Set theory and logic throughout mathematics

Chris Lambie-Hanson

April 28, 2024

Contents

Chapter 1

Lecture 1: Ordinals and the hydra

1.1 Well-orders

Let us begin by briefly reviewing the definition of *partial order*, *linear order*, and *well-order*.

Definition 1.1.1. Suppose that X is a set and $\leq$ is a binary relation on X. Then $\leq$ is a *partial order* on X (or $(X, \leq)$ is a *partial order*) if it is

1. *Reflexive*: $x \leq x$ for all $x \in X$;
2. *Transitive*: for all $x, y, z \in X$, if $x \leq y$ and $y \leq z$, then $x \leq z$; and
3. *Anti-symmetric*: for all $x, y \in X$, if $x \leq y$ and $y \leq x$, then $x = y$.

A partial order $\leq$ on a set X is a *linear order* if, in addition, it is *total*, i.e., for all $x, y \in X$, we have $x \leq y$ or $y \leq x$.

If $\leq$ is a partial order on a set X and $x, y \in X$, then we will write $x < y$ to mean that $x \leq y$ and $x \neq y$. The relation $<$ is then referred to as the *strict* part of $\leq$.

Definition 1.1.2. Suppose that X is a set and R is a binary relation on X. Then R is *well-founded* if every nonempty subset of X has an R-minimal element. In other words, for every nonempty $Y \subseteq X$, there is $y \in Y$ such that, for all $x \in Y$ with $x \neq y$, $\neg(xRy)$. A well-founded linear order is called a *well order*.

Exercise 1.1.3. Suppose that $\leq$ is a linear order on a set X. Prove that the following are equivalent.

1. $\leq$ is a well order.
2. There are no infinite, strictly decreasing sequences with respect to $\leq$. In other words, there does not exist a sequence $\langle x_0, x_1, x_2, \ldots \rangle$ of elements of X such that, for all n, we have $x_{n+1} < x_n$.

There is a natural way to assert that two partial orders are "essentially" the same, i.e., *isomorphic*.

Definition 1.1.4. Suppose that $\leq_0$ is a partial order on X_0 and $\leq_1$ is a partial order on X_1. Then we say that $\leq_0$ and $\leq_1$ are *isomorphic* if there is a bijection $F : X_0 \to X_1$ such that, for all $x, y \in X_0$, we have

$$x \leq_0 y \iff F(x) \leq_1 F(y).$$

Example 1.1.5. The following are some examples and non-examples of isomorphic partial orders.

1. The open interval $(0, 1)$ and the open interval $(0, 2)$, both with the usual ordering of real numbers, are isomorphic via the bijection $x \mapsto 2x$.

2. The open interval $(0, 1)$ and the closed interval $[0, 1]$ are not isomorphic. One way to see this is to note that $[0, 1]$ has a maximal element and $(0, 1)$ does not, so any order-preserving map from $(0, 1)$ to $[0, 1]$ could not include 1 in its range.

3. Let Y be any nonempty set. Let $X_0 = \mathscr{P}(Y)$ be the *power set* of Y, i.e., the collection of all subsets of Y. Let $\leq_0$ be the partial order on X_0 defined by letting $u \leq v$ if and only if $u \leq v$.

   Let X_1 be the collection of all functions $f : Y \to \{0, 1\}$, and let $\leq_1$ be the partial order on X_1 defined by letting $f \leq g$ if and only if $f(y) \leq g(y)$ for all $y \in Y$.

   Then $\leq_0$ and $\leq_1$ are isomorphic via the bijection $F : X_0 \to X_1$ that sends each $u \in X_0$ to the *characteristic function* of u, i.e., the function $f_u : Y \to \{0, 1\}$ that takes value 1 on all elements in u and value 0 on all elements of Y that are not in u.

1.2 Ordinal numbers

Roughly speaking, an ordinal number can be thought of as a description of the order type of a well-order. In other words, to each well-order, we assign an ordinal, and two well-orders are isomorphic if and only if they are assigned the same ordinal.

Example 1.2.1. For each natural number n, all well-orders of size n are isomorphic; their order type is itself referred to as "n".

However, there are many non-isomorphic countably infinite well-orders. The ordinal describing the order type of the natural numbers,

$$0 < 1 < 2 < 3 < \dots$$

is denoted "ω". But we can form a new order type by adding a new element (call it ∞) that is larger than all of the natural numbers:

$$0 < 1 < 2 < 3 < \dots < \infty.$$

The ordinal describing this order type is denoted "$\omega + 1$". Or we can form yet another order type by placing two copies of the natural numbers one after the other:

$$0 < 1 < 2 < 3 < \dots < 0' < 1' < 2' < 3' < \dots.$$

The ordinal describing this order type is denoted "$\omega + \omega$".

There is a natural way to order the ordinal numbers themselves. To make this precise, we need the following definition.

