3. $y < \infty = x$. Similar.

4. $x = y = \infty$. As $d(b_i, b_{i+1}) = \infty$, there are

   $$b_i \lhd c_1 \lhd c_2 \lhd \cdots \leq \cdots \lhd d_2 \lhd d_1 \lhd b_{i+1}.$$

   The partial type $\{x > c_i : i < \omega\} \cup \{x < d_i : i < \omega\}$ is realized in M, by $\aleph_1$-saturation. Let β be a realization. Then $b_i < \beta < b_{i+1}$, and $d(b_i, \beta) = d(\beta, b_{i+1}) = \infty$. □

Theorem 11.6.6. *The theory T' has quantifier elimination.*

Corollary 11.6.7. *Let M be an infinite model of T. Let M_0 be the set of $x \in M$ such that $d(x, \min(M)) < \infty$ or $d(x, \max(M)) < \infty$. Then $M_0 \preceq M$.*

Proof. Working in the expanded language $\mathcal{L}'$, it is easy to see that M_0 is a substructure of M and $M_0 \models T'$. Then $M_0 \preceq M$ because submodels are elementary substructures in theories with quantifier elimination (Theorem 8.3.6(2)). □

Definition 11.6.8. If M is a model of T, the *length* of M, written $\ell(M)$, is $d(\min(M), \max(M)) \in \mathbb{N} \cup \{\infty\}$.

Corollary 11.6.9. *Two models $M, N \models T$ are elementarily equivalent if and only if $\ell(M) = \ell(N)$.*

Proof. If $M \equiv N$, then certainly $\ell(M) = \ell(N)$, essentially because the relations R_n are definable, or simply because $\ell(M)$ is $|M| - 1$.

Conversely, suppose $\ell(M) = \ell(N)$. Let M' and N' be the expansions of M and N to models of T. Note that the minimal substructure $\langle \varnothing \rangle_{M'}$ contains only the two points $\min(M)$ and $\max(M)$. This substructure is determined up to isomorphism by $\ell(M)$. For example, $R_n(\min(M), \max(M))$ holds iff $\ell(M) = n$. Because $\ell(M) = \ell(N)$, we have $\langle \varnothing \rangle_{M'} \cong \langle \varnothing \rangle_{N'}$, and so $M' \equiv N'$ by quantifier elimination (because of Theorem 8.3.5). Restricting to $\mathcal{L}$-sentences, we see $M \equiv N$. □

Corollary 11.6.10. *The theory of infinite models of T is complete and decidable.*

Corollary 11.6.11. *The class $\mathcal{K}$ of models of T is the elementary class generated by finite non-empty linear orders.*

Proof. Certainly $\mathcal{K}$ is an elementary class containing the finite non-empty linear orders. If $\mathcal{K}'$ is a smaller such elementary class, take $M \in \mathcal{K} \setminus \mathcal{K}'$. Then M is infinite or else $M \in \mathcal{K}'$. Because $\mathcal{K}'$ contains models of size $> n$ for each n, it must contain an infinite model N (Theorem 5.4.5). Then M, N are infinite models of T, so Corollary 11.6.10 shows $M \equiv N \in \mathcal{K}'$. Then $M \in \mathcal{K}'$, contradicting the choice of M. □

Corollary 11.6.12. *If φ is a sentence in the language of orders, then the following are equivalent:*

- *$T \vdash \varphi$.*
- *Every finite non-empty linear order satisfies φ.*

Chapter 12

Countable categoricity

Recall that a theory is *κ-categorical* if it has exactly one model of cardinality κ. This chapter is about $\aleph_0$-categoricity, which behaves very different from κ-categoricity for $\kappa > \aleph_0$. We have seen one example of an $\aleph_0$-categorical theory already—the theory DLO of dense linear orders (Corollary 5.6.5). We showed that DLO is $\aleph_0$-categorical via a back-and-forth argument. We will see in Theorem 12.3.5 that this is the *only* way that a theory can be $\aleph_0$-ategorical.

Moreover, $\aleph_0$-categoricity of T is equivalent to a number of structural properties of T and its models. Specifically, the following are equivalent if T is a theory and M is a countable model:

1. T is $\aleph_0$-categorical.

2. For each n, the type space $S_n(T)$ is finite.

3. For each n and finite set $A \subseteq_f M$, there are only finitely many A-definable subsets of M^n.

4. For each n, the action of $\mathrm{Aut}(M)$ on M^n has only finitely many orbits.

5. Every countable model of T is ω-saturated.

This combination of facts is due to Engeler, Ryll-Nardzewski, and Svenonius, and is sometimes called the *Ryll-Nardzewski theorem.*

As an "application" of this theorem, we show that no theory of fields is $\aleph_0$-categorical (Theorem 13.4.3). That is, if T is a theory whose models are infinite fields, then T has at least two countable models.

The proof of the Ryll-Nardzewski theorem involves another important fact, the *omitting types theorem.* A type $p \in S_n(T)$ is *omitted* in a model M if it is not realized in M. It turns out that whether a type can be omitted is closely related to the topology on $S_n(T)$. Say that p is *non-isolated* if p is a limit point of $S_n(T) \setminus \{p\}$, and *isolated* otherwise. If p is isolated, then p is realized in any model (Theorem 12.2.2), but if p is non-isolated, then p is omitted in some model (Theorem 12.2.7). In fact, given any countable set of non-isolated types, there is a model omitting all of them. We will apply this in the proof of the Ryll-Nardzewski theorem, but there are other applications.

12.1 Baire category theorem

Let S be a non-empty Stone space (Definition 7.4.2).

Definition 12.1.1. $X \subseteq S$ is *dense* if X intersects any non-empty clopen set $Y \subseteq S$.

Definition 12.1.2. A set $X \subseteq S$ is *comeager* if X contains a countable intersection of dense open sets.

Remark 12.1.3. Dense open sets are comeager. A countable intersection of comeager sets is comeager.

Theorem 12.1.4 (Baire category theorem)**.** *If $X \subseteq S$ is comeager, then X is dense, hence non-empty.*

Proof. Because S is a Stone space, every open set is a union of clopen sets. Therefore every non-empty open set contains a non-empty clopen set.

Suppose $X \supseteq \bigcup_{i=1}^{\infty} U_i$ where each U_i is open and dense. Let V_0 be a non-empty clopen set. Then $V_0 \cap U_1$ is a non-empty open set. It contains a non-empty clopen set V_1. Similarly, $V_1 \cap U_2$ contains a non-empty clopen set V_2. Continuing, we can build a descending chain of clopen sets

$$V_0 \supseteq V_1 \supseteq V_2 \supseteq \cdots$$

with $V_i \subseteq U_i$. The family $\{V_0, V_1, V_2, \ldots\}$ has the FIP, so the intersection is non-empty by compactness (Theorem 7.1.15). Take $p \in \bigcap_{i=0}^{\infty} V_i \subseteq V_0 \cap \bigcap_{i=1}^{\infty} U_i \subseteq V_0 \cap X$. Then X intersects V_0 as desired. □

12.2 The omitting types theorem

Fix an $\mathcal{L}$-structure M, subset $A \subseteq M$, and $n < \omega$.

Definition 12.2.1. A complete type $p \in S_n(A)$ is *isolated* if $\{p\}$ is clopen.

Theorem 12.2.2. *If p is isolated, then p is realized in M.*

Proof. As $\{p\}$ is clopen, $\{p\} = [\![\varphi]\!] \subseteq S_n(A)$ for some $\mathcal{L}(A)$-formula $\varphi(\bar{x}) \in p(\bar{x})$. Then $\varphi(\bar{x})$ is satisfied by $b \in M$, as p is finitely satisfiable. If $p' = \operatorname{tp}(b/A) \in S_n(A)$, then $p' \in [\![\varphi]\!] = \{p\}$, so $p' = p$ and b realizes p. □

Fix a complete theory T in a countable language $\mathcal{L}$.

Definition 12.2.3. If $p \in S_n(T)$ and $M \models T$, then M *omits* p if p isn't realized in M.

Let $S_\omega(T)$ be the space of complete ω-types $\operatorname{tp}(a_0, a_1, a_2, \ldots)$, i.e., complete types in the variables $\bar{x} = (x_0, x_1, x_2, \ldots)$. Work in a monster model $\mathbb{M} \models T$.

Lemma 12.2.4. *There is a comeager set $W \subseteq S_\omega(T)$ such that if $\bar{c} \in \mathbb{M}^\omega$ and $\operatorname{tp}(\bar{c}) \in W$, then $\{c_i : i \in \omega\} \preceq \mathbb{M}$.*

Proof.

Claim. For any formula $\varphi(\bar{x}, y)$, the following open set is dense:

$$U_\varphi := [\![\neg\exists y\ \varphi(\bar{x}, y)]\!] \cup \bigcup_{i=0}^{\infty} [\![\varphi(\bar{x}, x_i)]\!].$$

Proof. Take non-empty $[\![\psi]\!] \subseteq S_\omega(T)$. Suppose for the sake of contradiction that $[\![\psi]\!] \cap U_\varphi = \varnothing$. Then $[\![\psi]\!]$ doesn't intersect the sets in the union, which means the following:

$$\psi(\bar{x}) \wedge (\neg\exists y\ \varphi(\bar{x}, y)) \text{ is inconsistent}$$
$$\psi(\bar{x}) \wedge \varphi(\bar{x}, x_i) \text{ is inconsistent, for each } i < \omega.$$

Take $\bar{c} \in \mathbb{M}^\omega$ realizing $\psi(\bar{x})$. By the first line, $\mathbb{M} \models \exists y\ \varphi(\bar{c}, y)$. Thus $\mathbb{M} \models \varphi(\bar{c}, e)$ for some $e \in \mathbb{M}$. Take $i \gg 0$ so that x_i doesn't occur in $\psi(\bar{x})$ or $\varphi(\bar{x}, y)$. Changing c_i to e, we may assume $\mathbb{M} \models \varphi(\bar{c}, c_i)$, contradicting the second line. $\square_{\text{Claim}}$

Now let W be the comeager set $\bigcap_\varphi U_\varphi$. Suppose $\bar{c} \in \mathbb{M}^\omega$ and $\mathrm{tp}(\bar{c}) \in W$. We claim that $M := \{c_i : i \in \omega\} \preceq \mathbb{M}$ by the Tarski-Vaught criterion (Theorem 5.3.1). Suppose $D \subseteq \mathbb{M}^1$ is M-definable, defined as $\varphi(\bar{c}, \mathbb{M})$ for some $\varphi(\bar{x}, y)$. If $D \neq \varnothing$, then $\mathbb{M} \models \exists y\ \varphi(\bar{c}, y)$, so $\mathrm{tp}(\bar{c}) \notin [\![\neg\exists y\ \varphi(\bar{x}, y)]\!]$. But $\mathrm{tp}(\bar{c}) \in U_\varphi$, so $\mathrm{tp}(\bar{c}) \in [\![\varphi(\bar{x}, x_i)]\!]$ for some i, which means $\mathbb{M} \models \varphi(\bar{c}, c_i)$, or equivalently, $c_i \in D$. Thus $M = \{c_i : i \in \omega\}$ intersects every non-empty M-definable set $D \subseteq \mathbb{M}^1$. □

Lemma 12.2.5. *For any $j_1, \ldots, j_n < \omega$, let $f_{\bar{j}} : S_\omega(T) \to S_n(T)$ be the restriction map $\mathrm{tp}(\bar{c}) \mapsto \mathrm{tp}(c_{j_1}, \ldots, c_{j_n})$.*

1. *f is continuous.*
2. *If $X \subseteq S_\omega(T)$ is clopen, then $f(X) \subseteq S_n(T)$ is clopen.*

Proof. 1. The preimage of $[\![\varphi(y_1, \ldots, y_n)]\!] \subseteq S_n(T)$ is $[\![\varphi(x_{j_1}, \ldots, x_{j_n})]\!] \subseteq S_\omega(T)$.

2. If $X = [\![\varphi]\!]$, then

$$X = \{\mathrm{tp}(\bar{c}) : \bar{c} \in \mathbb{M}^\omega,\ \mathbb{M} \models \varphi(\bar{c})\}$$
$$f(X) = \{\mathrm{tp}(c_{j_1}, \ldots, c_{j_n}) : \bar{c} \in \mathbb{M}^\omega,\ \mathbb{M} \models \varphi(\bar{c})\}.$$

(The first line holds by saturation of $\mathbb{M}$.) Now the set

$$\{(c_{j_1}, \ldots, c_{j_n}) : \bar{c} \in \mathbb{M}^\omega,\ \mathbb{M} \models \varphi(\bar{c})\}$$

is definable, defined by the formula

$$\psi(y_1, \ldots, y_n) := \exists x_0, \ldots, x_N \ \left(\varphi(\bar{x}) \wedge \bigwedge_{i=1}^n y_i = x_{j_i}\right),$$

where N is large enough to quantify away all x_i's appearing in $\varphi(\bar{x})$. Then

$$f(X) = \{\mathrm{tp}(\bar{a}) : \bar{a} \in \psi(\mathbb{M}^n)\} = [\![\psi]\!].$$ □

Lemma 12.2.6. *Let $p \in S_n(T)$ be non-isolated. There is a comeager set $V_p \subseteq S_\omega(T)$ such that if $\bar{c} \in \mathbb{M}^\omega$ and $\mathrm{tp}(\bar{c}) \in V_p$, then p is not realized by any tuple in $C = \{c_i : i < \omega\}$.*

Proof.

Claim. For any $j_1, \ldots, j_n \in \omega$, there is a dense open set $U_{\bar{j}} \subseteq S_\omega(T)$ such that if $\mathrm{tp}(\bar{c}) \in U_{\bar{j}}$, then $(c_{j_1}, \ldots, c_{j_n})$ doesn't realize p.

Proof. Let $f = f_{\bar{j}} : S_\omega(T) \to S_n(T)$ be the restriction map from Lemma 12.2.5. Points are closed (Theorem 7.1.11) so $S_n(T) \setminus \{p\}$ is open and the preimage $U := f^{-1}(S_n(T) \setminus \{p\})$ is open. For density, suppose $X \subseteq S_\omega(T)$ is clopen and non-empty, but $X \cap U = \varnothing$. Then $f(X) \subseteq \{p\}$. But $f(X)$ is clopen by Lemma 12.2.5(2), and non-empty, so $f(X) = \{p\}$ and p is isolated, a contradiction. Thus U is dense. Finally, if $\mathrm{tp}(\bar{c}) \in U$, then $\mathrm{tp}(c_{j_1}, \ldots, c_{j_n}) \in S_n(T) \setminus \{p\}$, meaning that $(c_{j_1}, \ldots, c_{j_n})$ doesn't realize p. $\square_{\text{Claim}}$

Take $V_p = \bigcap_{\bar{j} \in \mathbb{N}^n} U_{\bar{j}}$. If $\mathrm{tp}(\bar{c}) \in V_p$, then $(c_{j_1}, \ldots, c_{j_n})$ doesn't realize p for any $\bar{j} \in \mathbb{N}^\omega$. □

Theorem 12.2.7 (Omitting types theorem)**.** *Let $p_1, p_2, \ldots$ be a countable list of non-isolated complete types $p_i \in S_{n_i}(T)$. Then there is a countable model $M \models T$ omitting every p_i.*

Proof. Let W and V_p be the comeager sets from Lemmas 12.2.4 and 12.2.6. The set $Q = W \cap \bigcap_{i=1}^\infty V_{p_i}$ is comeager, hence non-empty by the Baire Category Theorem. Take $\bar{c} \in \mathbb{M}^\omega$ with $\mathrm{tp}(\bar{c}) \in Q$, and let $M = \{c_i : i < \omega\}$. Then $M \preceq \mathbb{M}$ because $\mathrm{tp}(\bar{c}) \in W$, and M omits p_i because $\mathrm{tp}(\bar{c}) \in V_{p_i}$. □

12.3 Countably categorical theories

Work in a monster model $\mathbb{M} \models T$.

