PMATH 433/633:
Set Theory and Model Theory

Rahim Moosa, University of Waterloo

January 10, 2009

Contents

Introduction

The set theory part of these notes are based on lecture notes of Tuna Altinel (Université Lyon 1). The faithfullness to that text is variable; certain sections are essentially translations, while other topics are substantially reworked. For the model theory I have used some of Altinel's notes but mostly Dave Marker's book "Model Theory: An Introduction" (Springer 2002) as a source for examples and ideas about exposition. I am grateful to both of these authors. I am, of course, responsible for any errors.

Part 1

Set Theory

CHAPTER 1

Ordinals

1.1. Basic notions

DEFINITION 1.1. Suppose R is a binary relation on a set E. The pair (E, R) is called a *partially ordered set* (or *poset*) if R satisfies the following properties

Reflexivity: aRa for all $a \in E$
Antisymmetry: if aRb and bRa then $a = b$, for all $a, b \in E$
Transitivity: if aRb and bRc then aRc, for all $a, b, c \in E$.

A poset (E, R) is *linearly ordered* (or *totally ordered*) if in addition it satisifies

Linearity: for all $a, b \in E$, either aRb, bRa, or $a = b$.

A linear ordering is *well-ordered* if every non-empty subset has a least element.

DEFINITION 1.2. A *strict partially ordered set* is a pair (E, R) where E is a set and R is abinary relation satisfying

Antireflexivity: $\neg(aRa)$ for all $a \in E$

as well as antisymmetry and transitivity. The notions of *strict linear order* and *strict well-order* are similarly defined by replacing reflexivity with antireflexivity.

Note that there is a canonical bijective correspondence between posets and strict posets: to any poset (E, R) we can associated the strict poset $(E, R_{\neq})$ where $aR_{\neq}b$ if and only if aRb and $a \neq b$. It is not hard to see that this correspondence preserves linearity and well-orderedness.

We often use $\leq$ to denote the ordering on a poset and $<$ to denote the corresponding strict ordering.

LEMMA 1.3. *Well-orderings are* rigid*; that is, the identity map is the only automorphism of a well-ordering.*

PROOF. Of course, by an automorphism of a poset $(E, \leq)$ we mean a bijective map $f : E \to E$ such that $a \leq b$ if and only if $f(a) \leq f(b)$, for all $a, b \in E$. Suppose f is such an automorphism of a well-ordering $(E, \leq)$, and suppose, toward a contradiction, that $f \neq \mathrm{id}$. Let $D := \{x \in E : f(x) \neq x\}$ be the (nonempty) set of points that are moved by f. Since $f(x) = x$ if and only if $x = f^{-1}(x)$, D is also the set of elements moved by f^{-1}. Now D must have a least element, say $a \in E$. Either $f(a) < a$ or $a < f(a)$. In the first case $f(a) \notin D$, so f^{-1} fixes $f(a)$, which means that $a = f^{-1}f(a) = f(a)$, contradicting that $a \in D$. In the second case, applying f^{-1} to both sides, we get that $f^{-1}(a) < a$ and hence $f^{-1}(a) \notin D$, which means it is fixed by f and so $a = ff^{-1}(a) = f^{-1}(a)$, again contradicting $a \in D$. $\square$

COROLLARY 1.4. *Suppose $(E, \leq)$ and $(F, \preceq)$ are isomorphic well-orderings. Then there exists a unique isomorphism from $(E, \leq)$ to $(F, \preceq)$.*

PROOF. Of course, an isomorphism from $(E, \leq)$ to $(F, \preceq)$ is a bijection $f : E \to F$ such that $a \leq b$ if and only if $f(a) \preceq f(b)$. Suppose f and g are two such isomorphisms. Then $g^{-1} \circ f$ is an automorphism of $(E, \leq)$ and hence, by Lemma 1.3, $g^{-1} \circ f = \mathrm{id}$. So $f = g$. □

LEMMA 1.5. *Suppose $(E, <)$ is a strict well-ordering. For any $b \in E$, $(E, <)$ and $(\{x \in E : x < b\}, <)$ are not isomorphic.*

PROOF. Suppose, toward a contradiction, that $f : E \to \{x \in E : x < b\}$ is an isomorphism. Let $D = \{x \in E : f(x) \neq x\}$ be the set of elements moved by f. Since $f(b) \neq b$ (as $b \notin \{x \in E : x < b\}$), D is nonempty. We finish as in the proof of Lemma 1.3 by considering a least element a of D, and showing that both $a < f(a)$ and $a > f(a)$ lead to a contradiciton. □

We are going to be studying posets where the ordering is given by the membership relation $\in$. This may seem at first rather strange; it implies that the elements of our posets are themselves sets, and indeed their elements are also sets, and so on. For example $E = \{\emptyset, \{\emptyset\}\}$ is such a set. This set has two members, each of which is itself a set, namely the empty set $\emptyset$ and the set $\{\emptyset\}$ which contains one element. Ordered by membership, the only relation holding in E is $\emptyset < \{\emptyset\}$.

DEFINITION 1.6. An *ordinal* is a set α satisfying the following two properties:

1. Every element of α is a subset of α.
2. The membership relation induces a strict well-ordering on α.

We equip an ordinal with the ordering induced by $\in$. So for $x, y \in \alpha$, $x < y$ will be synonymous with $x \in y$.

EXAMPLE 1.7 (The natural numbers). Let us make the following definitions

$$\begin{aligned} 0 &:= \emptyset \\ 1 &:= \{\emptyset\} \\ 2 &:= \{\emptyset, \{\emptyset\}\} \\ 3 &:= \{\emptyset,\ \{\emptyset\},\ \{\emptyset, \{\emptyset\}\}\} \\ &\vdots \end{aligned}$$

so that $S(n) := n \cup \{n\}$ for all n. Here S denotes the successor function. Each of these sets is a (finite) ordinal: you should check that the membership relation on each fixed n is antireflexive, antisymettric, transitive, and linear. That n is well-ordered is clear as it is finite.

Now let ω be the set whose members are all the above finite ordinals. That is, $\omega := \{0, 1, 2, 3, \dots\}$. Then ω is an (infinite) ordinal.

Before continuing let us pause to consider what set-theoretical axioms we have used to construct ω. To start with we needed a set that contained no elements.

AXIOM 1 (Emptyset). *There is a set, denoted by $\emptyset$, which has no members.*

Next, given a set x we needed to consider the set $\{x\}$. It is convenient to do this using the following axiom.

AXIOM 2 (Pairset). *For any two sets x and y there is a set p with the property that $t \in p$ if and only if $t = x$ or $t = y$. This set p is usually denoted by $\{x, y\}$.*

Note that we get the singleton $\{x\}$ by using the pairset axiom with $x = y$. To form $S(n)$ from n we needed to be able to take the union of two sets (namely n and $\{n\}$). This can be done using the pairset axiom together with

AXIOM 3 (Unionset). *For any set x there exists a set y with the property that $t \in y$ if and only if there exists $s \in x$ with $t \in s$.*

The above axioms does not allow us to produce the infinite ordinal ω. We could add an axiom asserting the existence of ω, but it is more convenient to allow the following apparently weaker (but actually sufficient) axiom.

AXIOM 4 (Infinity). *There exists a set I which contains $\emptyset$ as well as the* successor *of each of its members; that is, if $x \in I$ then $x \cup \{x\} \in I$.*

Actually we have missed an even more fundamental axiom, one that allows us to identify $\{x\}$ and $\{x, x\}$.

AXIOM 5 (Extensionality). *For any two sets x and y, $x = y$ if and only if x and y have exactly the same members.*

These are all the axioms we have used so far, but we are about to use one more axiom in the proofs of the lemmas that follow. For the purposes of stating this axiom let us say that a condition $P(x)$ is *definite* if for any object a it is determined unambigously whether $P(a)$ is true or false. (Note that we do not ask that the truth value can be *effectively* determined, just that it has a definite truth value.) This is somewhat vague, and can be made more precise by using the notion of a "definable property", a notion which will be studied extensively in the model theory part of this course.

AXIOM 6 (Separation). *Suppose $P(x)$ is a definite condition. For each set A there exists a set B such that $a \in B$ if and only if $a \in A$ and $P(a)$ is true.*

Let us at this point, for the sake of completeness, list the final two axioms of *Zermelo-Fraenkel* (**ZF**) set theory.

AXIOM 7 (Powerset). *For each set A there exists a set $\mathcal{P}(A)$ whose members are the subsets of A.*

AXIOM 8 (Replacement). *If H is a definite operation and A is a set then there exists a set B which is the image of A under H. That is, $y \in B$ if and only if there exists $x \in A$ such that $y = H(x)$.*

EXERCISE 1.8. *Show that in Zermelo-Fraenkel set theory ω exists.*

Let us now return to our study of the basic properties of ordinals.

LEMMA 1.9. *If α and β are ordinals with $\alpha \subset \beta$ and $\alpha \neq \beta$, then $\alpha \in \beta$.*

PROOF. Let $D := \beta \setminus \alpha$ be the (nonempty) set of elements in β that are not in α, and let γ be the least element of D in β. (That D is a set uses the axiom of separation.) Note that as β is an ordinal, γ being a member of β implies that it is a subset of β also. We will show that, as subsets of β, $\gamma = \alpha$. This will imply in particular that $\alpha \in \beta$, as desired.

Suppose there exists an element $\delta \in \gamma \setminus \alpha$. But then $\delta \in D$ and $\delta < \gamma$, which contradicts the minimal choice of γ. So $\gamma \subseteq \alpha$.

For the converse, suppose $\delta \in \alpha$. By linearity of β, of which δ and γ are members , either $\gamma = \delta$ or $\gamma < \delta$ or $\delta < \gamma$. As γ is in D, $\gamma \notin \alpha$, and hence it cannot be that $\gamma = \delta$. Now as α is an ordinal, each member of α is a subset of α, and so $\delta \subseteq \alpha$. Hence $\gamma < \delta$ would also imply the impossible $\gamma \in \alpha$. Hence $\delta < \gamma$, i.e., $\delta \in \gamma$. We have shown that $\alpha \subseteq \gamma$, as desired. □

PROPOSITION 1.10. (a) *Every member of an ordinal is an ordinal.*
(b) *No ordinal is a member of itself.*
(c) *If α is an ordinal then so is its* successor $S(\alpha) := \alpha \cup \{\alpha\}$.
(d) *The intersection of two ordinals is an ordinal.*

PROOF. For part (a), let α be an member of an ordinal β. So $\alpha \subseteq \beta$ and hence the membership relation on α is just the membership relation on β restricted to α. Now it is not hard to see that every subset of a strict well-ordering is again a strict well-ordering. Hence $\in$ induces a strict well-ordering on α. So it remains to show that every member of α is a subset of α. Suppose $x \in \alpha$ and $y \in x$. Since $\alpha \subseteq \beta$ we have that $x \in \beta$, and hence, using again that β is an ordinal, we have that $x \subseteq \beta$. So $y \in \beta$. We have that $x, y, \alpha \in \beta$, $y < x$, and $x < \alpha$. Hence by transitivity (in β) we have that $y < \alpha$, i.e., $y \in \alpha$. We have shown that $x \subseteq \alpha$, as desired.

For part (b) we point out that for α an ordinal, $\alpha \notin \alpha$. First, by antireflexivity of $\in$ on α we have that for all $x \in \alpha$, $x \notin x$. Hence, if $\alpha \in \alpha$, then $\alpha \notin \alpha$, as desired!

We leave parts (c) and part (d) as exercises. □

PROPOSITION 1.11. (a) *If α and β are ordinals then either $\alpha \in \beta$ or $\alpha = \beta$ or $\beta \in \alpha$.*
(b) *Every set of ordinals is strictly well-ordered by $\in$.*
(c) *If E is a set of ordinals then its* supremum $\sup E := \bigcup E$ *is an ordinal.*
(d) *There does not exist a set whose elements are all the ordinals.*

PROOF. If α and β are ordinals then $\alpha \cap \beta$ is an ordinal by Proposition 1.10(d), and it is a subset of both α and β. Hence by Lemma 1.9, if it is neither α nor β, then $\alpha \cap \beta \in \alpha$ and $\alpha \cap \beta \in \beta$. That is, $\alpha \cap \beta \in \alpha \cap \beta$, which contradicts the antireflexivity of $\in$ on α (of which $\alpha \cap \beta$ is a member). Hence, either $\alpha \cap \beta = \alpha$ or $\alpha \cap \beta = \beta$. In the first case we get $\alpha \subseteq \beta$, which by Lemma 1.9 again, implies that either $\alpha \in \beta$ or $\alpha = \beta$. Similarly, if $\alpha \cap \beta = \beta$ then either $\beta \in \alpha$ or $\beta = \alpha$. This proves part (a).

For part (b), suppose that E is a set of ordinals.

- Antireflexivity: This is Proposition 1.10(b).
- Antisymmetric: Suppose $\alpha, \beta \in E$. Note that under antireflexivity, antisymmetry is equivalent to saying that it is not the case that both $\alpha \in \beta$ and $\beta \in \alpha$. Indeed, if this were the case, then $\alpha \subseteq \beta$ (as every member of β is a subset of β) and so $\beta \in \beta$ which we know is impossible.
- Transitivity: Suppose $\alpha, \beta, \gamma \in E$ and $\alpha \in \beta$ and $\beta \in \gamma$. Then $\beta \subseteq \gamma$ (as every member of γ is a subset of γ) and so $\alpha \in \gamma$, as desired.

- Linearity: This is just part (a) of this Proposition.
- Well-orderedness: Suppose A is a nonempty subset of E. Let $\alpha \in A$. If $\alpha \cap A = \emptyset$ then α is the least element of A. Otherwise $\alpha \cap A$ is a nonempty subset of α and hence it contains a least element β in α. If $\gamma \in \beta \cap A$, then by transitivity of $\in$ on α, $\gamma \in \alpha \cap A$ and $\gamma < \beta$, contradiciting the minimal choice of β. So $\beta \cap A = \emptyset$, which imples that β is the least element of A.

This shows that every set of ordinals is strictly well-ordered by membership.

Now suppose that E is a set of ordinals and consider $\sup E$. By Proposition 1.10(a), $\sup E$ is itself a set of ordinals and hence strictly well-ordered by $\in$. So it remains to show that if $\alpha \in \sup E$ and $\beta \in \alpha$, then $\beta \in \sup E$. But, by definition of $\sup E$, there exists a $\gamma \in E$ with $\alpha \in \gamma$. Now by transitivity, $\beta \in \gamma$, and hence $\beta \in \sup E$.

For part (d), suppose there exists a set E consisting of all ordinals. Then by part (b), membership induces a strict well-ordering on E. Moreover, Proposition 1.10(a) tells us that every member of E is a subset of E. Hence E is itself an ordinal. But then $E \in E$, which contradicts E being an ordinal. □

Note that 1.11(d) is not inconsistent with the axiom of separation. While being an ordinal is a definite condition, it cannot be used with the axiom of separation to obtain "the set of all ordinals", since that axiom only applies when restricted to a set. So, if we start with a set A, then we can, using separation, form the subset of all elements *in* A that are ordinals. In fact, Proposition 1.11(d) shows that we cannot drop this restriction on the axiom of separation without running into "paradoxes".

NOTATION 1.12. As is somewhat justified by Proposition 1.11, from now on, given ordinals α and β, the notation $\alpha < \beta$ will be synonymous with $\alpha \in \beta$.

LEMMA 1.13. (a) *There is no ordinal strictly between an ordinal and its successor.*
(b) *If E is a nonempty set of ordinals then* $\sup E$ *is a least upper bound for E.*

PROOF. Suppose $\alpha \leq \gamma \leq S(\alpha)$. If $\gamma \neq S(\alpha)$ then $\gamma \in S(\alpha) = \alpha \cup \{\alpha\}$. Since $\alpha \leq \gamma$, it cannot be that $\gamma \in \alpha$ (by antireflexivity and transitivity). Hence $\gamma \in \{\alpha\}$, that is, $\gamma = \alpha$.

To see that $\sup E$ is an upper bound for E it suffices, by the totality of the ordering of ordinals (Proposition 1.11(a)), to show that no element of E is greater than $\sup E$. But $\alpha \in E$ and $\sup E \in \alpha$ would imply the impossible $\sup E \in \sup E$. Now suppose $\alpha < \sup E$. Then there is a $\beta \in E$ with $\alpha \in \beta$. Hence $\alpha < \beta$ and so α is not an upper bound. This shows that $\sup E$ is the least upper bound of E. □

DEFINITION 1.14. A *successor ordinal* is an ordinal of the form $S(\alpha)$ for some ordinal α. A *limit ordinal* is an ordinal that is not a successor.

1.2. Transfinite induction and recursion

THEOREM 1.15 (Transfinite Induction). *Suppose $P(x)$ is a definite condition with the property that if α is an ordinal and $P(\beta)$ is true of all $\beta < \alpha$, then $P(\alpha)$ is true. Then $P(x)$ is true of all ordinals.*

PROOF. Note that, vacuously, the hypothesis of the Theorem implies that $P(0)$ is true. Suppose, toward a contradiction, that there exists an ordinal α such that $P(\alpha)$ is false. Then $D := \{\beta \leq \alpha : P(\beta) \text{ is false}\}$ is a nonempty set of ordinals. (We use separation to see that it is a set at all.) Let α_0 be its least element, which exists by Proposition 1.11(b). So for every $\beta < \alpha_0$, $P(\beta)$ is true. Hence $P(\alpha_0)$ is true, which contradicts α_0 being in D. □

The following corollary is just another form of transifinite induction that is often useful.

COROLLARY 1.16 (Transfinite Induction – Second Form). *Suppose $P(x)$ is a definite condition satisfying the following:*

1. *$P(0)$ is true.*
2. *For all ordinals α, $P(\alpha)$ implies $P(S(\alpha))$.*
3. *For all limit ordinals $\alpha > 0$, if $P(\beta)$ is true for all $\beta < \alpha$ then $P(\beta)$ is true.*

Then $P(x)$ is true of all ordinals.

PROOF. Exercise. □

In what follows the domain of a *function* is always assumed to be a set, while an *operation* may be defined on "larger" classes of objects. For example, one can have an operation defined on all ordinals, like the successor operation. If F is an operation on ordinals and α is an ordinal, then $F \restriction \alpha$ denotes the retriction of F to α, which is a (partial) function on ordinals.

THEOREM 1.17 (Transfinite Recursion). *Suppose G is an operation which takes as input arbitrary partial functions on ordinals. Then there is a unique operation F on ordinals satisfying*

$$F(\alpha) = G(F \restriction \alpha)$$

for all ordinals α.

PROOF. First some terminology: we say that a function t with domain an ordinal α is an *α-function defined by G* if for all $\beta < \alpha$, $t(\beta) = G(t \restriction \beta)$. So such functions are approximations to the operation F that we are after. The first thing to observe is that an α-function defined by G is necessarily unique, and in fact, if s is an α-function defined by G and t is a β-function defined by G, and $\beta \leq \alpha$, then $t = s \restriction \beta$. This is straightforward to prove by transfinite induction on α, and we leave it as an exercise.

CLAIM 1.18. *For each ordinal α there exists a (unique) α-function defined by G.*

PROOF OF CLAIM 1.18. We use (the second form of) transfinite induction. For $\alpha = 0$, the empty function vacuously satisfies the condition. Suppose that $\alpha \neq 0$ and that there is an α-function t_α defined by G. Then define

$$t := t_\alpha \cup \big\{(\alpha, G(t_\alpha))\big\}$$

where the union here is really by identifying the function with its graph. Clearly t is a function whose domain is $S(\alpha)$. To see that it is the $S(\alpha)$-function defined by G, note that $t(\alpha) = G(t_\alpha) = G(t \restriction \alpha)$ while for $\beta < \alpha$ we have $t(\beta) = t_\alpha(\beta) = G(t_\alpha \restriction \beta) = G(t \restriction \beta)$.

Finally, suppose $\alpha \neq 0$ is a limit ordinal and that for each $\beta < \alpha$ there is a β-function, say t_β, that is defined by G. Let $T := \{t_\beta : \beta < \alpha\}$ and consider $t = \bigcup T$. To verify that t is the α-function defined by G we need to verify that:

- t is a function on α. This follows from the above observation that the t_βs form a chain of extensions.
- t is the α-function defined by G: for all $\beta < \alpha$, note that $S(\beta) < \alpha$ as α is a limit ordinal, and $\tau(\beta) = t_{S(\beta)}(\beta) = G(t_{S(\beta)} \restriction \beta) = G(\tau \restriction \beta)$.

□

Let us denote by t_α the α-function defined by G. Define the operation F by $F(\alpha) = t_{S(\alpha)}(\alpha)$, for all ordinals α. Note that for any $\beta < \alpha$, $F \restriction \alpha(\beta) = F(\beta) = t_{S(\beta)}(\beta) = t_{S(\alpha)}(\beta)$. That is, $F \restriction \alpha = t_{S(\alpha)} \restriction \alpha$ for all ordinals α. Hence, $F(\alpha) = t_{S(\alpha)}(\alpha) = G(t_{S(\alpha)} \restriction \alpha) = G(F \restriction \alpha)$, as desired. That F is the unique operation satisfying this condition is clear. □

Notice that the above proof used, for the first time, the Replacement Axiom; why else could we form the set $T := \{t_\beta : \beta < \alpha\}$ above? T is the image of the definite operatioon which assigns to each $\beta < \alpha$ the set t_β.

The following is another, often more useful, version of transfinite recursion.

COROLLARY 1.19 (Transfinite Recursion – Second Form). *Suppose G_1 is a set, G_2 is an operation on sets, and G_3 is an operation on partial functions on ordinals. There exists a unique operation F on ordinals, such that*

1. $F(0) = G_1$,
2. $F\big(S(\alpha)\big) = G_2\big(F(\alpha)\big)$ *for all ordinals* α,
3. $F(\alpha) = G_3(F \restriction \alpha)$ *for all limit ordinals* α.

PROOF. Exercise. □

For the sake of completeness, let us include, without proof, the following parametric version of transfinite recursion.

THEOREM 1.20 (Parametric Transfinite Recursion). *Suppose G is a binary operation. Then there exists a unique binary operation F such that*

$$F(z, \alpha) = G\big(z, F(z, -) \restriction \alpha\big)$$

for all ordinals z and α.

1.3. Ordinal arithmetic

In Example 1.7 we saw how to interpret the natural numbers as finite ordinals and we introduced the inifinite ordinal $\omega = \{0, 1, 2, \dots\}$. We can continue this construction:

$$\begin{aligned}
\omega + 1 &:= S(\omega) = \omega \cup \{\omega\} \\
\omega + 2 &:= S(\omega + 1) = \omega \cup \{\omega\} \cup \big\{\omega \cup \{\omega\}\big\} \\
&\vdots \\
\omega \cdot 2 &:= \sup\{\omega + n : n \in \omega\} = \omega \cup \{\omega, \omega + 1, \omega + 2, \cdots\} \\
\omega \cdot 3 &:= \sup\{\omega \cdot 2 + n : n \in \omega\} = \omega \cdot 2 \cup \{\omega \cdot 2, \omega \cdot 2 + 1, \omega \cdot 2 + 2, \cdots\} \\
&\vdots \\
\omega^2 &:= \sup\{\omega \cdot n : n \in \omega\} = \{\omega \cdot n \ + \ m \ : \ n, m \in \omega\} \\
&\vdots
\end{aligned}$$

To see how $\omega \cdot 2$, for example, is obtained, note that $\{\omega + n : n \in \omega\}$, being the image of the operation on ω which takes n to $\omega + n$, is a set by the replacement axiom. The arithmetic operations suggested by the above notation can be extended to all ordinals, and that is the purpose of this section.

Definition 1.21 (Ordinal addition). For all ordinals β we define the operation $\beta + \alpha$ recursively as follows:

$$\begin{aligned}
\beta + 0 &= \beta \\
\beta + S(\alpha) &= S(\beta + \alpha) \text{ for all ordinals } \alpha \\
\beta + \alpha &= \sup\{\beta + \gamma : \gamma < \alpha\} \text{ for all limit ordinals } \alpha \neq 0.
\end{aligned}$$

To see that the above definition is well-founded, i.e. that it does indeed define a binary operation on ordinals, one has to see how to express it as in instance of the recursion theorem. This can be done as follows: Fix an ordinal β and consider the following operations on ordinals

$$\begin{aligned}
G_1(x) &= \beta \\
G_2(x) &= S(x)
\end{aligned}$$

and the following operation on partial functions on ordinals

$$G_3(y) = \sup(\operatorname{Im} y).$$

Then the operation $F(x)$ determined by G_1, G_2, G_3 according to the second form of the transfinite recursion theorem (cf. 1.19) is exactly the operation $\beta + x$.

Note that by definition $\alpha + 1 = S(\alpha)$, and we will now tend to use the former rather than the latter.

Note that ordinal addition is not commutative. Indeed, $1 + \omega = \omega \neq \omega + 1$.

DEFINITION 1.22 (Ordinal product). For all ordinals β we define the operation $\beta \cdot \alpha$ recursively as follows:

$$\begin{aligned} \beta \cdot 0 &= 0 \\ \beta \cdot S(\alpha) &= \beta \cdot \alpha + \beta \text{ for all ordinals } \alpha \\ \beta \cdot \alpha &= \sup\{\beta \cdot \gamma : \gamma < \alpha\} \text{ for all limit ordinals } \alpha \neq 0. \end{aligned}$$

DEFINITION 1.23 (Ordinal exponentiation). For all ordinals β we define the operation β^α recursively as follows:

$$\begin{aligned} \beta^0 &= 1 \\ \beta^{S(\alpha)} &= \beta^\alpha \cdot \beta \text{ for all ordinals } \alpha \\ \beta^\alpha &= \sup\{\beta^\gamma : \gamma < \alpha\} \text{ for all limit ordinals } \alpha \neq 0. \end{aligned}$$

We leave it to you to express these precisely by transfinite recursion. Note that ordinal product is also not commutative as $2 \cdot \omega = \omega \neq \omega \cdot 2$.