Definition 1.2.2. Suppose that $\leq$ is a well-order of a set X. Then an *initial segment* of $(X, \leq)$ is a subset $Y \subseteq X$ such that, for all $y \in Y$ and all $x \in X$, if $x \leq y$, then $x \in Y$. In other words, if $y \in Y$, then Y also contains all elements of X that are smaller than y in the ordering $\leq$.

Exercise 1.2.3. Suppose that $\leq$ is a well-order of a set X and Y is an initial segment of $(X, \leq)$. Then either

- $Y = X$; or
- there is $x \in X$ such that $Y = \{y \in X \mid y < x\}$.

Exercise 1.2.4. Suppose that $(X_0, \leq_0)$ and $(X_1, \leq_1)$ are two well-orders. Then either

1. $(X_0, \leq_0)$ is isomorphic to an initial segment of $(X_1, \leq_1)$; or
2. $(X_1, \leq_1)$ is isomorphic to an initial segment of $(X_0, \leq_0)$.

If both 1. and 2. hold, then $(X_0, \leq_0)$ and $(X_1, \leq_1)$ are isomorphic.

With Exercise 1.2.4 in mind, we can make the following definition.

Definition 1.2.5. Suppose that α and β are ordinals. Then we say that $\alpha \leq_{\text{ord}} \beta$ if, whenever $(X_\alpha, \leq_\alpha)$ is a well-order of type α and $(X_\beta, \leq_\beta)$ is a well-order of type β, then $(X_\alpha, \leq_\alpha)$ is isomorphic to an initial segment of $(X_\beta, \leq_\beta)$.

Exercise 1.2.6. The class of ordinals is well-ordered by $\leq_{\text{ord}}$.

One can perform arithmetic on ordinal numbers. We will make this more precise later, but let us first give an informal description. Let α and β be ordinal numbers, and let $(X_\alpha, \leq_\alpha)$ and $(X_\beta, \leq_\beta)$ be well-orders of type α and β, respectively.

We first describe ordinal addition. The ordinal $\alpha+\beta$ is the ordinal describing the well-ordering formed by placing a copy of $(X_\beta, \leq_\beta)$ after a copy of $(X_\alpha, \leq_\alpha)$ (i.e., every element of X_β is declared to be larger than every element of X_α).

Note that ordinal addition is not commutative: it may not be the case that $\alpha + \beta = \beta + \alpha$. To see this, consider $2 + \omega$ and $\omega + 2$. Represent the ordinal 2 by the order $0' < 1'$, and represent ω by the usual natural numbers. Then $2 + \omega$ is the order type of the order

$$0' < 1' < 0 < 1 < 2 < 3 < \dots$$

This is isomorphic to the usual ordering of the natural numbers, via the map

$$\begin{aligned} 0' &\mapsto 0 \\ 1' &\mapsto 1 \\ n &\mapsto n + 2 \text{ for every natural number } n. \end{aligned}$$

Thus, $2 + \omega = \omega$. On the other hand, $\omega + 2$ is the order type of the order

$$0 < 1 < 2 < \ldots < 0' < 1'$$

This is clearly *not* isomorphic to the natural numbers; for example, it has a maximal element, whereas that natural numbers do not. Thus, $\omega + 2 \neq \omega$, and in fact $\omega <_{\text{ord}} \omega + 2$.

We next describe ordinal multiplication. The ordinal $\alpha \cdot \beta$ is the ordinal describing the well-ordering formed by starting with a copy of $(X_\beta, \leq_\beta)$ and replacing every element of X_β with a copy of $(X_\alpha, \leq_\alpha)$.

Again, ordinal multiplication is not commutative. For example, $2 \cdot \omega$ is the order type of the following order:

$$0 < 0' < 1 < 1' < 2 < 2' < 3 < 3' < \ldots$$

formed by replacing every natural number n with a copy $n < n'$ of the two-element order. It is not too hard to show that this order is isomorphic to the natural numbers, so $2 \cdot \omega = \omega$. On the other hand, $\omega \cdot 2$ is the order type of the following order:

$$0 < 1 < 2 < 3 < \ldots < 0' < 1' < 2' < 3' < \ldots$$

formed by replacing each element of the two-element order $* < *'$ by a copy of the natural numbers. This is not isomorphic to the set of natural numbers; for instance, it contains elements that are larger than infinitely many other elements, whereas the natural numbers do not. Thus, $\omega \cdot 2 \neq \omega$, and in fact $\omega <_{\text{ord}} \omega \cdot 2$.

We finally describe ordinal exponentiation. If $\alpha = 0$, then $\alpha^\beta = 0$. Otherwise, first let 0_α denote the *minimal* element of $(X_\alpha, \leq_\alpha)$. This must exist, since $\leq_\alpha$ is a well-order. We say that a function $f : X_\beta \to X_\alpha$ is *finitely supported* if the set $\{y \in X_\beta \mid f(y) \neq 0_\alpha\}$ is finite. The ordinal α^β is now defined as follows. Let Z be the set of all finitely-supported functions from X_β to X_α. Now describe an ordering $\preceq$ on Z as follows. Given $f, g \in Z$, set $f \preceq g$ if and only if either

- $f = g$; or
- $f \neq g$ and, letting $y \in X_\beta$ be the $\leq_\beta$-maximal element such that $f(y) \neq g(y)$, we have $f(y) \leq_\alpha g(y)$.