Lemma 12.3.1. *$S_n(A)$ is finite iff all types in $S_n(A)$ are isolated.*

Proof. Suppose $S_n(A)$ is finite. Every point is closed (Theorem 7.1.11), and a finite union of closed sets is closed, so every subset of $S_n(A)$ is closed, every subset is open, and every subset is clopen, implying every point is isolated.

Conversely, suppose every point is isolated. Then $S_n(A) = \bigcup_{p \in S_n(A)} \{p\}$ is an open cover. By compactness of $S_n(A)$, there is a finite subcover, and so $S_n(A)$ is finite. □

Lemma 12.3.2. *$S_n(A)$ is finite iff there are only finitely many A-definable sets $D \subseteq M^n$.*

Proof. The boolean algebra of A-definable sets is isomorphic to the boolean algebra of clopen sets in $S_n(A)$. If $S_n(A)$ is finite, then there are only finitely many clopen sets. Conversely, if there the number of clopen sets is $k < \infty$, then there are at most 2^k open sets, because every open set is a union of clopen sets. Then there are at most 2^k closed sets, hence 2^k points (as every point is closed by Theorem 7.1.11). □

Lemma 12.3.3. *If $\bar{b}, \bar{c} \in \mathbb{M}^n$ and $A = \{a_1, \ldots, a_m\} \subseteq \mathbb{M}$, then*

$$\bar{b} \equiv_A \bar{c} \iff \bar{a}\bar{b} \equiv_\varnothing \bar{a}\bar{c}.$$

Proof. Every $\mathcal{L}(A)$-formula has the form $\varphi(\bar{a}, \bar{x})$ for some $\mathcal{L}$-formula $\varphi(\bar{w}, \bar{x})$. Therefore both sides say that for any $\mathcal{L}$-formula $\varphi(\bar{w}, \bar{x})$,

$$\mathbb{M} \models \varphi(\bar{a}, \bar{b}) \iff \mathbb{M} \models \varphi(\bar{a}, \bar{c}).$$ □

Lemma 12.3.4. *If $|S_n(\varnothing)| < \infty$ for all n, then $|S_n(A)| < \infty$ for all n and all finite $A \subseteq \mathbb{M}$.*

Proof. Fix some $n < \omega$ and $A = \{a_1, \ldots, a_m\} \subseteq M$. Then the map

$$S_n(A) \to S_{m+n}(\varnothing)$$
$$\mathrm{tp}(\bar{b}/A) \mapsto \mathrm{tp}(\bar{a}\bar{b}/\varnothing)$$

is well-defined and injective by Lemma 12.3.3. Thus $|S_n(A)| \leq |S_{m+n}(\varnothing)| < \infty$. □

Recall that $S_n(\varnothing) = S_n(T)$ (Corollary 8.1.20).

Theorem 12.3.5 (Engeler, Ryll-Nardzewski, Svenonius)**.** *Let T be a complete theory in a countable language and let $\mathbb{M}$ be a monster model. The following are equivalent:*

1. *T has a unique countable model.*

2. *$S_n(T)$ is finite for all $n < \omega$.*

3. *$S_n(A)$ is finite for all $n < \omega$ and finite $A \subseteq \mathbb{M}$.*

4. *Every countable model of T is ω-saturated.*

Proof. (1) $\implies$ (2): Suppose $S_n(T)$ is infinite for some n. By Lemma 12.3.1, some $p \in S_n(T)$ is non-isolated. Then p is realized in some model M. By the downward Löwenheim-Skolem theorem (Theorem 5.4.3), we may assume M is countable. By the omitting types theorem (Theorem 12.2.7), there is a countable model N omitting p. Then $M \not\cong N$, and (1) fails.

(2) $\implies$ (3): Lemma 12.3.4.

(3) $\implies$ (4): Assume (3). Let M be a countable model. If A is a finite subset of M, then $S_n(A)$ is finite by (3), so every $p \in S_n(A)$ is isolated by Lemma 12.3.1, and then every $p \in S_n(A)$ is realized by Theorem 12.2.2. This shows that M is ω-saturated.

(4) $\implies$ (1): There is at most one countable ω-saturated model by Corollary 11.5.2. □

Theorem 12.3.6. *Let M be a countable structure in a countable language. The following are equivalent:*

1. $\mathrm{Th}(M)$ *is countably categorical.*

2. *For every n, the action of* $\mathrm{Aut}(M)$ *on M^n has finitely many orbits.*

Proof. (1) $\implies$ (2): by Theorem 12.3.5(4), M is ω-saturated, hence strongly ω-homogeneous by Corollary 11.5.3. Therefore $\bar{a}, \bar{b} \in M^n$ are in the same orbit of $\mathrm{Aut}(M)$ iff $\mathrm{tp}(\bar{a}) = \mathrm{tp}(\bar{b})$. By Theorem 12.3.5(2), there are only finitely many complete n-types.

(2) $\implies$ (1): if $D \subseteq M^n$ is 0-definable, then D is $\mathrm{Aut}(M)$-invariant so D is a union of orbits. There are only finitely many orbits, hence finitely many possibilities for D. Then the boolean algebra of 0-definable sets $D \subseteq M^n$ is finite. By Lemma 12.3.2, $S_n(\varnothing) = S_n(T)$ is finite. By Theorem 12.3.5, $\mathrm{Th}(M)$ is countably categorical. □

Chapter 13

Closure operators and pregeometries

This chapter is about the abstract notion of *closure operators*, which play a fundamental role in universal algebra and some parts of model theory. We have already seen several instances of closure operators. For example, the operation sending a set $S \subseteq M$ to the generated substructure $\langle S \rangle$ is a closure operation, and topologies can be regarded as a special kind of closure operation.

There are two closure operators which play a special role in model theory, the *definable closure* $\operatorname{dcl}(-)$ and the *algebraic closure* $\operatorname{acl}(-)$, which we discuss in Sections 13.2–13.3. The terminology "algebraic closure" comes from the example of ACF, where the model-theoretic algebraic closure $\operatorname{acl}(-)$ agrees exactly with the field theoretic notion of algebraic closure K^{alg} (Theorem 13.5.2). We use this to prove a purely field-theoretic fact: the set $\mathbb{Q}^{\mathrm{alg}}$ of *algebraic numbers* is itself a field (Example 13.5.5), and is even an elementary substructure of $\mathbb{C}$.

The final two sections are on a special class of closure operators called *pregeometries* (or *matroids*), which are important in combinatorics and some branches of model theory. One of the motivating examples of pregeometries comes from *vectors spaces* (Definition 13.6.1), and we use pregeometries to classify vector spaces (Theorem 13.7.3). As an application, the theory of vector spaces is κ-categorical for certain κ (Corollary 13.7.6).

In the next chapter, we will tie these ideas together, and study theories where $\operatorname{acl}(-)$ is a pregeometry. We will see that this happens in ACF, and more generally in any *strongly minimal* theory (Section 14.1).

13.1 Closure operators

Definition 13.1.1. A *closure operator* on a set S is an operation $\mathrm{cl}(-) : \mathfrak{P}(S) \to \mathfrak{P}(S)$ with the following properties:

- Idempotent: $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$.
- Monotone: $X \subseteq Y \implies \mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$.
- Increasing: $X \subseteq \mathrm{cl}(X)$.

The set $\mathrm{cl}(X)$ is called the *closure* of X.

Fix a set S and a closure operator $\mathrm{cl}(-)$ on S. We say that $X \subseteq S$ is *closed* if $X = \mathrm{cl}(X)$. By idempotence, the closed sets are exactly the sets of the form $\mathrm{cl}(X)$.

Theorem 13.1.2. *If* $X \subseteq S$*, then* $\mathrm{cl}(X)$ *is the smallest closed set containing* X.

Proof. The set $\mathrm{cl}(X)$ contains X because $\mathrm{cl}(-)$ is increasing, and $\mathrm{cl}(X)$ is closed because $\mathrm{cl}(-)$ is idempotent. Suppose Y is a closed set containing X. Then $Y = \mathrm{cl}(Y) \supseteq \mathrm{cl}(X)$, because $\mathrm{cl}(-)$ is monotone. □

Definition 13.1.3. A *closure system* on a set S is a family $\mathcal{C} \subseteq \mathfrak{P}(S)$ of sets, called *closed sets*, such that for any $X \subseteq S$ there is a smallest closed set containing X.

Remark 13.1.4. If $\mathcal{C}$ is a closure system, define $\mathrm{cl}(X)$ to be the smallest closed set containing X. It is easy to see that $\mathrm{cl}(-)$ is a closure operator on S. This gives a map from closure systems to closure operators. Conversely, any closure operator $\mathrm{cl}(-)$ defines a closure system $\{X \subseteq S : \mathrm{cl}(X) = X\}$ by Theorem 13.1.2. It is easy to see that these two maps are inverses. Thus closure operators correspond bijectively with closure systems.

Theorem 13.1.5. *A family* $\mathcal{C} \subseteq \mathfrak{P}(S)$ *is a closure system iff* $\mathcal{C}$ *is closed uder infinite intersections.*

Proof. If $\mathcal{C}$ is closed under infinite intersections, then the smallest closed set containing X exists—it is $\bigcap\{Y \in \mathcal{C} : Y \supseteq X\}$. Therefore $\mathcal{C}$ is a closure system.

Conversely, suppose $\mathcal{C}$ is a closure system. Let $\{X_i\}_{i\in I}$ be a family of closed sets and let $Y = \bigcap_{i\in I} X_i$. We claim that Y is closed. For each i, we have $\mathrm{cl}(Y) \subseteq \mathrm{cl}(X_i) = X_i$ by monotonicity. Thus $\mathrm{cl}(Y) \subseteq \bigcap_{i\in I} X_i = Y$. Conversely $Y \subseteq \mathrm{cl}(Y)$ because $\mathrm{cl}(-)$ is increasing. □

Example 13.1.6. If S is a topological space, the family of closed sets is a closure system. The closure $\mathrm{cl}(X)$ is the smallest closed set containing X.

Example 13.1.7. Let M be a structure. Recall that $\langle A\rangle_M$ is the smallest substructure of M containing A. Therefore the class of substructures of M is a closure system, and $\langle -\rangle_M$ is a closure operation.

Definition 13.1.8. A closure operator $\mathrm{cl}(-)$ on a set S is *finitary* if for any $a \in S$, $X \subseteq S$ with $a \in \mathrm{cl}(X)$, there is a finite subset $X_0 \subseteq_f X$ with $a \in \mathrm{cl}(X_0)$.

More generally, we say that an operation $F : \mathfrak{P}(S) \to \mathfrak{P}(S)$ is *finitary* if $F(X) \subseteq \bigcup\{F(X_0) : X_0 \subseteq_f X\}$.

Example 13.1.9. If M is a structure, the closure operation $\langle -\rangle_M$ is finitary: if $b \in \langle A\rangle$ then $b = t(\bar{a})$ for some term t and finite tuple $\bar{a}$. If $A_0 = \{a_1, \dots, a_n\}$, then $b \in \langle A_0\rangle_M$.

Lemma 13.1.10. *Suppose* $\mathrm{cl}(-) : \mathfrak{P}(S) \to \mathfrak{P}(S)$ *is monotone, finitary, increasing, and satisfies the property*

$$a \in \mathrm{cl}(X) \textit{ and } b \in \mathrm{cl}(X \cup \{a\}) \implies b \in \mathrm{cl}(X). \tag{$*$}$$

Then $\mathrm{cl}(-)$ *is idempotent, and therefore a finitary closure operator.*

Proof. Note that $(*)$ implies

$$\mathrm{cl}(X \cup \{a\}) = \mathrm{cl}(X) \text{ for } a \in \mathrm{cl}(X). \tag{$\dagger$}$$

Fix X. Then $\mathrm{cl}(\mathrm{cl}(X)) \supseteq \mathrm{cl}(X)$ because $\mathrm{cl}(-)$ is increasing. For the reverse inclusion, suppose $b \in \mathrm{cl}(\mathrm{cl}(X))$. As $\mathrm{cl}(-)$ is finitary, $b \in \mathrm{cl}(\{a_1, \dots, a_n\})$ for some $a_1, \dots, a_n \in \mathrm{cl}(X)$. By n applications of $(\dagger)$,

$$\mathrm{cl}(X) = \mathrm{cl}(X \cup \{a_1\}) = \mathrm{cl}(X \cup \{a_1, a_2\}) = \cdots = \mathrm{cl}(X \cup \{a_1, \dots, a_n\}).$$

Then

$$b \in \mathrm{cl}(\{a_1, \dots, a_n\}) \subseteq \mathrm{cl}(X \cup \{a_1, \dots, a_n\}) = \mathrm{cl}(X). \qquad \square$$

13.2 Algebraic and definable closure

Definition 13.2.1. Let M be a structure and $A \subseteq M$ be a subset.

1. $b \in M$ is *definable* over A if $\{b\}$ is A-definable.
2. $b \in M$ is *algebraic* over A if $b \in D$ for some finite A-definable $D \subseteq M$.
3. The *definable closure* of A, written $\mathrm{dcl}(A)$ or $\mathrm{dcl}^M(A)$, is the set of $b \in M$ definable over A.
4. The *algebraic closure* of A, written $\mathrm{acl}(A)$ or $\mathrm{acl}^M(A)$, is the set of $b \in M$ algebraic over A.

Lemma 13.2.2. *If $b \in \mathrm{acl}(A)$, then there is a finite A-definable set $X \ni b$ such that $\mathrm{tp}(c/A) = \mathrm{tp}(b/A)$ for every $c \in X$.*

Proof. Take a minimal finite A-definable set $X \ni b$. If X does not have the desired property, take $c \in x$ with $\mathrm{tp}(c/A) \neq \mathrm{tp}(b/A)$. Then there is an A-definable set D with $b \in D$ and $c \notin D$ (Remark 8.1.3). Then $X \cap D$ is a strictly smaller A-definable set containing b, a contradiction. □

Lemma 13.2.3. *Fix a structure M.*

1. *If $A \subseteq B$ then $\mathrm{acl}(A) \subseteq \mathrm{acl}(B)$.*
2. *If $b \in \mathrm{acl}(A)$, then $b \in \mathrm{acl}(A_0)$ for some finite subset $A_0 \subseteq A$.*
3. *$A \subseteq \mathrm{acl}(A)$.*
4. *If $b \in \mathrm{acl}(A)$ and $c \in \mathrm{acl}(A \cup \{b\})$, then $c \in \mathrm{acl}(A)$.*

Proof.

1. Any finite A-definable set is a finite B-definable set.
2. Any finite A-definable set is A_0-definable for some finite $A_0 \subseteq A$.
3. If $b \in A$, then the set $\{b\}$ is finite and A-definable, so $b \in \mathrm{acl}(A)$.
4. As $b \in \mathrm{acl}(A)$ and $c \in \mathrm{acl}(A \cup \{b\})$, there is a finite A-definable set $X \ni b$ and a finite Ab-definable set $Y \ni c$. By Lemma 13.2.2, we may assume all elements of X have the same type over A. Write Y as $\varphi(M, b)$ for some $\mathcal{L}(A)$-formula $\varphi(x, y)$. Let $n = |Y| = |\varphi(M, b)|$. Then $n = |\varphi(M, b')|$ for every $b' \in X$, since this is expressed by a formula in $\mathrm{tp}(b'/A)$. Let $Z = \bigcup_{b' \in X} \varphi(M, b')$. Then Z is a finite A-definable set containing c. □

Theorem 13.2.4. *Algebraic closure* acl(−) *is a finitary closure operator.*

Proof. Lemma 13.2.3 plus Lemma 13.1.10. □

A set $A \subseteq M$ is *algebraically closed* if $\operatorname{acl}(A) = A$. The algebraic closure of A is the smallest algebraically closed set containing A.

Theorem 13.2.5. *Definable closure* dcl(−) *is a finitary closure operator.*

Proof. Like Theorem 13.2.4 but slightly easier. □

A set $A \subseteq M$ is *definably closed* if $\operatorname{dcl}(A) = A$. The definable closure of A is the smallest definably closed set containing A.