Here are some basic properties of this arithmetic:

PROPOSITION 1.24. *Suppose α, β, δ are ordinals.*

(a) $\alpha < \beta$ *iff* $\delta + \alpha < \delta + \beta$
(b) $\alpha = \beta$ *iff* $\delta + \alpha = \delta + \beta$
(c) $(\alpha + \beta) + \delta = \alpha + (\beta + \delta)$
(d) *For* $\delta \neq 0$, $\alpha < \beta$ *iff* $\delta \cdot \alpha < \delta \cdot \beta$
(e) *For* $\delta \neq 0$, $\alpha = \beta$ *iff* $\delta \cdot \alpha = \delta \cdot \beta$
(f) $(\alpha \cdot \beta) \cdot \delta = \alpha \cdot (\beta \cdot \delta)$

PROOF. These are essentially an excercise in transfinite induction (cf. 1.16; we prove some and leave others to you.

Fix α and δ and consider the property $P(x)$ which says that "if $\alpha < x$ the $\delta + \alpha < \delta + x$". Now $P(0)$ is vacuously correct. If $P(\beta)$ is correct and $\alpha < \beta + 1$ then either $\alpha < \beta$, in which case we have $\delta + \alpha < \delta + \beta < \delta + \beta + 1$ and so $P(\beta + 1)$ is true, or $\alpha = \beta$ in which case $\delta + \alpha = \delta + \beta < \delta + \beta + 1$ and so $P(\beta + 1)$ is again true. If β is a limit ordinal and $\alpha < \beta$, then $\delta + \alpha < \sup\{\delta + \gamma : \gamma < \beta\} = \delta + \beta$ where the first inequality is by the fact that $\delta + \alpha \in \sup\{\delta + \gamma : \gamma < \beta\}$ since $\delta + \alpha \in S(\delta + \alpha) = \delta + S(\alpha)$ and $S(\alpha) < \beta$. Hence $P(\beta)$ is true. By the second form of transfinite induction, we have $P(\beta)$ for all ordinals β, which is the left-to-right implication of part (a).

For the converse, suppose $\delta + \alpha < \delta + \beta$. Then $\alpha \neq \beta$ by the well-definedness of ordinal addition, and $\neg(\beta < \alpha)$ by the left-to-right implication proved above. So it must be that $\alpha < \beta$. This completes the roof of part (a).

The left-to-right implication of part (b) is just the well-definedness of ordinal addition. For the converse, suppose $\delta + \alpha = \delta + \beta$. Then part (a) rules out $\alpha < \beta$ and $\beta < \alpha$, hence forcing $\alpha = \beta$.

Toward part (c), fix α and β and consider the condition $P(x)$ which says that $(\alpha+\beta)+x = \alpha+(\beta+x)$. It is clear that $P(0)$ is true. Suppose $P(\delta)$ is true. Then

$$\begin{aligned}(\alpha+\beta)+(\delta+1) &= \big((\alpha+\beta)+\delta\big)+1 \text{ by the definition of ordinal addition}\\ &= \big(\alpha+(\beta+\delta)\big)+1 \text{ by the truth of } P(\delta)\\ &= \alpha+\big((\beta+\delta)+1\big) \text{ by the definition of ordinal addition}\\ &= \alpha+\big(\beta+(\delta+1)\big) \text{ by the definition of ordinal addition}\end{aligned}$$

So $P(\delta)$ implies $P(\delta+1)$.

Now suppose that δ is a limit ordinal.

Claim 1.25. $\sup\{\alpha+(\beta+\gamma) : \gamma<\delta\} = \sup\{\alpha+\zeta : \zeta<\beta+\delta\}$

Proof of Claim 1.25. Indeed the left-to-right containment is just by part (a). For the converse suppose $x \in \alpha+\zeta$ for some $\zeta<\beta+\delta$. So, as δ is a limit ordinal, $\zeta<\beta+\gamma$ for some $\gamma<\delta$. Hence $\alpha+\zeta<\alpha+(\beta+\gamma)$ by part (a). So, by transitivity, $x \in \alpha+(\beta+\gamma)$, as desired □

Claim 1.26. *$\beta+\delta$ is again a limit ordinal.*

Proof of Claim 1.26. Assume toward a contradiction that for some ordinal ξ, $S(\xi) = \beta+\delta$. As $\xi<S(\xi)$, and δ is a limit ordinal, we get that $\xi<\beta+\gamma$ for some $\gamma<\delta$. But then $\beta+\delta = S(\xi) < S(\beta+\gamma) = \beta+S(\gamma)$. So by part (a), $\delta<S(\gamma)$. But $\gamma<\delta$ by choice, which is a contradiction (cf. Lemma 1.13(a)). □

If we now assume that $P(\gamma)$ is true of all $\gamma<\delta$, then we get

$$\begin{aligned}\alpha+(\beta+\delta) &= \sup\{\alpha+\zeta : \zeta<\beta+\delta\} \text{ by Claim 1.26}\\ &= \sup\{\alpha+(\beta+\gamma) : \gamma<\delta\} \text{ by Claim 1.25}\\ &= \sup\{(\alpha+\beta)+\gamma : \gamma<\delta\} \text{ by the truth of } P(\gamma)\\ &= (\alpha+\beta)+\delta \text{ as } \delta \text{ is a limit ordinal.}\end{aligned}$$

So $P(\delta)$ is true. This completes the proof of part (c).

Parts (d)–(f) are proved in a similar fashion, and left as an exercise. □

1.4. Well-orderings and ordinals

At this point one might have the impression that ordinals are a very special class of well-orderings. In fact the opposite is true. The following theorem says that, as well-orderings, ordinals are all there is.

Theorem 1.27. *Every strict well-ordering is isomorphic to an ordinal. More precisely, if $(E,\prec)$ is a strict well-ordering, then there exists a unique ordinal α and a unique isomorphism between $(E,\prec)$ and $(\alpha,<)$.*

Proof. The fact that if there exists such an isomorphism between $(E,\prec)$ and an ordinal α, then it must be unique, is just Corollary 1.4.

Suppose $(E,\prec)$ is isomorphic to ordinals α and β. Suppose $\alpha<\beta$. Then $(\alpha,<) = \big(\{\gamma\in\beta : \gamma<\alpha\},<\big)$. But, by Lemma 1.5, there can be no isomorphism between this latter

well-ordering and $(\beta, <)$, which contradicts that both are isomorphic to $(E, \prec)$. Similarly, $\beta < \alpha$ is impossible. Hence $\alpha = \beta$.

So it remains to find an ordinal α isomorphic to $(E, \prec)$. Given $x \in E$ let us denote by E_x the initial segment $\{e \in E : e \prec x\}$. Consider

$$A = \{x \in E : \ (E_x, \prec) \text{ is isomorphic to an ordinal}\}$$

Note that A is not empty since if $x \in E$ is the least element of E, then E_x is isomorphic to 0. By the uniqueness proved above we can consider the function f on A where $f(x)$ is the unique ordinal isomorphic to $(E_x, \prec)$. By replacement $\mathrm{Im}(f)$ is a set of ordinals. Let α be the least ordinal which is not in $\mathrm{Im}(f)$.[1] We prove that $f : A \to \mathrm{Im}(f)$ is in fact an isomorphism between $(E, \prec)$ and α.

1. *f preserves the ordering: in fact, if $y \in A$ and $x \prec y$ then $x \in A$ and $f(x) \in f(y)$.* Since $x \prec y$, E_x is an initial segment of E_y. Now, if h is the isomorphism between $(E_y, \prec)$ and $f(y)$, then the image of E_x by h must be an initial segment of $f(y)$. Indeed, $h(x) \in f(y)$ is an ordinal and
$$h(E_x) = \{\alpha \in f(y) : \alpha < h(x)\} = h(x)$$
So h restricts to an isomorphisms between E_x and the ordinal $h(x)$. By uniqueness, $h(x) = f(x)$, and so $f(x) \in f(y)$.
2. *f is a surjective function from A to α.* Suppose $\beta \in \alpha$. Then by choice of α, $\beta \in \mathrm{Im}(f)$. Conversely, suppose $\beta \in \mathrm{Im}(f)$, and h is the isomorphism between E_x and β for some $x \in A$. Then $\beta \neq \alpha$. If $\alpha < \beta$, then $\alpha = h(y)$ for some $y \prec x$. By (1) above, $y \in A$ and $f(y) = h(y) = \alpha$, which contradicts $\alpha \notin \mathrm{Im}(f)$. Hence $\beta < \alpha$, as desired.
3. *f is injective.* Suppose $f(x) = f(y)$. If $x \prec y$ then E_x is a proper initial segment of E_y that is isomorphic to E_y – but this is forbidden by Lemma 1.5. Similarly, $y \prec x$ is impossible. Hence $x = y$.
4. *f is defined on all of E.* Toward a contradiction assume that $E \setminus A$ is nonempty and let x be a least element of this set. By (1) above, no element greater than x is in A. On the other hand, by minimality, every element less than x is in A. That is, $A = E_x$. Since we have already proved that f is an isomorphism between $(A, \prec)$ and the ordinal α, this implies that $x \in A$, a contradiction.

This proves that f is an isomorphism between $(E, \prec)$ and $(\alpha, <)$, as desired. □

[1] To see that such an α exists, set $\beta = \sup\big(\mathrm{Im}(f)\big) + 1$ and then use Proposition 1.11(c) to see that $\beta \notin \mathrm{Im}(f)$ has a least element. That element is α.

CHAPTER 2

Axiom of Choice

2.1. A first look at cardinals

The ordinals were introduced as a natural transfinite generalisation of the natural numbers. One aspect of the natural numbers is that they can be used to measure the size of finite sets; as set is of size n iff the exists a bijection between it and the finite ordinal n. Infinite ordinals do not serve the same purpose simply because there are many distinct ordinals that are of the "same size" in this sense – for example there is a bijection between ω and $\omega + 1$. Let us first formalise this notion of "same size".

DEFINITION 2.1. Two sets A and B are said to be *equinumerous* if there exists a bijection between them.

Let us record for future use the following well-known fact.

PROPOSITION 2.2 (Schröder-Bernstein). *Sets A and B are equinumerous if and only if there are injective maps from A to B and from B to A.*

PROOF. Only the right-to-left implication requires proof. We begin with a claim.

CLAIM 2.3. *Suppose X is a set and $f : X \to X$ is injective. Then for any $Y \subseteq X$ with $f(X) \subseteq Y$, Y is equinumerous with X.*

PROOF OF CLAIM 2.3. Let $X_n := f^n(X), Y_n := f^n(Y), Z_n := X_n \setminus Y_n$. Let $Z := \bigcup_{n\geq 0} Z_n$ and $W := X \setminus Z$. Since $Z_0 = X \setminus Y$ and $f(X) \subseteq Y$, it is clear that $f(Z) \cup W \subseteq Y$. For the converse consider $y \in Y \setminus W$. Then $y \in Z$. But $y \notin Z_0$, so $y \in Z_n$ for some $n > 0$. That is, $y = f^n(x)$ for some $x \in X$. Since $y \notin Y_n$, $f^{n-1}(x) \in X_{n-1} \setminus Y_{n-1} = Z_{n-1} \subseteq Z$. Hence $x \in f(Z)$. We have shown that $Y = f(Z) \cup W$. Hence, $g : X \to Y$ defined by

$$g(x) = \begin{cases} f(x) & \text{if } x \in Z \\ x & \text{if } x \in W \end{cases}$$

is a bijection between X and Y. □

Now suppose we have injective maps $i : A \to B$ and $j : B \to A$. Apply the claim to $X = A, Y = j(B)$, and $f = j \circ i$. This tells us that A and $j(B)$ are equinumerous. But of course B and $j(B)$ are equinumerous. Hence A and B are equinumerous. □

LEMMA 2.4. *For every infinite ordinal α, α and $\alpha + 1$ are equinumerous.*

PROOF. Define $f : \alpha + 1 \to \alpha$ as follows:

$$f(x) = \begin{cases} x + 1 & \text{if } x \in \omega \\ 0 & \text{if } x = \alpha \\ x & \text{otherwise} \end{cases}$$

Since α is infinite, $\alpha \notin \omega$, and hence f is well-defined on all of $\alpha + 1$. It is surjective since its image clearly contains ω and if $x \in \alpha \setminus \omega$ then $f(x) = x$. It is clearly injective. □

This problem of equinumerous distinct infinite ordinals can be overcome by choosing canonically one ordinal from each collection of equinumerous ordinals:

DEFINITION 2.5 (Cardinals). An ordinal α is called a *cardinal* if α is not equinumerous to any ordinal $\beta < \alpha$.

For example, every finite ordinal is a cardinal. It is also clear that ω is a cardinal. Are there other cardinals? The answer is yes.

PROPOSITION 2.6. *For every set E there exists a unique cardinal $h(E)$ which is the least ordinal that is not equinumerous with any subset of E.*

PROOF. It suffices to prove the existence of such an ordinal $h(E)$, it will be a cardinal as all ordinals less than it are equinumerous with subsets of E but it is not. Consider

$$W := \big\{(A, \prec) : A \subseteq E,\ \prec \text{ is a well-ordering of } A\big\}.$$

This is a (nonempty) set.[1] By Theorem 1.27 we have a function on W which assigns to each member of W the ordinal that is order-isomorphic to it. So, by replacement,

$$H := \{\alpha :\ \alpha \text{ is an ordinal equinumerous with a subset of } E\}$$

is a set of ordinals. Hence, by Proposition 1.11(d) there is an ordinal not in H, and so by part (b) of that same proposition, there is a least ordinal not in H. That's $h(E)$. □

In particular, there exist uncountable cardinals, for example $h(\omega)$.

But we want much more of our cardinals. If they are to measure the size of arbitrary sets then every set must be equinumerous with a cardinal. But that would in particular imply that every set is well-orderable: indeed, a set is equinumerous with an ordinal if and only if it is strictly well-orderable.[2] However, our axioms so far do not allow us to prove that every set is well-orderable; we need the axiom of choice.

[1] One needs to first show that if X and Y are sets then $X \times Y$ is a set, and then use the powerset and separation axioms to see that W is a set.

[2] The right-to-left implication follows from Theorem 1.27 while the left-to-right is proved by using the bijection with an ordinal to carry over the well-ordering.

2.2. The axiom of choice and its equivalents

What makes the axiom of choice different from the other axioms we have used so far is that it asserts the existence of objects that are not at all "definable" from $\in$ and $=$. Definability here is meant in the sense of model theory, which is the topic of the second part of the course. As a result, the axiom of choice has many surprising consequences. Nevertheless, this axiom is indispensable to much of contemporary mathematics.

DEFINITION 2.7 (Choice functions). Suppose $\mathcal{F}$ is a set of sets. A *choice function* on $\mathcal{F}$ is a function which assigns to each $F \in \mathcal{F}$ a member of F.

AXIOM 9 (Choice). *Every set of nonempty sets has a choice function.*

THEOREM 2.8. *The following are equivalent:*

1. *The axiom of choice.*
2. *The well-ordering principle: every set is well-orderable.*
3. *Zorn's lemma: If $(E, \prec)$ is a nonempty poset with the property that every totally ordered subset of E has an upper bound in E, then E has a maximal element.*

PROOF. Let us assume the axiom of choice and derive from it the well-ordering principle. Let A be an arbitrary set and let c be a choice function on the powerset $\mathcal{P}(A)$. Consider the operation on ordinals defined (using transfinite recursion) as follows:

$$F(\alpha) = \begin{cases} c\big(A \setminus \mathrm{Im}(F \restriction \alpha)\big) & \text{if } A \setminus \mathrm{Im}(F \restriction \alpha) \neq \emptyset \\ \zeta & \text{else} \end{cases}$$

where ζ is some fixed ordinal not in A that is used as a default value. To show that A is well-ordered it will suffice to show that

- F halts, in the sense that it takes on the value ζ at some ordinal, and hence at every future ordinal.
- If α is the least ordinal at which F halts, then $F \restriction \alpha$ is a bijection onto A.

To see that F halts, let $h(A)$ be the cardinal whose existence is guaranteed by Proposition 2.6; so $h(A)$ is the least ordinal which is not equinumerous with any suibset of A. Given ordinals $\alpha < \beta$ in $h(A)$, note that if $F(\beta) \neq \zeta$ then $F(\beta) = c\big(A \setminus \mathrm{Im}(F \restriction \beta)\big) \in A \setminus \mathrm{Im}(F \restriction \alpha)$, while $F(\alpha) \in \mathrm{Im}(F \restriction \alpha)$. Hence $F(\alpha) \neq F(\beta)$. So, if $F(\beta) \neq \zeta$ for every $\beta \in h(A)$, then we have shown that F restricts to an embedding of $h(A)$ in A. But by definition of $h(A)$, this is not possible. Hence, for some $\beta \in h(A)$, $F(\beta) = \zeta$. Moreover, if we let α be the least such β, then we have shown that $F \restriction \alpha$ is an injection from α to A. It remains to show that this map is surjective. But this is immediate since $F(\alpha) = \zeta$ implies that $A = \mathrm{Im}(F \restriction \alpha)$.

Now let us assume the well-ordering principle and prove Zorn's lemma. Suppose $(E, \prec)$ is a poset satisfying the stated condition on totally ordered subsets. By the well-ordering principle there exists a well-ordering, say $<$, on E. Without loss of generality we may assume that both orderings are strict. By Theorem 1.27 we may as well assume that E is an ordinal and $<$ is $\in$. Let $h(E)$ be the cardinal given by Proposition 2.6, that is $h(E)$ is the least ordinal that is not equinumerous with any subset of E. We will verify Zorn's lemma as follows: we will assume toward a contradicton that E has no $\prec$-maximal element and use that to construct an (impossible) embedding of $h(E)$ into E. Let $F : h(E) \to E$ be defined

by transfinite recursion (cf. Corollary 1.19), as follows:

$$F(0) \;=\; 0$$

For all ordinals $\alpha < h(E)$,

$$F(\alpha+1) \;=\; \text{the } <\text{-least } \beta \text{ such that } F(\alpha) \prec \beta$$

For all limit ordinals $\alpha < h(E)$,

$$F(\alpha) \;=\; \begin{cases} <\text{-least } \beta \text{ such that } F(\gamma) \prec \beta \text{ for all } \gamma < \alpha & \text{if such a } \beta \text{ exists} \\ 0 & \text{else} \end{cases}$$

This function is well-defined because E has no $\prec$-maximal element and $<$ is a well-ordering on E. To show that F is injective (which would be the desired contradiction proving that E must have a $\prec$-maximal element) it will suffice to prove the following:

Claim 2.9. *For all $\alpha < h(E)$, $F \restriction \{\gamma : \gamma < \alpha\}$ is strictly order preserving; that is, for all $x < y < \alpha$, $F(x) \prec F(y)$.*

Proof of Claim 2.9. We prove this by transfinite induction on $\alpha < h(E)$. For $\alpha = 0$ there is nothing to prove. If α is a limit ordinal then $\{\gamma : \gamma < \alpha\} = \bigcup_{\beta<\alpha} \{\gamma : \gamma < \beta\}$ and so the claim follows by the induction hypothesis. Finally, suppose α is any ordinal and consider $F \restriction \{\gamma : \gamma < \alpha + 1\}$. There are two possibilities: either α is itself a successor or a limit. If $\alpha = \beta + 1$ then $F \restriction \{\gamma : \gamma < \alpha + 1\} = F \restriction \{\gamma : \gamma \leq \beta + 1\}$, and by definition $F(\beta) \prec F(\beta + 1)$. Together with the induction hypothesis shows that $F \restriction \{\gamma : \gamma < \alpha + 1\}$ is strictly order preserving. So suppose α is a limit ordinal. By the induction hypothesis, $F \restriction \{\gamma : \gamma < \alpha\}$ is strictly order preserving, and hence $F(\{\gamma : \gamma < \alpha\})$ forms a totally $\prec$-ordered set. It follows that there exists an upper bound to this set, and hence by definition $F(\alpha)$ is such a bound. So, $F(\gamma) \prec F(\alpha)$ for all $\gamma < \alpha$. Hence, $F \restriction \{\gamma : \gamma < \alpha + 1\}$ is strictly order preserving. □

Finally, let us assume Zorn's lemma and derive the axiom of choice from it. Suppose $\mathcal{F}$ is a set of nonempty sets, and let us consider the set Λ of all *partial* choice functions on $\mathcal{F}$, identified with their graphs. That is, the elements of Λ are sets of the form

$$\big\{(G, x) : G \in \mathcal{G}, x \in G\big\}$$

where $\mathcal{G}$ is a subset of $\mathcal{F}$. Note that Λ is non-empty, it contains for example $\{(F, x)\}$ for each $F \in \mathcal{F}$ and $x \in F$. Now Λ forms a poset under $\subset$. Moreover, if Θ is a totally ordered subset of Λ, then $\bigcup \Theta$ is quite easily seen to be a partial choice function on $\mathcal{F}$, and hence an upper bound for Θ in Λ. So the assumptions of Zorn's lemma are satisfied, and Λ must have a maximal element, say f_∞. I claim that f_∞ is a (total) choice function on $\mathcal{F}$. If not, then there must exist some $F \in \mathcal{F}$, such that $F \notin \mathrm{Dom}(f_\infty)$. But then, fixing $x \in F$, $f_\infty \cup \{(F, x)\}$ is a strictly larger partial choice function on $\mathcal{F}$, contradicting the maximality of f_∞ in Λ. Hence f_∞ is a choice function on $\mathcal{F}$, and we have proven the axiom of choice. □

There are many other interesting equivalents to the axiom of choice, which I leave to you to investigate.

2.3. Axiom of choice and cardinals

Recall that cardinals were defined as those ordinals which are not equinumerous with any strictly lesser ordinals (cf. Section 2.1). In the presence of the axiom of choice, cardinals become a robust measure of the "size" of sets. We collect together in the following proposition several consequences of the axiom of choice to the theory of cardinals.

PROPOSITION 2.10. *Assume the Axiom of Choice.*

(a) *Every set is equinumerous with a unique cardinal. Given a set A we denote the unique cardinal equinumerous to it by $|A|$ and call this the* cardinality of A.
(b) *Given sets A and B, $|A| \leq |B|$ if and only if there is an injective map from A to B.*
(c) *Given sets A and B, either there is an injective map from A to B or there is an injective map from B to A.*
(d) *Suppose f is a function on a set A. Then $|\operatorname{Im}(f)| \leq |A|$.*
(e) *A countable union of countable sets is countable.*

PROOF. (a) Suppose X is a set. By the axiom of choice, and Theorem 2.8, X is well-orderable. It follows by Theorem 1.27 that X is in bijection with an ordinal. Let α be the least ordinal equinumerous with X. Clearly α is a cardinal, and it is the unique cardinal equinumerous with X.

(b) Let $|A| = \kappa$ and $|B| = \lambda$ and fix bijections $f : A \to \kappa$ and $g : B \to \lambda$. If $\kappa \leq \lambda$ then $\kappa \subseteq \lambda$ and hence $g^{-1} \circ f$ is an injective map from A to B. Conversely, if $h : A \to B$ is injective then $g \circ h \circ f^{-1}$ is an embedding of κ in λ. If $\lambda < \kappa$ then there is also an embedding of λ in κ (by containment). But then Schröder-Bernstein (Proposition 2.2) implies that κ and λ are equinumerous, contradicting that he cardinal κ cannot be equinumerous with a lesser ordinal. Hence, $\kappa \leq \lambda$, as desired.

Part (c) is an immediate consequences of (b).

(d) Let c be a choice function on $\mathcal{F} = \{f^{-1}(y) : y \in \operatorname{Im}(f)\}$, the set of fibres of f. Set $\iota : \operatorname{Im}(f) \to A$ to be $\iota(y) = c\big(f^{-1}(y)\big)$. Now if x and y are distinct in $\operatorname{Im}(f)$ then $f^{-1}(x)$ and $f^{-1}(y)$ are disjoint, and hence $\iota(x) \neq \iota(y)$. So ι is injective and $|\operatorname{Im}(f)| \leq |A|$.

(e) First we leave it as an exercise for you to see that $\omega \times \omega$ is countable. Now suppose A is a countable set with the property that every member of A is countable. Since A is countable we have an embedding $g : A \to \omega$. Moreover, for each $x \in A$ we have an embedding $f_x : x \to \omega$. If $\bigcup A = \emptyset$ then it is countable and we are done, so assume there exists $c \in \bigcup A$. Now define $h : \omega \times \omega \to \bigcup A$ as follows:

$$h(n,m) = \begin{cases} f^{-1}_{g^{-1}(n)}(m) & \text{if } n \in \operatorname{Im}(g) \text{ and } m \in \operatorname{Im}(f_{g^{-1}(n)}) \\ c & \text{else} \end{cases}$$

Note that if $a \in \bigcup A$ then $a \in x$ for some $x \in A$ and $h\big(g(x), f_x(a)\big) = a$. So h is surjctive and so by part (e), $\bigcup A$ is countable. (Where did we use the axiom of choice?) □

REMARK 2.11. If X is a set of cardinality κ then we can enumerate X as $X = \{x_i : i < \kappa\}$. Indeed, let $f : \kappa \to X$ be a bijection and set $x_i := f(i)$.

In the rest of this course we will assume the axiom of choice, along with the Zermelo-Fraenkel axioms of set theory, without explicitly saying so. That is we work in ZFC; Zermelo-Fraenkel set theory with choice.

CHAPTER 3

Cardinals

In the last chapter we introduced cardinals and showed that in the presence of the axiom of choice cardinality is a robust measure of the size of a set, and that our intuition about the relative sizes of sets corresponds exactly to the ordering of the cardinals by $\in$. In this chapter we pursue further the structure of infinite cardinals. We use the axiom of choice freely.

3.1. Hierarchy of infinite cardinals

Our goal here is to describe a complete hierarchy of cardinals.

DEFINITION 3.1. We define, using transfinite recursion, the following ordinal-enumerated collection of ordinals.