Then let α^β be the ordinal describing the order type of $(Z, \preceq)$.

Exercise 1.2.7. Prove that the order $(Z, \preceq)$ described in the preceding paragraph is indeed a well-order.

A concrete representation of the ordinals.

In practice we often work with a particular concrete realization of the ordinals, and we think of an ordinal α as the set of all ordinals that are strictly less than α (with respect to the ordering $\leq_{\text{ord}}$ introduced above. At first glance, this may appear like a circular definition, but it is not, due to the fact that $\leq_{\text{ord}}$ is itself a well-ordering. In particular, there is a least ordinal, 0. Since there are no ordinals strictly less than 0, we represent 0 as the empty set, $\emptyset$. The

next smallest ordinal is 1. It only has one ordinal less than it, namely, 0, so 1 is represented as $\{0\} = \{\emptyset\}$. The first few ordinals are thus represented as follows:

$$
\begin{aligned}
0 &= \emptyset \\
1 &= \{0\} = \{\emptyset\} \\
2 &= \{0, 1\} = \{\emptyset, \{\emptyset\}\} \\
3 &= \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
4 &= \{0, 1, 2, 3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \\
&\dots \\
\omega &= \{0, 1, 2, 3, 4, \dots\} \\
\omega + 1 &= \omega \cup \{\omega\} = \{0, 1, 2, 3, 4, \dots\} \cup \{\omega\} \\
\omega + 2 &= \omega \cup \{\omega, \omega + 1\} \\
&\dots \\
\omega + \omega &= \omega \cdot 2 = \{0, 1, 2, 3, 4, \dots\} \cup \{\omega, \omega + 1, \omega + 2, \omega + 3, \omega + 4, \dots\}
\end{aligned}
$$

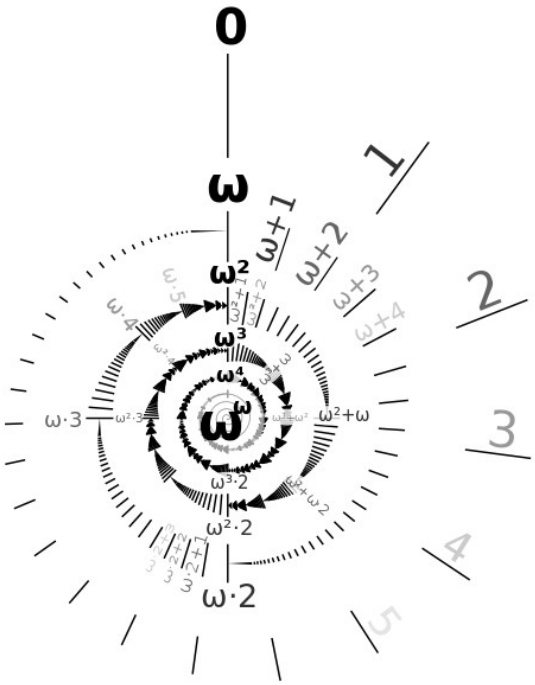


Figure 1.1: A stylized image of the ordinals up to ω^ω

With this concrete representation of the ordinals, we can easily be more precise about ordinal arithmetic. We first introduce the following notions.

Definition 1.2.8. Let X be a nonempty set of ordinals. Then the *supremum* of X, denoted $\sup(X)$, is the least ordinal that is greater than or equal to every element of X.

Exercise 1.2.9. Working with our concrete representation of the ordinals, prove that, for every nonempty set of ordinals X, the supremum of X is equal to the union of all of the elements of X, i.e.,

$$\sup(X) = \bigcup X.$$

Definition 1.2.10. Suppose that β is an ordinal.

1. We say that β is a *successor* ordinal if $\beta = \alpha + 1$ for some ordinal α.
2. If β is not a successor ordinal, we say that β is a *limit* ordinal.

We can now rigorously define ordinal arithmetic by recursion. We first deal with addition. For all ordinals α, we let:

- $\alpha + 0 = \alpha$;
- $\alpha + 1 = \alpha \cup \{\alpha\}$;
- for all ordinals β, we have $\alpha + (\beta + 1) = (\alpha + \beta) + 1$;
- if γ is a nonzero limit ordinal, then $\alpha + \gamma = \sup\{\alpha + \beta \mid \beta < \gamma\}$.

Next, multiplication:

- $\alpha \cdot 0 = 0$;
- $\alpha \cdot 1 = \alpha$;
- for all ordinals β, we have $\alpha \cdot (\beta + 1) = (\alpha \cdot \beta) + \alpha$;
- if γ is a nonzero limit ordinal, then $\alpha \cdot \gamma = \sup\{\alpha \cdot \beta \mid \beta < \gamma\}$.