13.3 Definable closure, algebraic closure, and substructures

Theorem 13.3.1. *Let M be a structure. If $A \subseteq M$ and $A = \operatorname{dcl}(A)$, then A is a substructure of M.*

Proof. Let f be a k-ary function symbol, and let $a_1, \ldots, a_k$ be elements of A. Then $f(a_1, \ldots, a_k)$ is in $\operatorname{dcl}(A)$, as it is defined by the $\mathcal{L}(A)$-formula $x = f(a_1, \ldots, a_k)$. □

Theorem 13.3.2. *Suppose $M \preceq N$ and φ is an $\mathcal{L}(M)$-formula.*

1. *$\varphi(M) \subseteq \varphi(N)$.*
2. *If $\varphi(M)$ is finite, then $\varphi(M) = \varphi(N)$.*

Proof.

1. If $\bar{b} \in \varphi(M)$, then $M \models \varphi(\bar{b})$, so $N \models \varphi(\bar{b})$, and $\bar{b} \in \varphi(N))$.
2. Let $n = |\varphi(M)|$. Then $M \models \exists^{=n}\bar{x}\ \varphi(\bar{x})$, so the same sentence holds in N, and so $|\varphi(N)| = n$. As $\varphi(M) \subseteq \varphi(N)$, the two sets must be equal. □

Theorem 13.3.3. *If $A \subseteq M \preceq N$, then $\operatorname{acl}^M(A) = \operatorname{acl}^N(A)$.*

Proof. If $b \in \operatorname{acl}^M(A)$, then b is in a finite set of the form $\varphi(M)$ for some $\mathcal{L}(A)$-formula $\varphi(x)$. By Theorem 13.3.2, $\varphi(N) = \varphi(M)$. Then $b \in \varphi(N) \implies b \in \operatorname{acl}^N(A)$. Thus $\operatorname{acl}^M(A) \subseteq \operatorname{acl}^N(A)$.

The proof that $\operatorname{acl}^N(A) \subseteq \operatorname{acl}^M(A)$ is identical, exchanging M and N (even though there is no symmetry between M and N). □

Theorem 13.3.4. *If $M \preceq N$, then M is algebraically closed as a subset of N.*

Proof. $\mathrm{acl}^N(M) = \mathrm{acl}^M(M) = M$. □

Theorem 13.3.5. *Let $\mathbb{M}$ be a monster model, let A be a small subset, and let b be an element. Let S be the set of realizations of* $\mathrm{tp}(b/A)$.

1. *If $b \in \mathrm{acl}(A)$, then S is finite.*
2. *If $b \notin \mathrm{acl}(A)$, then S is large.*

Proof. If $b \in \mathrm{acl}(A)$, then there is a finite A-definable set $X \ni b$. Every realization of $\mathrm{tp}(b/A)$ is in X, so $S \subseteq X$.

Conversely, suppose S is small. Let

$$\Sigma(x) = \mathrm{tp}(b/A) \cup \{x \neq c : c \in S\}.$$

Then $\Sigma(x)$ is a set of formulas over the small set $A \cup S$ with no realizations in $\mathbb{M}$. By saturation, $\Sigma(x)$ isn't finitely realizable. Therefore there is $\varphi(x) \in \mathrm{tp}(b/A)$ and $c_1, \ldots, c_n \in S$ such that

$$\varphi(x) \cup \{x \neq c_i : 1 \leq i \leq n\}$$

isn't realized in $\mathbb{M}$. This means that $\varphi(\mathbb{M}) \subseteq \{c_1, \ldots, c_n\}$. Then b is in the finite A-definable set $\varphi(\mathbb{M})$. □

Remark 13.3.6. By strong homogeneity, the set S in Theorem 13.3.5 is the set $\{\sigma(b) : \sigma \in \mathrm{Aut}(\mathbb{M}/A)\}$.

13.4 Countably categorical fields

Theorem 13.4.1. *Let M be a field and A be a definably closed subset. Then A is a subfield.*

Proof. By Theorem 13.3.1, A is a substructure, i.e., a subring. It remains to show that A is closed under multiplicative inverses. If $a \in A$ is non-zero, then the $\mathcal{L}(A)$-formula $xa = 1$ defines the set $\{a^{-1}\}$, so $a^{-1} \in \mathrm{dcl}(A) = A$. □

Lemma 13.4.2. *Let T be $\aleph_0$-categorical, let M be a model of T, and let A be a finite subset of M. Then* $\mathrm{dcl}(A)$ *is finite.*

Proof. By Theorem 12.3.5(3), $S_1(A)$ is finite. Therefore there are only finitely many A-definable sets $D \subseteq M^1$. By definition, $b \in \operatorname{dcl}(A)$ if and only if $\{b\}$ is definable. Thus $\operatorname{dcl}(A)$ is finite. □

Theorem 13.4.3. *There is no $\aleph_0$-categorical theory of fields.*

Proof. Let T be an $\aleph_0$-categorical theory of fields and let K be an $\aleph_1$-saturated model. For any $n > 0$, the set $\{x \in K : x^n - 1 = 0\}$ is finite, by Theorem 9.1.6. Then the following partial type is finitely satisfiable in K:

$$\Sigma(x) = \{x \neq 0, x \neq 1, x^2 \neq 1, x^3 \neq 1, x^4 \neq 1, \ldots\}.$$

Then $\Sigma(x)$ is realized in K. Take $b \in K$ realizing $\Sigma(x)$. Then $b^n \in \operatorname{dcl}(\{b\})$ for each $n \in \mathbb{N}$, and $\operatorname{dcl}(\{b\})$ is finite, so we can find $n < m$ such that $b^n = b^m$. Then

$$(b^{m-n} - 1)b^n = b^{m-n}b^n - b^n = b^m - b^n = 0,$$

so either $b = 0$ or $b^{m-n} - 1 = 0$. Either way, b doesn't satisfy $\Sigma(x)$, a contradiction. □

Corollary 13.4.4. *If K is an infinite field, then there are two countable fields F_1, F_2 such that*

$$F_1 \equiv F_2 \equiv K$$
$$F_1 \not\cong F_2.$$

Proof. By Theorem 13.4.3, $\operatorname{Th}(K)$ is not $\aleph_0$-categorical. □

13.5 Algebraic closure in ACF

If $M \models \mathrm{ACF}$ and K is a subfield, then K^{alg} denotes the set of $a \in M$ that are algebraic over K, meaning that $P(a) = 0$ for some non-zero polynomial $P(x) \in K[x]$ (Definition 9.3.1).

Lemma 13.5.1. *Suppose $M \models \mathrm{ACF}$ and K is a subfield. If $D \subseteq M^1$ is K-definable, then there is a finite subset $S \subseteq K^{\mathrm{alg}}$ such that $D = S$ or $D = M \setminus S$.*

Proof. Let $\mathcal{F}$ be the class of sets of the form S or $M \setminus S$ for finite $S \subseteq K^{\text{alg}}$. We must show $D \in \mathcal{F}$. Note that $\mathcal{F}$ is closed under boolean combinations.

By quantifier-elimination, $D = \varphi(K)$ for some quantifier-free $\mathcal{L}(K)$-formula φ, which is a boolean combination of atomic formulas. Because $\mathcal{F}$ is closed under boolean combinations, we may assume that φ is atomic.

Then φ has the form $P(x) = Q(x)$ for some polynomials $P, Q \in K[x]$. If $P - Q$ is identically zero, then $\varphi(M) = M$. Otherwise, $\varphi(M)$ is the set of roots of $P - Q$, which is a subset of K^{alg} by definition of K^{alg}, and finite by Theorem 9.1.6. Either way, $\varphi(M) \in \mathcal{F}$. □

Fix $M \models \text{ACF}$.

Theorem 13.5.2. *Let K be a subfield of M. Then* $\text{acl}(K) = K^{\text{alg}}$.

Proof. If $a \in K^{\text{alg}}$, then a is in a finite K-definable set of the form $\{x \in M : P(x) = 0\}$ for some $P(x) \in K[x]$, and so $a \in \text{acl}(K)$.

Conversely, suppose $a \in \text{acl}(K)$. Then $a \in D$ for some finite K-definable set D. By Lemma 13.5.1, $D \subseteq K^{\text{alg}}$, so $a \in K^{\text{alg}}$. □

Theorem 13.5.3. *Let K be a subset of M. The following are equivalent:*

1. *K is a subfield and $K = K^{\text{alg}}$.*

2. *K is a substructure and $K \models$ ACF.*

3. *$K \preceq M$.*

4. *$K = \text{acl}(K)$.*

Proof. We show (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) $\Longrightarrow$ (4) $\Longrightarrow$ (1).

Assume (1). If $P(x) \in K[x]$ is non-constant, then there is $c \in M$ with $P(c) = 0$, because $M \models \text{ACF}$. The element c is in K^{alg} by definition, so $c \in K$. Thus $K \models \text{ACF}$.

Assume (2). Then $K \preceq M$ because ACF has quantifier elimination and both K and M are models of ACF (see Theorem 8.3.6).

Assume (3). Then $K = \text{acl}(K)$ by Theorem 13.3.4.

Assume (4). Then K is a subfield by Theorem 13.3.1 (definably closed sets are subfields) and $K = \text{acl}(K) = K^{\text{alg}}$ by Theorem 13.5.2. □

Corollary 13.5.4. *If K is a subfield of M, then K^{alg} is also a subfield, and $K^{\text{alg}} \preceq M$.*

Proof. $\operatorname{acl}(K^{\text{alg}}) = \operatorname{acl}(\operatorname{acl}(K)) = \operatorname{acl}(K) = K^{\text{alg}}$, so K^{alg} satisfies condition (4) of Theorem 13.5.3. Then K^{alg} is a subfield and an elementary substructure by (1) and (3) of Theorem 13.5.3. □

Example 13.5.5. The set of algebraic numbers $\mathbb{Q}^{\text{alg}} \subseteq \mathbb{C}$ is an algebraically closed field, and an elementary substructure of $\mathbb{C}$.

13.6 Pregeometries and vector spaces

Definition 13.6.1. Let K be a field. A *K-vector space* is an abelian group $(V, +)$ with a function

$$\cdot : K \times V \to V$$

satisfying the axioms

$$\begin{gathered} a \cdot (v + w) = (a \cdot v) + (a \cdot w) \\ 1 \cdot v = v \\ (a + b) \cdot v = a \cdot v + b \cdot v \qquad (\dagger) \\ (a \cdot b) \cdot v = a \cdot (b \cdot v). \end{gathered}$$

For fixed K, we can regard the class of K-vector spaces as an equational class by thinking of the map $\cdot : K \times V \to V$ as a family of unary maps

$$\begin{gathered} \mu_a : V \to V \\ \mu_a(v) = a \cdot v, \end{gathered}$$

one for each $a \in K$. The axioms in Definition 13.6.1 become axiom schemas. For example, axiom (†) becomes the axiom schema

$$\mu_{a+b}(x) = \mu_a(x) + \mu_b(x) \text{ for each } a, b \in K.$$

Subalgebras of vector spaces are called *linear subspaces*.

Remark 13.6.2. In a vector space, the following equations hold:

$$\begin{gathered} (-1) \cdot v = -v \\ 0 \cdot v = 0 \\ a \cdot (-v) = -(a \cdot v) \\ a \cdot 0 = 0. \end{gathered}$$

Fix a field K and vector space V.

Definition 13.6.3. The *span* of a set $S \subseteq V$, written $\operatorname{span}(S)$, is the collection of elements of the form

$$a_1 v_1 + \cdots + a_n v_n$$

where $n \geq 0$, $a_1, \ldots, a_n \in K$, and $v_1, \ldots, v_n \in S$.

Theorem 13.6.4. *The span of S is the linear subspace of V generated by S:*

$$\operatorname{span}(S) = \langle S \rangle_V .$$

Proof. It is an exercise in algebra (using Remark 13.6.2) to see that $\operatorname{span}(S)$ is a linear subspace. It contains S because if $v \in S$, then $v = 1 \cdot v \in \operatorname{span}(S)$. Therefore $\operatorname{span}(S) \supseteq \langle S \rangle_V$. On the other hand, every element of $\operatorname{span}(S)$ has the form $t(v_1, \ldots, v_n)$ for some term t and tuple $\bar{v}$ in S, and so $\operatorname{span}(S) \subseteq \langle S \rangle_V$. □

Corollary 13.6.5. *Span is a finitary closure operator on V.*

Definition 13.6.6. A *pregeometry* is a pair (X, cl) where X is a set, cl is a finitary closure operator on X, and the following *exchange property* holds for $a, b \in X$ and $C \subseteq X$:

$$a \in \mathrm{cl}(C \cup \{b\}) \setminus \mathrm{cl}(C) \implies b \in \mathrm{cl}(C \cup \{a\}).$$

Theorem 13.6.7. *In a vector space,* $\operatorname{span}(-)$ *has the exchange property, and therefore defines a pregeometry.*

Proof. Suppose $v \in \operatorname{span}(S \cup \{w\})$ but $v \notin \operatorname{span}(S)$. Then

$$v = a_1 v_1 + \cdots + a_n v_n + bw \tag{$*$}$$

for some $a_1, \ldots, a_n, b \in K$ and $v_1, \ldots, v_n \in S$. If $b = 0$, then $v \in \operatorname{span}(S)$, a contradiction. Thus $b \neq 0$, and b^{-1} exists. Rearranging $(*)$, we see

$$\begin{aligned} -bw &= a_1 v_1 + \cdots + a_n v_n - v \\ w &= (-b^{-1} a_1) v_1 + \cdots + (-b^{-1} a_n) v_n + b^{-1} v \\ w &\in \operatorname{span}(S \cup \{v\}). \end{aligned}$$

□

Rank

Fix a pregeometry (X, cl).

Definition 13.6.8. If $\bar{a} \in X^n$ and $B \subseteq X$, the *rank* of $\bar{a}$ over B, written $\mathrm{rk}(\bar{a}/B)$, is defined to be the number of $i \in \{1, \ldots, n\}$ such that $a_i \notin \mathrm{cl}(B \cup \{a_1, \ldots, a_{i-1}\})$. We write $\mathrm{rk}(\bar{a}/\varnothing)$ as $\mathrm{rk}(\bar{a})$.

Theorem 13.6.9. $\mathrm{rk}(\bar{a}, \bar{b}/C) = \mathrm{rk}(\bar{a}/C) + \mathrm{rk}(\bar{b}/C\bar{a})$.

Proof. Clear from the definition. □

Theorem 13.6.10. $\mathrm{rk}(\bar{a}/B) = 0 \iff \{a_1, \ldots, a_n\} \subseteq \mathrm{cl}(B)$.

Proof. If $a_i \in \mathrm{cl}(B)$ for each i, then $a_i \in \mathrm{cl}(B \cup \{a_1, \ldots, a_{i-1}\})$ for each i, so $\mathrm{rk}(\bar{a}/B) = 0$. Conversely, if $\mathrm{rk}(\bar{a}/B) = 0$, then $a_i \in \mathrm{cl}(B \cup \{a_1, \ldots, a_{i-1}\})$ for each i. If S is a closed set containing B, then

$$\{a_1, \ldots, a_{i-1}\} \subseteq S \implies a_i \in S$$

and so $\{a_1, \ldots, a_n\} \subseteq S$ by induction. Taking $S = \mathrm{cl}(B)$, we see $\{a_1, \ldots, a_n\} \subseteq \mathrm{cl}(B)$. □

Lemma 13.6.11. $\mathrm{rk}(a, b/C) = \mathrm{rk}(b, a/C)$.

Proof. Both sides are in $\{0, 1, 2\}$. It suffices to show

$$\mathrm{rk}(a, b/C) = 0 \iff \mathrm{rk}(b, a/C) = 0 \tag{13.1}$$
$$\mathrm{rk}(a, b/C) = 2 \iff \mathrm{rk}(b, a/C) = 2 \tag{13.2}$$

By symmetry it suffices to show the $\Rightarrow$ directions.

(13.1): by Theorem 13.6.10, both sides say $\{a, b\} \subseteq C$.