- $\aleph_0 = \omega$.
- For all ordinals α, $\aleph_{\alpha+1} = h(\aleph_\alpha)$, where $h(\aleph_\alpha)$ is the least ordinal not equinumerous with any subset of $\aleph_\alpha$ (see Propsoition 2.6).
- For all limit ordinals α, $\aleph_\alpha = \sup\{\aleph_\beta : \beta < \alpha\}$.

LEMMA 3.2. *For all ordinals α, $\aleph_\alpha$ is a cardinal.*

PROOF. By transfinite induction on α. This is clear for $\alpha = 0$. At successor stages we use the fact that $h(E)$ is a cardinal for any set E, by Proposition 2.6. Finally suppose that α is a limit ordinal, and $\beta < \aleph_\alpha$. By definition of $\aleph_\alpha$ we have that for some $\gamma < \alpha$, $\beta < \aleph_\gamma$. So we have $\beta < \aleph_\gamma \leq \aleph_\alpha$ and hence $|\beta| < |\aleph_\gamma| \leq |\aleph_\alpha|$, where the first inequality uses the fact that $\aleph_\gamma$ is a cardinal by the inductive hypothesis. So $\aleph_\alpha$ is not equinumerous with any lesser ordinal – that is, it is a cardinal. □

NOTATION 3.3. Note that for any cardinal κ, $h(\kappa)$ is also the least cardinal strictly bigger than κ. For that reason, we will denote $h(\kappa)$ by κ^+.

LEMMA 3.4. *For all ordinals $\alpha < \beta$, $\aleph_\alpha < \aleph_\beta$.*

PROOF. By transfinite induction on β. There is nothing to prove for $\beta = 0$. If $\beta = \gamma + 1$ then $|\aleph_\beta| = |\aleph_\gamma^+| > |\aleph_\gamma|$ and the result follows by the inductive hypothesis. If β is a limit ordinal then there exists $\gamma < \beta$ with $\alpha < \gamma$. So $|\aleph_\alpha| < |\aleph_\gamma|$ by the inductive hyptohesis, and $|\aleph_\gamma| \leq |\aleph_\beta|$ since $\aleph_\gamma \subseteq \aleph_\beta$. Hence $|\aleph_\alpha| < |\aleph_\beta|$, as desired. □

LEMMA 3.5. *For all ordinals α, $\alpha \leq \aleph_\alpha$.*

PROOF. By transfinite induction on α. This is clear for $\alpha = 0$. If $\alpha = \beta + 1$ then by the induction hypothesis $\beta \leq \aleph_\beta$. On the other hand, $\aleph_\beta = |\aleph_\beta| < |\aleph_\beta^+| = |\aleph_\alpha| = \aleph_\alpha$, where the first and last equalities use Lemma 3.2. Hence $\alpha < \aleph_\alpha$. Finally suppose α is a limit ordinal.

For every $\beta < \alpha$, $\beta \leq \aleph_\beta < \aleph_\alpha$, where the first inequality is by the induction hypothesis and the second is by definition of $\aleph_\alpha$. Hence, $\alpha = \sup\{\beta : \beta < \alpha\} \leq \aleph_\alpha$, as desired. □

One cannot replace $\leq$ with $<$ in Lemma 3.5. For example, consider the sequence of ordinals defined recursively by $\alpha_0 = 0$ and $\alpha_{n+1} = \aleph_{\alpha_n}$. Now let $\alpha = \sup\{\alpha_n : n \in \mathbb{N}\}$. Verify that $\alpha = \aleph_\alpha$. In fact, this works with α_0 any ordinal, not just 0.

PROPOSITION 3.6. *Every infinite cardinal is of the form $\aleph_\alpha$ for some ordinal α.*

PROOF. Suppose κ is a cardinal. By Lemma 3.5 $\kappa \leq \aleph_\kappa < \aleph_{\kappa+1}$. Hence it will suffice to show that *for every ordinal β and every infinite cardinal $\kappa < \aleph_\beta$, there exists an ordinal $\alpha < \beta$ such that $\kappa = \aleph_\alpha$*. We prove that statement by transfinite induction on β. Since there are are no infinite cardinals strictly below ω, there is nothing to prove in the case $\beta = 0$. Suppose $\beta = \gamma + 1$ and let $\kappa < \aleph_\beta$. Then, as there is no cardinal strictly between $\aleph_\gamma$ and $\aleph_\gamma^+ = \aleph_\beta$, $\kappa \leq \aleph_\gamma$. Hence either $\kappa = \aleph_\gamma$ or by the induction hypothesis $\kappa = \aleph_\alpha$ for some $\alpha < \gamma$. This deals with the successor stage. Suppose now that β is a limit ordinal and $\kappa < \aleph_\beta$. Then by defnition $\kappa < \aleph_\gamma$ for some $\gamma < \beta$. Hence by the induction hypothesis $\kappa = \aleph_\alpha$ for some $\alpha < \gamma$, as desired. □

We call a cardinal of the form $\aleph_{\alpha+1}$ a *successor cardinal* and one of the form $\aleph_\beta$ for some limit ordinal β a *limit cardinal*. Note that by Proposition 3.6, successor cardinals are exactly those of the form κ^+ for some cardinal κ, and limit cardinals are exactly those that are not successors. It is important to net get confused between successor/limit cardinals and successor/limit ordinals. In fact, it follows easily from Lemma 2.4 that every cardinal is a limit ordinal (though not a limit cardinal).

3.2. A word on the continuum hypothesis

THEOREM 3.7 (Cantor's diogonalisation). *For every set E, $|E| < |\mathcal{P}(E)|$.*

PROOF. Since $x \mapsto \{x\}$ is an embedding of E in $\mathcal{P}(E)$, we have $|E| \leq |\mathcal{P}(E)|$. Suppose, toward a contradiciton that there exists a bijective function $f : E \to \mathcal{P}(E)$. Let $\Delta := \{x \in E : x \notin f(x)\}$. So $\Delta \in \mathcal{P}(E)$ and hence $\Delta = f(x)$ for some $x \in E$. If $x \in \Delta$ then by definition $x \notin f(x) = \Delta$, a contradiction. Hence $x \notin \Delta$. But then $x \notin f(x)$ and so by definition $x \in \Delta$, again a contradiction. Hence no such f exists and $|E| < |\mathcal{P}(E)|$. □

The question arises as to what cardinal $|\mathcal{P}(\aleph_0)|$ is in terms of the hierarchy described in the previous section. One might expect that $|\mathcal{P}(\aleph_0)| = \aleph_1$. In fact, that statement, which is called the *continuum hypothesis* (CH), cannot be proved from the set-theoretic axioms we have introduced so far, nor can its negation be proved. This is also the case for the stronger statement, called the *generalised continuum hypothesis* (GCH), which states that $|\mathcal{P}(\kappa)| = \kappa^+$ for all cardinals κ. Unlike the axiom of choice, the (generalised) continuum hypothesis is not indispensable to most of contemporary mathematics. So we do not add a set-theoretic axiom determining the value of $|\mathcal{P}(\aleph_0)|$, but rather work independently of its status.

3.3. Cardinal arithmetic

LEMMA 3.8. *Suppose* $\{X_1, \ldots, X_n\}$ *and* $\{Y_1, \ldots, Y_n\}$ *are such that* $|X_i| = |Y_i|$, *for each* $1 \leq i \leq n$.

(a) *If for each* $1 \leq i < j \leq n$, $X_i \cap X_j = Y_i \cap Y_j = \emptyset$, *then* $|\bigcup_{i=1}^{n} X_i| = |\bigcup_{i=1}^{n} Y_i|$.

(b) $|X_1 \times \cdots \times X_n| = |Y_1 \times \cdots \times Y_n|$.

PROOF. By induction on n it suffices to consider the case of $n = 2$. Let $f_i : X_i \to Y_i$ be a bijection witnessing the equinumerousity of X_i and Y_i, for $i = 1$ and 2. Then $g : X_1 \cup X_2 \to Y_1 \cup Y_2$ given by $g(x) = \begin{cases} f_1(x) & \text{if } x \in X_1 \\ f_2(x) & \text{if } x \in X_2 \end{cases}$ and $h : X_1 \times X_2 \to Y_1 \times Y_2$ given by $h(a, b) = (f_1(a), f_2(b))$, are easily seen to be a bijections. □

DEFINITION 3.9 (Cardinal sum and product). Given cardinals $\kappa_1, \ldots, \kappa_n$ we define their *sum* to be

$$\sum_{i=1}^{n} \kappa_i := |\bigcup_{i=1}^{n} X_i|$$

where $X_1, \cdots X_n$ are pairwise disjoint sets of cardinality $\kappa_1, \ldots, \kappa_n$, respectively. Similarly, we define the *product* to be

$$\prod_{i=1}^{n} \kappa_i := |X_1 \times \cdots \times X_n|$$

where $X_1, \cdots X_n$ are sets of cardinality $\kappa_1, \ldots, \kappa_n$. By Lemma 3.8 this is well-defined; it does not depend on the choice of $X_1, \ldots, X_n$.

REMARK 3.10. It is very important here to distinguish between cardinal sum/product and ordinal sum/product. For example, viewing ω and 1 as cardinals we have that there sum is the cardinal ω (see part (c) of Lemma 3.11 below), while viewing them as ordinals their sum is the ordinal $\omega + 1 \neq \omega$. We hope that the context will always make clear which is meant. One way to do so is to use the $\aleph$ notation for cardinals. So for example, in the above case, for ordinal sum we would write $\omega + 1$, while for cardinal sum we would write $\aleph_0 + 1$ (which is equal to $\aleph_0$).

EXERCISE 3.11. (a) *Sum and product are commutative and associative.*

(b) *Product distributes over sum:* $\kappa_1 \cdot (\kappa_2 + \kappa_3) = \kappa_1 \cdot \kappa_2 + \kappa_1 \cdot \kappa_3$.

(c) *For all* $n \in \omega$, $\aleph_0 + n = \aleph_0 \cdot n = \aleph_0$.

(d) $\aleph_0 + \aleph_0 = \aleph_0$.

(e) $\aleph_0 \cdot \aleph_0 = \aleph_0$.

Hint: Use Proposition 2.10(f) for parts (c)–(e).

THEOREM 3.12. *For all infinite cardinals* κ, $\kappa \cdot \kappa = \kappa$.

PROOF. First, given a cardinal κ, we desrcibe a well-ordering on $\kappa \times \kappa$. This ordering denoted by $\prec$ will be essentially the lexicographic one. We define $(x, y) \prec (x', y')$ if $\max\{x, y\} < \max\{x', y'\}$, or if $\max\{x, y\} = \max\{x', y'\}$ and $x < x'$, or if $\max\{x, y\} = \max\{x', y'\}$ and $x = x'$ and $y < y'$. We leave it to you to check that this is a strict linear ordering on $\kappa \times \kappa$. That it is well-ordered can be seen as follows: If X is a nonempty subset of $\kappa \times \kappa$ we let δ

be the least ordinal such that $\delta = \max\{x, y\}$ for some $(x, y) \in X$, and we let D be the set of $(x, y) \in X$ with $\delta = \max\{x, y\}$. So D is a nonempty subset of X and a $\prec$-least element of D will, by definition, be a $\prec$-least element of X. Now set x to be least such that $(x, y) \in D$ for some y, and let E be the set of all such $y \in \kappa$. Then E is a nonempty subset of κ and if y is the least element in E, then (x, y) is the $\prec$-least element of D and hence of X.

Now to the proof that $\kappa \cdot \kappa = \kappa$. The diagonal map embeds κ into $\kappa \times \kappa$, so it remains to show that $\kappa \cdot \kappa \leq \kappa$. Writing $\kappa = \aleph_\alpha$ for some ordinal α (Proposition 3.6), we prove by induction on α that $\aleph_\alpha \cdot \aleph_\alpha \leq \aleph_\alpha$. The case of $\alpha = 0$ is Exercise 3.11(e) (or the fact that a countable union of countable sets is countable – Proposition 2.10(f)). Suppose $\aleph_\beta \cdot \aleph_\beta \leq \aleph_\beta$ for all $\beta < \alpha$.

Let γ be the ordinal to which $(\aleph_\alpha \times \aleph_\alpha, \prec)$ is order-isomorphic (Theorem 1.27). Now, if $\aleph_\alpha < \aleph_\alpha \cdot \aleph_\alpha$ then as $\aleph_\alpha < |\aleph_\alpha \times \aleph_\alpha|$ and hence $\aleph_\alpha < \gamma$. It follows that $\aleph_\alpha$ is a proper initial segment of γ, and hence order-isomorphic to a proper initial segment of $(\aleph_\alpha \times \aleph_\alpha, \prec)$. So it will suffice to show that every proper initial segment of $(\aleph_\alpha \times \aleph_\alpha, \prec)$ is of cardinality strictly less than $\aleph_\alpha$. This is what we now do.

Suppose S is a proper initial segment of $(\aleph_\alpha \times \aleph_\alpha, \prec)$. That is, $S = \{(x, y) : (x, y) \prec (x_0, y_0)\}$ for some $x_0, y_0 \in \aleph_\alpha$. Let $\zeta = \max\{x_0, y_0\} + 1$. Note that $S \subseteq \zeta \times \zeta$. Now, as every cardinal is a limit ordinal, $\zeta < \aleph_\alpha$. Hence, as in the proof of Theorem 3.6, there is a $\beta < \alpha$ such that $|\zeta| = \aleph_\beta$. So we have $|S| \leq |\zeta \times \zeta| = \aleph_\beta \cdot \aleph_\beta \leq \aleph_\beta < \aleph_\alpha$, as desired. □

It follows that (finite) cardinal arithmetic for infinite cardinals trivialises to computing maxima:

COROLLARY 3.13. *For all cardinals $\kappa_1 \leq \kappa_2$ with κ_2 infinite we have:*

(a) *If $\kappa_1 \neq 0$, then $\kappa_1 \cdot \kappa_2 = \kappa_2$.*
(b) $\kappa_1 + \kappa_2 = \kappa_2$.

PROOF. As κ_2 is an infinite cardinal it is of the form $\aleph_\alpha$ for some ordinal α. Now

$$\begin{aligned} \aleph_\alpha &\leq \kappa_1 \cdot \aleph_\alpha \quad \text{as } \aleph_\alpha \text{ embeds into } \kappa_1 \times \aleph_\alpha \\ &\leq \aleph_\alpha \cdot \aleph_\alpha \quad \text{as } \kappa_1 \subseteq \kappa_2 = \aleph_\alpha \text{ and hence } \kappa_1 \times \aleph_\alpha \subseteq \aleph_\alpha \times \aleph_\alpha \\ &= \aleph_\alpha \quad \text{by Theorem 3.12.} \end{aligned}$$

This proves part (a). For part (b) we have

$$\begin{aligned} \aleph_\alpha &\leq \kappa_1 + \aleph_\alpha \\ &\leq \aleph_\alpha + \aleph_\alpha \quad \text{as } \kappa_1 \subseteq \kappa_2 = \aleph_\alpha \\ &= 2 \cdot \aleph_\alpha \quad \text{as the disjoint union of two } \aleph_\alpha\text{-cardinality sets is equinumerous with } \{0, 1\} \times \aleph_\alpha \\ &= \aleph_\alpha \quad \text{by part (a).} \end{aligned}$$

□

The notions of cardinal sum and product can be extended to infinite sums and infinite products.

DEFINITION 3.14. Suppose $\{\kappa_i : i \in I\}$ is a set of cardinals. Then we can define the infinite sum

$$\sum_{i \in I} \kappa_i = |\bigcup_{i \in I} X_i|$$

where $\{X_i : i \in I\}$ is a set of pairwise disjoint sets with $|X_i| = \kappa_i$ for all $i \in I$. Similarly we define the infinite product

$$\prod_{i\in I} \kappa_i = |\bigotimes_{i\in I} X_i|$$

where $\{X_i : i \in I\}$ is such that $|X_i| = \kappa_i$ for all $i \in I$, and $\bigotimes_{i\in I} X_i$ is the cartesian product of the X_i's.

LEMMA 3.15. *The sums and products of Definition 3.14 are well-defined; they do not depend on the choice of* $\{X_i : i \in I\}$.

PROOF. This is exactly as in the finite case (cf. the proof of Lemma 3.8), except that we need to use the axiom of choice. Suppose $\{X_i : i \in I\}$ and $\{X'_i : i \in I\}$ are such that $|X_i| = |X'_i|$ for all $i \in I$. Using the axiom of choice, for each $i \in I$, fix a bijection $f_i : X_i \to X'_i$. We obtain the bijection $f : \bigcup_{i\in I} X_i \to \bigcup_{i\in I} X'_i$ given by $f(x) = f_i(x)$ where $i \in I$ is the (unique) index such that $x \in X_i$. Similarly we get the bijection $g : \bigotimes_{i\in I} X_i \to \bigotimes_{i\in I} X'_i$ given by $g(x_i : i \in I) = \big(f_i(x_i) : i \in I\big)$. □

Infinite cardinal sums also reduce to computing suprema, as Proposition 3.18 below demonstrates. But we begin with some easy lemmas.

LEMMA 3.16. *If* κ *and* λ *are cardinals, then* $\sum_{i<\lambda} \kappa = \lambda \cdot \kappa$.

PROOF. It suffices to show that if X_i, for $i < \lambda$, are pairwise disjoint sets with each $|X_i| = \kappa$, then there is a bijection between $\bigcup_{i<\lambda} X_i$ and $\lambda \times \kappa$. But this is clear since each X_i is equinumerous with $\{i\} \times \kappa$. □

LEMMA 3.17. *For any cardinal* λ *and any set of cardinals* $\{\kappa_i : i < \lambda\}$,

$$\sup\{\kappa_i : i < \lambda\} \leq \sum_{i<\lambda} \kappa_i.$$

PROOF. Immediate since $\kappa_j \leq \sum_{i<\lambda} \kappa_i$ for all $j < \lambda$. □

PROPOSITION 3.18. *If* λ *is an infinite cardinal and* $\{\kappa_i : i < \lambda\}$ *is a set of nonzero cardinals, then*

$$\sum_{i<\lambda} \kappa_i = \lambda \cdot \sup\{\kappa_i : i < \lambda\} = \sup\{\lambda, \kappa_i : i < \lambda\}.$$

PROOF. The second equality is just by Corollary 3.13(a). For the first equality, let $\kappa := \sup\{\kappa_i : i < \lambda\}$. Then it is easy to see that $\sum_{i<\lambda} \kappa_i \leq \sum_{i<\lambda} \kappa$, and the latter is $\lambda \cdot \kappa$ by Lemma 3.16. Hence $\sum_{i<\lambda} \kappa_i \leq \lambda \cdot \kappa$ and we need only show the opposite inequality. Now

$\lambda = \lambda \cdot 1 = \sum_{i<\lambda} 1 \leq \sum_{i<\lambda} \kappa_i$, where the second equality is by 3.16 and the inequality is by the fact that each κ_i is nonzero and hence ≥ 1. On the other hand, by Lemma 3.17, $\kappa \leq \sum_{i<\lambda} \kappa_i$ also. Taking products we get

$$\lambda \cdot \kappa \leq \big(\sum_{i<\lambda} \kappa_i\big) \cdot \big(\sum_{i<\lambda} \kappa_i\big) = \sum_{i<\lambda} \kappa_i$$

where the final equality uses the fact that $\sum_{i<\lambda} \kappa_i$ is an infinite cardinal (since λ is and each κ_i is nonzero). □

Infinite cardinal products, on the other hand, do not reduce to computing suprema: Given any cardinal λ, letting $\kappa_i = 2$ for all $i < \lambda$, we see that an element of $\bigotimes_{i<\lambda} \kappa_i$ corresponds to a subset of λ; indeed, if $a = (a_i : i < \lambda)$ is such an element then we can associate to it the set $\{i \in \lambda : a_i = 1\}$. This shows that $\prod_{i<\lambda} \kappa_i = |\mathcal{P}(\lambda)|$, which, by Cantor's diagonalisation (Theorem 3.7), is strictly larger than λ (and the κ_i).

The above example leads us to the connection between infinite products and exponentiation, which we now discuss.

Definition 3.19 (Cardinal exponentiation). If κ and λ are cardinals then κ^λ is defined to be the cardinality of the set of all functions from λ to κ.

Lemma 3.20. *If κ and λ are cardinals, then $\prod_{i<\lambda} \kappa = \kappa^\lambda$.*

Proof. This follows from the fact that the λth cartesian power of a set is exactly the set of functions from λ to that set. □

Lemma 3.21. *Suppose κ, λ, μ are cardinals. Then*

(a) *If $\lambda \leq \mu$ the $\kappa^\lambda \leq \kappa^\mu$ and $\lambda^\kappa \leq \mu^\kappa$.*
(b) *$\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$, and*
(c) *$(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$.*

Proof. Part (a) follows rather easily from the definition.

For part (b) let X be a set of cardinality λ and Y a set, disjoint from X, of cardinality μ. Let $\mathrm{Mor}(X, \kappa)$ denote the set of all functions from X to κ, and similarly for Y. Then $\kappa^\lambda \cdot \kappa^\mu$ is equinumerous with $\kappa^\lambda \times \kappa^\mu$ which is in turn equinumerous with $\mathrm{Mor}(X, \kappa) \times \mathrm{Mor}(Y, \kappa)$. But this latter set is equinumerous with $\mathrm{Mor}(X \cup Y, \kappa)$ via the association $(f, g) \mapsto f \cup g$. Finally, as $X \cup Y$ is of cardinality $\lambda + \mu$, $\mathrm{Mor}(X \cup Y, \kappa)$ is of cardinality $\kappa^{\lambda+\mu}$, as desired.

For part (c) it suffices to show that $\mathrm{Mor}(\lambda \times \mu, \kappa)$ is equinumerous with $\mathrm{Mor}\big(\mu, \mathrm{Mor}(\lambda, \kappa)\big)$. To see that this is the case suppose $f : \lambda \times \mu \to \kappa$. Then for each $x \in \mu$ let $g_x : \lambda \to \kappa$ be given by $g_x(y) = f(y, x)$ for all $y \in \lambda$. The association $f \longmapsto (x \mapsto g_x : x \in \mu)$ is a bijection between $\mathrm{Mor}(\lambda \times \mu, \kappa)$ and $\mathrm{Mor}\big(\mu, \mathrm{Mor}(\lambda, \kappa)\big)$. □

Exercise 3.22. (a) *Show that for any infinite cardinal κ, $\kappa^\kappa = 2^\kappa$.*
(b) *Show that $\prod_{i<\aleph_0, i\neq 0} i = 2^{\aleph_0}$ and so $\sum_{i<\aleph_0} i < \prod_{i<\aleph_0, i\neq 0} i$.*

The following is a generalisation of Cantor's diaogonalisation.

THEOREM 3.23 (König's Theorem). *Suppose* $\{\kappa_i : i \in I\}$ *and* $\{\lambda_i : i \in I\}$ *are families of cardinals with* $\kappa_i < \lambda_i$ *for all* $i \in I$. *Then* $\sum_{i\in I} \kappa_i < \prod_{i\in I} \lambda_i$.

PROOF. Let $\{X_i : i \in I\}$ be a pairwise disjoint set of sets with $|X_i| = \kappa_i$ for all $i \in I$, and let $\{Y_i : i \in I\}$ be such that $|Y_i| = \lambda_i$ for all $i \in I$. We will show that there is an injection from $\bigcup_{i\in I} X_i$ to $\bigotimes_{i\in I} Y_i$, but no surjection.

For each $i \in I$, let $\pi_i : X_i \to Y_i$ be the embedding given by the asumption that $\kappa_i < \lambda_i$. Fix also an element $c \in \bigotimes_{i\in I} Y_i$ such that for each $i \in I$, $c_i \in Y_i \setminus \pi_i(X_i)$. For each $x \in \bigcup_{i\in I} X_i$ let

$$f(x)_i \;=\; \begin{cases} \pi_i(x) & \text{if } x \in X_i \\ c_i & \text{else.} \end{cases}$$

Then $f(x) \in \bigotimes_{i\in I} Y_i$ and we have constructed a function $f : \bigcup_{i\in I} X_i \to \bigotimes_{i\in I} Y_i$. Note that $f(x)$ differs from c at exactly the (unique) ith co-ordinate where $x \in X_i$, and then for that i, $f(x)_i = \pi_i(x)$. So by the injectivity of the π_i's we have that f is injective.

Suppose, toward a contradiction, that there is a surjection $h : \bigcup_{i\in I} X_i \to \bigotimes_{i\in I} Y_i$. For each $i \in I$, let $p_i : \bigotimes_{i\in I} Y_i \to Y_i$ be the projection onto the ith coordinate. We obtain $h_i := p_i \circ (h \restriction X_i) : X_i \to Y_i$ which cannot be surjective since $\kappa_i < \lambda_i$ (cf. Proposition 2.10(e)). Fix $c \in \bigotimes_{i\in I} Y_i$ such that for each $i \in I$, $c_i \in Y_i \setminus h_i(X_i)$. By the assumption that h is surjective there must exist some $j \in I$ and some $x \in X_j$ with $h(x) = c$. But then $h_j(x) = c_j$ which contradicts our choice of c. □

3.4. Regularity and cofinality

LEMMA 3.24. *Suppose* κ *is a cardinal. The following are equivalent.*

(i) *For every subset* X *of* κ, *of cardinality strictly less than* κ, $\sup X < \kappa$.
(ii) *Suppose* $\{X_i : i < \lambda\}$ *is a set of subsets of* κ *such that* λ *is an ordinal* $< \kappa$ *and* $|X_i| < \kappa$ *for all* $i < \lambda$. *Then* $|\bigcup_{i<\lambda} X_i| < \kappa$.

PROOF. Suppose (i) holds. Then for each $i < \lambda$, for X_i as in the statement of (ii) we have $\lambda_i := \sup X_i < \kappa$. So $\Lambda := \{\lambda_i : i < \lambda\}$ is a subset of κ of cardinality $\leq \lambda < \kappa$. Applying (i) again, $\sup \Lambda < \kappa$. Now every member of X_i is $\leq \lambda_i < \sup \Lambda + 1$. Hence $\bigcup_{i<\lambda} X_i \subseteq \sup \Lambda + 1$. Hence, $|\bigcup_{i<\lambda} X_i| \leq |\sup \Lambda + 1| = |\sup \Lambda| \leq \sup \Lambda < \kappa$, as desired.