Finally, exponentiation:

- $\alpha^0 = 1$;
- $\alpha^1 = \alpha$;
- for all ordinals β, we have $\alpha^{\beta+1} = (\alpha^\beta) \cdot \alpha$;
- if γ is a nonzero limit ordinal, then $\alpha^\gamma = \sup\{\alpha^\beta \mid \beta < \gamma\}$.

1.3 The hydra

We end this first lecture with a surprising demonstration of the utility of infinite ordinals: the hydra game. You may be familiar with the Hydra from Greek mythology. It is a fearsome water monster with many heads with the property that, whenever you chop off one of its heads, two heads will grow back in its place. Eventually, the hydra was slain by Heracles, with the assistance of his nephew Iolaus.

We will be examining a game played using a mathematical version of the Hydra introduced in the paper "Accessible independence results for Peano Arithmetic" by Laurie Kirby and Jeff Paris. For us, a *hydra* is a finite tree with a root. In other words, a hydra consists of finitely many nodes and edges. There is a root node at the bottom, which has finitely many edges coming out of it,

each leading to another node. In turn, each of these nodes has finitely many edges coming out of it, each leading to a further node, and so on. For example, this is a hydra:

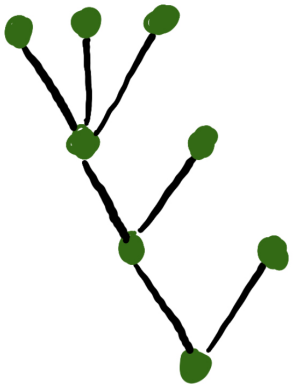


Figure 1.2: A hydra

We will always draw hydras with the root at the bottom. A *terminal node* of a hydra is a non-root node that is connected to only one other node. A *head* of a hydra consists of a terminal node and the single edge that leads to it. For example, the hydra pictured above has five heads:

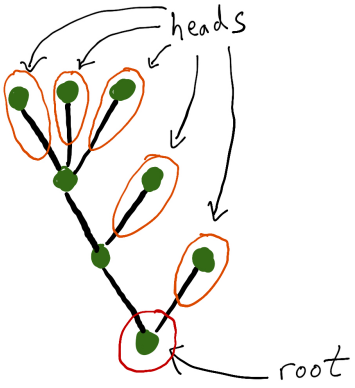


Figure 1.3: A hydra with its root and heads labeled

Given a head, the single node that it is attached to is called its *parent*. If its parent is not the root, then the node that is one step closer to the root from its parent is called its *grandparent*:

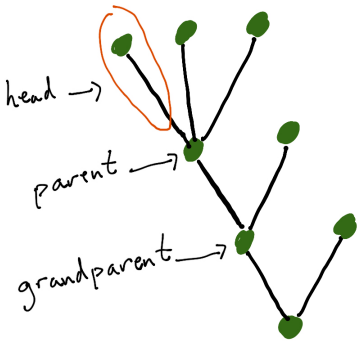


Figure 1.4: A hydra with a labeled head, its parent, and its grandparent

In the hydra game, we start with a hydra and, on each move (starting with Move 1), we chop off one of its heads. Our goal is to reduce the hydra to only a root node in a finite number of moves. However, like its mythological counterpart, the hydra regenerates, according to the following rules:

- If, on Move n, we chop off a head directly connected to the root, then the hydra does not create any new heads.
- If, on Move n, we chop off a head *not* directly connected to the root, then first delete the node and edge that make up that head. Then, move down one edge towards the root, to the edge connecting the parent and the grandparent of the head that was removed. The hydra makes n new copies of the subtree consisting of this edge and everything above it and attaches each of these new copies to the grandparent of the head that was removed.

This is best illustrated with a picture. Suppose that we are about to make Move 2 of a game, and we are confronted with the hydra pictured above. One option is to chop off the head in the bottom right, directly connected to the root:

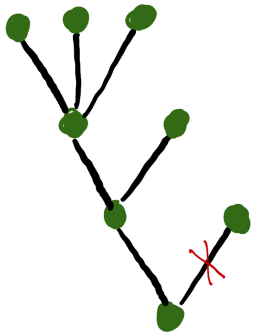


Figure 1.5: Chopping off a head directly connected to the root

Since this head is directly connected to the root, the hydra does not generate any new heads, so on our next move we see the following hydra:

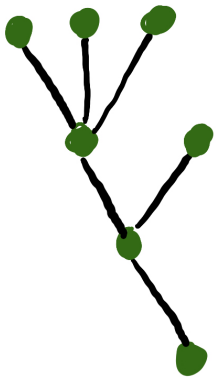


Figure 1.6: The result of the move in Figure 1.5

However, we could have done something different on Move 2 and instead chopped off the head on the upper left:

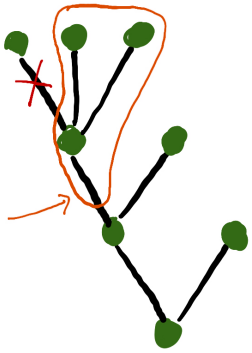


Figure 1.7: Chopping off a head not directly connected to the root

Now, to generate the hydra for the next move, we first remove the head. Then we consider the subtree consisting of the edge between the head's parent and grandparent and everything above it (circled in orange in Figure 1.6). Since we are on Move 2, we make 2 new copies of it and attach them to the grandparent of the removed head, resulting in the following hydra:

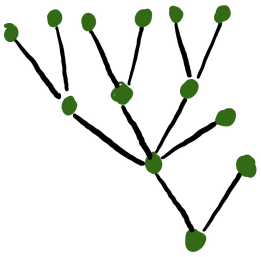


Figure 1.8: The result of making the move in Figure 1.7 on Move 2

Let us see now a complete play of the game, starting from a very simple hydra:

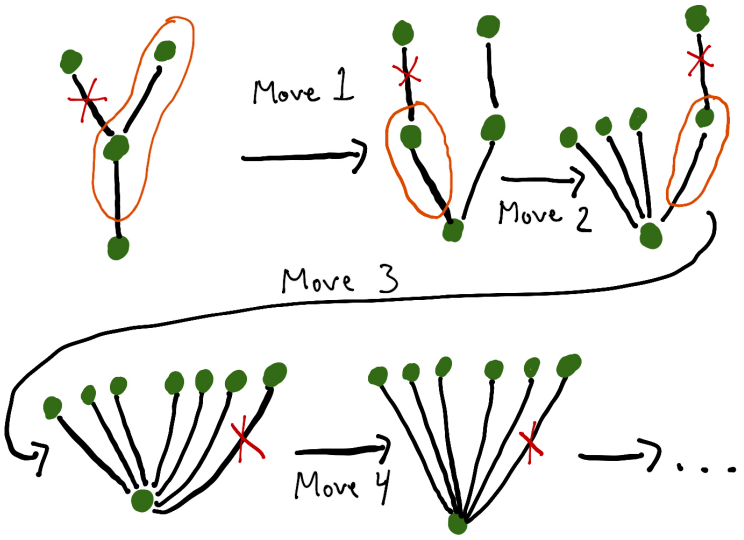


Figure 1.9: A play of the hydra game

We begin with a simple hydra with two heads. In Move 1, we chop off the left head. The head is not connected to the root, so we make one new copy of the circled region and connect it to the head's grandparent (which in this case is the root). The hydra we are left with still has two heads. In Move 2, we chop off the left head. Again, this is not connected to the root, so we make two new copies of the circled region and connect them them to the head's grandparent. In Move 3, we chop off the right head (the only one left that is not directly connected to the root). We make three new copies of the circled region and connect them to the head's grandparent. We are then left with a hydra that has seven heads, but each of them is directly connected to the root. We can thus chop them off one at a time, winning the game after seven more moves.

We thus won this round of the hydra game, but maybe that is only because we started with a very simple hydra. Consider the following diagram, taken from the paper by Kirby and Paris in which the hydra game was intro-

duced, depicting the first three moves in a hydra game starting from a more complicated hydra:

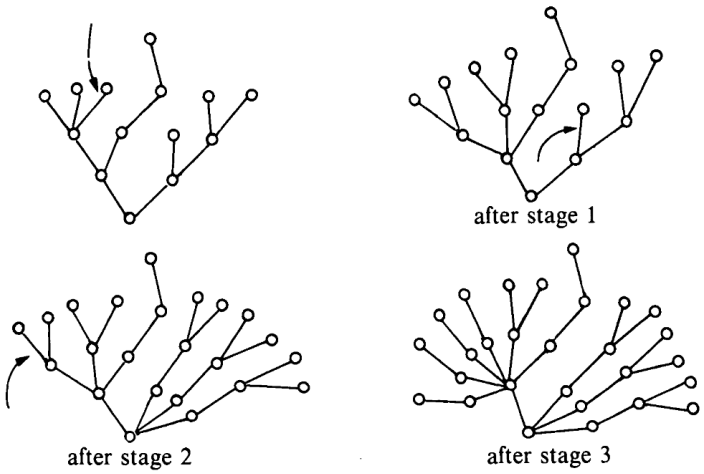


Figure 1.10: The first three moves of a more complicated hydra game

Here, the hydra we end up with after three moves looks, to the untrained eye, to be significantly larger and more complicated than the one we started with, and it seems conceivable that we will never win this hydra game. However, we will prove the following somewhat surprising theorem, showing that not only can we win *every* hydra game, but in fact we *cannot lose*.

Theorem 1.3.1. *In every hydra game, no matter how we play, we will always win after a finite number of moves.*

Proof. We will denote runs of the hydra game by $\langle H_0, H_1, H_2, \ldots \rangle$, where H_0 is the initial hydra that starts the game, H_1 is the hydra resulting after Move 1, H_2 is the hydra resulting after Move 2, and, in general, H_k is the hydra resulting after Move k. If we ever reach an n such that H_n is the hydra consisting of just a root node, then we have won the game, so the complete run of the game is then $\langle H_0, H_1, H_2, \ldots, H_n \rangle$. We must show that every possible run of the hydra game is finite.