(13.2): suppose $\mathrm{rk}(a, b/C) = 2$. Then $a \notin \mathrm{cl}(C)$ and $b \notin \mathrm{cl}(Ca)$. By monotonicity, $b \notin \mathrm{cl}(C)$. If $a \in \mathrm{cl}(Cb)$, then

$$a \in \mathrm{cl}(Cb) \setminus \mathrm{cl}(C) \text{ but } b \notin \mathrm{cl}(Ca),$$

contradicting the exchange property. Thus $a \notin \mathrm{cl}(Cb)$. With $b \notin \mathrm{cl}(C)$, this implies $\mathrm{rk}(b, a/C) = 2$. □

Lemma 13.6.12. *If $\bar{a}, \bar{d}$ are tuples and b, c are elements and A is a set, then*

$$\mathrm{rk}(\bar{a}, b, c, \bar{d}/A) = \mathrm{rk}(\bar{a}, c, b, \bar{d}/A).$$

Proof. Using Theorem 13.6.9 and Lemma 13.6.11,

$$\begin{aligned}\mathrm{rk}(\bar{a}, b, c, \bar{d}/A) &= \mathrm{rk}(\bar{a}/A) + \mathrm{rk}(b, c/A, \bar{a}) + \mathrm{rk}(\bar{d}/A, \bar{a}, b, c)\\ &= \mathrm{rk}(\bar{a}/A) + \mathrm{rk}(c, b/A, \bar{a}) + \mathrm{rk}(\bar{d}/A, \bar{a}, c, b)\\ &= \mathrm{rk}(\bar{a}, c, b, \bar{d}/A).\end{aligned}$$ □

Theorem 13.6.13. *If π is a permutation of $\{1, \ldots, n\}$, then*

$$\mathrm{rk}(a_1, \ldots, a_n/B) = \mathrm{rk}(a_{\pi(1)}, \ldots, a_{\pi(n)}/B).$$

Proof. Repeated applications of Lemma 13.6.12. □

Theorem 13.6.14. *If $\bar{a} \subseteq \mathrm{cl}(C\bar{b})$, then $\mathrm{rk}(\bar{a}/C) \leq \mathrm{rk}(\bar{b}/C)$.*

Proof.

$$\begin{aligned}\mathrm{rk}(\bar{a}/C) &\leq \mathrm{rk}(\bar{a}/C) + \mathrm{rk}(\bar{b}/C\bar{a}) = \mathrm{rk}(\bar{a}, \bar{b}/C)\\ &= \mathrm{rk}(\bar{b}, \bar{a}/C) = \mathrm{rk}(\bar{b}/C) + \mathrm{rk}(\bar{a}/C\bar{b}) = \mathrm{rk}(\bar{b}/C).\end{aligned}$$ □

Theorem 13.6.15. *If $C \supseteq B$, then $\mathrm{rk}(\bar{a}/C) \leq \mathrm{rk}(\bar{a}/B)$.*

Proof. For each i, monotonicity of $\mathrm{cl}(-)$ shows

$$a_i \notin \mathrm{cl}(C \cup \{a_1, \ldots, a_{i-1}\}) \implies a_i \notin \mathrm{cl}(B \cup \{a_i, \ldots, a_{i-1}\}).$$ □

Independence and bases

Definition 13.6.16. A set $I \subseteq X$ is *independent* if $a \notin \mathrm{cl}(I \setminus \{a\})$ for each $a \in I$.

Theorem 13.6.17. *In a vector space V, a set $I \subseteq V$ is independent if and only if the following condition holds: for any distinct $v_1, \ldots, v_n \in V$ and $a_1, \ldots, a_n \in K$,*

$$a_1v_1 + \cdots + a_nv_n = 0 \implies v_1 = v_2 = \cdots = v_n = 0. \qquad (*)$$

Proof. If I is not independent, then there is some $v_1 \in \mathrm{span}(I \setminus \{v_1\})$. Thus there are distinct $v_2, \ldots, v_n \in I \setminus \{v_1\}$ with

$$v_1 = a_2v_2 + \cdots + a_nv_n.$$

Setting $a_1 = -1 \in K$, we get $\sum_{i=1}^{n} a_i v_i = 0$, contradicting $(*)$.

Conversely, suppose $(*)$ fails. Permuting the v_i, we may assume $a_1 \neq 0$. Then

$$a_1 v_1 + \cdots + a_n v_n = 0$$
$$v_1 = (-a_1^{-1} a_2) v_2 + \cdots + (-a_1^{-1} a_n) v_n \in \operatorname{span}(v_2, \ldots, v_n),$$

and I is not independent. □

Now return to a general pregeometry.

Definition 13.6.18. A *basis* is a maximal independent set.

Remark 13.6.19.

1. If I is independent and $J \subseteq I$, then J is independent, by monotonicity of $\operatorname{cl}(-)$.
2. A set $I \subseteq X$ is independent if and only if every finite subset is independent, because $\operatorname{cl}(-)$ is finitary.

Theorem 13.6.20. *There is at least one basis.*

Proof. Zorn's lemma. □

Lemma 13.6.21. *If $a_1, \ldots, a_n \in X$ are distinct, then $\operatorname{rk}(\bar{a}) = n$ if and only if the set $I = \{a_1, \ldots, a_n\}$ is independent.*

Proof. Note that $\operatorname{rk}(\bar{a}) = n$ if and only if

$$a_i \notin \operatorname{cl}(a_1, \ldots, a_{i-1}) \text{ for all } 1 \leq i \leq n, \qquad (*)$$

by definition of rank. Moreover, the condition $\operatorname{rk}(\bar{a}) = n$ is invariant under permuting $\bar{a}$, by Theorem 13.6.13.

Independence clearly implies $(*)$, as $\operatorname{cl}(-)$ is monotone. For the converse, suppose $\operatorname{rk}(\bar{a}) = n$ and $i \leq n$. We must show $a_i \notin \operatorname{cl}(I \setminus \{a_i\})$. Permuting $\bar{a}$, we reduce to the case $i = n$. Then we must show $a_n \notin \operatorname{cl}(a_1, \ldots, a_{n-1})$, which is a case of $(*)$. □

Lemma 13.6.22. *If I is independent and $a \notin \operatorname{cl}(I)$, then $I \cup \{a\}$ is independent.*

Proof. By Remark 13.6.19(2), we may assume I is a finite set $\{b_1, \ldots, b_n\}$. By Lemma 13.6.21 and Theorem 13.6.9

$$\mathrm{rk}(\bar{b}, a) = \mathrm{rk}(\bar{b}) + \mathrm{rk}(a/\bar{b}) = n + 1,$$

and so $\{b_1, \ldots, b_n, a\}$ is independent. □

Theorem 13.6.23. *If B is a basis, then $\mathrm{cl}(B) = X$.*

Proof. Otherwise, take $a \in X \setminus \mathrm{cl}(B)$, and $B \cup \{a\}$ is independent, contradicting the fact that B is a maximal independent set. □

Remark 13.6.24. Conversely, if B is independent and $\mathrm{cl}(B) = X$, then B is a basis. Otherwise, if $I \supsetneq B$ is a larger independent set, then $I \subseteq X = \mathrm{cl}(B)$, contradicting Lemma 13.6.25 below. Thus B is a basis if and only if B is independent and $\mathrm{cl}(B) = X$.

Lemma 13.6.25. *If I is independent and J is a proper subset, then $I \not\subseteq \mathrm{cl}(J)$.*

Proof. Otherwise, take $a \in I \setminus J$. Then $J \subseteq I \setminus \{a\}$, and so

$$a \in I \subseteq \mathrm{cl}(J) \subseteq \mathrm{cl}(I \setminus \{a\}),$$

contradicting independence. □

Theorem 13.6.26. *If B and C are two bases, then $|B| = |C|$.*

Proof. Suppose not. Without loss of generality, $|B| < |C|$. There are two cases:

1. B and C are finite. Let $\bar{b}$ and $\bar{c}$ enumerate B and C. Then

   $$\mathrm{rk}(\bar{b}) = |B| < |C| = \mathrm{rk}(\bar{c})$$

   by Lemma 13.6.21. However, $C \subseteq X = \mathrm{cl}(B)$ by Theorem 13.6.23, and so $\mathrm{rk}(\bar{c}) \leq \mathrm{rk}(\bar{b})$ by Theorem 13.6.14.

2. C is infinite. By Theorem 13.6.23, $B \subseteq \mathrm{cl}(C)$ and $C \subseteq \mathrm{cl}(B)$. As $\mathrm{cl}(-)$ is finitary, we can find a finite subset $C_b \subseteq C$ for each $b \in B$ such that $b \in \mathrm{cl}(C_b)$. Let $C' = \bigcup_{b \in B} C_b$. Then $B \subseteq \mathrm{cl}(C')$, implying $C \subseteq \mathrm{cl}(B) \subseteq \mathrm{cl}(\mathrm{cl}(C')) = \mathrm{cl}(C')$. This contradicts independence of C (see Lemma 13.6.25) unless $C' = C$.

   However, $|C'| < |C|$. Indeed, if B is finite then C' is finite, and so $|C'| < |C|$. If B is infinite then $|C'| \leq |B| < |C|$. Thus C' is a proper subset of C, a contradiction. □

Definition 13.6.27. The *rank* of a pregeometry is the cardinality of any basis.

13.7 The classification of vector spaces

Fix a field K. We can regard K as a vector space by defining

$$\begin{aligned} a \cdot v &= a \cdot v \\ v + w &= v + w \end{aligned}$$

where the left-hand $\cdot$ and $+$ are the vector space operations, and the right-hand $\cdot$ and $+$ are the field operations.

If λ is a cardinal, let K^λ be the power vector space, i.e., the set of functions $f : \lambda \to K$ with the vector space operations defined pointwise:

$$\begin{aligned} (f + g)(x) &= f(x) + g(x) \\ (a \cdot f)(x) &= a \cdot (f(x)). \end{aligned}$$

Say that $f \in K^\lambda$ has *finite support* if

$$\operatorname{supp}(f) := \{x \in \lambda : f(x) \neq 0\}$$

is finite. Note that

$$\begin{aligned} \operatorname{supp}(f + g) &\subseteq \operatorname{supp}(f) + \operatorname{supp}(g) \\ \operatorname{supp}(af) &\subseteq \operatorname{supp}(f) \\ \operatorname{supp}(0) &= \varnothing. \end{aligned}$$

Therefore, $F_\lambda := \{f \in K^\lambda : \operatorname{supp}(f) \text{ is finite}\}$ is a linear subspace of K^λ.

Lemma 13.7.1. *Let V be a K-vector space. Suppose $v_i \in V$ for each $i \in \lambda$.*

1. *There is a homomorphism $\alpha : F_\lambda \to V$ defined by*

$$\alpha(f) = \sum_{i \in \operatorname{supp}(f)} f(i) \cdot v_i.$$

2. *α is surjective if and only if $V = \operatorname{span}\{v_i : i \in \lambda\}$.*

3. *α is injective if and only if $\{v_i : i \in \lambda\}$ is independent (and the v_i are distinct).*

4. *α is an isomorphism if and only if $\{v_i : i \in \lambda\}$ is a basis (and the v_i are distinct).*

5. *All homomorphisms $F_\lambda \to V$ arise as in part (1).*

Proof. 1. An exercise in algebra. Essentially this works because $\alpha(f) = \sum_{i\in\lambda} f(i) \cdot v_i$, which depends linearly on f. The sum makes sense as almost all the terms in it are zero.

2. True by definition of span.

3. α is injective if and only if $\ker(\alpha) = \{0\}$. This condition means that if $f \in K^\lambda$ has finite support and

$$\sum_{i\in\lambda} f(i)v_i = 0,$$

then f must vanish. This is a rephrasing of Theorem 13.6.17.

4. α is an isomorphism if and only if it is injective and surjective. By the previous two points, this means that the set $B = \{v_i : i \in \lambda\}$ is independent and has $\operatorname{span}(B) = V$. By Remark 13.6.24, this means that B is a basis.

5. Let $\beta : F_\lambda \to V$ be a homomorphism. Let $e_i : \lambda \to K$ be the function

$$e_i(x) = \begin{cases} 1 & \text{if } x = i \\ 0 & \text{if } x \neq i. \end{cases}$$

Then $\operatorname{supp}(e_i) = \{i\}$, so $e_i \in F_\lambda$. Note that for any $f \in F_\lambda$,

$$f = \sum_{i\in\operatorname{supp}(f)} f(i) \cdot e_i.$$

Therefore

$$\beta(f) = \sum_{i\in\operatorname{supp}(f)} f(i) \cdot \beta(e_i).$$

Taking $v_i = \beta(e_i)$, we see that β has the desired form. □

Lemma 13.7.1 immediately yields the following:

Theorem 13.7.2. *Let V be a K-vector space. Then $V \cong F_\lambda$ if and only if V has a basis of cardinality λ.*

By Theorems 13.6.20 and 13.6.26, there is a unique cardinal λ such that V has a basis of cardinality λ.

Theorem 13.7.3. *Let V be a K-vector space. Then $V \cong F_\lambda$ for a unique cardinal λ, called the* dimension *of V.*

Lemma 13.7.4. *Let V be a K-vector space of dimension λ.*

1. *If λ is finite, then $|V| = |K|^\lambda$.*

2. *If λ or $|K|$ is infinite, then $|V| = |K| + \lambda$.*

Proof. Without loss of generality, $V = F_\lambda$.

1. $F_\lambda = K^\lambda$, whose cardinality if $|K|^\lambda$.

2. If $B \subseteq V$ is a basis of size λ, then $B \subseteq V \implies \lambda \leq |V|$. If $v \in V$ is non-zero, then there is an injection

$$\begin{aligned} K &\to V \\ a &\mapsto av, \end{aligned}$$

and so $|K| \leq |V|$. Thus $|V| \geq \max(|K|, |\lambda|) = |K| + |\lambda|$. On the other hand, V is generated by a set of size λ, and the language has size $\aleph_0 + |K|$, so that $|V| \leq \lambda + |K| + \aleph_0 = |K| + \lambda$. □

Theorem 13.7.5. *If V is an infinite K-vector space and $|V| > |K|$, then $\dim(V) = |V|$.*

Proof. Let $\lambda = \dim(V)$. If K and λ are both finite then $|V| = |K|^\lambda < \aleph_0$, a contradiction. Therefore K or λ is infinite, and so $|V| = \max(|K|, \lambda)$. As $|V| > |K|$, this implies $|V| = \lambda$. □

Corollary 13.7.6. *Let K be a field. The theory of infinite K-vector spaces is complete and λ-categorical for every infinite $\lambda > |K|$.*

Definition 13.7.7. A theory T in a countable language is *totally categorical* if T is λ-categorical for any λ.

Corollary 13.7.8. *If K is a finite field, then the theory of infinite K-vector spaces is totally categorical.*

Chapter 14

Strong minimality and geometric theories

A theory is *strongly minimal* if for every model M and definable set $D \subseteq M$, either D or $M \setminus D$ is finite. We have already seen one example of a strongly minimal theory, namely ACF (Lemma 13.5.1).

Although the definition of strong minimality only mentions definable sets in one variable, strong minimality has very strong consequences for definable sets $D \subseteq M^n$ in n variables. Specifically, strong minimality allows one to define the *dimension* $\dim(D)$ of any definable set. The intuition one should have is that $\dim(D)$ is something like topological dimension. For example, points have dimension 0, lines and circles have dimension 1, planes and spheres have dimension 2, and so on. In the case of algebraically closed fields, the model-theoretic dimension $\dim(-)$ corresponds to something that algebraic geometers know as "Krull dimension".

The abstract model-theoretic dimension in strongly minimal theories satisfies many intuitive properties. For example, $\dim(D_1 \times D_2) = \dim(D_1) + \dim(D_2)$. Dimension is also invariant under definable bijections: if $f : D_1 \to D_2$ is a definable bijection, then $\dim(D_1) = \dim(D_2)$.