For the converse let $\lambda := |X|$ and enumerate $X = \{x_i : i < \lambda\}$. Then each x_i is an ordinal less than κ and hence $x_i \subseteq \kappa$ with $|x_i| \leq x_i < \kappa$. Applying (ii) we get that $|\sup X| = |\bigcup X| = |\bigcup_{i<\lambda} x_i| < \kappa$. But this forces $\sup X < \kappa$. □

Definition 3.25 (Regular/Singular Cardinals). A cardinal is called *regular* if it satisfies the equivalent conditions of Lemma 3.24. A cardinal is *singular* if it is not regular.

For example every finite cardinal is regular, as is $\aleph_0$. An example of a singular cardinal is $\aleph_\omega$ (which is by definition $= \bigcup_{i<\omega} \aleph_i$). Indeed, for each $i < \omega$ fix $x_i \in \aleph_{i+1} \setminus \aleph_i$. Then $X := \{x_i : i < \omega\}$ is a countable subset of $\aleph_\omega$ but $\sup X = \aleph_\omega$. This example motivates the following notion:

Definition 3.26 (Cofinality). The *cofinality* of an ordinal α, denoted by $\mathrm{cof}(\alpha)$, is the least ordinal β for which there exists a strictly increasing unbounded function $f : \beta \to \alpha$. That is, $f(x) < f(y)$ for all $x < y < \beta$, and for every $z < \alpha$ there is an $x < \beta$ with $z \leq f(x)$.

Note that the cofinality always exists since the identity function $\mathrm{id} : \alpha \to \alpha$ is strictly increasing and unbounded.

Lemma 3.27. *Suppose α is an ordinal. Then*

(a) $\mathrm{cof}(\alpha)$ *is a cardinal, and*
(b) $\mathrm{cof}\big(\mathrm{cof}(\alpha)\big) = \mathrm{cof}(\alpha)$.

Proof. We will need the following claim.

Claim 3.28. *If $\beta < \alpha$ are equinumerous ordinals, then there exists $\beta' \leq \beta$ and a strictly increasing unbounded function $f : \beta' \to \alpha$.*

Proof of Claim 3.28. Suppose $g : \beta \to \alpha$ is a bijection. Define $g' : \beta \to \alpha$ by transfinite recursion as follows:

$$g'(0) = g(0),$$

for all ordinals $\gamma < \beta$ with $\gamma + 1 < \beta$

$$g'(\gamma+1) \;=\; \begin{cases} g(x) \text{ where } x \text{ is least such that } g'(\gamma) < g(x) & \text{if such } x \text{ exists} \\ g'(\gamma) & \text{else} \end{cases}$$

and for all limit ordinals $\gamma < \beta$,

$$g'(\gamma) = \sup\{g(\gamma), g'(x) : x < \gamma\}.$$

Then it is not hard to see that g' is an increasing (though not necessarily strictly increasing) function with the property that for all $y < \beta$, $g'(y) \geq g(x)$ for all $x \leq y$. In particular, $\mathrm{Im}\, g'$ has no strict upper bound in α. If g' is strictly increasing then set $\beta' = \beta$ and $f = g'$ and we are done. If g' is not strictly increasing then let $\gamma < \beta$ be least such there exists η with $\gamma < \eta < \beta$ and $g'(\eta) = g(\gamma)$. Since g' is increasing it must be that $g'(\gamma+1) = g'(\gamma)$. But then by definition $g'(\gamma) = \sup \alpha$. Hence setting $\beta' = \gamma + 1$ and $f = g' \restriction (\gamma + 1)$ satisfies the claim. □

Now to the proof of part (a) of Lemma 3.27. Suppose toward a contradiction that there exists a $\beta < \mathrm{cof}(\alpha)$ equinumerous with $\mathrm{cof}(\alpha)$. Applying the claim to this pair of ordinals we obtain $\beta' \leq \beta$ and a strictly increasing unbounded function $f : \beta' \to \mathrm{cof}(\alpha)$. Now by definition we have a strictly increasing unbounded $g : \mathrm{cof}(\alpha) \to \alpha$. But then $g \circ f : \beta' \to \alpha$ is strictly increasing and unbounded. As $\beta' < \mathrm{cof}(\alpha)$ this contradicts the definition of $\mathrm{cof}(\alpha)$. So no such β can exist and $\mathrm{cof}(\alpha)$ is shown to be a cardinal.

For part (b) note that by definition we have a strictly increasing unbounded $f : \mathrm{cof}\big(\mathrm{cof}(\alpha)\big) \to \mathrm{cof}(\alpha)$, and we have a strictly increasing unbounded $g : \mathrm{cof}(\alpha) \to \alpha$. But then $g \circ f : \mathrm{cof}\big(\mathrm{cof}(\alpha)\big) \to \alpha$ is strictly increasing and unbounded. Hence $\mathrm{cof}\big(\mathrm{cof}(\alpha)\big) \geq \mathrm{cof}(\alpha)$. But $\mathrm{id} : \mathrm{cof}(\alpha) \to \mathrm{cof}(\alpha)$ winesses that $\mathrm{cof}\big(\mathrm{cof}(\alpha)\big) \leq \mathrm{cof}(\alpha)$. Hence $\mathrm{cof}\big(\mathrm{cof}(\alpha)\big) = \mathrm{cof}(\alpha)$, as desired. □

Our explanation above of why $\aleph_\omega$ is singular also showed that $\mathrm{cof}(\aleph_\omega) \leq \omega$. More generally:

PROPOSITION 3.29. *A cardinal κ is regular if and only if $\mathrm{cof}(\kappa) = \kappa$.*

PROOF. Suppose $\mathrm{cof}(\kappa) = \kappa$ and X is a subset of κ of cardinality $\lambda < \kappa$. Now the induced ordering $(X, <)$ is strictly well-ordered and hence is order-isomorphic to an ordinal α. That is, we have a strictly increasing bijection $f : \alpha \to X$. Since $|\alpha| = |X| < \kappa$, $\alpha < \kappa$. As $\mathrm{cof}(\kappa) = \kappa > \alpha$, it follows that f is bounded in κ. That is, there exists $z < \kappa$ such that z is a strict upper bound for $\mathrm{Im}\, f = X$. Hence $\sup X < \kappa$. We have shown that κ is regular.

Now suppose $\mathrm{cof}(\kappa) = \alpha < \kappa$, so that there exists a strictly increasing unbounded $f : \alpha \to \kappa$. This means that $\sup(\mathrm{Im}\, f) = \sup \kappa$. As κ is a limit ordinal (it is a cardinal and all cardinals are limit ordinals by Lemma 2.4), $\sup \kappa = \kappa$. So we have a subset $\mathrm{Im}\, f \subseteq \kappa$ whose cardinality is $|\alpha| \leq \alpha < \kappa$ but with supremum equal to κ. It follows that κ is not regular. □

EXERCISE 3.30. *Every successor cardinal (i.e., cardinal of the form $\aleph_{\alpha+1}$) is regular.*

Note that cof is not an increasing operation on cardinals. For example $\mathrm{cof}(\aleph_n) = \aleph_n$ for all $n < \omega$ by Exercise 3.30 and Proposition 3.29, but $\mathrm{cof}(\aleph_\omega) = \aleph_0$.

The following is a strengthening of Cantor's diagonalisation, and it is the principal corollary of König's Theorem.

PROPOSITION 3.31. *For all cardinals κ, $\mathrm{cof}(2^\kappa) > \kappa$.*

PROOF. This is immediate for κ finite, so we assume κ is infinite. Let $\lambda \leq \kappa$ and suppose $f : \lambda \to 2^\kappa$ is a strictly increasing function. Then $\sup(\mathrm{Im}\, f) = \bigcup_{i<\lambda} f(i)$. But we can compute

$$\begin{aligned}
\Big|\bigcup_{i<\lambda} f(i)\Big| &\leq \sum_{i<\lambda} |f(i)| \\
&< \prod_{i<\lambda} 2^\kappa \quad \text{by 3.23 (König's Theorem) since each } |f(i)| < 2^\kappa \\
&= (2^\kappa)^\lambda \quad \text{by Lemma 3.20} \\
&= 2^{\kappa\cdot\lambda} \quad \text{by Lemma 3.21(c)} \\
&= 2^\kappa \quad \text{by Corollary 3.13(a) as } \lambda \leq \kappa \text{ and } \kappa \text{ is infinite.}
\end{aligned}$$

Hence $\sup(\operatorname{Im} f) < 2^\kappa$. That is, f must be bounded in 2^κ. We have shown that λ cannot be the cofinality of 2^κ. So $\operatorname{cof}(2^\kappa) > \kappa$, as desired. □

This gives us a little bit more information on the continuum:

COROLLARY 3.32. $2^{\aleph_0} \neq \aleph_\omega$ □

Part 2

Model Theory

CHAPTER 4

First-order Logic

4.1. Structures

DEFINITION 4.1. A *structure* $\mathcal{M}$ consists of a nonempty underlying set M, called the *universe* of $\mathcal{M}$, together with

- a set $\{c_i : i \in I_C\}$ of distinguished elements of M, called *constants*;
- a set $\{f_i : M^{n_i} \to M : i \in I_F\}$ of distinguished maps from various cartesian powers of M to M itself, called *basic functions*; and,
- a set $\{R_i \subseteq M^{k_i} : i \in I_R\}$ of distinguished subsets of various cartesian powers of M, called *basic relations*.

Each of the natural numbers n_i and k_i that appear above are assumed to be nonzero and are called the *arity* of the corresponding function or relation. The constants, basic functions and basic relations together make up the *signature* of $\mathcal{M}$.

REMARK 4.2. (a) Any of the the set of constants, relations or functions may be empty. So for example a nonempty set M by itself forms a structure.

(b) Note that constants are nothing other than 0-ary functions, under the convention that $M^0 = \{\emptyset\}$. So if we had allowed 0-ary functions we could have done without constants.

(c) Some treatments of this material ask that the equality relation on M always be included among the relations in a structure. We will not do so here, only because our point of view will be that equality is an inherent part of the set M itself, and hence need not be distinguished as a named relation.

The notion of structure here is very natural, it is nothing other than a set M equipped with a signature which dictates what "structure" on M we are interested in studying. For example, consider the set of real numbers $\mathbb{R}$. If we wish to view $\mathbb{R}$ purely as a *set* (with equality), then we can consider the structure whose universe is $\mathbb{R}$ and whose signature is empty. On the other hand, to study the structure $(\mathbb{R}, 0, +, -)$, where we have a constant for 0, a binary function for addition and a unary function for additive inverse (i.e., taking negatives), is to study the reals as a *group* under addition. If we wish to study the reals as a *ring* then we can consider the structure $(\mathbb{R}, 0, 1, +, -, \times)$; or $(\mathbb{R}, 0, 1, +, -, \times, ^{-1})$, where $^{-1}$ is the unary function of taking the multipilicative inverse, if we are interested in the *real field*. The structure $(\mathbb{R}, 0, 1, +, -, \times, ^{-1}, <)$ where $<$ is the usual ordering on the reals (as a binary relation) corresponds to the *ordered field* of real numbers. Each of the examples above have the same underlying set, just equipped with ever expanding signatures. A natural question, very much at the heart of model theory, would be to ask whether, for example, the ordered field of reals can be recovered from the real field, or whether the real field can be recovered from the additive group of reals. Of course we need to make precise what we mean by

"recovered", but once we have done so we will see that the answer to the former is yes (this is easy), and to the latter is no (this is a little harder). We are, however, getting ahead of ourselves. For now, let us just record this notion of expansion we have been discussing.

DEFINITION 4.3 (Expansion/Reduct). Suppose $\mathcal{M}$ and $\mathcal{N}$ are structures. We say that $\mathcal{N}$ is an *expansion* of $\mathcal{M}$ if they have the same universe and the signature of $\mathcal{N}$ contains the signature of $\mathcal{M}$. We also say in this case that $\mathcal{M}$ is a *reduct* of $\mathcal{N}$.

4.2. Languages

Consider the structures $(\mathbb{R}, 0, 1, +, -, \times, ^{-1})$ and $(\mathbb{F}_5, 0, 1, +, -, \times, ^{-1})$, where $\mathbb{F}_5$ is the set of integers mod 5. They do not actually have the same signature, since, for example, the $+$ in the first case denotes addition on the reals while the $+$ in the second denotes addition on $\mathbb{F}_5$. There is however a sense in which both $+$s are interpretations of some "additive structure". This is made precise by the notion of a common *language*.

DEFINITION 4.4 (Language/L-structure). A *language* L is determined by specifying the following three sets of symbols:

(i) a set of *constant symbols* L^{con};
(ii) a set of *function symbols* L^{fun}, together with a positive integer n_f for every $f \in L^{\text{fun}}$ called the *arity* of f; and,
(iii) a set of *relation symbols* L^{rel}, together with a positive integer k_R for every $R \in L^{\text{rel}}$ called the *arity* of R.

An *L-structure* is then a structure $\mathcal{M}$ together with a bijective correspondence between L and the signature of $\mathcal{M}$ that associates

- to each constant symbol $c \in L^{\text{con}}$ a constant $c^{\mathcal{M}} \in M$ from $\mathcal{M}$,
- to each function symbol $f \in L^{\text{fun}}$ a function $f^{\mathcal{M}} : M^{n_f} \to M$ from $\mathcal{M}$, and,
- to each relation symbol $R \in L^{\text{rel}}$ a relation $R^{\mathcal{M}} \subseteq M^{k_R}$ from $\mathcal{M}$.

We say that the constants, functions, and relations, $c^{\mathcal{M}}, f^{\mathcal{M}}, R^{\mathcal{M}}$, are the *interpretations* in $\mathcal{M}$ of the corresponding symbols.

So, for example, $(\mathbb{R}, 0, 1, +, -, \times, ^{-1})$ and $(\mathbb{F}_5, 0, 1, +, -, \times, ^{-1})$ are both naturally L-structures where $L := \{0, 1, +, -, \times, ^{-1}\}$ is made up of two constant symbols, two binary function symbols, two unary function symbols, and no relation symbols. This particular language is often called the *language of fields* for obvious reasons.

REMARK 4.5. Note that we have already begun to abuse the notation: we have used the same notation, $+$ for example, to denote both the function symbol in L and its interpretations in the L-structures $\mathcal{R} := (\mathbb{R}, 0, 1, +, -, \times, ^{-1})$ and $\mathcal{F} := (\mathbb{F}_5, 0, 1, +, -, \times, ^{-1})$. To be correct and unambiguous, if we used $+$ for the symbol in the language then we should use $+^{\mathcal{R}}$ for addition on $\mathbb{R}$ and $+^{\mathcal{F}}$ for addition on $\mathbb{F}$. This would indeed become unwieldy and it is common to not make this notational distinction, at least when the context makes clear whether we mean a symbol in a language or its interpretation in some particular structure.

Let us consider some further examples.

EXAMPLE 4.6 (Orderings). In the first part of this course we studied ordinals. The structure we were interested in was the ordering on the ordinal as given by the membership relation. In model-theoretic terms we were interested in structures of the form $\mathcal{A} := (\alpha, \in)$ where α is an ordinal. A natural language for this structure is the *language of orderings*, $L := \{<\}$, consisting of a single binary relation symbol (and no constant or function symbols). Thus $\mathcal{A}$ is an L-structure with $<^{\mathcal{A}} = \in$. The abuse of notation described in Remark 4.5 is thus consistent with (and explains) our convention from the last chapter that $<$ and $\in$ are synonymous when dealing with ordinals. However there are other L-structures that look very different than ordinals. For example, the usual ordering on the rational numbers, $(\mathbb{Q}, <)$, is an L-structure. This linear ordering is not an ordinal, it is dense which is very far from well-ordered. In fact, it is important to note that an L-structure need not be a linear ordering at all; an L-structure is just a nonempty set together with a binary relation. For example, consider the L-structure $\mathcal{C}$ whose universe is the complex numbers and where $<$ is so interpreted that $a <^{\mathcal{C}} b$ if and only if $a^2 + b^2 = 1$. This L-structure is not even a poset.

EXAMPLE 4.7 (Vector spaces). Suppose F is a field. The *language of F-vector spaces* usually refers to the language $L := \{0, +, -, \lambda_a : a \in F\}$ consisting of one constant symbol 0, one binary function symbol $+$, a unary function symbol $-$, and a set of unary function symbols $\{\lambda_a : a \in F\}$, indexed by F. Any F-vector space, V, is made into an L-structure by interpreting 0 as the zero vector, $+$ as vector addition, $-$ as the operation which takes the negative of a vector, and for each $a \in F$, interprets λ_a as scalar multiplication by a. As in the previous example the converse is not true; not every L-structure is a vector space. Only those L-structures *satisfying certain axioms* about how the interpretations behave will be F-vector spaces. We will study this notion of satisfaction later.

We ended the previous section by defining expansions and reducts: when the universe of a structure is unchanged but the signature is expanded or reduced. One can also vary structures in the opposite way: let the universe increase or decrease but leave the signature, or rather the language, constant.

DEFINITION 4.8 (Embedding). Suppose L is a language and $\mathcal{M}$ and $\mathcal{N}$ are L-structures with universes M and N respectively. An L-embedding of $\mathcal{M}$ in $\mathcal{N}$ is an injective map $j : M \to N$ such that

(i) for all $c \in L^{\text{con}}$, $j(c^{\mathcal{M}}) = c^{\mathcal{N}}$;
(ii) for all $f \in L^{\text{fun}}$ and all $a \in M^{n_f}$, $j\big(f^{\mathcal{M}}(a)\big) = f^{\mathcal{N}}\big(j(a)\big)$; and,
(iii) for all $R \in L^{\text{rel}}$ and all $a \in M^{k_R}$, $a \in R^{\mathcal{M}}$ if and only if $j(a) \in R^{\mathcal{N}}$.

A surjective L-embedding is called an *L-isomorphism*.

If $M \subseteq N$ and the inclusion map is an L-embedding then we say that $\mathcal{M}$ is a *L-substructure* of $\mathcal{N}$, or that $\mathcal{N}$ is an *L-extension* of $\mathcal{M}$. In this case we write $\mathcal{M} \subseteq \mathcal{N}$.

REMARK 4.9. (a) It is important that in (iii) we have an "if and only if" and not just an "only if". That, together with the injectivity of ι, distinguish L-embeddings from *L-homomorphisms*, which we will not discuss here. The injectivity of ι is itself just the "if" part of (iii) applied to the implicit equality relation.

(b) Note that $\mathcal{M} \subseteq \mathcal{N}$ if and only if $M \subseteq N$, $c^{\mathcal{M}} = c^{\mathcal{N}}$ for all $c \in L^{\text{con}}$, $f^{\mathcal{M}} = f^{\mathcal{N}} \restriction M^{n_f}$ for all $f \in L^{\text{fun}}$, and $R^{\mathcal{M}} = R^{\mathcal{N}} \cap M^{k_R}$ for all $R \in L^{\text{rel}}$.

The notion of substructure is sensitive to the choice of language, and indeed often informs what language we choose. For example, consider the languages $L_1 = \{0, 1, +, -, \times, ^{-1}\}$, $L_2 = \{0, 1, +, -, \times\}$, $L_3 = \{0, +, -\}$, and $L_4 = \emptyset$. Then, under the natural interpretations, the L_1-substructures of $\mathbb{R}$ are its *subfields*, the L_2-substructures are its *subrings*, the L_3-substructures of $\mathbb{R}$ are the *subgroups* of the additive group of reals, and finally, the L_4-substructures of $\mathbb{R}$ are the *subsets* of $\mathbb{R}$.

EXERCISE 4.10. *Show that if $\mathcal{N}$ is an L-structure and M is a nonempty subset of the universe of $\mathcal{N}$ then M is the universe of a substructure of $\mathcal{N}$ if and only if M contains all the constants of $\mathcal{N}$ and is preserved by all the functions in $\mathcal{N}$. Moreover, if this is the case, then there is a unique L-substructure of $\mathcal{N}$ that has M as its underlying set.*

4.3. Some syntax

In this section we will describe the formal rules for writing down *first-order formulas* in a given language L. These formulas will be used, in later sections, on the one hand to express properties that tuples from a particular L-structure may or may not possess (giving rise to *definable sets*), and on the other hand to express axioms that L-structures may or may not satisfy (giving rise to the class of *models of a theory*). The study of these two kinds of objects, the sets definable in L-structures and the class of models of a theory, is essentially what model theory is about.

The starting point is the notion of term which makes precise which functions can be defined, in a finitary manner, from the function and constant symbols in the language. We will make use of a fixed countably infinite set of distinct *variable symbols* $\mathrm{Var} = \{v_0, v_1, \dots\}$.

Let us fix a language L.

DEFINITION 4.11 (Term). The set of *L-terms* is the smallest set of strings of symbols satisfying:

(i) A variable symbol is an L-term.
(ii) A constant symbol is an L-term.
(iii) If $f \in L^{\mathrm{fun}}$ and $t_1, \dots, t_{n_f}$ are L-terms then $f(t_1, \dots, t_{n_f})$ is an L-term.

We sometimes write a term t as $t(x_1, \dots, x_n)$ to mean that the variable symbols appearing in t come from the list $x_1, \dots, x_n$. (Though not all of these variables need appear in t.)

For the sake of readability we may often diverge from the above rules for writing terms according to the natural use of the symbols in everyday mathematics. For example we will write $(v_0 + v_1) - 1$ for the more accurate but rather inscrutable $+(+(v_0, v_1), -(1))$. Another example is $(1 + v_1)^{-1}$ rather than the official $^{-1}(+(1, v_1))$.

The next step is the atomic formula, which is the simplest kind of formula and is obtained by equating or relating terms.

DEFINITION 4.12 (Atomic formula). An *atomic L-formula* is a string of symbols of the form

(i) $(t = s)$ where t and s are L-terms, or
(ii) $R(t_1, \dots, t_{k_R})$ where $R \in L^{\mathrm{rel}}$ and $t_1, \dots, t_{k_R}$ are L-terms.

Again we may use common abbreviations for the sake of readability. For example, we write $v_2 < -v_1$ instead of $<(v_2, -(v_1))$.

Finally, we can build recursively on atomic formulas, using the logical *connectives* $\{\neg, \wedge, \vee\}$ and the *quantifiers* $\{\forall, \exists\}$, to define the set of formulas.

DEFINITION 4.13 (Formula). The set of *L-formulas* is the smallest set of strings of symbols satisfying:

(i) Every atomic formula is a formula.
(ii) If ϕ and ψ are formulas then $\neg\phi$, $(\phi \wedge \psi)$, and $(\phi \vee \psi)$ are all formulas.
(iii) If ϕ is a formula and x is a variable symbol then $\forall x\phi$ and $\exists x\phi$ are formulas.

We also make the following two abbreviations: For any L-formulas ϕ and ψ,

- $(\phi \to \psi)$ abbreviates the formula $(\neg\phi \ \vee \ \psi)$, and,
- $(\phi \leftrightarrow \psi)$ abbreviates the formula $((\phi \to \psi) \wedge (\psi \to \phi))$.

EXAMPLE 4.14. In the first part of this course we talked a little about Zermelo-Fraenkel set theory. The axioms of ZF can all be viewed as formulas in the *language of set theory*, namely $L := \{\in\}$. For example, let $\phi(x, y)$ be the formula saying that y is the successor of x. That is, $\phi(x, y)$ is the formula

$$(x \in y) \wedge \forall z\big(z \in y \to (z \in x \ \vee \ z = x)\big).$$

Note that for the sake of readability we have dropped some of the parantheses. So actually this formula should be written $((x \in y) \wedge \forall z((z \in y) \to ((z \in x) \vee (z = x))))$. Now the Axiom of Infinity, which says there is a set containing $\emptyset$ and closed under the successor function, can be expressed using $\phi(x, y)$ as follows:

$$\exists w \exists v\big(\forall z(z \notin v) \ \wedge \ (v \in w) \ \wedge \ \forall x \forall y((x \in w \ \wedge \ \phi(x, y)) \to y \in w)\big).$$

Note that we use x, y, z, etc., for variable symbols. This will be common.

DEFINITION 4.15. Suppose ϕ is an L-formula. An occurrence of a variable x in ϕ is said to be *bound* if it appears inside the scope of a quantifier $\exists x$ or $\forall x$. If the occurrence is not bound then it is said to be *free*. Sometimes we write ϕ as $\phi(x_1, \ldots, x_n)$ to mean that the variables which occur freely in ϕ all come from the list $x_1, \ldots, x_n$. (Though not all of these variable need appear freely in ϕ.) A formula in which all variable symbols always occurr bound is called a *sentence*.

So in the formula $\phi(x, y)$ of Example 4.14 all the occurrences of x and y are free while all the occurrences of z are bound. Still working in Example 4.14, the formula expressing the Axiom of Infinity is a sentence. In the formula $((x > 0) \ \vee \ \exists x(x \times x = 1))$ the first occurrence of x is free while the other occurrences are all bound.

REMARK 4.16. As a simplification we will assume that no variable occurs both free and bound in the same formula; so the formula $((x > 0) \ \vee \ \exists x(x \times x = 1))$ discussed above would be implicitly replaced by $((x > 0) \ \vee \ \exists z(z \times z = 1))$ where z is a variable symbol distinct from x.

4.4. Truth and satisfaction

Until now terms and formulas are officially just certain strings of symbols; they do not *mean* anything. In this section we describe how, given an L-structure $\mathcal{M}$, it makes sense to interpret what L-terms and L-formulas mean in $\mathcal{M}$. We begin with terms. These will be interpreted as functions on the universe of $\mathcal{M}$.