To do this, given an arbitrary hydra H, we will assign it an ordinal number, $\#(H)$ in the following way. Starting with the terminal nodes and working our way down to the root, we will assign an ordinal number to each node of the hydra. Each terminal node gets labeled with a 0. Now suppose that u is a non-terminal node of H and we have labeled all of the nodes that are directly above u (i.e., above u and connected to it by an edge). Suppose that there are m such nodes, and they are labeled with ordinal numbers $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_m$ (arranged in non-increasing order). Then label u with the ordinal

$$\omega^{\alpha_1} + \omega^{\alpha_2} + \cdots + \omega^{\alpha_m}.$$

Finally, let $\#(H)$ equal the ordinal number that is assigned to the root of H by this process. Here are a couple of simple examples to illustrate this.

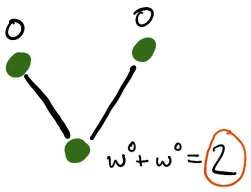


Figure 1.11: A hydra H with $\#(H) = 2$

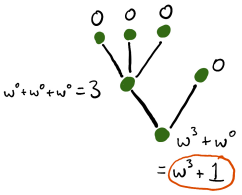


Figure 1.12: A hydra H with $\#(H) = \omega^3 + 1$

If we calculate $\#(H)$ for the first hydra presented above, we find that it is equal to $\omega^{\omega^3+1} + 1$:

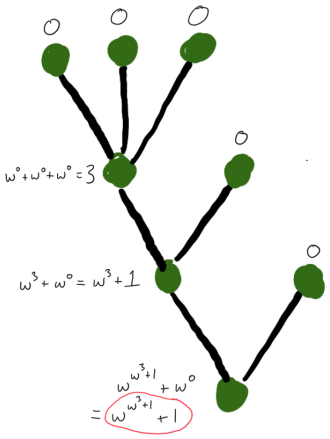


Figure 1.13: A hydra H with $\#(H) = \omega^{\omega^3+1} + 1$.

Now let's see what happens to the ordinal number assigned to this hydra if we make a play of the hydra game and chop off one of its heads. Let's suppose that we are at Move 2 and chop off the left head of this hydra, as depicted in Figure 1.7 above. The resulting hydra H' is depicted in Figure 1.8 above, and we can calculate $\#(H')$ to be $\omega^{\omega^{2\cdot 3+1}} + 1$:

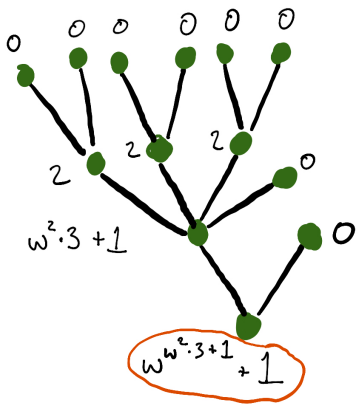


Figure 1.14: A hydra H' with $\#(H') = \omega^{\omega^2 \cdot 3+1} + 1$

Notice that $\omega^2 \cdot 3 < \omega^3$, so $\omega^{\omega^2 \cdot 3+1} + 1 < \omega^{\omega^3+1} + 1$, i.e., $\#(H') < \#(H)$. Thus, by making a move in the hydra game and chopping off a head of H, we created a new hydra H' such that, even though H' has more heads than H, its ordinal value is strictly *smaller*. This is not a coincidence.

Exercise 1.3.2. Calculate the ordinal numbers assigned to the hydras appearing in the run of the hydra game depicted in Figure 1.9 above.

You should have found in the above exercise that the ordinal values assigned to the hydras were strictly decreasing throughout the run of the game. We can in fact prove that this is always the case. The following is the key step of this proof; for now, we leave it as an exercise.

Exercise 1.3.3. Suppose that $\langle H_0, H_1, H_2, H_3, \ldots \rangle$ is a run of the hydra game. Prove that $\#(H_0) > \#(H_1) > \#(H_2) > \#(H_3) > \ldots$. In other words, performing a move in the hydra game always strictly decreases the value of the ordinal assigned to the hydra. (**Hint.** First prove the following basic fact about ordinal arithmetic: for every ordinal α and every natural number n, we have $\omega^\alpha \cdot n < \omega^{\alpha+1}$.)