Another important property of strongly minimal theories is that they are κ-categorical for all $\kappa > \aleph_0$ (Corollary 14.2.7), at least when the theory is complete.[1] Even though $\aleph_0$-categoricity usually fails, one can classify the countable models. For example, we classify all models of ACF (i.e., alge-

[1] For example, the complete theory ACF_0 is κ-categorical, but the incomplete theory ACF is not κ-categorical by the Łoś-Vaught criterion.

braically closed fields) in Theorem 14.2.10.

The proofs of dimension theory and uncountable categoricity involve two technical properties possessed by strongly minimal theories:

1. The algebraic closure operation $\mathrm{acl}(-)$ is a pregeometry.

2. The quantifier $\exists^\infty$ is eliminated (see Section 14.3).

A theory is said to be *geometric* if it has these two properties. There are many geometric theories other than strongly minimal theories, including the complete theory of $\mathbb{R}$. As we will see, the dimension theory (but not the uncountable categoricity) generalizes from strongly minimal theories to geometric theories.

14.1 Strong minimality

Definition 14.1.1. Let S be a set. A subset $X \subseteq S$ is *cofinite* (in S) if $S \setminus X$ is finite.

Definition 14.1.2. A structure M is *minimal* if M is infinite, and every definable set $X \subseteq M$ is finite or cofinite.

Note this is only a statement about definable sets in one variable; it says nothing about definable subsets of M^n for $n > 1$.

Definition 14.1.3. A theory T is *strongly minimal* if all its models are minimal. A structure M is *strongly minimal* if its complete theory is strongly minimal.

Note that models of a strongly minimal theory are strongly minimal.

Example 14.1.4. ACF is strongly minimal by Lemma 13.5.1.

Theorem 14.1.5. *Suppose M is strongly minimal and $A \subseteq M$. Then $A \preceq M$ if and only if $A = \mathrm{acl}(A)$ and A is infinite.*

Proof. First suppose $A \preceq M$. Then A is infinite because M is (Lemma 5.5.4), and $A = \mathrm{acl}(A)$ because A is an elementary substructure (Theorem 13.3.4).

Conversely, suppose $A = \mathrm{acl}(A)$ and A is infinite. Then $A \preceq M$ by the Tarski-Vaught criterion (Theorem 5.3.1). Indeed, suppose $D \subseteq M$ is nonempty and A-definable. By strong minimality, D is finite or cofinite. If D is finite then $D \subseteq \mathrm{acl}(A) = A$, so $A \cap D = D \neq \varnothing$. If D is cofinite, it intersects A because A is infinite. □

Theorem 14.1.6. *If M is strongly minimal, then* $\operatorname{acl}(-)$ *satisfies the exchange property:*

$$a \in \operatorname{acl}(Cb) \setminus \operatorname{acl}(C) \implies b \in \operatorname{acl}(Ca).$$

Consequently, $\operatorname{acl}(-)$ *defines a pregeometry.*

Proof. Because $a \in \operatorname{acl}(Cb)$, there is a finite Cb-definable set X containing a. Write X as $\varphi(M, b)$ for some $\mathcal{L}(C)$-formula $\varphi(x, y)$. Let $n = |X|$. Replacing $\varphi(x, y)$ with

$$\varphi(x, y) \wedge \neg\exists^{\geq n+1} z\ \varphi(z, y),$$

we may assume that $|\varphi(M, b')| \leq n$ for any $b' \in M$. As $\varphi(a, b)$ holds, $b \in \varphi(a, M)$. If $\varphi(a, M)$ is finite then $b \in \operatorname{acl}(Ca)$ as desired.

Otherwise, $\varphi(a, M)$ is cofinite, and its complement has cardinality $k < \infty$. Let D be the C-definable set of $a' \in M$ such that $|M \setminus \varphi(a', M)| = k$. Then $a \in D$, so D is infinite because $a \notin \operatorname{acl}(C)$. Take distinct $a_1, \ldots, a_{n+1} \in D$. Then $\varphi(a_i, M)$ is cofinite for each i. An intersection of cofinite sets is cofinite, hence non-empty, so there is some

$$b' \in \bigcap_{i=1}^{n+1} \varphi(a_i, M).$$

This means that $\varphi(a_i, b')$ holds for all i, and so $|\varphi(M, b')| \geq n + 1$, contradicting the choice of φ. □

14.2 Uncountable categoricity

Let $\mathbb{M}$ be a monster model of a *complete* strongly minimal theory in a countable language.

Theorem 14.2.1. *For any small set $A \subseteq \mathbb{M}$, there is a unique 1-type $p \in S_1(A)$ whose realizations are the elements of* $\mathbb{M} \setminus \operatorname{acl}(A)$*.*

Proof. In other words, we must show $b, c \notin \operatorname{acl}(A)$ implies $b \equiv_A c$. Otherwise there is an A-definable set D with $b \in D$ and $c \notin D$ (Remark 8.1.3). If D is finite, then $b \in \operatorname{acl}(A)$ and if D is cofinite, then $c \in \operatorname{acl}(A)$. Either way, we get a contradiction. □

The pregeometry rank $\mathrm{rk}(\bar{a}/B)$ (Definition 13.6.8) is usually written as $\dim(\bar{a}/B)$. Say that a finite tuple $\bar{a} \in \mathbb{M}^n$ is *independent* if $\dim(\bar{a}) = n$. By definition, this means $a_i \notin \mathrm{acl}(a_1, \ldots, a_{i-1})$ for each i. By Lemma 13.6.21, $\bar{a}$ is independent if and only if the a_i are pairwise distinct and $\{a_1, \ldots, a_n\}$ is independent as a set.

Lemma 14.2.2. *Let $\bar{a}, \bar{b}$ be two finite tuples of length n in $\mathbb{M}$. If $\dim(\bar{a}) = n$ and $\dim(\bar{b}) = n$, then $\bar{a} \equiv_\varnothing \bar{b}$.*

Proof. Proceed by induction on n. The case $n = 0$ is trivial. Note that the subtuples $(a_1, \ldots, a_{n-1})$ and $(b_1, \ldots, b_{n-1})$ are independent. By induction, $(a_1, \ldots, a_{n-1}) \equiv_\varnothing (b_1, \ldots, b_{n-1})$. Take $\sigma \in \mathrm{Aut}(\mathbb{M})$ moving $(a_1, \ldots, a_{n-1})$ to $(b_1, \ldots, b_{n-1})$. Replacing $\bar{a}$ with $\sigma(\bar{a})$, we may assume $a_i = b_i$ for $i < n$. By independence,

$$\begin{aligned} a_n &\notin \mathrm{acl}(a_1, \ldots, a_{n-1}) \\ b_n &\notin \mathrm{acl}(b_1, \ldots, b_{n-1}) = \mathrm{acl}(a_1, \ldots, a_{n-1}). \end{aligned}$$

By Theorem 14.2.1, a_n and b_n have the same type over $(a_1, \ldots, a_{n-1})$. Therefore $(a_1, \ldots, a_n) \equiv_\varnothing (a_1, \ldots, a_{n-1}, b_n) = \bar{b}$. □

Theorem 14.2.3. *Let M be a model of T. Let $f : I_1 \to I_2$ be a bijection between two independent sets. Then f is a partial elementary map.*

Proof. If $a_1, \ldots, a_n$ are distinct elements of I_1, then $f(a_1), \ldots, f(a_n)$ are distinct elements of I_2, and the two tuples $\bar{a}$ and $f(\bar{a})$ are both independent n-tuples. By Lemma 14.2.2, they have the same type. □

Definition 14.2.4. If $M \models T$, the *rank* of M, written $\mathrm{rk}(M)$, is the rank of the pregeometry $(M, \mathrm{acl}(-))$, i.e., the cardinality of a basis.

Remark 14.2.5. If $M \models T$, and B is a basis, then $M = \mathrm{acl}(B)$ (Theorem 13.6.23), and so

$$|M| = |\mathrm{acl}(B)| = |B| + \aleph_0 = \mathrm{rk}(M) + \aleph_0.$$

Theorem 14.2.6. *Two models M_1, M_2 are isomorphic if and only if $\mathrm{rk}(M_1) = \mathrm{rk}(M_2)$.*

Proof. If $M_1 \cong M_2$, it is easy to see that $\mathrm{rk}(M_1) = \mathrm{rk}(M_2)$. Conversely, suppose the ranks are equal. Embed M_1 and M_2 into a monster model $\mathbb{M}$. Let B_i be a basis of M_i for $i = 1, 2$. Then $|B_1| = |B_2|$. Take a bijection $f : B_1 \to B_2$. By Theorem 14.2.3, f is a partial elementary map from $\mathbb{M}$ to $\mathbb{M}$. By strong homogeneity, f extends to an automorphism $\sigma \in \mathrm{Aut}(\mathbb{M})$. Then $\sigma(M_1) = \sigma(\mathrm{acl}(B_1)) = \mathrm{acl}(B_2) = M_2$. The automorphism σ restricts to an isomorphism from M_1 to M_2. □

Corollary 14.2.7. *T is κ-categorical for all $\kappa > \aleph_0$.*

Theorem 14.2.8. *Suppose that in models of T, algebraically closed sets are infinite. Then there is a unique model of rank κ for every cardinal κ, finite or infinite.*

Proof. Take a model M_0 of size greater than $\kappa + \aleph_0$, and let B_0 be a basis of M_0. Then $|B_0| > \kappa$. Take a subset $I \subseteq B_0$ with $|I| = \kappa$, and let $M = \mathrm{acl}(I)$. By assumption, M is infinite. Then $M \preceq M_0$ by Theorem 14.1.5. By Remark 13.6.24, the independent set I is a basis of M, so $\mathrm{rk}(M) = |I| = \kappa$. □

The classification of algebraically closed fields

Definition 14.2.9. The *transcendence degree* of an algebraically closed field K is its rank in the sense of Definition 14.2.4.

Theorem 14.2.10. *For each $p \in \{0, 2, 3, 5, 7, \ldots\}$ and each cardinal κ, there is a unique algebraically closed field of characteristic p and transcendence degree κ.*

Proof. The theory ACF_p is complete and strongly minimal. Algebraically closed sets are infinite by Theorem 13.5.3(2) and Theorem 9.2.3. Therefore Theorem 14.2.8 applies, giving a unique model $M \models \mathrm{ACF}_p$ with transcendence degree κ. □

14.3 Uniform finiteness

The notation $\exists^\infty x\ P(x)$ means that there are infinitely many x such that $P(x)$ holds. In general, $\exists^\infty x$ cannot be expressed in first-order logic.

Definition 14.3.1. A structure M *eliminates* $\exists^\infty$ if for any first-order formula $\varphi(x, \bar{y})$, there is a formula $\psi(\bar{y})$ such that for any $\bar{b}$,

$$M \models \exists^\infty x\ \varphi(x, \bar{b}) \iff M \models \psi(\bar{b}).$$

Here, the left-hand side really means $\exists^\infty a \in M : M \models \varphi(a, \bar{b})$, or equivalently, $\varphi(M, \bar{b})$ is infinite.

Recall from Section 3.3 that the notation $\exists^{\geq n} x\ P(x)$ means that there are at least n values of x such that $P(x)$ holds. Unlike $\exists^\infty$, this can be expressed in first-order logic.

Definition 14.3.2. A structure M has *uniform finiteness* if for any formula $\varphi(x, \bar{y})$, there is a number n_φ such that for any $\bar{b}$ in M,

$$|\varphi(M, \bar{b})| < \infty \iff |\varphi(M, \bar{b})| < n_\varphi.$$

Theorem 14.3.3. *Let M be a structure.*

1. *If M has uniform finiteness, then M eliminates $\exists^\infty$.*

2. *If M has uniform finiteness and $N \equiv M$, then N has uniform finiteness.*

3. *M has uniform finiteness if and only if every $N \equiv M$ eliminates $\exists^\infty$.*

Proof. 1. Uniform finiteness says $(\exists^\infty x)\varphi(x, \bar{y}) \iff (\exists^{\geq n_\varphi} x)\varphi(x, \bar{y})$.

2. Given φ, if n_φ works for M then it works for N. Otherwise there is $\bar{b}$ in N such that $n_\varphi \leq |\varphi(N, \bar{b})| < \infty$. Let $k = |\varphi(N, \bar{b})|$. Then

$$N \models \exists \bar{y}\ \exists^{=k} x\ \varphi(x, \bar{y}).$$

This says that there is a $\bar{b}$ in N such that $\varphi(N, \bar{b})$ has size exactly k. As $M \equiv N$, the same holds in M, so there is a $\bar{b}$ in M such that $\varphi(M, \bar{b})$ has size exactly $k \geq n_\varphi$, contradicting the choice of n_φ.

3. If M has uniform finiteness and $N \equiv M$, then N has uniform finiteness and therefore eliminates $\exists^\infty$. Conversely, suppose every $N \equiv M$ eliminates $\exists^\infty$. Fix an $\aleph_1$-saturated elementary extension $N \succeq M$. By

part (2), it suffices to show that N has uniform finiteness. Fix $\varphi(x, \bar{y})$. Let

$$D_\infty = \{\bar{b} : |\varphi(N, \bar{b})| < \infty\}$$
$$D_k = \{\bar{b} : |\varphi(N, \bar{b})| < k\} \text{ for } k < \omega.$$

Then D_∞ is definable by elimination of $\exists^\infty$, and D_k is definable easily. Moreover,

$$D_0 \subseteq D_1 \subseteq \cdots \subseteq D_\infty$$

and $D_\infty = \bigcup_{i=0}^\infty D_i$. By $\aleph_0$-compactness (Theorem 11.2.7(3)), $D_\infty = D_{n_\varphi}$ for some n_φ, which means

$$|\varphi(N, \bar{b})| < \infty \implies |\varphi(N, \bar{b})| < n_\varphi. \qquad \square$$

Theorem 14.3.4. *If M is strongly minimal, then M has uniform finiteness.*

Proof. Without loss of generality, M is $\aleph_1$-saturated. Let $\varphi(x; y_1, \ldots, y_n)$ be a formula. Let D_k be the set of $\bar{b}$ such that $\varphi(M, \bar{b})$ or $M \setminus \varphi(M, \bar{b})$ has size less than k. Then $D_0 \subseteq D_1 \subseteq \cdots \subseteq M^n$. Strong minimality means that $M^n = \bigcup_{k=0}^\infty D_k$. By $\aleph_0$-compactness (Theorem 11.2.7(3)), $D_k = M^n$ for some k. This means that for any $\bar{b}$,

$$|\varphi(M, \bar{b})| < k \text{ or } |M \setminus \varphi(M, \bar{b})| < k.$$

Therefore,

$$|\varphi(M, \bar{b})| < k \text{ or } |\varphi(M, \bar{b})| = \infty,$$

which is uniform finiteness. □

14.4 Pregeometric theories

Definition 14.4.1. A theory T is *pregeometric* if $\operatorname{acl}(-)$ satisfies exchange in models of T.

Definition 14.4.2. A complete theory T is *geometric* if it is pregeometric and has uniform finiteness.

For example, strongly minimal theories are geometric.

Let $\mathbb{M}$ be a monster model of a pregeometric theory. Let $\dim(\bar{a}/B)$ denote the rank of $\bar{a}$ over B with respect to $\operatorname{acl}(-)$, i.e., the number of values $i \in \{1, \ldots, n\}$ such that $a_i \notin \operatorname{acl}(Ba_1a_2 \cdots a_{i-1})$.

Theorem 14.4.3. *1.* $\dim(\bar{a}/B) = \dim(\sigma(\bar{a})/\sigma(B))$ *for any* $\sigma \in \mathrm{Aut}(\mathbb{M})$*.*

2. If $\bar{a} \equiv_C \bar{b}$*, then* $\dim(\bar{a}/C) = \dim(\bar{b}/C)$*.*

Proof. 1. The definition of $\dim(-/-)$ is clearly automorphism-invariant.

2. Take $\sigma \in \mathrm{Aut}(\mathbb{M}/C)$ with $\sigma(\bar{a}) = \bar{b}$ and apply part (1). □

In particular, $\mathrm{tp}(\bar{a}/C)$ determines $\dim(\bar{a}/C)$. If $p \in S_n(C)$, we let $\dim(p)$ denote $\dim(\bar{a}/C)$ for any $\bar{a}$ realizing p.