DEFINITION 4.17 (Interpreting terms). Suppose $\mathcal{M}$ is an L-structure with universe M, and $t = t(x_1, \ldots, x_n)$ is an L-term. Then the *interpretation of* $t(x_1, \ldots, x_n)$ *in* $\mathcal{M}$ is the function $t^{\mathcal{M}} : M^n \to M$ defined inductively as follows:

(i) If t is a variable symbol x_i for some $1 \leq i \leq n$, then $t^{\mathcal{M}} : M^n \to M$ is the function $(a_1, \ldots, a_n) \mapsto a_i$.
(ii) If t is a constant symbol c, then $t^{\mathcal{M}} : M^n \to M$ is the function $(a_1, \ldots, a_n) \mapsto c^{\mathcal{M}}$.
(iii) If $t = f(t_1, \ldots, t_{n_f})$ where $f \in L^{\text{fun}}$ and $t_1(x_1, \ldots, x_n), \ldots, t_{n_f}(x_1, \ldots, x_n)$ are L-terms, then $t^{\mathcal{M}} : M^n \to M$ is the function

$$(a_1, \ldots, a_n) \longmapsto f^{\mathcal{M}}\big(t_1^{\mathcal{M}}(a_1, \ldots, a_n), \ldots, t_{n_f}^{\mathcal{M}}(a_1, \ldots, a_n)\big).$$

Note that the function $t^{\mathcal{M}}$ depends not only on the term t but on its presentation as $t = t(x_1, \ldots, x_n)$.

For example, the interpretation of the term $(v_0 + v_1) - 1$, presented as $t(v_1, v_2)$, in the structure $(\mathbb{R}, 0, 1, +, -, \times)$, is the function $(a, b) \mapsto a + b - 1$.

EXERCISE 4.18. *Suppose $L = \{0, 1, +, -, \times\}$ is the language of rings. Show that the L-terms are the polynomials with integer coefficients. More precisely, for every L-term $t = t(x_1, \ldots, x_n)$ there exists a polynomial $P_t \in \mathbb{Z}[X_1, \ldots, X_n]$ such that, for every ring $\mathcal{R}$, viewed in the natural way as an L-structure, $t^{\mathcal{R}} = P_t$ as functions on R^n. Conversely, every polynomial in $\mathbb{Z}[X_1, \ldots, X_n]$ is of the form P_t for some L-term $t = t(x_1, \ldots, x_n)$.*

EXERCISE 4.19. *Suppose F is a field and $L = \{0, +, -, \lambda_a : a \in F\}$ is the language of F-vector spaces. What, in the spirit of Exercise 4.18, do the L-terms look like?*

DEFINITION 4.20 (Satisfaction). Suppose $\mathcal{M}$ is an L-structure with universe M, $\phi = \phi(x)$ is an L-formula where $x = (x_1, \ldots, x_n)$, and $a = (a_1, \ldots, a_n) \in M^n$. We define $\mathcal{M} \models \phi(a)$ inductively as follows:

(i) If ϕ is $(t_1 = t_2)$ where $t_1(x)$ and $t_2(x)$ are L-terms, then $\mathcal{M} \models \phi(a)$ means that $t_1^{\mathcal{M}}(a) = t_1^{\mathcal{M}}(a)$.
(ii) If ϕ is $R(t_1, \ldots, t_{k_R})$ where $R \in L^{\text{rel}}$ and $t_1(x), \ldots, t_{k_R}(x)$ are L-terms, then $\mathcal{M} \models \phi(a)$ means that $\big(t_1^{\mathcal{M}}(a), \ldots, t_{k_R}^{\mathcal{M}}(a)\big) \in R^{\mathcal{M}}$.
(iii) If ϕ is $\neg\psi$ where $\psi(x)$ is an L-formulau, then $\mathcal{M} \models \phi(a)$ means that $\mathcal{M} \not\models \psi(a)$.
(iv) If ϕ is $(\psi \wedge \theta)$ where $\psi(x)$ and $\theta(x)$ are L-formulas, then $\mathcal{M} \models \phi(a)$ means that $\mathcal{M} \models \psi(a)$ and $\mathcal{M} \models \theta(a)$.
(v) If ϕ is $(\psi \vee \theta)$ where $\psi(x)$ and $\theta(x)$ are L-formulas, then $\mathcal{M} \models \phi(a)$ means that $\mathcal{M} \models \psi(a)$ or $\mathcal{M} \models \theta(a)$.
(vi) If ϕ is $\exists z\psi$ where z is a variable symbol and $\psi(x, z)$ is an L-formula, then $\mathcal{M} \models \phi(a)$ menas that there exists $b \in M$ such that $\mathcal{M} \models \psi(a, b)$.
(vii) If ϕ is $\forall z\psi$ where z is a variable symbol and $\psi(x, z)$ is an L-formula, then $\mathcal{M} \models \phi(a)$ means that $\mathcal{M} \models \psi(a, b)$ for all $b \in M$.

If $\mathcal{M} \models \phi(a)$ then we say that $\mathcal{M}$ *satisfies* $\phi(a)$ or that $\phi(a)$ *is true in* $\mathcal{M}$, or that a *realises* $\phi(x)$ *in* $\mathcal{M}$. The set of all realisation of ϕ in $\mathcal{M}$, $\{a \in M^n : \mathcal{M} \models \phi(a)\}$, is denoted by $\phi^{\mathcal{M}}$ and is called *the set defined by* ϕ *in* $\mathcal{M}$.

Let us consider the case when when $n = 0$, that is when ϕ is a sentence. Since, by convention, $M^0 = \{\emptyset\}$, the only question in this case is whether $\emptyset$ realises ϕ or not. If it does then we say that ϕ *is true in* $\mathcal{M}$ and write $\mathcal{M} \models \phi$. Note that if ϕ is a sentence then it is either true or false in $\mathcal{M}$ (the latter case being equivalent to $\mathcal{M} \models \neg\phi$).

EXAMPLE 4.21. Suppose $\phi(y)$ is $\exists x(x^2 = y)$, where x^2 is an abbreviation for $x \times x$. Then $(\mathbb{R}, 0, 1, +, -, \times) \models \phi(2)$ while $(\mathbb{Q}, 0, 1, +, -, \times) \models \neg\phi(2)$ and $(\mathbb{C}, 0, 1, +, -, \times) \models \forall y\phi(y)$.

The following proposition shows that satisfaction for formulas without quantifiers – we call them *quantifier-free formulas* – is particularly simple.

PROPOSITION 4.22. *Suppose $\mathcal{M} \subseteq \mathcal{N}$ are L-structures with universes $M \subseteq N$, $\phi = \phi(x_1, \ldots, x_n)$ is an L-formula, and $a \in M^n$.*

(a) *If ϕ is quantifier-free then $\mathcal{M} \models \phi(a)$ if and only if $\mathcal{N} \models \phi(a)$.*
(b) *If ϕ of the form $\exists y_1 \cdots \exists y_m \psi$ for some quantifier-free L-formula ψ, then $\mathcal{M} \models \phi(a)$ implies $\mathcal{N} \models \phi(a)$.*
(c) *If ϕ of the form $\forall y_1 \cdots \forall y_m \psi$ for some quantifier-free L-formula ψ, then $\mathcal{N} \models \phi(a)$ implies $\mathcal{M} \models \phi(a)$.*

PROOF. This proposition has a very typical proof. In order to prove something about all formulas one usually has to begin by proving something about terms and then proceeding by induction on the complexity of the formula. The result about terms is itself usually proved by induction on the complexity of the term.

Let $x = (x_1, \ldots, x_n)$. We first observe that *if $t = t(x)$ is any L-term then $t^{\mathcal{M}} = t^{\mathcal{N}} \restriction M^n$.* Indeed, we prove this by induction on the complexity of t. If t is a constant or variable symbol then this is clear. Suppose $t = f(t_1, \ldots, t_{n_f})$, where $f \in L^{\text{fun}}$ and $t_1(x), \ldots, t_{n_f}(x)$ are L-terms for which the result is known. Then for any $a \in M^n$,

$$\begin{aligned} t^{\mathcal{M}}(a) &= f^{\mathcal{M}}\big(t_1^{\mathcal{M}}(a), \ldots, t_{n_f}^{\mathcal{M}}(a)\big) \text{ by definition of the interpretation of terms} \\ &= f^{\mathcal{M}}\big(t_1^{\mathcal{N}}(a), \ldots, t_{n_f}^{\mathcal{N}}(a)\big) \text{ by the induction hypothesis} \\ &= f^{\mathcal{N}}\big(t_1^{\mathcal{N}}(a), \ldots, t_{n_f}^{\mathcal{N}}(a)\big) \text{ since } f^{\mathcal{M}} = f^{\mathcal{N}} \restriction M^{n_f}, \text{ see Remark 4.9(b)} \\ &= t^{\mathcal{N}}(a) \end{aligned}$$

as desired.

We now prove part(a) by induction on the complexity of the quantifier-free formula ϕ. If ϕ is of the form $(t_1 = t_2)$ for some L-terms $t_1(x)$ and $t_2(x)$, then

$$\begin{aligned} \mathcal{M} \models \phi(a) &\iff t_1^{\mathcal{M}}(a) = t_2^{\mathcal{M}}(a) \\ &\iff t_1^{\mathcal{N}}(a) = t_2^{\mathcal{N}}(a) \text{ since } t_i^{\mathcal{M}} = t_i^{\mathcal{N}} \restriction M^n, \text{ for } i = 1, 2 \\ &\iff \mathcal{N} \models \phi(a). \end{aligned}$$

If ϕ is of the form $R(t_1, \ldots, t_{k_R})$ for some $R \in L^{\text{rel}}$ and $t_1(x), \ldots, t_{k_R}(x)$ L-terms, then

$$\begin{aligned}
\mathcal{M} \models \phi(a) &\iff \left(t_1^{\mathcal{M}}(a), \ldots, t_{k_R}^{\mathcal{M}}(a)\right) \in R^{\mathcal{M}} \\
&\iff \left(t_1^{\mathcal{N}}(a), \ldots, t_{k_R}^{\mathcal{N}}(a)\right) \in R^{\mathcal{M}} \text{ since } t_i^{\mathcal{M}} = t_i^{\mathcal{N}} \restriction M^n, \text{ for } i = 1, \ldots, k_R \\
&\iff \left(t_1^{\mathcal{N}}(a), \ldots, t_{k_R}^{\mathcal{N}}(a)\right) \in R^{\mathcal{N}} \text{ since } R^{\mathcal{M}} = R^{\mathcal{N}} \cap M^{k_r}, \text{ see Remark 4.9(b)} \\
&\iff \mathcal{N} \models \phi(a).
\end{aligned}$$

Now suppose $\psi(x)$ and $\theta(x)$ are quantifier-free L-formulas for which the result is known. If ϕ is $\neg\psi$ then

$$\begin{aligned}
\mathcal{M} \models \phi(a) &\iff \mathcal{M} \not\models \psi(a) \\
&\iff \mathcal{N} \not\models \psi(a) \text{ by the induction hypothesis} \\
&\iff \mathcal{N} \models \phi(a).
\end{aligned}$$

If ϕ is $(\psi \wedge \theta)$ then

$$\begin{aligned}
\mathcal{M} \models \phi(a) &\iff \mathcal{M} \models \psi(a) \text{ and } \mathcal{M} \models \theta(a) \\
&\iff \mathcal{N} \models \psi(a) \text{ and } \mathcal{N} \models \theta(a) \text{ by the induction hypothesis} \\
&\iff \mathcal{N} \models \phi(a).
\end{aligned}$$

If ϕ is $(\psi \vee \theta)$ then

$$\begin{aligned}
\mathcal{M} \models \phi(a) &\iff \mathcal{M} \models \psi(a) \text{ or } \mathcal{M} \models \theta(a) \\
&\iff \mathcal{N} \models \psi(a) \text{ or } \mathcal{N} \models \theta(a) \text{ by the induction hypothesis} \\
&\iff \mathcal{N} \models \phi(a).
\end{aligned}$$

Since ϕ is a quantifier-free formula, this completes the induction.

To prove part (b) we write $\phi(x) = \exists y \psi(x, y)$ where $y = (y_1, \ldots, y_m)$ and ψ is quantifier-free. Then

$$\begin{aligned}
\mathcal{M} \models \phi(a) &\implies \text{there exists } b \in M^m \text{ such that } \mathcal{M} \models \psi(a, b) \\
&\implies \text{there exists } b \in M^m \text{ such that } \mathcal{N} \models \psi(a, b) \quad \text{by part (a)} \\
&\implies \text{there exists } b \in N^m \text{ such that } \mathcal{N} \models \psi(a, b) \quad \text{as } M \subseteq N \\
&\implies \mathcal{N} \models \phi(a).
\end{aligned}$$

To prove part (c), write $\phi(x) = \forall y \psi(x, y)$. Then

$$\begin{aligned}
\mathcal{N} \models \phi(a) &\implies \text{for all } b \in N^m, \mathcal{N} \models \psi(a, b) \\
&\implies \text{for all } b \in M^m, \mathcal{N} \models \psi(a, b) \quad \text{as } M \subseteq N \\
&\implies \text{for all } b \in M^m, \mathcal{M} \models \psi(a, b) \quad \text{by part (a)} \\
&\implies \mathcal{M} \models \phi(a).
\end{aligned}$$

This completes the proof of the proposition. □

The formulas of the form $\exists y_1 \cdots \exists y_m \psi$ where ψ is quntifier-free are called *existential formulas*, while those of the form $\forall y_1 \cdots \forall y_m \psi$ are called *universal formulas*.

While Proposition 4.22 is about $\mathcal{M} \subseteq \mathcal{N}$, the proof clearly goes through for any L-embedding $j : \mathcal{M} \to \mathcal{N}$. We can strengthen the notion of embedding to force 4.22(a) to hold for all formulas ϕ, and not just quantifier-free ones.

DEFINITION 4.23 (Elementary embedding). Suppose $\mathcal{M}$ and $\mathcal{N}$ are L-structures with universes M and N, respectively. An L-embedding $j : \mathcal{M} \to \mathcal{N}$ is called an *elementary embedding* if for all L-formulas $\phi(x_1, \ldots, x_n)$ and all n-tuples $a \in M^n$, $\mathcal{M} \models \phi(a)$ if and only if $\mathcal{N} \models \phi(j(a))$.

If $M \subseteq N$ and the containment map is an elementary embedding, then we say that $\mathcal{M}$ is an *elementary substructure* of $\mathcal{N}$, or that $\mathcal{N}$ is an *elementary extension* of $\mathcal{M}$; and we denote this by $\mathcal{M} \preceq \mathcal{N}$.

COROLLARY 4.24. *Every isomorphism is an elementary embedding.*

PROOF. Suppose $f : \mathcal{N} \to \mathcal{M}$ is an L-isomorphism between L-structures. We need to show that for any formula $\phi(x_1, \ldots, x_n)$ and any tuple $a \in N^n$, $\mathcal{N} \models \phi(a)$ if and only if $\mathcal{M} \models \phi\big(f(a)\big)$. This is a routine induction on the complexity of ϕ. The case of ϕ atomic, as well as the inductive steps corresponding to $\neg, \wedge$ and $\vee$ are exactly as in Proposition 4.22(a). Since we can write $\forall$ as $\neg\exists\neg$, it remians to consider the case when $\phi(x) = \exists y \psi(x, y)$. In that case

$$\begin{aligned}
\mathcal{N} \models \phi(a) &\iff \mathcal{N} \models \psi(a, b) \text{ for some } b \in N \\
&\iff \mathcal{M} \models \psi\big(f(a), f(b)\big) \text{ for some } b \in N \quad \text{by the induction hypothesis} \\
&\iff \mathcal{M} \models \psi\big(f(a), c\big) \text{ for some } c \in M \quad \text{as } f \text{ is surjective} \\
&\iff \mathcal{M} \models \phi\big(f(a)\big)
\end{aligned}$$

as desired. □

By virtue of Proposition 4.22(a) the difference between substructures and elementary substructures can only be seen by considering formulas with quantifiers. For example, $(\mathbb{Z}, 0, +, -) \subseteq (\mathbb{Q}, 0, +, -)$ as the integers form a subgroup of the rationals, but $(\mathbb{Z}, 0, +, -) \not\preceq (\mathbb{Q}, 0, +, -)$ since if $\phi(x)$ is $\exists y(y+y = x)$ then $(\mathbb{Z}, 0, +, -) \models \neg\phi(1)$ while $(\mathbb{Q}, 0, +, -) \models \phi(1)$. This example can be restated as saying that the equation $y + y = 1$ has a solution in $\mathbb{Q}$ but not in $\mathbb{Z}$. In fact, this is the typical way in which substructures fail to be elementary substructures, as the following proposition explains:

PROPOSITION 4.25. *(Tarski-Vaught Test) Suppose $\mathcal{M} \subseteq \mathcal{N}$ with universes $M \subseteq N$. Then the following are equivalent:*

(i) $\mathcal{M} \preceq \mathcal{N}$

(ii) *For every L-formula $\phi(x_1, \ldots, x_n, y)$ and all n-tuples $a \in M^n$, if $\mathcal{N} \models \exists y \phi(a, y)$ then there exists $b \in M$ such that $\mathcal{N} \models \phi(a, b)$.*

PROOF. Suppose $\mathcal{M} \preceq \mathcal{N}$, and $\mathcal{N} \models \exists y \phi(a, y)$ as in the statement of (ii). Let $\psi(x) = \exists y \phi(x, y)$. By definition, since $\mathcal{N} \models \psi(a)$, we have $\mathcal{M} \models \psi(a)$. The latter means that there is a $b \in M$ such that $\mathcal{M} \models \phi(a, b)$. Applying the definition of an elementary substructure again, we have that $\mathcal{N} \models \phi(a, b)$, as desired.

For the converse we assume that (ii) holds and show by induction on the complexity of formulas $\psi(x_1, \ldots, x_n)$ that for any $a \in M^n$, $\mathcal{M} \models \psi(a)$ if and only if $\mathcal{N} \models \psi(a)$. Since $\mathcal{M} \subseteq \mathcal{N}$, this is true of all quantifier-free formulas ψ by Proposition 4.22(a). Since $\forall$ can be written as $\neg\exists\neg$, it suffices to consider the case when ψ is of the form $\exists y \phi(x_1, \ldots, x_n, y)$, and the result is known for ϕ. Now if $\mathcal{M} \models \psi(a)$ then there exists $b \in M$ such that $\mathcal{M} \models \phi(a, b)$ and so by the inductive hypothesis $\mathcal{N} \models \phi(a, b)$, and so $\mathcal{N} \models \psi(a)$. On the other hand, if

$\mathcal{N} \models \psi(a)$ then (ii) tells us that there is a $b \in M$ with $\mathcal{N} \models \phi(a, b)$, and so by the inductive hypothesis again we have $\mathcal{M} \models \phi(a, b)$, which implies that $\mathcal{M} \models \psi(a)$, as desired. □

The Tarski-Vaught test can be stated as follows: Suppose $\mathcal{M} \subseteq \mathcal{N}$. Then $\mathcal{M} \preceq \mathcal{N}$ if and only if every formula with parameters from $\mathcal{M}$ that has a realisation in $\mathcal{N}$, already has a realisation in $\mathcal{M}$. This is the right way to think about elementary extensions.

In general, it is hard to apply the Tarski-Vaught test unless we know more about the the theory of the structures involved. We will return to this theme later.

4.5. Definable sets and parameters

Suppose $\mathcal{M}$ is an L-structure with universe M, and $B \subseteq M$. Then by L_B we mean the language obtained by adding to L a new constant symbol, $\underline{b}$, for each $b \in B$. We can canonically extend $\mathcal{M}$ to an L_B-structure, denoted sometimes by $\mathcal{M}_B$, by interpreting $\underline{b}^{\mathcal{M}_B} = b$. This process is often called "naming constants". Often we drop the underscore and rely on context to distinguish between $b \in B$ and $b \in L_B^{\text{con}}$.

Definition 4.26 (Definable set). A set $X \subseteq M^n$ is *definable over* B (or B*-definable*) *in* $\mathcal{M}$ if there exists an L_B-formula $\phi(x_1, \ldots, x_n)$, such that

$$X = \{a \in M^n : \mathcal{M}_B \models \phi(a)\}.$$

In this case we write $X = \phi^{\mathcal{M}}$ and say that ϕ *defines* X. We sat that X is *definable* if it is M-definable and that it is 0-*definable* if it is $\emptyset$-definable.

Remark 4.27. Note that if $\phi(x_1, \ldots, x_n)$ is an L_B-formula then there exists an L-formula $\psi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ and a tuple $b \in B^m$, such that $\phi(x_1, \ldots, x_n) = \psi(x_1, \ldots, x_n, b)$. Hence X is B-definable if and only if $X = \{a \in M^n : \mathcal{M} \models \psi(a, b)\}$ for some L-formula $\psi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ and some $b \in B^m$.

Let us consider a few examples.

Example 4.28 (Zero sets of polynomials). Suppose $\mathcal{M} = (R, 0, 1, +, -, \times)$ where R is a ring. Then for any finite set of polynomials $p_1, \ldots, p_\ell \in R[X_1, \ldots, X_n]$, the *zero set*,

$$V(p_1, \ldots, p_\ell) := \{a \in R^n : p_1(a) = \cdots = p_\ell(a) = 0\}$$

is a definable set in $\mathcal{M}$. It follows from exercise 4.18 that the quantifier-free definable sets in $\mathcal{M}$ are exactly the finite boolean combinations of such zero sets. An immediate consequence of this is that every quantifier-free definable subset of R is either finite or cofinite.

Example 4.29 (Ordering in the ring of reals). Suppose $\mathcal{M} = (\mathbb{R}, 0, 1, +, -, \times)$ and let $\phi(x, y)$ be the formula

$$\exists z\big((z \neq 0) \wedge (y = x + z^2)\big).$$

Note that $a < b$ if and only if $\mathcal{M} \models \phi(a, b)$. So $\phi^{\mathcal{M}} \subset \mathbb{R}^2$ is the ordering on $\mathbb{R}$. Hence the ordering is 0-definable in the ring of real numbers. This answers a question we posed in the beginning of this chapter.

In particular, the set of positive real numbers is 0-definable. It follows, by example 4.28, that the ordering is *not* quantifier-free definable.

EXAMPLE 4.30 (Ordering in the ring of integers). Suppose $\mathcal{M} = (\mathbb{Z}, 0, 1, +, -, \times)$ and let $\phi(x, y)$ be the formula

$$\exists z_1 \exists z_2 \exists z_3 \exists z_4 \big((z_1 \neq 0) \wedge (y = x + z_1^2 + z_2^2 + z_3^2 + z_4^2) \big).$$

By Lagrange's theorem an integer is positive if and only if it is the sum of four squares. Hence, $m < n$ if and only if $\mathcal{M} \models \phi(m, n)$. So the ordering is also 0-definable in the integers.

EXAMPLE 4.31 (Constants in the ring of polynomials). Suppose $\mathcal{M} = (K[X], 0, 1, +, -, \times)$ where K is a field and $X = (X_1, \ldots, X_m)$ is a sequence of indeterminates. So we are dealing with the ring of polynomials in m variables over the field K. Then K is definable in $\mathcal{M}$. Indeed, K is the set of units in $K[X]$, and hence is defined by $(x = 0) \vee (\exists z(xz = 1))$.

EXAMPLE 4.32. Suppose $\mathcal{M} = (M, \in)$ where M is a set. Let $\phi(x, y)$ be the formula of example 4.14, namely $(x \in y) \wedge \forall z \big(z \in y \rightarrow (z \in x \ \vee \ z = x) \big)$. What set does $\psi(y) = \exists x \phi(x, y)$ define? At first it might seem that ψ defines the set of elements in M that are successors of elements in M. But since the variables range only over the universe M, this is not exactly correct. In fact, $\mathcal{M} \models \psi(a)$ if and only if $a \cap M = (b \cap M) \cup \{b\}$ for some $b \in M$. However, if we assume that M is a *transitive* set – that is, that every member of M is a subset of M – then indeed $\psi^{\mathcal{M}} = \{a \in M : a = S(b) \text{ for some } b \in M\}$.

The following is an alternate characterisation of the definable sets in a structure, avoiding logic – that is, making no reference to formulas and satisfaction:

PROPOSITION 4.33. *Suppose $\mathcal{M}$ is an L-structure, let $\mathrm{Def}_n(\mathcal{M})$ be the collection of all definable subsets of M^n in $\mathcal{M}$, and let $\mathrm{Def}(\mathcal{M}) := \bigcup_n \mathrm{Def}_n(\mathcal{M})$. Then $\mathrm{Def}(\mathcal{M})$ satisfies the following closure properties:*

(i) *For each n-ary function symbol f, the graph of $f^{\mathcal{M}}$ is in $\mathrm{Def}_{n+1}(\mathcal{M})$.*
(ii) *For each n-ary relation symbol R, $R^{\mathcal{M}}$ is in $\mathrm{Def}_n(\mathcal{M})$.*
(iii) *For all $i, j \leq n$, $\Delta_{i,j}^{(n)} := \{(a_1, \ldots, a_n) \in M^n : a_i = a_j\} \in \mathrm{Def}_n(\mathcal{M})$.*
(iv) *If $X \in \mathrm{Def}_n(\mathcal{M})$ then $X \times M \in \mathrm{Def}_{n+1}(\mathcal{M})$.*
(v) *Each $\mathrm{Def}_n(\mathcal{M})$ is closed under complements, unions, and intersections.*
(vi) *If $X \in \mathrm{Def}_{n+1}(\mathcal{M})$ and $\pi : M^{n+1} \rightarrow M^n$ is the projection onto the first n co-ordinates, then $\pi(X) \in \mathrm{Def}_n(\mathcal{M})$.*
(vii) *If $X \in \mathrm{Def}_{n+m}(\mathcal{M})$ and $b \in M^m$ then $X_b := \{a \in M^n : (a, b) \in X\} \in \mathrm{Def}_n(\mathcal{M})$.*

Moreover, $\mathrm{Def}(\mathcal{M})$ is the smallest collection of subsets of cartesian powers of M satisfying (i) through (vii).