With the previous exercise, though, we can finish the proof of the theorem! For every run of the hydra game $\langle H_0, H_1, H_2, H_3, \ldots \rangle$, we obtain a strictly decreasing sequence of ordinals $\#(H_0) > \#(H_1) > \#(H_2) > \#(H_3) > \ldots$. Since the ordinals are themselves well-ordered, there can be no infinite strictly decreasing sequences of ordinals. Therefore, *every* run of the hydra game must be finite. In other words, no matter how you play the hydra game, you will always win after some finite number of moves. □

1.4 Peano arithmetic

Our use of infinite ordinals to prove that every hydra game must end after finitely many moves may seem counterintuitive and perhaps unnecessary. The theorem about hydra games is, after all, a statement that is entirely about finite objects. Why should we need to reason about infinite ordinals in order

to prove it? However, a remarkable theorem of Kirby and Paris shows that something like this *is* indeed necessary to prove the theorem.

You may have seen before the axioms of Peano Arithmetic (PA), introduced by Giuseppe Peano in the 19th century. These axioms are meant to capture our intuition about the behavior of the natural numbers, and hence about finite discrete objects more broadly.

The language of Peano arithmetic consists of

- the equality sign $=$;
- a constant symbol 0;
- a unary function symbol S.

The intended interpretation of the function S is that it returns the *successor* of its input, i.e., $S(n) = n + 1$. Peano arithmetic has five axioms that are meant to describe the arithmetical properties of the *natural numbers*. These axioms can be stated as follows:

1. 0 is a natural number.
2. For every natural number n, $S(n)$ is also a natural number.
3. For all natural numbers m and n, if $S(m) = S(n)$, then $m = n$.
4. For every natural number n, $0 \neq S(n)$, i.e., 0 is not the successor of any natural number.
5. (Induction) If K is a set such that
   - 0 is in K; and
   - for every natural number n, if n is in K, then $S(n)$ is also in K,

   then K contains every natural number.

Peano Arithmetic captures much of our intuition about the natural numbers, and many theorems about the natural numbers or finite discrete objects can be proven using only PA. For example, much of number theory, as well as the finite Ramsey theorem, can be established in PA. However, Kirby and Paris proved that PA is *not* strong enough to prove that every hydra game must end in a finite number of moves. In fact, they proved the following (stated in a slightly imprecise way):

Theorem 1.4.1 (Kirby–Paris)**.** *If a set of axioms can prove that every hydra game must end in a finite number of moves, then it can also prove the consistency of* PA*.*

By Gödel's Second Incompleteness Theorem, PA cannot prove its own consistency. Therefore, the Kirby–Paris theorem implies that we cannot prove our theorem about hydra games using PA alone; we must use *something* that goes beyond it.

Chapter 2

Lecture 2: Transfinite induction and recursion

Two of the principal reasons for the centrality of well-orderings in set theory and its applications to other fields of mathematics are the techniques of transfinite induction and transfinite recursion. Let us briefly recall these techniques, in both a formal formulation and a more informal one that better reflects how we actually think about them in practice.

2.1 Transfinite induction

To motivate the statement of transfinite induction, recall classical induction on the natural numbers:

Principle of induction: Suppose that P is a property that can hold of natural numbers and suppose that we know the following:

> For all $n \in \mathbb{N}$, if $P(m)$ holds for all $m < n$, then $P(n)$ holds.

Then $P(n)$ holds for all $n \in \mathbb{N}$.

A similar principle holds for arbitrary well-ordered sets, not just for $\mathbb{N}$.

Theorem 2.1.1 (Transfinite induction)**.** *Suppose that $(X, \preceq)$ is a well-order, (or X is the class of all ordinals, and $\preceq$ is the usual ordering of ordinals) and suppose that P is a property that can hold of elements of X. Suppose moreover that we know the following:*

> *For all $y \in X$, if $P(x)$ holds for all $x \prec y$, then $P(y)$ holds.*

Then $P(y)$ holds for all $y \in X$.

As a simple illustration, let us prove that ordinal addition is associative.

Theorem 2.1.2. *For all ordinals α, β, γ, we have $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.*

Proof. The proof is by induction on γ. Thus, fix ordinals α and β. We will prove the following:

> For every ordinal γ, if $(\alpha + \beta) + \varepsilon = \alpha + (\beta + \varepsilon)$ for all $\varepsilon < \gamma$, then $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.

Theorem 2.1.1 will them imply that $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ for all ordinals γ.

To this end, fix an ordinal γ, and suppose that $(\alpha+\beta)+\varepsilon = \alpha+(\beta+\varepsilon)$ for all $\varepsilon < \gamma$. We must show that $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$. The proof splits into three cases, based on whether $\gamma = 0$, γ is a successor ordinal, or γ is a nonzero limit ordinal.

Case 1: $\gamma = 0$**.** Recall that, for any ordinal δ, we have $\delta + 0 = \delta$. Thus, we have

$$(\alpha + \beta) + 0 = \alpha + \beta = \alpha + (\beta + 0),$$

as desired.