Theorem 14.4.4 (Extension)**.** *Let* $B \subseteq C$ *be small sets in* $\mathbb{M}$*.*

1. If $p \in S_n(B)$*, then there is an extension* $q \in S_n(C)$ *with* $q \supseteq p$*.*

2. If $\bar{a} \in \mathbb{M}^n$*, then there is* $\bar{a}' \equiv_B \bar{a}$ *with* $\dim(\bar{a}'/C) = \dim(\bar{a}/B)$*.*

Proof. Note that (1) $\iff$ (2), by taking $p = \mathrm{tp}(\bar{a}/B)$ and $q = \mathrm{tp}(\bar{a}'/B)$. We prove (2) by induction on n. First suppose $n = 1$. If $a \notin \mathrm{acl}(B)$, then the set X of realizations of $\mathrm{tp}(a/B)$ is large by Theorem 13.3.5, so there is $a' \in X \setminus \mathrm{acl}(C)$. Then $a' \equiv_B a$ and $\dim(a'/C) = 1 = \dim(a/B)$. On the other hand, if $a \in \mathrm{acl}(B) \subseteq \mathrm{acl}(C)$, then $\dim(a/C) = 0 = \dim(a/B)$, and we can take $a' = a$.

Next suppose $n > 1$. Write $\bar{a}$ as $(\bar{a}_1, \bar{a}_2)$, where $\bar{a}_1$ and $\bar{a}_2$ are tuples of shorter length. By induction there is $\bar{a}_1' \equiv_B \bar{a}_1$ with $\dim(\bar{a}_1'/C) = \dim(\bar{a}_1/B)$. Moving $\bar{a}$ by an automorphism over B sending $\bar{a}_1$ to $\bar{a}_1'$, we may assume $\bar{a}_1 = \bar{a}_1'$. Then

$$\dim(\bar{a}_1/C) = \dim(\bar{a}_1/B). \tag{$*$}$$

By induction applied to $\bar{a}_2$ and the inclusion $B\bar{a}_1 \subseteq C\bar{a}_1$, there is $\bar{a}_2' \equiv_{B\bar{a}_1} \bar{a}_2$ with $\dim(\bar{a}_2'/C\bar{a}_1) = \dim(\bar{a}_2/B\bar{a}_1)$. Moving $\bar{a}$ by an automorphism over $B\bar{a}_1$ sending $\bar{a}_2$ to $\bar{a}_2'$, we may assume $\bar{a}_2' = \bar{a}_2$. Then

$$\dim(\bar{a}_2/C\bar{a}_1) = \dim(\bar{a}_2/B\bar{a}_1). \tag{$\dagger$}$$

Adding equations ($*$) and ($\dagger$) and using additivity,

$$\dim(\bar{a}_1\bar{a}_2/C) = \dim(\bar{a}_1\bar{a}_2/B).$$

□

14.5 Dimension theory in the monster

Work in a monster model $\mathbb{M}$ of a pregeometric theory.

Definition 14.5.1. If B is small and $X \subseteq \mathbb{M}^n$ is B-definable, then $\dim_B(X) = \max_{\bar{a} \in X} \dim(\bar{a}/B)$. If X is empty, we set $\dim(X) = -\infty$.

Theorem 14.5.2. *If X is B-definable and C-definable, then* $\dim_B(X) = \dim_C(X)$.

Proof. First suppose $B \subseteq C$. Note that $\dim(\bar{a}/B) \geq \dim(\bar{a}/C)$ for any $\bar{b}$ (Theorem 13.6.15), so

$$\dim_B(X) = \max_{\bar{a} \in X} \dim(\bar{a}/B) \geq \max_{\bar{a} \in X} \dim(\bar{a}/C) = \dim_C(X).$$

Conversely, take $\bar{a} \in X$ with $\dim(\bar{a}/B) = \dim_B(X)$. By Theorem 14.4.4, there is $\bar{a}' \equiv_B \bar{a}$ with $\dim(\bar{a}'/C) = \dim(\bar{a}/B)$. Then $\bar{a} \in X \implies \bar{a}' \in X$ because X is B-definable (Remark 8.1.3), and so

$$\dim_C(X) \geq \dim(\bar{a}'/C) = \dim(\bar{a}/B) = \dim_B(X).$$

This completes the case where $B \subseteq C$. The general case then follows:

$$\dim_B(X) = \dim_{B \cup C}(X) = \dim_C(X). \qquad \square$$

By Theorem 14.5.2, $\dim_B(X)$ doesn't depend on B, so we just write $\dim(X)$. The following two facts are a restatement of the definition:

- If X is B-definable and $\bar{a} \in X$, then $\dim(\bar{a}/B) \leq \dim(X)$.
- If X is B-definable and non-empty, then there is $\bar{a} \in X$ with $\dim(\bar{a}/B) = \dim(X)$.

We will use these repeatedly in what follows.

Theorem 14.5.3 (Basic properties of dimension)**.** *Let X, Y be definable sets.*

1. $\dim(X) \leq 0$ *if and only if* $|X| < \infty$.
2. *If $X \subseteq Y$, then* $\dim(X) \leq \dim(Y)$.
3. *If $X, Y \subseteq \mathbb{M}^n$, then* $\dim(X \cup Y) = \max(\dim(X), \dim(Y))$.

4. $\dim(X \times Y) = \dim(X) + \dim(Y)$.

5. $\dim(\mathbb{M}^n) = n$, *assuming* $\mathbb{M}$ *is infinite.*

6. *If* $f : X \to Y$ *is a definable surjection, then* $\dim(X) \geq \dim(Y)$.

7. *If* $f : X \to Y$ *is a definable bijection, then* $\dim(X) = \dim(Y)$.

8. *If* $f : X \to Y$ *is a definable injection, then* $\dim(X) \leq \dim(Y)$.

Proof. Take a small set C over which all the sets and functions are defined.

1. If X is finite, then every $\bar{a} \in X$ is algebraic over C, and so $\dim(\bar{a}/C) \leq 0$ (Theorem 13.6.10). Thus $\dim(X) \leq 0$.

   Conversely, if X is infinite, then X is large (Corollary 11.2.8), so there is $\bar{a} \in X$ with $\bar{a} \notin \operatorname{acl}(C)$. Then $\dim(X) \geq \dim(\bar{a}/C) > 0$.

2. Clear.

3. Clear.

4. If $(\bar{a}, \bar{b}) \in X \times Y$, then

   $$\dim(\bar{a}\bar{b}/C) = \dim(\bar{a}/C) + \dim(\bar{b}/C\bar{a}) \leq \dim(X) + \dim(Y)$$

   because $\bar{a}$ is in the C-definable set X and $\bar{b}$ is in the $C\bar{a}$-definable set Y. As this holds for all $(\bar{a}, \bar{b}) \in X \times Y$, we have $\dim(X \times Y) \leq \dim(X) + \dim(Y)$.

   Conversely, take $\bar{a} \in X$ with $\dim(\bar{a}/C) = \dim(X)$. The set Y is $C\bar{a}$-definable, so there is $\bar{b} \in Y$ with $\dim(\bar{b}/C\bar{a}) = \dim(Y)$. Then

   $$\dim(X \times Y) \geq \dim(\bar{a}\bar{b}/C) = \dim(\bar{a}/C) + \dim(\bar{b}/C\bar{a}) = \dim(X) + \dim(Y).$$

5. By part (4), it suffices to show $\dim(\mathbb{M}^1) = 1$. If $a \in \mathbb{M}^1$, then $\dim(a/C) \leq 1$, as a has length 1. Thus $\dim(\mathbb{M}^1) \leq 1$. On the other hand, $\dim(\mathbb{M}) \geq 1$ by part (1).

6. Take $\bar{b} \in Y$ with $\dim(\bar{b}/C) = \dim(Y)$. Since f is surjective, there is $\bar{a} \in X$ with $f(\bar{a}) = \bar{b}$. Then $\bar{b} \in \operatorname{dcl}(C\bar{a}) \subseteq \operatorname{acl}(C\bar{a})$, so by Theorem 13.6.14,

   $$\dim(X) \geq \dim(\bar{a}/C) \geq \dim(\bar{b}/C) = \dim(Y).$$

7. Apply part (6) to f and f^{-1}.

8. By parts (2) and (7), $\dim(X) = \dim(\mathrm{im}(f)) \le \dim(Y)$. □

Theorem 14.5.4 (Fiber dimension theorem). *Let $f : X \to Y$ be a definable function. For every $b \in Y$, let $X_b = f^{-1}(b) = \{x \in X : f(x) = b\}$. If $\dim(X_b) = k$ for all $b \in Y$, then $\dim(X) = k + \dim(Y)$.*

Proof. Take a small set C defining f, X, and Y. Note that $\bar{a}$ and $(\bar{a}, f(\bar{a}))$ are interalgebraic over C for any $\bar{a} \in X$, so

$$\dim(\bar{a}/C) = \dim(\bar{a}, f(\bar{a})/C) = \dim(\bar{a}/Cf(\bar{a})) + \dim(f(\bar{a})/C)$$

by Theorem 13.6.14 and additivity (Theorem 13.6.9). If $\bar{b} = f(\bar{a})$, then

$$\dim(\bar{a}/C) = \dim(\bar{a}/C\bar{b}) + \dim(\bar{b}/C) \le \dim(X_b) + \dim(Y) = k + \dim(Y).$$

because $\bar{a}$ is in the $C\bar{b}$-definable set X_b, and $\bar{b}$ is in the C-definable set Y. As this holds for any $\bar{a} \in X$, we see

$$\dim(X) \le k + \dim(Y).$$

For the converse, take $\bar{b} \in Y$ with $\dim(\bar{b}/C) = \dim(Y)$. The set X_b is $C\bar{b}$-definable, so there is $\bar{a} \in X_{\bar{b}}$ with $\dim(\bar{a}/C\bar{b}) = \dim(X_b) = k$. Then $\bar{b} = f(\bar{a})$, so

$$\dim(X) \ge \dim(\bar{a}/C) = \dim(\bar{a}/C\bar{b}) + \dim(\bar{b}/C) = k + \dim(Y). \quad \square$$

Proof. Let $Z_k = f^{-1}(Y_k)$. Then $\dim(Z_k) = k + \dim(Y_k)$, and $X = \bigcup_k Z_k$. □

Now suppose the the theory is geometric (Definition 14.4.2), meaning that uniform finiteness holds.

Lemma 14.5.5. *Let $\varphi(x_1, \ldots, x_n)$ be an $\mathcal{L}(\mathbb{M})$-formula and let $\psi(x_1, \ldots, x_{n-1})$ be an $\mathcal{L}(\mathbb{M})$-formula equivalent to $\exists^\infty x_n\ \varphi$. Then $\varphi(\mathbb{M}^n)$ has dimension n if and only if $\psi(\mathbb{M}^{n-1})$ has dimension $n-1$.*

Proof. Take a finite set B such that φ and ψ are $\mathcal{L}(B)$-formulas. If $\psi(\mathbb{M}^{n-1})$ has dimension $n-1$, take $\bar{a} \in \psi(\mathbb{M}^{n-1})$ with $\dim(\bar{a}/B) = n-1$. Then $\varphi(\bar{a}, \mathbb{M})$ is infinite, hence large. Take $a_n \in \varphi(\bar{a}, \mathbb{M}) \setminus \mathrm{acl}(B\bar{a})$. Then $(\bar{a}, a_n) \in \varphi(\mathbb{M}^n)$ and

$$\dim(\bar{a}, a_n/B) = \dim(\bar{a}/B) + \dim(a_n/B\bar{a}) = (n-1) + 1 = n,$$

and $\varphi(\mathbb{M}^n)$ has dimension n.

Conversely, suppose $\varphi(\mathbb{M}^n)$ has dimension n. Take $(\bar{a}, a_n) \in \varphi(\mathbb{M}^n)$ with $\dim(\bar{a}, a_n/B) = n$. Then $a_n \notin \operatorname{acl}(B\bar{a})$ and $\dim(\bar{a}/B) = n - 1$. As $\varphi(\bar{a}, \mathbb{M})$ is $B\bar{a}$-definable and contains $a_n \notin \operatorname{acl}(B\bar{a})$, it must be infinite, meaning that $\bar{a} \in \psi(\mathbb{M}^{n-1})$, and then $\dim(\psi(\mathbb{M}^{n-1})) \geq \dim(\bar{a}/B) = n - 1$. □

Lemma 14.5.6. *Let $\varphi(x_1, \ldots, x_n; y_1, \ldots, y_m)$ be an $\mathcal{L}$-formula. The set*

$$\{\bar{b} \in \mathbb{M}^m : \dim(\varphi(\mathbb{M}^n, \bar{b})) = n\}$$

is definable.

Proof. The case $n = 0$ is easy. If $n > 0$, let $\psi(x_1, \ldots, x_{n-1}; \bar{y})$ be the $\mathcal{L}$-formula equivalent to $\exists^\infty x_n\ \varphi$. Then for any $\bar{b} \in \mathbb{M}^m$,

$$\dim(\varphi(\mathbb{M}^n, \bar{b})) = n \iff \dim(\psi(\mathbb{M}^{n-1}, \bar{b})) = n - 1,$$

by Lemma 14.5.5, and the right hand side is definable by induction on n. □

Lemma 14.5.7. *Let $D \subseteq \mathbb{M}^n$ be definable and let k be in $\{0, 1, \ldots, n\}$. Then $\dim(D) \geq k$ if and only if there is a coordinate projection $\pi : \mathbb{M}^n \to \mathbb{M}^k$ such that $\pi(D) \subseteq \mathbb{M}^k$ has dimension k.*

Proof. If $\dim(\pi(D)) = k$, then $\dim(D) \geq k$ by Theorem 14.5.3(6). Conversely, suppose $\dim(D) \geq k$. Take a small set B over which D is defined, and take $\bar{a} \in D$ with $\dim(\bar{a}/B) = \dim(D) \geq k$. There are at least k values of i such that $a_i \notin \operatorname{acl}(Ba_1, \ldots, a_{i-1})$. Let $i_1 < i_2 < \cdots < i_k$ be some such values. Then

$$a_{i_j} \notin \operatorname{acl}(Ba_{i_1}a_{i_2} \cdots a_{i_{j-1}})$$

for each j, and so

$$\dim(a_{i_1}a_{i_2} \cdots a_{i_k}/B) = k.$$

Let $\pi : \mathbb{M}^n \to \mathbb{M}^k$ be the coordinate projection $\pi(x_1, \ldots, x_n) = (x_{i_1}, \ldots, x_{i_k})$. Then $\pi(D)$ is B-definable, $\pi(\bar{a}) \in \pi(D)$, and $\dim(\pi(\bar{a})/B) = k$. We conclude that $\dim(\pi(D)) \geq k$. □

Theorem 14.5.8 (Definability of dimension)**.** *Let $\varphi(x_1, \ldots, x_n; y_1, \ldots, y_m)$ be a formula. For each $k \leq n$, the set*

$$\{\bar{b} \in \mathbb{M}^m : \dim(\varphi(\mathbb{M}^n; \bar{b})) = k\}$$

is definable.