PROOF. We first show that $\mathrm{Def}(\mathcal{M})$ satisfies (i) through (vii):

(i) The graph of $f^{\mathcal{M}}$ is defined by $\big(f(x_1, \ldots, x_n) = x_{n+1}\big)$.
(ii) $R^{\mathcal{M}}$ is defined by $R(x_1, \ldots, x_n)$.
(iii) $\Delta_{i,j}^{(n)} = \phi^{\mathcal{M}}$ where $\phi(x_1, \ldots, x_n)$ is the formula $(x_i = x_j)$.
(iv) If X is defined by $\phi(x_1, \ldots, x_n)$ then $X \times M$ is defined by $\psi(x_1, \ldots, x_n, x_{n+1})$, where $\psi = \phi$.
(v) If X is defined by $\phi(x_1, \ldots, x_n)$ and Y is defined by $\psi(x_1, \ldots, x_n)$ then $M^n \setminus X$ is defined by $\neg\phi$, $X \cup Y$ is defined by $\phi \vee \psi$, and $X \cap Y$ is defined by $\phi \wedge \psi$.
(vi) If X is defined by $\phi(x_1, \ldots, x_{n+1})$ then $\pi(X)$ is defined by $\exists x_{n+1} \phi(x_1, \ldots, x_n, x_{n+1})$.

(vii) If X is defined by $\phi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ then X_b is defined by $\phi(x_1, \ldots, x_n, \underline{b})$.

Next we show that if $D = \bigcup_n D_n$ with $D_n \subseteq \mathcal{P}(M^n)$ satisfies (i) through (vii), then all definable sets are in D. One thing that will be useful is to note that (iii), (iv) and (vi) imply D is preserved by co-ordinate permutations. We begin with the claim

CLAIM 4.34. *For each L-term $t(x_1, \ldots, x_n)$, the graph of $t^{\mathcal{M}}$ is in D_{n+1}.*

PROOF OF CLAIM 4.34. This is by induction on the complexity of the term t. If t is x_i then the graph of $t^{\mathcal{M}}$ is $\Delta^{(n+1)}_{i,n+1}$. If t is a constant c, then the graph of $t^{\mathcal{M}}$ is $\big(\Delta^{(n+1)}_{1,1}\big)_{c^{\mathcal{M}}}$. Finally suppose t is $f(t_1, \ldots, t_m)$ where f is an m-ary function symbol and $t_1, \ldots, t_m$ are L-terms for which we know the claim. So by repeated use of (iv) we have that $\Gamma(t_i^{\mathcal{M}}) \times M^m \in D_{n+m+1}$. Hence, for each $i \leq m$, by permuting co-ordinates,

$$\{(a_1, \ldots, a_n, b_1, \ldots, b_m, c) : t_i^{\mathcal{M}}(a_1, \ldots, a_n = b_i\} \in D_{n+m+1}.$$

Also, by (i) and (iv) and permuting co-ordinates again, we have

$$\{(a_1, \ldots, a_n, b_1, \ldots, b_m, c) : f^{\mathcal{M}}(b_1, \ldots, b_m = c\} \in D_{n+m+1}.$$

Taking intersections and projecting onto the appropriate $n+1$ co-ordinates – by repeated applications of (vi) after a co-ordinate permutation – we get that

$$\Gamma(t^{\mathcal{M}}) = \{(a_1, \ldots, a_n, c) : f^{\mathcal{M}}\big(t_1^{\mathcal{M}}(a_1, \ldots, a_n), \ldots, t_m^{\mathcal{M}}(a_1, \ldots, a_n)\big) = c\} \in D_{n+1}$$

as desired. □

Now, using the claim, as well as properties (i) through (vi) as we have been doing, it is not hard to show by induction on L-formulas that all 0-definable sets are in D. By (vii), every definable set is in D. □

How can we show that some set is not definable?

EXERCISE 4.35. *Suppose $\mathcal{M}$ is an L-structure and $\kappa = \max\{\aleph_0, |L|, |M|\}$. Show that there are at most κ-many definable sets in $\mathcal{M}$. Deduce that if $\mathcal{M}$ is infinite and of cardinality at least that of the language, then there exists non-definable subsets of M^n for all $n > 0$.*

The above exercise is just counting, but the following lemma gives us one tool for actually showing that a set is not definable.

LEMMA 4.36. *If $X \subset M^n$ is B-definable and f is an L-automorphism of $\mathcal{M}$ fixing B pointwise, then $f(X) = X$.*

PROOF. Suppose $X = \phi^{\mathcal{M}}$ where $\phi(x_1, \ldots, x_n)$ is an L_B-formula. Then $\phi(x) = \psi(x, b)$ for some tuple $b \in B^m$ and L-formula ϕ. Now

$$\begin{aligned} a \in X &\iff \mathcal{M} \models \psi(a, b) \\ &\iff \mathcal{M} \models \psi\big(f(a), f(b)\big) \quad \text{by Corollary 4.24} \\ &\iff \mathcal{M} \models \psi\big(f(a), b\big) \quad \text{as } f(b) = b \\ &\iff f(a) \in X \end{aligned}$$

as desired. □

Together with some knowledge about the automorphisms of a structure, this can be used to produce non-definable sets.

COROLLARY 4.37. *The real numbers are not definable in* $(\mathbb{C}, 0, 1, +, -, \times)$.

PROOF. Suppose toward a contradiction that they were. Then they would be definable over some finite set $B \subset \mathbb{C}$. Since the transcendence degree of $\mathbb{R}$ over $\mathbb{Q}$ is infinite, there exists $r \in \mathbb{R} \setminus \mathbb{Q}(B)^{\text{alg}}$. Now choose $s \in \mathbb{C} \setminus \mathbb{Q}(B, r)^{\text{alg}}$ such that s is not real (check that this is possible!). Since s and r are algebraically independent over $\mathbb{Q}(B)$, there is an L-automorphism f of $\mathbb{C}$ that takes r to s and fixes $\mathbb{Q}(B)$ pointwise. But then $f(\mathbb{R}) \neq \mathbb{R}$ contradicting Lemma 4.36. □

EXERCISE 4.38. *Show that the addition is not definable in* $(\mathbb{R}, <)$.

This method of proving that something is not definable relies on the existence of many automorphisms. When a structure does not have many automorphisms one has to work harder to understand which sets are definable and which are not. For example, $(\mathbb{R}, 0, 1, +, -, \times)$ has no automorphisms except the identity (why?). So to prove, for example, that the integers are not definable in this structure (and they aren't) requires a more thorough understanding of what the definable sets look like. One has to first prove a "quantifier elimination theorem". We will return to this important theme in model theory later.

4.6. Theories and their models

Model theory can be described as the study of the definable sets in a given structure on the one hand, as well as the study of classes of structures that are axiomatisable by a first-order theory, on the other. Having introduced definable sets in the previous section, we now discuss theories and their models.

DEFINITION 4.39. An *L-theory* is a set of L-sentences. A *model* of a theory T is an L-structure $\mathcal{M}$ such that $\mathcal{M} \models \sigma$ for each $\sigma \in T$. This is written $\mathcal{M} \models T$. If T has a model then it is said to be *consistent*.

We denote the class of all models of a theory T by $\text{Mod}(T)$. A class $\mathcal{K}$ of L-structures is called *elementary* or *axiomatisable* if there exists an L-theory T such that $\mathcal{K} = \text{Mod}(T)$.

Given an L-structure $\mathcal{M}$, by the *theory of* $\mathcal{M}$, denoted by $\text{Th}(\mathcal{M})$, we mean the set of all L-sentences true in $\mathcal{M}$. Two structures $\mathcal{M}$ and $\mathcal{N}$ are *elementarily equivalent*, denoted by $\mathcal{M} \equiv \mathcal{N}$, if $\text{Th}(\mathcal{M}) = \text{Th}(\mathcal{N})$.

Given a theory T and a sentence σ, we write $T \models \sigma$, and say that T *entails* σ, or that σ is a *consequence of* T, if $\mathcal{M} \models \sigma$ for every model $\mathcal{M}$ of T. We say that T is *complete* if for every L-sentence σ, either $T \models \sigma$ or $T \models \neg\sigma$.

Let's consider some examples of theories.

EXAMPLE 4.40. (a) Suppose $L = \{e, \cdot, ^{-1}\}$ is the language of (multiplicatively written) groups made up of a constant symbol e, a binary function symbol $\cdot$, and a unary function symbol $^{-1}$. The following classes of L-structures are axiomatisable: groups, abelian groups, torsion-free groups, groups of order N (for any fixed N), divisible groups. I leave it to you to write down the L-theories. Let me only point out

that the torsion-free groups require infinitely many sentences, including the sentence $\forall x\big((x = e) \vee \neg(x^n = e)\big)$ for each n, where x^n is just an abbreviation for the product of x with itself n-times. Divisible groups also require infinitely many axioms. We will see later that the class of torsion groups is not elementary.

(b) Suppose $L = \{0, 1, +, -, \times\}$ is the langauge of rings. The following classes of L-structures are elementary: rings, integral domains, fields, algebraically closed fields, algebraically closed fields of characteristic p (for any fixed prime p or $p = 0$). Again I leave it to you to write the appropriate L-sentences, mentioning only that algebraic closure is expressed by the sentences

$$\forall a_0 \ldots \forall a_n \exists x\big(x^n + \sum_{i=0}^{n-1} a_i x^i = 0\big),$$

one for each $n \geq 1$. Characteristic p for a prime p is expressed by $\forall x(px = 0)$, while characteristic zero requires the negation of all the above sentences as p ranges over all primes. As we will see later, the class of all finite fields is not axiomatisable.

(c) Suppose $L = \{R\}$ is the language consisting of a single binary relation symbol. The following classes of L-structures are elementary: graphs (antireflexivity and symmetry), posets, linear orders, dense linear orders, discrete linear orders (where every element has a least greater element), equivalence relations.

(d) For any fixed field K the class of K-vector spaces is an elementary class of L-structures where $L = \{0, +, -, \lambda_a : a \in K\}$.

(e) Suppose $L = \emptyset$. The class of sets and the class of infinite sets are both axiomatisable as L-structures. The former is given by the empty theory, the latter by the infinite theory with sentences saying that there are at least n elements, one for each $n \geq 1$. The class of finite sets is not elementary, as we shall see later.

(f) Let $L = \{\in\}$. The class of all set of sets (or *universes* of sets) that satisfy the Zermelo-Fraenkel axioms is axiomatisable. Indeed, the Zermelo-Fraenkel axioms can all be expressed as L-sentences, once we insist that by "definite" property or function we mean a property or function that can be expressed by an L-formula. It is not known (and indeed is in some sense impossible to prove) that ZF is consistent.

LEMMA 4.41. (a) *For any L-structure $\mathcal{M}$, $\mathrm{Th}(\mathcal{M})$ is a complete consistent theory which contains all its consequences.*

(b) *Suppose T is a consistent theory. The following are equivalent:*
   (i) *T is complete*
   (ii) *The set of consequences of T is a maximally consistent theory.*
   (iii) *The set of consequences of T is of the form $\mathrm{Th}(\mathcal{M})$ for some (equivalently any) $\mathcal{M} \models T$.*
   (iv) *Any two models of T are elementarily equivalent.*

(c) *If $j : \mathcal{M} \to \mathcal{N}$ is an elementary embedding then $\mathcal{M} \equiv \mathcal{N}$. In particular, isomorphic structures are elementarily equivalent.*

PROOF. The completeness of $\mathrm{Th}(\mathcal{M})$ follows from the fact that for every σ, either $\mathcal{M} \models \sigma$ or $\mathcal{M} \models \neg\sigma$. Consistency, as well as the fact that $\mathrm{Th}(\mathcal{M})$ contains all its consequences, is immediate from the definitions.

For part (b) let T' be the set of consequences of T. Suppose T is complete. If $T' \subsetneq S$ then there is some $\sigma \in S \setminus T'$. Hence $T \models \neg\sigma$ and so $\sigma, \neg\sigma \in S$. This implies that S has no models. So T' is maximally consistent, as desired. Now assume the maximality of T' and let $\mathcal{M} \models T$. Then $T' \subseteq \mathrm{Th}(\mathcal{M})$ and so by the consistency of $\mathrm{Th}(\mathcal{M})$ we must have $T' = \mathrm{Th}(\mathcal{M})$. We have shown that if T' is maximally consistent then $T' = \mathrm{Th}(\mathcal{M})$ for some $\mathcal{M} \models T$. Now assume $T' = \mathrm{Th}(\mathcal{M})$ for some $\mathcal{M} \models T$. Suppose $\mathcal{N} \models T$. Then $\mathcal{N} \models \mathrm{Th}(\mathcal{M})$, and so $\mathrm{Th}(\mathcal{M}) \subseteq \mathrm{Th}(\mathcal{N})$. So by part (a), $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{N})$. Finally, assume that every two models of T are elementarily equivalent. Suppose σ is a sentence such that $T \not\models \sigma$. Then there exists $\mathcal{M} \models T$ such that $\mathcal{M} \models \neg\sigma$. As every other model of T is elementarily equivalent to $\mathcal{M}$, $\neg\sigma$ is true in every model of T. That is $T \models \neg\sigma$. Hence T is complete.

Part (c) follows from the $n = 0$ case of the definition of an elementary embedding (Definition 4.23). Since isomorphisms are elementary embeddings (Corollary 4.24), isomorphic structures are elementarily equivalent. □

Note that the converse to part (c) is false: there exist elementarily equivalent substructures that are not elementary substructures. For example $(\mathbb{N} \setminus \{0\}, <) \subseteq (\mathbb{N}, <)$ and the map $n \mapsto n - 1$ shows that $(\mathbb{N} \setminus \{0\}, <)$ is isomorphic to, and hence elementarily equivalent to, $(\mathbb{N}, <)$. But $(\mathbb{N} \setminus \{0\}, <)$ is not an elementary substructure since the formula $y < 1$ has a realisation in $(\mathbb{N}, <)$ but not in $(\mathbb{N} \setminus \{0\}, <)$. The connection between these notions is explained by the following exercise:

Exercise 4.42. *Suppose $\mathcal{M} \subseteq \mathcal{N}$ with universes $M \subseteq N$. Then $\mathcal{M} \preceq \mathcal{N}$ if and only if $\mathcal{M}_M \equiv \mathcal{N}_M$. More generally, for any two L-structures $\mathcal{M}$ and $\mathcal{N}$, there is an elementary embedding $j : \mathcal{M} \to \mathcal{N}$ if and only if $\mathcal{N}$ can be expanded to a model of $\mathrm{Th}(\mathcal{M}_M)$.*

The following proposition shows that if a complete theory has a finite model then in fact it has only one model up to isomorphism.

Proposition 4.43. *Suppose $\mathcal{M}$ and $\mathcal{N}$ are* finite *structures. That is their universes, M and N respectively, are finite sets. Then $\mathcal{M} \equiv \mathcal{N}$ if and only if $\mathcal{M}$ and $\mathcal{N}$ are isomorphic.*

Proof. As we have just remarked, the right-to-left direction is always true (without the finiteness assumption) by Corollary 4.24. For the other direction, assume $\mathcal{M} \equiv \mathcal{N}$ are finite elementarily equivalent structures. Then $|M| = |N|$ (why?). Suppose $M = \{a_1, \ldots, a_n\}$. For $k < n$, having found $\{b_1, \ldots, b_k\}$ inductively, we find b_{k+1} as follows: Let $X_{k+1,1}, \ldots, X_{k+1,m_{k+1}}$ be all the $\{a_1, \ldots, a_k\}$-definable subsets of M containing a_{k+1}. (There are only finitely many as $\mathcal{P}(M)$ is finite.) Choose and fix formulas $\phi_{k+1,1}(x), \ldots, \phi_{k+1,m_{k+1}}(x)$ defining $X_{k+1,1}, \ldots, X_{k+1,m_{k+1}}$, respectively. Now $\mathcal{M} \models \bigwedge_{i=1}^{m_{k+1}} \phi_{k+1,i}(a_{k+1})$. Hence $\mathcal{M} \models \exists x \bigwedge_{i=1}^{m_{k+1}} \phi_{k+1,i}(x)$, and so $\mathcal{N} \models \exists x \bigwedge_{i=1}^{m_{k+1}} \phi_{k+1,i}(x)$. Let $b_{k+1} \in N$ realise this formula. In this way, we eventually construct $N = \{b_1, \ldots, b_n\}$. Then it is not hard to check that the map $a_i \mapsto b_i$ is an isomorphism. □

Hence, one is usually interested in complete theories with infinite models.

Exercise 4.44. *Suppose T is a complete and consistent theory. If T has one infinite model then every model is infinite.*

CHAPTER 5

Compactness and Consequences

The compactness theorem for first-order logic is of fundamental importance and is the starting point for model theory and its applications.

THEOREM 5.1 (Compactness Theorem). *Suppose L is a language and T is an L-theory. T is consistent if and only if every finite subset of T is consistent.*

Here is an equivalent formulation.

COROLLARY 5.2. *Suppose T is an L-theory and σ is an L-structure. Then $T \models \sigma$ if and only if there exists a finite subset $\Sigma \subseteq T$ such that $\Sigma \models \sigma$.*

PROOF. Observe that $T \models \sigma$ if and only if $T \cup \{\neg\sigma\}$ is inconsistent. □

In many texts the compactness theorem is seen as an immediate consequence of Gödel's completeness theorem, which says that T is consistent if and only if there is no "formal derivation" of a contradiction using the sentences in T as assumptions. The finite character of derivations then implies the Compactness Theorem. This approach however takes us into the realm of proof theory, which it is our intention in this course to avoid. We will present an attractive "algebraic" proof of the compactness theorem using ultraproducts; a subject of interest in its own right.

5.1. A proof of compactness using ultraproducts

DEFINITION 5.3 (Filter). Suppose I is a nonempty set. A subset $\mathcal{F} \subseteq \mathcal{P}(I)$ is called a *filter on I* if the following conditions hold:

(i) $I \in \mathcal{F}$ and $\emptyset \notin \mathcal{F}$.
(ii) If $A, B \in \mathcal{F}$ then $A \cap B \in \mathcal{F}$.
(iii) If $A \subseteq B$ and $A \in \mathcal{F}$ then $B \in \mathcal{F}$.

It is reasonable to think of a filter as giving a notion of "bigness" for subsets of I. Here are some examples:

- $\{\mathbb{R} \setminus X \ : \ X$ has Lebesgue measure $0\}$ is a filter on $\mathbb{R}$.
- Suppose I is any infinite set and κ is an infinite cardinal such that $\kappa \leq |I|$. Then $\{I \setminus X \ : \ |X| < \kappa\}$ is a filter on I. In particular the set of all cofinite subsets of I forms a filter, called the *Frechet filter*.
- Suppose I is any nonempty set. A *principal filter* on I is a filter of the form $\{A \subseteq I \ : \ x \in A\}$ for some fixed $x \in I$.

An *ultrafilter* on I is a maximal filter; that is, a filter not properly contained in any other filter on I. It is not hard to see that every principal filter is an ultrafilter – any larger filter would contain a set that does not contain x and hence its intersection with $\{x\}$, which is

also in the filter, would be $\emptyset$, contradicting the fact that $\emptyset$ is not a member of any filter. It is rather difficult to describe nonprincipal ultrafilters. However they do exist by Zorn's Lemma (and hence in ZFC). Indeed, start with any filter $\mathcal{F}$ and consider all the filters on I extending $\mathcal{F}$. As the union of a chain of filters is a filter, there exists an ultrafilter $\mathcal{U}$ containing $\mathcal{F}$. If $\mathcal{F}$ was the Frechet filter on I (the set of all cofinite subsets of I), for example, then $\mathcal{U}$ cannot be principal (as for any $x \in I$, $I \setminus \{x\} \in \mathcal{F} \subseteq \mathcal{U}$).

LEMMA 5.4. *A filter $\mathcal{U}$ is an ultrafilter if and only if for every $A \subseteq I$, either $A \in \mathcal{U}$ or $I \setminus A \in \mathcal{U}$.*

PROOF. The right-to-left direction is clear: if $\mathcal{U} \subsetneq \mathcal{F}$ then there is $A \in \mathcal{F} \setminus \mathcal{U}$. Since $\mathcal{F}$ is closed under intersections and does not contain $\emptyset$, $I \setminus A \notin \mathcal{F}$. Hence neither A nor $I \setminus A$ are in $\mathcal{U}$. For the left-to-right direction, suppose $\mathcal{U}$ is an ultrafilter and $A \notin \mathcal{U}$. Consider $\mathcal{F} = \{X \subseteq I \ : \ Y \setminus A \subseteq X \text{ for some } Y \in \mathcal{U}\}$. Then it is not hard to see that $\mathcal{F}$ is a filter containing $\mathcal{U}$. Hence $\mathcal{U} = \mathcal{F}$. But $I \setminus A \in \mathcal{F}$. □

DEFINITION 5.5 (Ultraproduct). Suppose L is a language, I is an infinite set, and $\mathcal{M}_i$ is an L-structure for each $i \in I$. Let $\mathcal{U}$ be an ultrafilter on I. The *ultraproduct of* $\{\mathcal{M}_i : i \in I\}$ *with respect to* $\mathcal{U}$ will be the L-structure $\mathcal{M}$ given as follows:

- The universe of $\mathcal{M}$ is $M := \big(\prod_{i\in I} M_i\big)/E$ where E is the equivalence relation given by: fEg if $\{i \in I : f(i) = g(i)\} \in \mathcal{U}$. That is, fEg if the indices on which sequences f and g agree is a member of the ultrafilter $\mathcal{U}$.
- For every constant symbol $c \in L^{\text{con}}$, set $c^{\mathcal{M}}$ to be the E-class of the sequence $f : I \to \bigcup_{i\in I} M_i$ given by $f(i) = c^{\mathcal{M}_i}$ for each $i \in I$.
- For every function symbol $f \in L^{\text{fun}}$, and all $g_1, \ldots, g_{n_f} \in M$, define $f^{\mathcal{M}}(g_1/E, \ldots, g_{n_f}/E)$ to be g/E where $g : I \to \bigcup_{i\in I} M_i$ is the sequence $g(i) = f^{\mathcal{M}_i}\big(g_1(i), \ldots, g_{n_f}(i)\big)$. Check that this definition does not depend on the choice of representative $g_1, \ldots, g_{n_f}$.
- For every relation symbol $R \in L^{\text{rel}}$, define $R^{\mathcal{M}} \subseteq M^{k_R}$ as follows: for all $g_1, \ldots, g_{k_R} \in M$, $(g_1/E, \ldots, g_{k_R}/E) \in R^{\mathcal{M}}$ if and only if $\{i \in I : \big(g_1(i), \ldots, g_{k_R}(i)\big) \in R^{\mathcal{M}_i}\} \in \mathcal{U}$. Check that this does not depend on the choice of representatives $g_1, \ldots, g_{k_R}$.

We often denote the ultraproduct by $\big(\prod_{i\in I} \mathcal{M}_i\big)/\mathcal{U}$.

The following lemma points out that if we start with a principal ultrafilter then this construction does not produce anything new.

LEMMA 5.6. *Suppose $\{\mathcal{M}_i : i \in I\}$ is a set of L-structures, $j \in I$, and $\mathcal{U}_j$ is the principal ultrafilter $\{X \subseteq I : j \in X\}$. Then the jth projection map, $\pi : \prod_{i\in I} M_i \to M_j$, induces an isomorphism from $\big(\prod_{i\in I} \mathcal{M}_i\big)/\mathcal{U}_j$ to $\mathcal{M}_j$.*

PROOF. Note that a set of indices is in the ultrafilter if and only if it contains j. So if gEg' then $g(j) = g'(j)$. Hence π does induce a map from the universe of $\big(\prod_{i\in I} \mathcal{M}_i\big)/\mathcal{U}_j$ to M_j. That it is surjective is clear, and that it is an L-embedding is not hard to check from the definitions. □

PROPOSITION 5.7 (Łoś' Theorem). *Suppose $\mathcal{M} = \big(\prod_{i\in I} \mathcal{M}_i\big)/\mathcal{U}$ where $\{\mathcal{M}_i : i \in I\}$ is a set of L-structures and $\mathcal{U}$ is an ultrafiler on I. Suppose $\phi(x_1, \ldots, x_n)$ is an L-formula, and*

$g_1, \ldots, g_n \in \prod_{i \in I} M_i$. *Then* $\mathcal{M} \models \phi(g_1/E, \ldots, g_n/E)$ *if and only if*

$$\{i \in I : \mathcal{M}_i \models \phi\big(g_1(i), \ldots, g_n(i)\big)\} \in \mathcal{U}.$$

In particular, for an L-sentence σ, $\mathcal{M} \models \sigma$ *if and only if* $\{i \in I : \mathcal{M}_i \models \sigma\} \in \mathcal{U}$.

PROOF. First of all, one observes that *if* $t(x_1, \ldots, x_n)$ *is an L-term and* $g_1, \ldots, g_n \in \prod_{i \in I} M_i$, *then*

$$t^{\mathcal{M}}(g_1/E, \ldots, g_n/E)(i) = t^{\mathcal{M}_i}\big(g_1(i), \ldots, g_n(i)\big)$$

for each $i \in I$. Indeed, this claim follows very easily by induction on the complexity of t using the fact that the corresponding statement is by definition true of function symbols.