Proof. Let Π_k^n be the finite set of coordinate projections $\mathbb{M}^n \to \mathbb{M}^k$. For each $\pi \in \Pi_k^n$, let $\theta_\pi(z_1, \ldots, z_k, \bar{y})$ be the formula

$$\exists \bar{x}\ \varphi(\bar{x}; \bar{y}) \wedge (\pi(\bar{x}) = \bar{z}).$$

Then $\theta_\pi(\mathbb{M}^k, \bar{b})$ is the image of $\varphi(\mathbb{M}^n, \bar{b})$ under π. By Lemma 14.5.7,

$$D_k := \{\bar{b} \in \mathbb{M}^m : \dim(\varphi(\mathbb{M}^n; \bar{b})) \geq k\} = \bigcup_{\pi \in \Pi_k^n} \{\bar{b} \in \mathbb{M}^m : \dim(\theta_\pi(\mathbb{M}^k; \bar{b})) = k\},$$

and the sets on the right-hand side are definable by Lemma 14.5.6. Thus each D_k is definable. The set we want is $D_k \setminus D_{k-1}$. □

Theorem 14.5.9. *Let $f : X \to Y$ be a definable function. For each $b \in Y$, let $X_b = f^{-1}(b)$. For each $k \leq \dim(X)$, let $Y_k = \{b \in Y : \dim(X_b) = k\}$. Then each set Y_k is definable, and*

$$\dim(X) = \max_k (k + \dim(Y_k)).$$

Proof. Theorems 14.5.8 and 14.5.4. □

14.6 Dimension theory in small models

If D is a definable set in a model M, and N is an elementary extension of M, then $D(N)$ denotes $\varphi(N)$, where $\varphi(\bar{x})$ is the $\mathcal{L}(M)$-formula defining D in M. The choice of φ doesn't matter, because

$$\begin{gathered}\varphi(M) = \psi(M) \iff M \models \forall \bar{x}(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x})) \\ \iff N \models \forall \bar{x}(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x})) \iff \varphi(N) = \psi(N).\end{gathered}$$

Note that $D(M) = D$.

Lemma 14.6.1. *Let $M \preceq N$ be monster models of a pregeometric theory.*

1. *If $\bar{a} \in M^n$ and $B \subseteq M$ is small, then $\dim^M(\bar{a}/B) = \dim^N(\bar{a}/B)$.*
2. *If D is M-definable, then $\dim(D(M)) = \dim(D(N))$.*

Proof. 1. By Theorem 13.3.3, $\operatorname{acl}(Ba_1, \ldots, a_{i-1})$ is the same whether calculated in M or N.

2. Take a small set $B \subseteq M$ defining D. Take $\bar{a} \in D(M)$ with $\dim(\bar{a}/B) = \dim(D(M))$. Then $\bar{a} \in D(N)$ and $\dim(\bar{a}/B) = \dim(D(M))$, so

$$\dim(D(M)) \leq \dim(D(N)).$$

Conversely, take $\bar{a} \in D(N)$ with $\dim(\bar{a}/B) = \dim(D(N))$. Then $\operatorname{tp}(\bar{a}/B)$ is realized in M by some $\bar{c}$. The formula defining $D(N)$ is in $\operatorname{tp}(\bar{a}/B)$, so $\bar{c} \in D(N) \cap M^n = D(M)$. Also, $\dim(\bar{c}/B) = \dim(\bar{a}/B)$ by automorphism invariance. The fact that $\bar{c} \in D(M)$ then shows

$$\dim(D(M)) \geq \dim(\bar{c}/B) = \dim(\bar{a}/B) = \dim(D(N)). \qquad \square$$

Definition 14.6.2. Let M be a small model of a pregeometric theory. If $D \subseteq M^n$ is definable, then $\dim(D)$ is defined to be $\dim(D(\mathbb{M}))$ where $\mathbb{M}$ is a monster model extending M.

Theorem 14.6.3. *The choice of* $\mathbb{M}$ *doesn't matter in Definition 14.6.2.*

Proof. Let $\mathbb{M}_1, \mathbb{M}_2$ be two monster models extending M. Then $\mathbb{M}_1$ and $\mathbb{M}_2$ are elementarily equivalent as $\mathcal{L}(M)$-structures. By elementary amalgamation there is a third monster model $\mathbb{M}_3$ extending $\mathbb{M}_1$ and $\mathbb{M}_2$, up to isomorphism. Then

$$\dim(D(\mathbb{M}_1)) = \dim(D(\mathbb{M}_3)) = \dim(D(\mathbb{M}_2))$$

by two applications of Lemma 14.6.1. □

Corollary 14.6.4. *Dimension is invariant in elementary extensions: if* $M \preceq N$ *and* D *is a definable set in* M*, then* $\dim(D(M)) = \dim(D(N))$.

Proof. Take a monster model $\mathbb{M}$ extending N (and M). Then $\dim(D(M)) = \dim(D(\mathbb{M})) = \dim(D(N))$ by two applications of Definition 14.6.2. □

Theorem 14.6.5. *Let* M *be a model of a pregeometric theory* T*. Define* $\dim(-)$ *as in Definition 14.6.2.*

1. *The basic properties of dimension (Theorem 14.5.3) hold in* M.

2. *If* T *is geometric, then the fiber dimension theorem (Theorem 14.5.4) and definability of dimension (Theorem 14.5.8) hold in* M.

Proof. 1. For example, we show $\dim(D_1 \times D_2) = \dim(D_1) + \dim(D_2)$. If $\varphi(\bar{x})$ defines D_1 and $\psi(\bar{y})$ defines D_2, then the formula $\theta(\bar{x}, \bar{y}) :\equiv \varphi(\bar{x}) \wedge \psi(\bar{y})$ defines $D_1 \times D_2$. Therefore

$$(D_1 \times D_2)(\mathbb{M}) = \theta(\mathbb{M}) = D_1(\mathbb{M}) \times D_2(\mathbb{M}).$$

Thus

$$\begin{gathered}\dim(D_1 \times D_2) = \dim((D_1 \times D_2)(\mathbb{M})) \\ = \dim(D_1(\mathbb{M}) \times D_2(\mathbb{M})) = \dim(D_1(\mathbb{M})) + \dim(D_2(\mathbb{M})) \\ = \dim(D_1) + \dim(D_2).\end{gathered}$$

2. Suppose we have the configuration $f : X \to Y$ of Theorem 14.5.4, where $X_b = f^{-1}(b)$ has dimension k for every $b \in Y$. In order to reduce from M to the known case of $\mathbb{M}$, we need to show that the property

$$\dim(X_b) = k \text{ for every } b \in Y$$

transfers from M to $\mathbb{M}$. Let $f_{\mathbb{M}} : X(\mathbb{M}) \to Y(\mathbb{M})$ be the function defined by the same formula as f, and for $b \in Y(\mathbb{M})$ let $X_b(\mathbb{M})$ denote the fiber of $f_{\mathbb{M}}^{-1}(b)$. Note that when $b \in Y = Y(M)$, the set $X_b(\mathbb{M})$ really is the extension of X_b. By the definability of dimension (Theorem 14.5.8), the set

$$Z = \{b \in Y(\mathbb{M}) : \dim(X_b(\mathbb{M})) \neq k\}$$

is definable. It is $\mathrm{Aut}(\mathbb{M}/M)$-invariant, hence M-definable (Theorem 11.3.8). If $b \in Y(M)$, then $\dim(X_b(\mathbb{M})) = \dim(X_b) = k$, so $b \notin Z$. Therefore there are no M-points in Z. By the Tarski-Vaught criterion, $Z = \varnothing$. Thus $Z = \varnothing$, and $\dim(X_b(\mathbb{M})) = k$ for every $b \in Y(\mathbb{M})$. Then we can apply Theorem 14.5.4 over $\mathbb{M}$ to get what we want.

For Theorem 14.5.8, fix a formula $\varphi(\bar{x}, \bar{y})$. The set

$$Z_k = \{\bar{b} \in \mathbb{M} : \dim(\varphi(\mathbb{M}; \bar{b})) = k\}$$

is definable by Theorem 14.5.8 applied to $\mathbb{M}$, and clearly $\mathrm{Aut}(\mathbb{M}/\varnothing)$-invariant. By Theorem 11.3.8, it is 0-definable, defined by some formula $\psi_k(\bar{y})$. Then for any $\bar{b}$ in M,

$$\begin{gathered}\dim(\varphi(M, \bar{b})) = k \iff \dim(\varphi(\mathbb{M}, \bar{b})) = k \\ \iff \mathbb{M} \models \psi_k(\bar{b}) \iff M \models \psi_k(\bar{b}).\end{gathered}$$

The first equivalence holds by Definition 14.6.2. The second holds by choice of ψ_k. The third holds as $M \preceq \mathbb{M}$.

Therefore $\{\bar{b} \in M^m : \dim(\varphi(M^n; \bar{b})) = k\}$ is the definable set $\psi_k(M^m)$. □

Appendix A

Mathematical background

This appendix reviews the mathematical background assumed throught the book.

A.1 Logical notation

We write $a := b$ or $b =: a$ to mean that a is defined to be b, i.e., "let $a = b$."

If φ, ψ are statements, then $\varphi \implies \psi$ means that φ logically implies ψ. In other words,

$$\varphi \implies \psi$$

means

If φ then ψ.

The notation $\varphi \iff \psi$ means that $\varphi \implies \psi$ and $\psi \implies \varphi$. We say that φ holds "if and only if" ψ holds. "If and only if" is often abbreviated to iff. The notation $\forall x\ (\ldots)$ means "for every x, ..." Similarly, the notation $\exists x\ (\ldots)$ means "there is an x such that ...." If we are only interested in values of x coming from a set A, we write $\forall x \in A$ or $\exists x \in A$. In other words, these things

$$\forall x \in A\ (\ldots)$$
$$\exists x \in A\ (\ldots)$$

mean the following, respectively:

For every x in A, ...

There is an x in A such that ....

A.2 Sets

If A is a set and x is a value, then $x \in A$ means that x is an element of A, and $x \notin A$ means that a is not an element of A. If A and B are sets, then $A \subseteq B$ means that A is a subset of B, i.e., every element of A is an element of B. It is an axiom of set theory that $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. The notation $A \subsetneq B$ means that A is a proper subset of B: $A \subseteq B$ and $A \neq B$. We avoid the ambiguous notation $A \subset B$. Remember to distinguish $A \subsetneq B$ (A is a proper subset of B) from $A \not\subseteq B$ (A is not a subset of B). We write $A \subseteq_f B$ to mean that A is a finite subset of B. (This relation comes up frequently in model theory.)

We write the empty set as $\varnothing$; this is the unique set with no elements. If A is a set, then $\mathfrak{P}(A)$ denotes the powerset of A, the set of all subsets of A:

$$\mathfrak{P}(A) = \{X : X \subseteq A\}.$$

Here, the set-builder notation $\{x : \ldots\}$ means "the set of x such that ...." Similarly, $\{x \in A : \ldots\}$ means "the set of x in A such that ..." and $\{f(x) : x \in A, \ldots\}$ means "the set of values $f(x)$ where x is in A and ...".

If A and B are sets, then $A \cap B$ and $A \cup B$ denote the intersection and union of A and B:

$$\begin{aligned} A \cap B &= \{x : x \in A \text{ and } x \in B\} \\ A \cup B &= \{x : x \in A \text{ or } x \in B\}. \end{aligned}$$

If $A_1, \ldots, A_n$ are sets, then we write their intersection and union as follows:

$$\begin{aligned} \bigcap_{i=1}^{n} A_i &= A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n \\ \bigcup_{i=1}^{n} A_i &= A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n. \end{aligned}$$

Additionally, we write the "set difference" of A and B as $A \setminus B$:

$$A \setminus B = \{x : x \in A \text{ and } x \notin B\}.$$

This should be distinguished from the "symmetric difference" $(A \setminus B) \cup (B \setminus A)$, which we will not use.

Two sets A and B are *disjoint* if $A \cap B = \varnothing$. A list of sets $A_1, \ldots, A_n$ is *pairwise disjoint* if any two of them are disjoint: $A_i \cap A_j = \varnothing$ for any $i \neq j$. A list of values $x_1, \ldots, x_n$ is *pairwise distinct* if $x_i \neq x_j$ for $i \neq j$.

A.3 $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

We use the following blackboard bold symbols. $\mathbb{N}$ denotes the natural numbers $\{0, 1, 2, \ldots\}$. Note that we include 0 in $\mathbb{N}$. We sometimes denote $\mathbb{N}$ as ω. Notation like $n < \omega$ and $n \in \omega$ means that n is a natural number. The reason for this notation comes from set theory, where ω is another name for $\mathbb{N}$ and ω is the first ordinal number after the natural numbers. $\mathbb{Z}$ denotes the integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$. $\mathbb{Q}$ denotes the set of rational numbers, values of the form x/y where $x, y \in \mathbb{Z}$. $\mathbb{R}$ denotes the usual real numbers. $\mathbb{C}$ denotes the complex numbers, values of the form $x + iy$ where $x, y \in \mathbb{R}$ and $i = \sqrt{-1}$. To summarize,

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}.$$

A.4 Tuples, products, and relations

An *n-tuple* is a list of n values $(x_1, x_2, x_3, \ldots, x_n)$. 2-tuples are called *pairs* or *ordered pairs*, and 3-tuples are called *triples*. Two n-tuples

$$(x_1, \ldots, x_n)$$
$$(y_1, \ldots, y_n)$$

are equal if and only if $x_i = y_i$ for all i between 1 and n (inclusive). For example, $(x_1, x_2) = (y_1, y_2)$ if and only if $x_1 = y_1$ and $x_2 = y_2$.

If A and B are sets, the *direct product* or *cartesian product*, written $A \times B$, is the set of ordered pairs (x, y) where $x \in A$ and $y \in B$:

$$A \times B = \{(x, y) : x \in A \text{ and } y \in B\}.$$

For example,

$$\begin{aligned}\{1, 2, 3\} \times \{\text{up}, \text{down}\} = \{&(1, \text{up}), (1, \text{down}), (2, \text{up}), \\ &(2, \text{down}), (3, \text{up}), (3, \text{down})\}.\end{aligned}$$

A *relation* between A and B is a subset $R \subseteq A \times B$. If $x \in A$ and $y \in B$, then $x \; R \; y$ means $(x, y) \in R$.

A *relation on a set* A is a relation between A and A, i.e., a subset $R \subseteq A^2$. A relation R on A is said to be…

- *reflexive* if $x \; R \; x$ for any $x \in A$.
- *symmetric* if $x \; R \; y \implies y \; R \; x$
- *transitive* if $x \; R \; y$ and $y \; R \; z$ imply $x \; R \; z$.
- *antisymmetric* if $x \; R \; y$ and $y \; R \; x$ imply $x = y$.

For example, the relation $=$ is reflexive, symmetric, transitive, and antisymmetric. The relation $<$ is transitive, and antisymmetric, but not reflexive or symmetric. The relation $\leq$ is reflexive, transitive, and antisymmetric, but not symmetric.

An *equivalence relation* on A is a relation that is reflexive, symmetric, and transitive. Fix an equivalence relation $\sim$. If $x \in A$, the *equivalence class* of x is the set of $y \in A$ equivalent to x:

$$[x] = \{y \in A : x \sim y\}.$$

The *quotient set* is the set of equivalence classes:

$$A/{\sim} = \{[x] : x \in A\}.$$

Using the definition of equivalence relation, one can show that $[x] = [y] \iff x \sim y$. Moreover, the collection of equivalence classes is a *partition* of A—a collection $\mathcal{C}$ of non-empty subsets of A such that each $x \in A$ belongs to exactly one set in $\mathcal{C}$. In fact, there is a one-to-one correspondence between equivalence relations on A and partitions of A.

A *partial order* on A is a relation $\leq$ that is reflexive, transitive, and antisymmetric. The prototypical examples of partial orders are:

- The relation $\leq$ on $\mathbb{R}$.
- The relation $\subseteq$ on the power set $\mathfrak{P}(X)$.

If $\leq$ is a partial order, then $x < y$ means $x \leq y$ and $x \neq y$. The relation $<$ is always transitive and irreflexive ($x \not< x$ for any x). A *strict partial order* is a relation $<$ that is transitive and irreflexive. In fact, there is a one-to-one correspondence between partial orders on A and strict partial orders on A.

A *poset* or *partially ordered set* is a pair $(A, \leq)$ where $\leq$ is a partial order on A. In a poset $(A, \leq)$, two elements x, y are *comparable* if $x \leq y$ or $y \leq x$; otherwise they are *incomparable.* A *linear order* or *total order* is a partial order in which any two elements are comparable. The relation $\leq$ on $\mathbb{R}$ is a linear order, but $\subseteq$ is usually not a linear order on $\mathfrak{P}(X)$.

A.5 Functions

A *function* or *map* from A to B is a relation $f \subseteq A \times B$ such that for every $x \in A$, there is exactly one $y \in B$ such that $x\ f\ y$. We write this unique value of y as $f(x)$, so that

$$f(x) = y \iff (x\ f\ y) \iff (x, y) \in f.$$

The notation $x \mapsto y$ means that $f(x) = y$ for whatever function f we are talking about. Note the bar at the left end of $\mapsto$. The notation $f : A \to B$ means that A and B are sets and f is a function from A to B. The sets A and B are called the *domain* and *codomain* of f. The domain of f is written $\mathrm{dom}(f)$. The *range* or *image* of f is

$$\mathrm{im}(f) = \{f(x) : x \in A\} = \{y \in B : \text{ there is } x \in A \text{ such that } f(x) = y\}.$$

If X is a subset of A, then the *image* or *direct image* of X is the set

$$f(X) = \{f(x) : x \in X\} = \{y \in B : \text{ there is } x \in X \text{ such that } f(x) = y\}.$$

If Y is a subset of B, then the *preimage* or *inverse image* of Y is the set

$$f^{-1}(Y) = \{x \in B : f(x) \in Y\}.$$

If f is a function from A to B, then f is a…

1. *surjection* if for every $y \in B$, there is at least one $x \in A$ with $f(x) = y$.
2. *injection* if for every $y \in B$, there is at most one $x \in A$ with $f(x) = y$.
3. *bijection* if for every $y \in B$, there is exactly one $x \in A$ with $f(x) = y$.

We say that f is *surjective*, *injective*, or *bijective* if f is a surjection, injection, or bijection. Note the following:

- f is a surjection if and only if $\mathrm{im}(f) = A$.
- f is an injection if and only if

  $$f(x) = f(y) \implies x = y$$

  if and only if

  $$x \neq y \implies f(x) \neq f(y).$$

- f is a bijection if and only if f is injective and surjective.

If $f : A \to B$ is a bijection, then there is an *inverse function* $f^{-1} : B \to A$ defined by

$$f^{-1}(y) = x \iff f(x) = y.$$

If $f : A \to B$ and $g : B \to C$ are functions, then the *composition* is the function $h : A \to C$ defined by

$$h(x) = f(g(x)).$$

The composition is usually written $f \circ g$. Note that $f \circ g$ is the function where g is applied first and f is applied second.

If A is a set, then id_A or id denotes the *identity function* on A, the function

$$\begin{gathered} \mathrm{id}_A : A \to A \\ \mathrm{id}_A(x) = x. \end{gathered}$$

Note that if $f : A \to B$ is a function then

$$\begin{gathered} f \circ \mathrm{id}_A = f \\ \mathrm{id}_B \circ f = f. \end{gathered}$$

If $f : A \to B$ is a bijection and $f^{-1} : B \to A$ is the inverse, then

$$\begin{gathered} f^{-1} \circ f = \mathrm{id}_A \\ f \circ f^{-1} = \mathrm{id}_B\,. \end{gathered}$$

If A, B, C are sets, then a function $f : A \times B \to C$ is a function from the cartesian product $A \times B$ to C. If $x \in A$ and $y \in B$, we write $f((x, y))$ as $f(x, y)$, and we think of f as a function which takes one input x from A and one input y from B, and then outputs a value $f(x, y)$ in C.

If A is a set, then A^2, A^3, ... denote the cartesian product of A with itself n times:

$$\begin{gathered} A^2 = A \times A \\ A^3 = A \times A \times A \\ \cdots \\ A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ times}}. \end{gathered}$$

So A^n is the set of n-tuples $(x_1, \ldots, x_n)$ such that $x_1, x_2, \ldots, x_n$ are all in A. A function $f : A^n \to B$ can be thought of as a function which takes n inputs $x_1, \ldots, x_n$ from A and outputs a value in B. We think of operations like $+$ (addition) and $\cdot$ (multiplication) as functions $\mathbb{R}^2 \to \mathbb{R}$, taking two inputs from $\mathbb{R}$ and outputting one value in $\mathbb{R}$. But we usually write $x + y$ rather than $+(x, y)$.

A.6 Cardinalities

If X is a set, then $|X|$ denotes the *size* or *cardinality* of X, the number of elements of X. For example, $|\varnothing| = 0$. When X is finite, $|X|$ is an element of $\mathbb{N}$. Otherwise, $|X|$ is one of Cantor's *infinite cardinal numbers*, of which the first few are $\aleph_0, \aleph_1, \aleph_2, \ldots$. It is worth knowing that

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$$
$$|\mathbb{R}| = |\mathbb{C}| = 2^{\aleph_0} > \aleph_0.$$

The axioms of set theory neither prove nor disprove the *continuum hypothesis*, the statement that $2^{\aleph_0} = \aleph_1$. If X and Y are sets, then

$$|X \times Y| = |X| \cdot |Y|$$
$$|X \cup Y| \le |X| + |Y|$$
$$|X \cup Y| = |X| + |Y| \text{ if } X \cap Y = \varnothing$$
$$|\mathfrak{P}(X)| = 2^{|X|} > |X|$$
$$X \subseteq Y \implies |X| \le |Y|.$$

Moreover, $|X| = |Y|$ if and only if there is a bijection $f : X \to Y$, and $|X| \le |Y|$ if and only if there is an injection $f : X \to Y$. When X and Y are non-empty, $|X| \ge |Y|$ if and only if there is a surjection $X \to Y$.

If X is a proper subset of Y, then $|X| \le |Y|$, but it can happen that $|X| = |Y|$ when X and Y are infinite. For example, $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q}$, but $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$.

It is worth knowing that if κ, λ are infinite cardinals, then $\kappa \cdot \lambda = \kappa + \lambda = \max(\kappa, \lambda)$.

The notation $|X| < \infty$ means that the set X is finite, and $|X| = \infty$ means that X is infinite. This is an abuse of notation—there is no cardinal number "∞." In fact,

$$\begin{aligned} |X| < \infty &\iff |X| < \aleph_0 \\ |X| = \infty &\iff |X| \geq \aleph_0. \end{aligned}$$

In set theory, $\aleph_0$, $\mathbb{N}$, and ω are all the same thing, so we sometimes write $\aleph_0$ as ω.

Appendix B

Set theory

We will use the following slightly more advanced definitions and facts from set theory.

B.1 Ordinals

In set theory, one defines a class *Ord* of *von Neumann ordinal numbers*, also called *ordinal numbers* or *ordinals*. Rather than defining *Ord*, we treat it as a black box. Here are its important properties:

Fact B.1.1. *1. There is a linear order $\le$ on the class of ordinals.*

2. $\le$ is a well-ordering: if S is a non-empty set or class of ordinals, then $\min(S)$ exists.

3. For each $x \in Ord$,

$$x = \{y \in Ord : y < x\}.$$

In particular, the right hand side is a set, not a proper class.

4. Consequently, if $x, y \in Ord$, then $x < y \iff x \in y$.

5. Also, if $x, y \in Ord$, then $x \le y \iff x \subseteq y$.

*6. If S is a set of ordinals (*not *a proper class), then the supremum* $\sup(S)$ *exists.*

The first few ordinals are

$$0, 1, 2, 3, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega 2, \omega 2 + 1, \ldots$$

where

$$\begin{aligned}
&0 = \{\} = \varnothing \\
&1 = \{0\} \\
&2 = \{0, 1\} \\
&3 = \{0, 1, 2\} \\
&\ldots \\
&\omega = \{0, 1, 2, 3, \ldots\} = \mathbb{N} \\
&\omega + 1 = \{0, 1, 2, 3, \ldots, \omega\} \\
&\omega + 2 = \{0, 1, 2, 3, \ldots, \omega, \omega + 1\} \\
&\ldots \\
&\omega \cdot 2 = \{0, 1, 2, 3, \ldots, \omega, \omega + 1, \omega + 2, \ldots\} \\
&\omega \cdot 2 + 1 = \{0, 1, 2, 3, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega \cdot 2\} \\
&\ldots
\end{aligned}$$

If α is an ordinal, there is a smallest ordinal greater than α, which is called $\alpha + 1$. Ordinals of the form $\alpha + 1$ are called *successor ordinals*. Non-zero ordinals that are not successors are called *limit ordinals*. The first few limit ordinals are ω and $\omega \cdot 2$.

B.2 Induction and recursion

Let α be an ordinal and S be a subset of α, i.e., a set of ordinals less than α. Suppose that the following condition holds for any $x \in \alpha$:

$$\text{If every } y < x \text{ is in } S, \text{ then } x \in S. \tag{$*_x$}$$

Then $S = \alpha$, a fact called *induction*. To prove this, suppose $S \subsetneq \alpha$. Then $\alpha \setminus S$ is a non-empty set of ordinals, so it has a minimum $x = \min(\alpha \setminus S)$. If $y < x$, then $y \notin \alpha \setminus S$ because x was the minimum, and so $y \in S$. Then $(*_x)$ says that $x \in S$, contradicting the fact that we took x in the complement of S.

Closely related to induction is the fact that we can recursively define functions on α:

Fact B.2.1. *Let α be an ordinal and V be a set. Let $\mathcal{P}$ be the set of pairs (x, f), where $x \in \alpha$ and f is a function from x to V. Let $G : \mathcal{P} \to V$ be a function. Then there is a unique function $f : \alpha \to V$ such that for every $x \in \alpha$, $f(x) = G(f|_x)$, where $f|_x$ is the restriction of f to the set $x = \{y \in \alpha : y < x\}$.*

The notation is confusing, but the point is that the value $f(x)$ is determined by the values $f(y)$ for $y < x$. The uniqueness of f is an easy consequence of induction, but the existence of f takes more work. See a book on set theory for a proof.

B.3 Cardinals

If A, B are sets, formally define $|A| = |B|$ to mean that there is a bijection from A to B. This is an equivalence relation on the class of sets.

Fact B.3.1. *If S is any set, then there is an ordinal x with $|S| = |x|$.*

The well-ordering property lets us choose a system of representatives for the equivalence relation $|A| = |B|$.

Definition B.3.2. $|S|$ is the smallest ordinal x such that $|x| = |S|$.

Then $|A| = |B|$ agrees with the previous notation, but $|A|$ now has a concrete meaning.

Definition B.3.3. A *(von Neumann) cardinal number* or *cardinal* is an ordinal of the form $|A|$ for some set A.

Equivalently, an ordinal x is a cardinal if $|y| < |x|$ for every $y < x$ (i.e., every $y \in x$).

The class of cardinals is well-ordered: for any non-empty set of cardinals there is a smallest member. The first few cardinals are

$$0, 1, 2, 3, \ldots, \aleph_0, \aleph_1, \aleph_2, \ldots, \aleph_\omega, \aleph_{\omega+1}, \ldots$$

The cardinal $\aleph_0$ is the same as the ordinal ω. The cardinal $\aleph_1$ equals an ordinal called ω_1, the first uncountable ordinal. Between ω and ω_1 there are MANY countable ordinals, of which the first few are

$$\omega, \omega + 1, \ldots, \omega \cdot 2, \ldots, \omega \cdot 3, \ldots, \omega^2, \ldots, \omega^\omega, \ldots, \omega^{\omega^\omega}, \ldots, \omega^{\omega^{\omega^\omega}}, \ldots.$$

B.4 Zorn's lemma

Let $(P, \leq)$ be a poset, i.e., a pair P and a partial order $\leq$ on P. A *chain* is a set $I \subseteq P$ that is linearly ordered by $\leq$, in the sense that for any $x, y \in I$, either $x \leq y$ or $y \leq x$. If $I \subseteq P$ is a chain, an *upper bound* is an element $b \in P$ such that $b \geq I$, meaning that $b \geq x$ for all $x \in I$.

For example, if $(P, \leq) = (\mathfrak{P}(\mathbb{N}), \subseteq)$, then the family of sets

$$\begin{aligned}&\{0\},\\&\{0,2\},\\&\{0,2,4\},\\&\{0,2,4,6\},\\&\ldots\end{aligned}$$

is a chain, and $\{0, 2, 4, 6, 8, 10, \ldots\}$ is an upper bound.

An element $x \in P$ is *maximal* if there is no $y \in P$ with $y > x$. For example, in $(\mathfrak{P}(\mathbb{N}), \subseteq)$, the element $\mathbb{N}$ is the unique maximal element. In general, there can be more than one maximal element, or none.

Fact B.4.1 (Zorn's lemma)**.** *Let $(P, \leq)$ be a poset such that every chain $I \subseteq P$ has an upper bound. Then P has a maximal element.*

If you're curious, here is a sketch of the proof:

Proof sketch. Suppose for the sake of contradiction that P has no maximal element. For any $x \in P$, there is $x' \in P$ with $x' > x$; otherwise x is maximal. Choose a function $x \mapsto x'$ with this property.

Take an ordinal α with $|\alpha| > |P|$.[1] Recursively define $f : \alpha \to P$ as follows. At step α, let $I_\alpha = \{f(x) : x < \alpha\}$. The set I_α will be a chain in P by induction. Take an upper bound $b \geq I_\alpha$ and set $f(\alpha) = b'$. Then $f(\alpha) > I_\alpha$, so $f(\alpha) > f(x)$ for all $x < \alpha$.

This gives a map $f : \alpha \to P$ which is strictly increasing:

$$x < y \implies f(x) < f(y).$$

Then f is an injection, and $|\alpha| \leq |P|$, contradicting the choice of α. □

For more details of the proof, see any book on set theory.

Most applications of Zorn's lemma take the following form:

[1] More precisely, we want $|\alpha| \not\leq |P|$. Finding α is the hard part of the proof.

Corollary B.4.2. *Let S be a set and let $\mathcal{F} \subseteq \mathfrak{P}(S)$ be a collection of subsets of S. Suppose that whenever $\mathcal{I}$ is a chain in $(\mathcal{F}, \subseteq)$, the union $\bigcup \mathcal{I}$ is in $\mathcal{F}$. Then $\mathcal{F}$ has a maximal element.*

Proof. Apply Zorn's lemma to the poset $(\mathcal{F}, \subseteq)$. □

Example B.4.3. A *graph* is a pair (S, R) where S is a set and $R \subseteq S^2$ is a relation that is symmetric and irreflexive:

$$x \; R \; y \implies y \; R \; x$$
$$x \not R \; x.$$

(If you know graph theory, think of S as the set of vertices, and $x \; R \; y$ as the relation saying that there is an edge from x to y. We are only considering simple, undirected graphs.)

Fix a graph (S, R). Say that $X \subseteq S$ is *independent* if for any $x, y \in X$, we have $x \not R \; y$. Let $\mathcal{F} \subseteq \mathfrak{P}(S)$ be the collection of independent sets. Then there is a maximal independent set by Zorn's lemma, specifically Corollary B.4.2. To apply Corollary B.4.2, we must show that if $\mathcal{I} \subseteq \mathcal{F}$ is a chain, then $X_\infty := \bigcup \mathcal{I}$ is indepedent. Suppose for the sake of contradiction that $x_1, x_2 \in X_\infty$ and $x_1 \; R \; x_2$. As $x_1 \in X_\infty = \bigcup \mathcal{I}$, there is some $X_1 \in \mathcal{I}$ such that $x_1 \in X_1$. Similarly, there is $x_2 \in X_2 \in \mathcal{I}$. As $\mathcal{I}$ is a chain, either $X_1 \subseteq X_2$ or $X_2 \subseteq X_1$. In the first case, $x_1, x_2 \in X_2$, and X_2 fails to be independent, contradicting the fact that $X_2 \in \mathcal{I} \subseteq \mathcal{F}$. Similarly, if $X_2 \subseteq X_1$ then $x_1, x_2 \in X_1$, and X_1 fails to be independent. Thus X_∞ is independent and Zorn's lemma applies.

In this case, maximality means that we have an independent set X such that $X \cup \{a\}$ is *not* independent for any $a \in S \setminus X$. Therefore, for any $a \in S \setminus X$ there is $b \in X$ with $a \; R \; b$. Thus X is an independent set and every element outside of X is adjacent (connected by an edge) to an element of X.