The proof of Łoś' Theorem is now a straightforward induction on the complexity of ϕ. The atomic case is an immediate consequence of the above claim on terms (and the definition of the ultraproduct). The inductive steps of $\neg$, $\wedge$, and $\vee$ are easily verified using properties of ultrafilters; namely Lemma 5.4 (for $\neg$), that ultrafilters are closed under intersections (for $\wedge$), and that they are closed under unions (for $\vee$). As usual the case of the universal quantifier is reduced to that of the existential quantifier. So it remains to prove that if we know Łoś theorem for $\psi(x_1, \ldots, x_n, y)$ then it follows for $\exists y \psi$. By the inductive hypothesis

$$\mathcal{M} \models \exists y \psi(g_1/E, \ldots, g_n/E, y)$$

if and only if

$$\text{there exists } f \in \prod_{i \in I} M_i \text{ such that } X_f := \{i \in I : \mathcal{M}_i \models \psi\big(g_1(i), \ldots, g_n(i), f(i)\big)\} \in \mathcal{U}$$

Now X_f is contained in $Y := \{i \in I : \mathcal{M}_i \models \exists y \psi\big(g_1(i), \ldots, g_n(i), y\big)\}$, and since ultrafilters are preserved under supersets, we see that if $\mathcal{M} \models \exists y \psi(g_1/E, \ldots, g_n/E, y)$ then $Y \in \mathcal{U}$. Conversely, suppose $Y \in \mathcal{U}$. For each $i \in Y$ choose $a_i \in M_i$ such that $\mathcal{M}_i \models \psi\big(g_1(i), \ldots, g_n(i), a_i\big)$. Define $f : I \to \bigcup_{i \in I} M_i$ by setting $f(i) = a_i$ for $i \in Y$, and anything otherwise. Then, X_f will contain Y and hence $X_f \in \mathcal{U}$. By the above equivalence, this means that $\mathcal{M} \models \exists y \psi(g_1/E, \ldots, g_n/E, y)$. □

As a corollary we can prove the compactness theorem. Let T be an L-theory each of whose finite subsets are consistent. Let I be the set of finite subsets of T. For each $i \in I$, let $\mathcal{M}_i$ be a model of i. Also for each $i \in I$, let X_i be the set of finite subsets of T extending i. Note that $\{X_i : i \in I\}$ does not include the empty set, does include I (indeed, $I = X_\emptyset$), and is closed under intersections (as $X_i \cap X_j = X_{i \cup j}$). Hence $\mathcal{F} := \{X \subseteq I : X_i \subseteq X \text{ for some } i \in I\}$ is a filter on I. Extend $\mathcal{F}$ to an ultrafilter $\mathcal{U}$ on I. Let $\mathcal{M} := \big(\prod_{i \in I} \mathcal{M}_i\big)/\mathcal{U}$. I claim that $\mathcal{M} \models T$. Indeed, let $\sigma \in T$. If $j \in X_{\{\sigma\}}$ – that is, if j is a finite subset of T containing σ – then $\mathcal{M}_j \models \sigma$ since $\mathcal{M} \models j$. Hence, $\{i \in I : \mathcal{M}_i \models \sigma\}$ contains $X_{\{\sigma\}}$, and the latter is a member of $\mathcal{F}$ (and hence $\mathcal{U}$) by construction. So $\{i \in I : \mathcal{M}_i \models \sigma\} \in \mathcal{U}$. By Łoś' theorem, $\mathcal{M} \models \sigma$. So $\mathcal{M} \models T$. This completes the proof of the compactness theorem. □

In fact, Łoś' Theorem tells us more:

COROLLARY 5.8. *Suppose* $\mathcal{M}$ *is an L-structure,* I *is a nonempty set, and* $\mathcal{U}$ *is an ultrafilter on* I. *Then the diagonal induces an elementary embedding* $\mathcal{M} \to (\prod_{i \in I} \mathcal{M})/\mathcal{U}$.

PROOF. For each $a \in M$ let $f_a \in \prod_{i\in I} M$ be given by $f_a(i) = a$ for all $i \in I$. Then the map induced by the diagonal is the one that takes a to f_a/E. Suppose $\phi(x_1, \ldots, x_n)$ is an L-formula and $a_1, \ldots, a_n \in M$. Then

$$\begin{aligned}
\mathcal{M} \models \phi(a_1, \ldots, a_n) &\implies \mathcal{M} \models \phi(f_{a_1}(i), \ldots, f_{a_n}(i)) \text{ for each } i \\
&\implies \{i \in I : \mathcal{M} \models \phi(f_{a_1}(i), \ldots, f_{a_n}(i))\} = I \in \mathcal{U} \\
&\implies (\prod_{i\in I} \mathcal{M})/\mathcal{U} \models \phi(f_{a_1}/E, \ldots, f_{a_n}/E) \quad \text{by Łoś' Theorem}
\end{aligned}$$

Conversely if $\{i \in I : \mathcal{M} \models \phi(f_{a_1}(i), \ldots, f_{a_n}(i))\} \in \mathcal{U}$, then this set is nonempty and hence $\mathcal{M} \models \phi(f_{a_1}(i), \ldots, f_{a_n}(i))$ for some $i \in I$. As each $f_{a_j}(i) = a_j$, $\mathcal{M} \models \phi(a_1, \ldots, a_n)$, as desired. □

Such an ultraproduct, $\prod_{i\in I} \mathcal{M}/\mathcal{U}$ is called an *ultrapower* and often denoted by $\mathcal{M}^I/\mathcal{U}$. So we have that every structure elementarily embeds in every ultrapower of itself. Identifying $\mathcal{M}$ with its image under the diagonal, we see that this gives us a very useful technique for producing elementary extensions.

For example, suppose $\mathcal{R} = (\mathbb{R}, 0, 1, +, -, \times, <)$ and let $\mathcal{U}$ be an ultrafilter on ω that extends the Frechet filter. Let $\epsilon := (\frac{1}{n+1} : n \in \omega)/E$, which is an element of the universe of the elementary extension $\mathcal{R}^* := \mathcal{R}^\omega/\mathcal{U}$. Łoś' theorem implies that $\mathcal{R}^* \models (0 < \epsilon)$ but $\mathcal{R}^* \models (\epsilon < r)$ for every positive real number r. Indeed, $\{n : \frac{1}{n+1} < r\}$ is cofinite, hence in the Frechet filter and hence in $\mathcal{U}$. Such an ϵ is called an *infinitesimal*. So we have shown that there exist elementary extensions of the reals with infinitesimals. This is the beginning of *nonstandard analysis*. (Note that we are viewing $\mathcal{R} \preceq \mathcal{R}^*$ by identifying $\mathcal{R}$ with its image under the diagonal.)

5.2. Some typical applications of compactness

PROPOSITION 5.9. *Let $L = \{0, +, -\}$ be the language of (additively written) groups. The class of torsion groups is not axiomatisable.*

PROOF. Suppose T was an axiomatisation of the torsion groups. Consider the language $L' := L \cup \{c\}$ where we have added a new constant symbol. Let T' be the L'-theory $T \cup \{nc \neq 0 : n > 0\}$. *We claim that T' is consistent.* Indeed, if Σ is a finite subset of T' then, for some $\ell > 0$, Σ is contained in $T \cup \{nc \neq 0 : n = 1, \ldots, \ell\}$. Now $(\mathbb{Z}/(\ell+1)\mathbb{Z}, 0, +, -)$ is a torsion group, and if we interpret c as 1 then we get a model of $T \cup \{nc \neq 0 : n = 1, \ldots, \ell\}$. Hence Σ is consistent. So by compactness, T' is consistent. But this is absurd since in any model, which must be a torsion group, the interpretation of c will be torsion free. □

The compactness thoerem can also be used to show that certain elementary classes are not *finitely* axiomatisable.

PROPOSITION 5.10. *Let $L = \{0, +, -\}$ be the language of (additively written) groups. The class of torsion free groups is not finitely axiomatisable.*

PROOF. Suppose it were and seek a contradiction. Let σ be the conjunction of the (finitely many) sentences in this finite axiomatisation of the torsion free groups. Let T be the natural axiomatisation of the class of torsion free groups. That is, T is made up of the axioms for groups, G, together with sentences τ_n, saying $\forall x(x \neq 0 \to nx \neq 0)$, for each $n > 0$ (see Example 4.40(a)). So $T \models \sigma$. Hence, by compactness, there exists an $\ell > 0$ such that $G \cup \{\tau_1 \ldots, \tau_\ell\} \models \sigma$. But then $\mathbb{Z}/p\mathbb{Z} \models \sigma$, if p is chosen to be a prime greater than ℓ. But this contradicts the assumption that σ axiomatises torsion free groups. □

Here is another typical use of the compactness theorem, similar to that of Proposition 5.9 above, though the same result could be obtained more explicitly using ultrapowers (how?).

PROPOSITION 5.11. *There exists an elementary extension of* $\mathcal{Q} = (\mathbb{Q}^{\text{alg}}, 0, 1, +, -, \times)$ *with a transcendental element.*

PROOF. Let L be the language of rings and let $L' = L_{\mathbb{Q}^{\text{alg}}} \cup \{c\}$ where c is a new constant symbol. Consider the L'-theory

$$T = \text{Th}(\mathcal{Q}_{\mathbb{Q}^{\text{alg}}}) \ \cup \ \{p(c) \neq 0 : p \in \mathbb{Q}[X], p \neq 0\}$$

By compactness, T is consistent – $\mathcal{Q}$ itself is a model for any finite subset of T by interpreting c to be a an algebraic number whose minimal polynomial over $\mathbb{Q}$ is of sufficiently large degree. Suppose $\mathcal{M}' \models T$ and let $\mathcal{M}$ be the reduct of $\mathcal{M}'$ to L. By Exercise 4.42, there is an elementary embedding of $\mathcal{Q}$ in $\mathcal{M}$; this is just the map that takes $q \in \mathbb{Q}^{\text{alg}}$ to the interpretation of $\underline{q}$ in $\mathcal{M}'$. Finally, the interpretation of c in $\mathcal{M}'$ gives us a transcendental element in $\mathcal{M}$. □

What Proposition 5.11 tells us is that the algebraicity of the algebraic closure of $\mathbb{Q}$ is not part of the first-order theory of the structure, even after naming all parameters.

5.3. Löwenheim-Skolem and Vaught

THEOREM 5.12 (The Löwenheim-Skolem Theorem). *Suppose L is a language and $\mathcal{M}$ is an infinite L-structure.*

(a) *Suppose $A \subseteq M$. Then there exists an elementary substructure of $\mathcal{M}$ that contains A and is of cardinality* $\max\{|A|, |L|, \aleph_0\}$.
(b) *Suppose $\kappa \geq \max\{|M|, |L|\}$. Then there exists an elementary extension of $\mathcal{M}$ of cardinality κ.*

PROOF. For part (a), let $\kappa = \max\{|A|, |L|, \aleph_0\}$. If $|M| = \kappa$ then we are done, so we may assume that $|M| > \kappa$. Now by increasing A if necessary we may also assume that $|A| = \kappa$.

We define recursively a countable chain of sets of cardinality κ, $A = A_0 \subseteq A_1 \subseteq \cdots \subseteq M$ such that: *for each $n \geq 0$, if $\phi(y)$ is any L_{A_n}-formula with $\mathcal{M} \models \exists y \phi(y)$, then there exists $a \in A_{n+1}$ with $\mathcal{M} \models \phi(a)$.* Given A_n we construct A_{n+1} as follows: First observe that an L_{A_n}-formula is a finite string from a set of symbols of size $|L| + |A_n| + \aleph_0 = \kappa$. Hence the set of all L_{A_n}-formulas of the form $\phi(y)$ such that $\mathcal{M} \models \exists y \phi(y)$ has cardinality at most $\sum_{n \in \omega} \kappa^n = \kappa$. For each such formula, we choose a realisation and include it in A_{n+1}. Note that $A_n \subseteq A_{n+1}$ (consider the formulas $(y = a)$ for each $a \in A_n$), $|A_{n+1}| = \kappa$, and A_{n+1} satisfies

the desired property. Having constructed the chain, let $B := \sum_{n\in\omega} A_n$. Then $|B| = \kappa$ and for every L_B-formula $\phi(y)$ with $\mathcal{M} \models \exists y\phi(y)$, there exists $b \in B$ such that $\mathcal{M} \models \phi(a)$. Hence B contains all the constants of $\mathcal{M}$ (consider the formulas $y = c$ for each $c \in L^{\text{con}}$), and is preserved under all the basic function of $\mathcal{M}$ (consider the formulas $y = F(b_1, \ldots, b_{n_f})$ for all $F \in L^{\text{fun}}$ and $b_1, \ldots b_{n_f} \in B$). So B is the universe of a substructure $\mathcal{N} \subseteq \mathcal{M}$. Now by the Tarski-Vaught test, $\mathcal{N} \preceq \mathcal{M}$. This elementary substructure satisfies part (a).

For part (b) we first find an elementary extension of $\mathcal{M}$ of size at least κ (here $\kappa \geq \max\{|M|, |L|\}$ is given). We use compactness: Let $L' = L_M \cup \{c_\lambda : \lambda < \kappa\}$ where the c_λs are new constant symbols. Let

$$T = \text{Th}(\mathcal{M}_M) \ \cup \ \{c_\lambda \neq c_\gamma : \lambda < \gamma < \kappa\}$$

We claim that T is consistent. Indeed, $\mathcal{M}$ itself is a model of any finite subset of T by interpreting the c_λs which appear as distinct elements (possible as M is infinite). Hence by the compactness theorem, T is consistent. Let $\mathcal{N}' \models T$ and let $\mathcal{N}$ be the reduct of $\mathcal{N}'$ to L. Then $\mathcal{N}$ is of cardinality at least κ (witnessed by the interpretation of the c_λs in $\mathcal{N}'$) and by Exercise 4.42 there is an elementary embedding of $\mathcal{M}$ in $\mathcal{N}$. Identifying $\mathcal{M}$ with its image we may assume that $\mathcal{M} \preceq \mathcal{N}$.

Now apply part (a) to get an elementary substructure $\mathcal{N}_1 \preceq \mathcal{N}$ of cardinality κ and such that $M \subseteq N_1$. So we have $\mathcal{M} \subseteq \mathcal{N}_1 \preceq \mathcal{N}$ and we have $\mathcal{M} \preceq \mathcal{N}$. It follows that $\mathcal{M} \preceq \mathcal{N}_1$. Indeed, for any L-formula $\phi(x_1, \ldots, x_n)$ and any $a \in M^n$, $\mathcal{M} \models \phi(a) \iff \mathcal{N} \models \phi(a) \iff \mathcal{N}_1 \models \phi(a)$. So $\mathcal{N}_1$ is an elementary extension of $\mathcal{M}$ of size κ. □

Corollary 5.13 (Vaught Test). *Suppose T is an L-theory all of whose models are infinite. If there exists an infinite cardinal $\kappa \geq |L|$ such that all models of T of size κ are isomorphic (we say that T is* κ-categorical*) then T is complete.*

Proof. Suppose $\mathcal{M}_1, \mathcal{M}_2$ are models of T. By Löwenheim-Skolem there exist $\mathcal{M}_1'$ and $\mathcal{M}_2'$ of size κ such that $\mathcal{M}_i'$ is either an elementary substructure of $\mathcal{M}_i$ or an elementary extension of $\mathcal{M}_i$, for $i = 1, 2$. In either case, $\mathcal{M}_i' \equiv \mathcal{M}_i$ and so $\mathcal{M}_i' \models T$. By κ-categoricity, $\mathcal{M}_1' \approx \mathcal{M}_2'$ and hence $\mathcal{M}_1' \equiv \mathcal{M}_2'$. So $\mathcal{M}_1 \equiv \mathcal{M}_1' \equiv \mathcal{M}_2' \equiv \mathcal{M}_2$. Hence T is complete by Lemma 4.41(b). □

Let us apply this to a few examples.

Example 5.14 (DLO is complete). Let $L = \{<\}$ be the language of orderings and let DLO be the theory of dense linear orderings without endpoints. We show that DLO is $\aleph_0$-categorical. The method we apply is ubiquitous in model theory and is called *back-and-forth*. Suppose $(E_1, \leq_1)$ and $(E_2, \leq_2)$ are (infinite) countable models of DLO. We enumerate them as $E_1 = \{a_i : i < \omega\}$ and $E_2 = \{b_i : i < \omega\}$. Note that these enumerations are not in any way related to the given orderings. We build a chain of partial order-preserving bijections $f_i : A_i \to B_i$ where $A_i \subset E_1$ and $B_i \subset E_2$ are finite sets, such that $f_0 \subset f_1 \subset \cdots$, $E_1 = \bigcup_i A_i$ and $E_2 = \bigcup_i B_i$. Once we do this the union $f = \bigcup_i f_i$ will be the desired isomorphism.

Stage 0. Let $A_0 = B_0 = f_0 = \emptyset$.

Stage $n + 1 = 2m + 1$. At this stage we ensure that $a_m \in A_{n+1}$. If $a_m \in A_n$ then set $A_{n+1} = A_n$, $B_{n+1} = B_n$, and $f_{n+1} = f_n$. Suppose $a_m \notin A_n$. Then set $A_{n+1} = A_n \cup \{a_m\}$. Now exactly one of the following three cases is possible:

(i) a_m is greater than every element of A_n, or
(ii) a_m is less than every element of A_n, or
(iii) there exists $\alpha <_1 \beta$ in A_n without any elements of A_n between them and $\alpha <_1 a_m <_1 \beta$.

In case (i) let $b \in E_2$ be less than every element of B_n (which is possible as B_n is finite and E_2 has no endpoints). In case (ii) let $b \in E_2$ be greater than every element of B_n. In case (iii) let $b \in E_2$ be such that $f_n(\alpha) <_2 b <_2 f_n(\beta)$ (possible since $\alpha <_1 \beta$ and so $f_n(\alpha) <_2 f_n(\beta)$ and E_2 is dense). In any case, set $B_{n+1} = B_n \cup \{b\}$ and $f_{n+1} = f_n \cup \{(a_m, b)\}$. Then we have that $f_{n+1} : A_{n+1} \to B_{n+1}$ is an order preserving bijection.

Stage $n+1 = 2m+2$. At this stage we ensure that $b_m \in B_{n+1}$. If $b_m \in B_n$ the we do nothing and set $B_{n+1} = B_n$, $A_{n+1} = A_n$, and $f_{n+1} = f_n$. Otherwise let $B_{n+1} = B_n \cup \{b_m\}$. Now b_m sits with respect to the elements of B_n in three possible ways analogously to (i),(ii), and (iii) above. Then just as in the odd stage we choose $a \in E_1$ according to which case b_m satisfies. Finally we let $A_{n+1} = A_n \cup \{a\}$ and $f_{n+1} = f_n \cup \{(a, b_m)\}$.

Then $f = \bigcup_i f_i : E_1 = \bigcup_i A_i \to \bigcup_i B_i = E_2$ is an isomorphism. We have shown that DLO is $\aleph_0$-categorical, and hence, as dense linear orderings without endpoints are all infinite, Vaught's test implies that DLO is complete.

EXAMPLE 5.15 (ACF_p is complete). We can use the Vaught test to see that for p a prime number or 0 the theory of algebraically closed fields of charcateristic p (ACF_p), in the language of rings, is complete. Indeed, let $K \models \mathrm{ACF}_p$ and let $\mathbb{F} \subseteq K$ be the prime field. (So $\mathbb{F} = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ if p is prime and $\mathbb{F} = \mathbb{Q}$ if $p = 0$.) Let B be a transcendence basis for K over $\mathbb{F}$. So $K = \mathbb{F}(B)^{\mathrm{alg}}$. I leave it as an exercise for you to check that either B is finite and $|\mathbb{F}(B)^{\mathrm{alg}}| = \aleph_0$, or $|\mathbb{F}(B)^{\mathrm{alg}}| = |B|$. Hence, if K is uncountable then $|B| = |K|$. Assume this is the case. Now if $L \models \mathrm{ACF}_p$ and $|L| = |K|$ then L has a transcendence basis C over $\mathbb{F}$ with $|C| = |B|$. We obtain therefore that L and K are isomorphic fields (any bijection between C and B will extend to an isomorphism). We have shown that ACF_p is κ-categorical for any uncountable cardinal κ. Also, every algebraically closed field is infinite. Hence, by Vaught's test (which actually only requires κ-categoricity for *some* infinite κ), ACF_p is complete. So for example, $(\mathbb{Q}^{\mathrm{alg}}, 0, 1, +, -, \times) \equiv (\mathbb{C}, 0, 1, +, -, \times)$.

EXERCISE 5.16. *Let F be any fixed field and consider T the theory of infinite F-vector spaces. Show that T is compete.*

.

CHAPTER 6

Quantifier Elimination

At the end of the last chapter we were able to prove, using Vaught's test, that the theory of algebraically closed fields of characteristic p, where $p = 0$ or p is a prime, is a complete theory. In particular, $(\mathbb{Q}^{\text{alg}}, 0, 1, +, -, \times) \equiv (\mathbb{C}, 0, 1, +, -, \times)$. But is the algebraic closure of the rationals an elementary substucture of the complex field? Equivalently, do they satisfy the same $L_{\mathbb{Q}^{\text{alg}}}$-sentences? Now an $L_{\mathbb{Q}^{\text{alg}}}$-sentence is a sentence of the form $\phi(a_1, \ldots, a_n)$ where $\phi(x_1, \ldots, x_n)$ is an L-formula and $a_1, \ldots, a_n \in \mathbb{Q}^{\text{alg}}$. If ϕ happens to be quantifier-free, then the answer is "yes" by Proposition 4.22(a). In order to show that the answer is unconditionally "yes" we will need to show that every formula is equivalent to a quantifier-free formula.

Definition 6.1 (Quantifier Elimination). An L-theory T admits *quantifier elimination* (QE) if for every L-formula $\phi(x_1, \ldots, x_n)$, where $n > 0$, there exists a quantifier-free L-formula $\psi(x_1, \ldots, x_n)$ such that $T \models \forall x_1 \cdots x_n \big(\phi(x_1, \ldots, x_n) \leftrightarrow \psi(x_1, \ldots, x_n)\big)$.

In this chapter we will develop a criterion for quantifier-elimination and then use it to prove that ACF_p admits quantifier elimination. This result has a number of consequences, among them being that $(\mathbb{Q}^{\text{alg}}, 0, 1, +, -, \times) \preceq (\mathbb{C}, 0, 1, +, -, \times)$.

We say that $\phi(x_1, \ldots, x_n)$ is *equivalent to* $\psi(x_1, \ldots, x_n)$ *modulo* T to mean that $T \models \forall x_1 \cdots x_n \big(\phi(x_1, \ldots, x_n) \leftrightarrow \psi(x_1, \ldots, x_n)\big)$. Equivalently, for all $\mathcal{M} \models T$, $\phi^{\mathcal{M}} = \psi^{\mathcal{M}}$. So QE says that every L-formula in at least one free variable is equivalent modulo T to a quantifier-free formula in the same free variables. Note that we ask for $n > 0$, so the definition does not seem to apply to L-sentences. Of course if σ is an L-sentence then we can write $\phi(x) := \sigma$, and quantifier elimination would produce a quantifier-free formula $\psi(x)$ that is equivalent to σ modulo T. Note that in $\psi(x)$ the variable x may in fact appear free, even though it did not in $\phi(x)$. So, assuming QE, we can eliminate the quantifers from σ but at the cost of (possibly) introducing a free variable.

Exercise 6.2. *Show that if L contains a constant symbol and T admits QE then every L-sentence is equivalent modulo T to a quantifier-free L-sentence.*

6.1. Preliminaries on substructures

We introduce a couple more basic notions that we will need to prove our desired criterion for quantifier elimination, and that are of independent interest.

Definition 6.3. Suppose $\mathcal{M}$ is an L-structure and $A \subseteq M$. Then the *substructure generated by* A is the smallest substructure of $\mathcal{M}$ whose universe contains A. If this happens to be $\mathcal{M}$ itself, the we say that A *generates* $\mathcal{M}$.

LEMMA 6.4. *Suppose $\mathcal{M}$ is an L-structure and $A \subseteq M$. Assume either that A is nonempty or that L has a constant symbol. The universe of the substructure generated by A is $\{t^{\mathcal{M}}(a_1, \ldots, a_n) \ : \ n \in \omega,\ a_1, \ldots, a_n \in A,\ t(x_1, \ldots, x_n)$ an L-term$\}$.*

PROOF. By Exercise 4.10 we know that a nonempty subset is the universe of a substructure if and only if it contains all the constants and is preserved by all the basic functions. We first show this is the case for

$$N = \{t^{\mathcal{M}}(a_1, \ldots, a_n) \ : \ n \in \omega,\ a_1, \ldots, a_n \in A,\ t(x_1, \ldots, x_n) \text{ an } L\text{-term}\}.$$

First of all N is nonempty since either A is nonempty and taking the term x we see that $A \subseteq N$, or else L has a constant symbol c by assumption and so the term c shows that $c^{\mathcal{M}} \in N$. By the same argument N contains all the constants of $\mathcal{M}$. If $F \in L^{\text{fun}}$ is ℓ-ary, and $a_i = t_i^{\mathcal{M}}(a_{i,1}, \ldots, a_{i,n_\ell})$ are elements of N for $i = 1, \ldots, \ell$, then

$$F^{\mathcal{M}}(a_1, \ldots, a_\ell) = t^{\mathcal{M}}(a_{1,1}, \ldots, a_{1,n}, \ldots, a_{\ell,1}, \ldots, a_{\ell,n_\ell})$$

where $t = F(t_1, \ldots, t_\ell)$. Hence $F^{\mathcal{M}}(a_1, \ldots, a_\ell) \in N$. So N is the universe of a substructure of $\mathcal{M}$, say $\mathcal{N}$.

To see that $\mathcal{N}$ is the substructure generated by A, we need to show that if $\mathcal{N}' \subseteq \mathcal{M}$ and $A \subseteq N'$, then $N \subseteq N'$. But this is the case since for every L-term t and $a_1, \ldots, a_n \in A \subseteq N'$, $t^{\mathcal{M}}(a_1, \ldots, a_n) = t^{\mathcal{N}'}(a_1, \ldots, a_n)$ since $\mathcal{N}' \subseteq \mathcal{M}$. Hence $t^{\mathcal{M}}(a_1, \ldots, a_n) \in N'$. □

In Exercise 4.42 we saw that there is an elementary embedding from $\mathcal{M}$ to $\mathcal{N}$ if and only if $\mathcal{N}$ can be expanded to a model of $\text{Th}(\mathcal{M}_M)$. We now give a similar criterion for the existence of an embedding, but we refine it a little to take into account a generating set.

LEMMA 6.5. *Suppose $\mathcal{M}$ is an L-structure generated by $A \subseteq M$. Assume either that A is nonempty or that L has a constant symbol. Consider the L_A-theory*

$$D := \{\phi(\underline{a}) : n \in \omega, a = (a_1, \ldots, a_n) \in A^n, \phi \text{ a quantifer-free } L\text{-formula, and } \mathcal{M} \models \phi(a)\}.$$

Suppose $\mathcal{N}$ is an L-structure. Then there exists an L-embedding $j : \mathcal{M} \to \mathcal{N}$ if and only if $\mathcal{N}$ can be expanded to an L_A-structure $\mathcal{N}'$ such that $\mathcal{N}' \models D$.

PROOF. If such an embedding j exists then expand $\mathcal{N}$ to an L_A-structure $\mathcal{N}'$ by $\underline{a}^{\mathcal{N}'} = j(a)$ for each $a \in A$. Then $\mathcal{N}' \models D$ by Proposition 4.22(a).

For the converse, let $\mathcal{N}' \models D$ be an expansion of $\mathcal{N}$. We define $j : \mathcal{M} \to \mathcal{N}$ as follows. Suppose $b \in M$. Then by Lemma 6.4 there is an L-term $t(x_1, \ldots, x_n)$, and $a \in A^n$, such that $b = t^{\mathcal{M}}(a)$. Now $t(\underline{a})$ is an L_A-term. Set $j(b) := t(\underline{a})^{\mathcal{N}'}$. This map is injective since if $b \neq b'$ are elements of M with $b = t^{\mathcal{M}}(a)$ and $b' = s^{\mathcal{M}}(a')$, where t and s are L-terms and $a \in A^n$ and $a' \in A^m$, then $\big(t(\underline{a}) \neq s(\underline{a'})\big) \in D$, and so $j(b) \neq j(b')$. For $c \in L^{\text{con}}$ let $b = c^{\mathcal{M}}$. Then by definition $j(b) = c^{\mathcal{N}'} = c^{\mathcal{N}}$. If $F \in L^{\text{fun}}$ is n-ary and $b_1, \ldots, b_n \in M$, then writing each $b_i = t_i^{\mathcal{M}}(a_i)$ where t_i is an L-term and $a_i \in A^{n_i}$, we have that $F^{\mathcal{M}}(b_1, \ldots, b_n) = F^{\mathcal{M}}\big(t_1^{\mathcal{M}}(a_1), \ldots, t_n^{\mathcal{M}}(a_n)\big)$ and so

$$\begin{aligned} j\big(F(b_1, \ldots, b_n)\big) &= F\big(t_1(\underline{a_1}), \ldots, t_n(\underline{a_n})\big)^{\mathcal{N}'} \\ &= F^{\mathcal{N}'}\big(t_1(\underline{a_1})^{\mathcal{N}'}, \ldots, t_n(\underline{a_n})^{\mathcal{N}'}\big) \\ &= F^{\mathcal{N}}\big(j(b_1), \ldots, j(b_n)\big). \end{aligned}$$

Finally, suppose $R \in L^{\mathrm{rel}}$ is n-ary and $b_1, \ldots, b_n \in M$. Again writing each $b_i = t_i^{\mathcal{M}}(a_i)$ where t_i is an L-term and $a_i \in A^{n_i}$ we have

$$\begin{aligned}(b_1, \ldots, b_n) \in R^{\mathcal{M}} &\iff (t_1^{\mathcal{M}}(a_1), \ldots, t_n^{\mathcal{M}}(a_n)) \in R^{\mathcal{M}} \\ &= R\big(t_1(\underline{a_1}), \ldots, t_n(\underline{a_n})\big) \in D \\ &\iff \big(t_1(\underline{a_1}(^{\mathcal{N}'}, \ldots, t_n(\underline{a_n})^{\mathcal{N}'}\big) \in R^{\mathcal{N}'} \\ &\iff \big(j(b_1), \ldots, j(b_n)\big) \in R^{\mathcal{N}}.\end{aligned}$$

Hence j is an L-embedding. □

6.2. A criterion for quantifier elimination

We begin with a criterion for eliminating quantifiers from a given formula.

THEOREM 6.6. *Suppose L conatins a constant symbol, T is an L-theory, and $\phi(x)$ is an L-formula where $x = (x_1, \ldots, x_n)$. The following are equivalent.*

(i) *$\phi(x)$ is equivalent to a quantifier-free formula $\psi(x)$ modulo T.*
(ii) *Suppose $\mathcal{M} \models T$, $\mathcal{N} \models T$, and $\mathcal{A}$ is an L-substructure of both $\mathcal{M}$ and $\mathcal{N}$. Then for all $a \in A^n$, $\mathcal{M} \models \phi(a)$ if and only if $\mathcal{N} \models \phi(a)$.*

PROOF. Suppose $\phi(x)$ is equivalent to a quantifier-free L-formula $\psi(x)$ modulo T. Let $\mathcal{M}, \mathcal{N}, \mathcal{A}$ be as in (ii). Then for any $a \in A^n$,

$$\begin{aligned}\mathcal{M} \models \phi(a) &\iff \mathcal{M} \models \psi(a) \text{ as } \psi \text{ is equivalent to } \psi \text{ modulo } T \text{ and } \mathcal{M} \models T \\ &\iff \mathcal{A} \models \psi(a) \text{ as } \mathcal{A} \subseteq \mathcal{M}, \text{ and by Proposition 4.22(a)} \\ &\iff \mathcal{N} \models \psi(a) \text{ as } \mathcal{A} \subseteq \mathcal{N}, \text{ and by Proposition 4.22(a)} \\ &\iff \mathcal{N} \models \phi(a) \text{ as } \psi \text{ is equivalent to } \psi \text{ modulo } T \text{ and } \mathcal{N} \models T\end{aligned}$$

as desired.

For the converse, suppose (ii) holds. We look for a quantifier-free formula equivalent to $\phi(x)$ modulo T. First consider

$$\Psi(x) := \{\psi(x) : \psi \text{ is quantifier-free and } T \models \forall x\big(\phi(x) \to \psi(x)\big)\}.$$

This is the set of all quantifier-free consequences of ϕ. Let $c_1, \ldots, c_n$ be new constant symbols and let $L' = L \cup \{c_1, \ldots, c_n\}$. Let $c = (c_1, \ldots, c_n)$ and denote by $\Psi(c)$ the set of L'-sentences $\{\psi(c) : \psi \in \Psi\}$.

CLAIM 6.7. $T \cup \Psi(c) \models \phi(c)$.

PROOF OF CLAIM 6.7. Suppose not. Then there is an L'-structure $\mathcal{M}' \models T \cup \Psi(c) \cup \{\neg\phi(c)\}$, with universe M. Let $\mathcal{A}'$ be the L'-substructure of $\mathcal{M}'$ generated by $\emptyset$. If $\mathcal{M}$ and $\mathcal{A}$ denote their reducts to L, then we have $\mathcal{M} \models \neg\phi(b)$ where $b_1 = c_1^{\mathcal{M}'}, \ldots, b_n = c_n^{\mathcal{M}'}$. Note that $\mathcal{A}$ is the substructure of $\mathcal{M}$ generated by $B := \{b_1, \ldots, b_n\}$. Our goal is to construct a model of T which is an extension of $\mathcal{A}$ and in which $\phi(b)$ is true. This will contradict (ii).

Consider the L_B-theory $D = \{\theta(\underline{b}) : \theta(x) \text{ is a quantifier-free } L\text{-formula and } \mathcal{A} \models \theta(b)\}$.

SUBCLAIM 6.8. *$\Sigma := T \cup D \cup \phi(\underline{b})$ is consistent.*

PROOF OF SUBCLAIM 6.8. By compactness we need only consider a finite subset $\Sigma_0 \subseteq \Sigma$. Only finitely many quantifier-free L_B-sentences from D appear in Σ_0; say $\theta_1(\underline{b}), \cdots, \theta_\ell(\underline{b})$. If Σ_0 is not consistent then $T \models \big(\bigwedge_{i=1}^{\ell} \theta(\underline{b}) \to \neg\phi(\underline{b})\big)$ and hence $T \models \big(\phi(\underline{b}) \to \bigvee_{i=1}^{\ell} \neg\theta_i(\underline{b})\big)$. Since $\underline{b}$ is a tuple of new constant symbols not in L, and T is an L-theory, this implies that

$$T \models \forall x\big(\phi(x) \to \bigvee_{i=1}^{\ell} \neg\theta(x)\big).$$

By definition, it follows that $\bigvee_{i=1}^{\ell} \neg\theta(x) \in \Psi(x)$ and hence $\mathcal{M} \models \bigvee_{i=1}^{\ell} \neg\theta(b)$. As this is a quantifier-free L'-sentence, we get $\mathcal{A} \models \bigvee_{i=1}^{\ell} \neg\theta(b)$. Which is absurd as $\theta_1(\underline{b}), \ldots, \theta_\ell(\underline{b}) \in D$. Hence Σ_0 must be consistent. So Σ is consistent. This completes the proof Subclaim 6.8. □

Let $\tilde{\mathcal{N}} \models \Sigma$ with universe N and let $\mathcal{N}$ be the reduct of $\tilde{\mathcal{N}}$ to L. So $\mathcal{N} \models T$. By Lemma 6.5, since B generates $\mathcal{A}$ and $\mathcal{N}$ expands to the L_B-structure $\tilde{\mathcal{N}} \models D$, we get an L-embedding $j : \mathcal{A} \to \mathcal{N}$. Under this mapping b maps to $\underline{b}^{\tilde{\mathcal{N}}}$. We can identify $\mathcal{A}$ with its image and thereby view $\mathcal{A} \subseteq \mathcal{N}$ with $b = \underline{b}^{\tilde{\mathcal{N}}}$. So $\mathcal{N} \models \phi(b)$. Since $\mathcal{M} \models \neg\phi(b)$, we have contradicted (ii). This completes the proof of Claim 6.7. □

We have shown that $T \cup \Psi(c) \models \phi(c)$. By compactness there exists $\psi_1, \ldots, \psi_\ell \in \Psi$ such that $T \cup \{\psi_1(c), \ldots, \psi_\ell(c)\} \models \phi(c)$. Let $\psi(x) := \bigwedge_{i=1}^{\ell} \psi_i(x)$. We have that $T \models \psi(c) \to \phi(c)$. Again, as c does not appear in T this means that $T \models \forall x\big(\psi(x) \to \phi(x)\big)$. On the other hand, $T \models \forall x\big(\phi(x) \to \psi(x)\big)$ since $T \models \forall x\big(\phi(x) \to \psi_i(x)\big)$ for each $i = 1, \ldots, \ell$. So $T \models \forall x\big(\phi(x) \leftrightarrow \psi(x)\big)$, and we have found a quantifier-free formula that is equivalent to ϕ modulo T. This completes the proof of Theorem 6.6. □

While the last theorem tells us how to test whether a given formula is equivalent to a quantifier-free formula, the following, rather easier proposition, tells us which formulas we need to consider in order to obtain quantifier elimination.

PROPOSITION 6.9. *Suppose L has a constant symbol and T is an L-theory. The following are equivalent,*

(i) *T admits quantifier-elimination.*
(ii) *For all $n \in \omega$ and all quantifier-free formulas $\theta(x, y)$ where $x = (x_1, \ldots, x_n)$, the formula $\exists y\theta(x, y)$ is equivalent modulo T to a quantifier-free formula $\psi(x)$.*

PROOF. That (i) implies (ii) is immediate. For the converse, we assume (ii) and prove by induction on complexity that every formula $\phi(x)$ is equivalent modulo T to a quantifier-free formula. For ϕ atomic we can take ϕ itself. If ϕ is $\xi_1 \wedge \xi_2$ and ξ_i is equivalent to a quantifer-free ξ_i' modulo T, for $i = 1, 2$, then ϕ is equivalent modulo T to the quantifier-free $\xi_1' \wedge \xi_2'$. We can deal simlarly with the case of $\vee$ and $\neg$. So assume that $\phi(x)$ is $\exists y\xi(x, y)$. By the induction hypothesis $T \models \forall xy\big(\xi(x, y) \leftrightarrow \theta(x, y)\big)$, where $\theta(x, y)$ is quantifier-free. Hence

$T \models \forall x\big(\phi(x) \leftrightarrow \exists y\theta(x,y)\big)$. By (ii), $T \models \forall x\big(\exists y\theta(x,y) \leftrightarrow \psi(x)\big)$ for some quantifier-free $\psi(x)$. But then we have $T \models \forall x\big(\phi(x) \leftrightarrow \psi(x)\big)$, as desired. (As usual the case of $\forall$ reduces to the cases of $\neg$ and $\exists$.) $\square$

Putting Theorem 6.6 and Proposition 6.9 together we obtain:

COROLLARY 6.10. *Suppose L has a constant symbol and T is an L-theory. Then the following are equivalent:*

(i) *T admits quantifier elimation.*
(ii) *Suppose $\mathcal{M} \models T$, $\mathcal{N} \models T$, $\mathcal{A}$ is an L-substructure of both $\mathcal{M}$ and $\mathcal{N}$, $a \in A^n$, and $\theta(x_1, \ldots, x_n, y)$ is a quantifier-free L-formula such that $\theta(a,y)$ has a realisation in $\mathcal{M}$. Then $\theta(a,y)$ has a realisation in $\mathcal{N}$.*

PROOF. By Propostion 6.9, (i) is equivalent to showing that every formula of the form $\exists y\theta(x_1, \ldots, x_n, y)$, where θ is quantifier-free, is equivalent modulo T to a quantifier-free formula. Applying Theorem 6.6 we get that this is equivalent to showing that: $(*)$ *whenever $\mathcal{M} \models T$, $\mathcal{N} \models T$, $\mathcal{A}$ is an L-substructure of both $\mathcal{M}$ and $\mathcal{N}$, and $a \in A^n$; $\mathcal{M} \models \exists y\theta(a,y)$ if and only if $\mathcal{N} \models \exists y\theta(a,y)$.* The statement $(*)$ clearly implies (ii). On the other hand, (ii) applied twice, once with the roles of $\mathcal{M}$ and $\mathcal{N}$ reversed, gives us $(*)$. $\square$

Let us refine the criterion a little further. By a *literal* we mean an atomic or negated atomic formula.

COROLLARY 6.11 (Criterion for QE). *Suppose T is an L-theory satisfying the following condition:*

(*) *Whenever $\mathcal{M}$ and $\mathcal{N}$ are models of T with a common substructure $\mathcal{A}$, and $\psi(y)$ is a conjunction of L_A-literals, if $\psi(y)$ has a realisation in $\mathcal{M}$ then it has a realisation in $\mathcal{N}$.*

Then T admits QE.

PROOF. Let us first prove this assuming that L has a constant symbol. We assume $(*)$ and show that (ii) of Corollary 6.10 holds. Indeed, by De Morgan's laws about how negation interacts with conjunctions and disjunctions, if $\theta(x_1, \ldots, x_n, y)$ is a quantifier-free formula and $a \in A^n$ then $\theta(a,y)$ is a quantifier-free L_A-formula that is equivalent (modulo the empty theory) to a disjunction of conjunctions of L_A-literals, say $\phi(y)$. If $\theta(a,y)$ has a solution on $\mathcal{M}$ then so does some disjunct, say $\psi(y)$ of ϕ. Now by $(*)$, $\psi(y)$ has a solution in $\mathcal{N}$. Hence so does $\phi(y)$, and thus $\theta(a,y)$. We have shown that condition (ii) of Corollary 6.10 is satisfied, so T admits QE.

Now let us show that this corollary holds even if L has no constant symbol. Assume $(*)$. Let $L' = L \cup \{c\}$ where c is a constant symbol. Suppose $\mathcal{M}'$ and $\mathcal{N}'$ are L'-structures which are models of T, $\mathcal{A}'$ is a common L'-substructure with universe A, and $\psi'(y)$ is a conjunction of L'_A-literals. Letting $\mathcal{N}$, $\mathcal{M}$, and $\mathcal{A}$ be the reducts to L, we still have models of T with a common L-substructure. Now let $\psi(y)$ be obtained from ψ' be replacing every occurrence of c with a where $a = c^{\mathcal{A}'} \in A$. Then $\psi(y)$ is a conjunction of L_A-literals and if ψ' has a solution in $\mathcal{M}'$ then ψ has a solution in $\mathcal{M}$. By $(*)$, $\psi(y)$ has a solution in $\mathcal{N}$, and so $\psi'(y)$ has one in $\mathcal{N}'$. We have shown that $(*)$ is true even when we view T as an L'-theory. So by the above, T admits QE as an L'-theory. I now leave it to you as an exercise to show that if

a theory admits QE in a language expanded by constants, then it already admits QE in the original language. □

Condition (∗) can be used to show that a number of theories admit QE. For example, consider $L = \emptyset$ and T the theory of infinite sets. Suppose M and N are infiinite sets with as common nonempty subset A. Note that an atomic L_A-formula in the variable y is of the form $y = y$ or $y = a$ for some $a \in A$. Of course $y = y$ is realised by everything while $y \neq y$ is realised by nothing, so the former adds no new information to a conjunction while the latter can never be a conjunct of a formula that has a solution. Similarly, any atomic L_A-formula not involving y is either true or false in A (and hence also in M and N) so either does not add any new information as a conjunct or cannot be present as a conjunct in a formula that has a solution in M. Hence a conjunction of L_A-literals in y, that has a realisation in M, is equivalent to one of the form:

$$\bigwedge_{i=1}^{k}(y = a_i) \ \wedge \ \bigwedge_{j=1}^{\ell}(y \neq b_j)$$

where the a_i and b_j come from A. If any of the $(y = a_i)$ actually appears in the formula then we have a solution in A and hence in N. If not, then as N is infinite we can find a solution in N. So we have shown (∗) for T – so the theory of inifnite sets admits QE.

Of course, the theory of infinite sets is simple enough that it seems unnecessary to have developed the above criterion to prove QE. So let us prove that ACF admits QE. Suppose M and N are algebraically closed fields, R is a common subring, $\psi(y)$ is a conjunction of L_R-literals such that $\psi(y)$ has a realisation in M. We need to show that $\psi(y)$ has a solution in N. First observe that R is an integral domain (as it is a subring of a field) and hence has a unque field of fractions F, which in turn has a unique algebraically closure F^{alg}. Hence we may as well assume that R is an algebraically closed subfield of both M and N. Now $\psi(y)$ is of the form

$$\bigwedge_{i=1}^{k} p_i(y) = 0 \ \wedge \ \bigwedge_{j=1}^{\ell} q_j(y) \neq 0$$

where the p_i and q_j are polynomials in one variable over R. Let b be a realisation of this in M. If any one of the p_is are nonzero then b is algebraic over R, and hence in R, and hence in N, and we would be done. So we can assume that all the p_is are zero polynomials. Now each q_j has only finitely many roots in N, but N is infinite as it is algebraically closed. So if we choose $b' \in N$ not equal to any of these roots, then b' will realise $\psi(y)$, as desired.

Exercise 6.12. *Let $L = \{E\}$ where E is a binary relation symbol. Let T be the theory which says that there are infinitely many E-classes and each class is infinite. Show that T is complete and admits quantifier elimination.*

Exercise 6.13. *Let F be any fixed field and consider T the theory of infinite F-vector spaces. Show that T admits quantifier-elimination.*

Similar arguments can be used to show QE for a number of theories, including the theory of torsion-free divisible abelian groups and the theory of dense linear orderings without endpoints. See chapter 3 of Marker's "Model Theory: An introduction" (Springer 2002).

6.3. Some consequences of quantifier elimination

Quantifier elimination on its own is not necessarily a very strong property. For example, suppose $\mathcal{M}$ is any L-structure, and consider the *Skolemisation* of $\mathcal{M}$: Let L' be the expanded language where there is a new n-ary relation symbol P_A for every 0-definable subset $A \subseteq M^n$, for all $n < \omega$. We can make $\mathcal{M}$ into an L'-structure canonically by interpreting P_A as A. Note that the definable subsets of $\mathcal{M}$ viewed as an L-structure and as an L'-structure are the same – because the expansion we are considering does not introduce any new definable sets – it just makes all the old definable sets atomic. Then, as an L'-theory, $\mathrm{Th}(\mathcal{M})$ has quantifier elimination (exercise). In this way we can always force quantifier elimination. So quantifier elimination is only useful if we have some control over the language. And when we do, it can be very useful. In this final section we point out some of its immediate consequences.

DEFINITION 6.14. A theory T is said to be *model-complete* if whenever $\mathcal{M}$ and $\mathcal{N}$ are models of T, if $\mathcal{M} \subseteq \mathcal{N}$ then $\mathcal{M} \preceq \mathcal{N}$.

PROPOSITION 6.15. *Quantifier elimination implies model-completeness.*

PROOF. Suppose T admits QE, $\mathcal{M} \models T$, $\mathcal{N} \models T$, and $\mathcal{M} \subseteq \mathcal{N}$. Given a formula $\phi(x_1, \ldots, x_n)$ with $n > 0$ we have a quantifier-free formula $\psi(x_1, \ldots, x_n)$ that is equivalent to ϕ modulo T. Hence, for any $a \in M^n$ we have

$$\begin{aligned} \mathcal{M} \models \phi(a) &\iff \mathcal{M} \models \psi(a) \text{ as } \mathcal{M} \models T \\ &\iff \mathcal{N} \models \psi(a) \text{ as } \psi \text{ is quantifier-free and } \mathcal{M} \subseteq \mathcal{N} \\ &\iff \mathcal{N} \models \phi(a) \text{ as } \mathcal{N} \models T. \end{aligned}$$

We have shown that $\mathcal{M} \preceq \mathcal{N}$. Actually, this is not strictly speaking correct as we do still have to deal with case when $n = 0$. But then we can still write the sentence ϕ as $\phi(x)$, and the above argument still shows that for all $a \in M$, $\mathcal{M} \models \phi(a)$ if an only if $\mathcal{N} \models \phi(a)$. Note that as x does not in fact appear in ϕ, fixing $a \in M$, $\mathcal{M} \models \phi$ if and only if $\mathcal{M} \models \phi(a)$. And similarly for $\mathcal{N}$. So $\mathcal{M} \models \phi$ if and only if $\mathcal{N} \models \phi$. □

Model-completeness is strictly weaker than quantifier-elimination. An example is $T = \mathrm{Th}(\mathbb{R}, 0, 1, +, -, \times)$ which we have already seen does not admit QE (as the ordering is definable but not quantifier-free definable, cf. Example 4.29). However, it is a fact (requiring some more work, including Tarski's theorem that $\mathrm{Th}(\mathbb{R}, 0, 1, +, -, \times, <)$ does admit QE) that T is model-complete.

One application of model-completeness is another technique for proving completeness.

PROPOSITION 6.16. *If T is model-complete and there exists a model $\mathcal{M}$ of T which embeds into every other model of T, then T is complete.*

PROOF. Suppose $\mathcal{N}_1 \models T$ and $\mathcal{N}_2 \models T$. By assumption we have $\mathcal{M} \subseteq \mathcal{N}_i$ for $i = 1, 2$. By model-completeness, $\mathcal{M} \preceq \mathcal{N}_i$ and hence $\mathcal{M} \equiv \mathcal{N}_i$. So $\mathcal{N}_1 \equiv \mathcal{N}_2$, as desired. □

It follows that the theory of infinite sets and the theory of an equivalence relation with infinitely many classes all infinite, are complete. Indeed, we (or rather you) have already pointed out that they admit QE and it is not hard to see that both of these theories have a model that embeds into every other model (exercise). Of course in both of these cases one can also get completeness more directly by $\aleph_0$-categoricity (exercise). Another example

is that the theory of torsion-free divisible abelian groups is complete: one shows it admits QE by applying Corollary 6.11, and then one observes that the additive group of rational numbers embeds in every model. Once again however, completeness could have been achieved by Vaught's test, since the theory of torsion-free divisible abelian groups is κ-categorical for any uncountable κ. To see an example where Proposition 6.16 gives us a proof of completenss while Vaught's test does not, one has to once again consider the structure $(\mathbb{R}, 0, 1, +, -, \times)$. This is a model of the theory of *real closed fields* (RCF), which we have not (and will not) define. Nevertheless, let me just say that RCF is model-complete (for reasons more or less hinted at above), but not categorical in any infinite cardinal (the latter also requires proof, and is by no means obvious). See Marker's "Model Theory: An introduction" for details.

From Proposition 6.15 we get that ACF is model-complete. Here is a corollary of this fact, which is a nice note to end on.

COROLLARY 6.17 (Hilbert's Nulstellensatz). *Suppose K is an algebraically closed field and I is an ideal in the polynomial ring $K[X_1, \ldots, X_n]$. Then there exists a tuple $a \in K^n$ such that $P(a) = 0$ for all $P \in I$.*

PROOF. Extending I to a prime ideal (for example a maximal ideal by Zorn's lemma) we may as well assume that I is prime. By Noetherianity of $K[X_1, \ldots, X_n]$ we know that I is generated by a finite set of polynomials, say $P_1, \ldots, P_\ell$. To find a common zero for all polynomials in I it will suffice to find a common zero for $P_1, \ldots, P_\ell$. This is what we will do.

Consider the integral domain $K[X_1, \ldots, X_n]/I$. Let F be its fraction field and let $L = F^{\mathrm{alg}}$ be its algebraic closure. Then K is a subfield (and hence a substructure) of L. As both are models of ACF, and ACF is model-complete, we get $K \preceq L$. Now in L the tuple $(X_1 I, \ldots, X_n I)$ is a root of all the polynomials in I. Hence $L \models \exists x_1 \cdots x_n \big(\bigwedge_{i=1}^{\ell} P_i(x) = 0 \big)$. Since the polynomials $P_1, \ldots, P_\ell$ have coefficients in K this is a formula over K. Hence $K \models \exists x_1 \cdots x_n \big(\bigwedge_{i=1}^{\ell} P_i(x) = 0 \big)$, as desired. □