Case 2: γ **is a successor ordinal.** Let ε be such that $\gamma = \varepsilon + 1$. Recall that, by definition of ordinal addition, we know that, for all ordinals δ, we have $\delta + (\varepsilon + 1) = (\delta + \varepsilon) + 1$. Then

$$\begin{aligned}(\alpha + \beta) + \gamma &= (\alpha + \beta) + (\varepsilon + 1)\\ &= ((\alpha + \beta) + \varepsilon) + 1\\ &= (\alpha + (\beta + \varepsilon)) + 1\\ &= \alpha + ((\beta + \varepsilon) + 1)\\ &= \alpha + (\beta + (\varepsilon + 1))\\ &= \alpha + (\beta + \gamma),\end{aligned}$$

where the equality between lines 2 and 3 follow from the inductive hypothesis and all other equalities follow from the definition of ordinal addition.

Case 3: γ **is a nonzero limit ordinal.** In this case recall that, by the definition of ordinal addition, for every ordinal δ,

$$\delta + \gamma = \sup\{\delta + \varepsilon \mid \varepsilon < \gamma\}.$$

Now we have

$$\begin{aligned}(\alpha + \beta) + \gamma &= \sup\{(\alpha + \beta) + \varepsilon \mid \varepsilon < \gamma\}\\ &= \sup\{\alpha + (\beta + \varepsilon) \mid \varepsilon < \gamma\}\\ &= \alpha + \sup\{\beta + \varepsilon \mid \varepsilon < \gamma\}\\ &= \alpha + (\beta + \gamma),\end{aligned}$$

where the equality between lines 1 and 2 follows from the inductive hypothesis and all other equalities follow from the definition of ordinal arithmetic.

This completes all three cases and thus the proof of the theorem. □

Another example of a proof by transfinite induction involves *strictly increasing functions*.

Definition 2.1.3. Suppose that $(A, \leq_A)$ and $(B, \leq_B)$ are two well-orders. Then a function $f : A \to B$ is said to be *strictly increasing* if, for all $x, y \in A$, we have

$$(x <_A y) \implies (f(x) <_B f(y)).$$

Exercise 2.1.4. Suppose that $(A, \leq_A)$ is a well-order and $f : A \to A$ is strictly increasing. Prove that $x \leq f(x)$ for all $x \in A$.

2.2 Transfinite recursion

You are probably familiar with the notion of a *sequence* indexed by the natural numbers. For example, the sequence $\langle 1/2^n \mid n < \omega \rangle$ is the sequence $\langle 1, 1/2, 1/4, 1/8, \ldots \rangle$. But we can equally well have sequences indexed by other ordinal numbers.

Definition 2.2.1. Let α be an ordinal. An *α-sequence* is a sequence of the form $\langle x_\eta \mid \eta < \alpha \rangle$, i.e., a sequence that is indexed by the set of ordinals less than η.

Roughly speaking, a construction of a sequence by *recursion* is a construction done by specifying one element at a time, with the choice of a particular element possibly depending on the initial segment of the sequence that has been constructed so far. For example, the ω-sequence $\langle 1/2^n \mid n < \omega \rangle$ can be given a recursive definition as follows:

- $x_0 = 1$;
- for all $n < \omega$, $x_{n+1} = x_n/2$.

In general, it is not hard to see that, if one is given a rule for selecting x_0 and, given x_n, a rule for selecting x_{n+1}, then there is exactly one sequence $\langle x_n \mid n < \omega \rangle$ that satisfies these rules.

Another well-known recursively defined sequence is the *Fibonacci* sequence, $\langle 0, 1, 1, 2, 3, 5, 8, 13, \ldots \rangle$, defined recursively as follows:

- $x_0 = 0$;
- $x_1 = 1$;
- for all $n < \omega$, $x_{n+2} = x_n + x_{n+1}$.

Just as with induction, recursion can be extended to arbitrary well-orders.

Theorem 2.2.2 (Transfinite recursion)**.** *Suppose that α is an ordinal and Z is a nonempty set. Let $\mathcal{S}$ be the set of all sequences of elements of Z of length less than α, and suppose that $F : \mathcal{S} \to Z$ is a function. Then there is a unique sequence $\langle x_\eta \mid \eta < \alpha \rangle$ such that, for all $\xi < \alpha$, we have*

$$x_\xi = F(\langle x_\eta \mid \eta < \xi \rangle).$$

Informally speaking, Theorem 2.2.2 is saying that one can construct sequences by (arbitrarily long) transfinite recursion. In applications of the theorem, one is typically seeking to construct an α-sequence for some ordinal α. The function F in the theorem is describing a rule that tells you how to pick the *next* element of the sequence given what has come so far. The theorem then says that there is exactly one sequence that satisfies all of these rules.

We have in fact already seen recursive constructions; the rigorous definitions of ordinal arithmetic given in Chapter 1 were definitions by transfinite recursion.

In practice, when applying transfinite recursion, we typically want to produce an α-sequence $\langle x_\eta \mid \eta < \alpha \rangle$ of elements of a set Z such that the sequence satisfies certain desired properties. The construction of such a sequence will typically consist of the following two steps:

1. For $\xi < \alpha$, describe a rule for choosing x_ξ based on the sequence $\langle x_\eta \mid \eta < \xi \rangle$ constructed so far. Sometimes this rule will break into cases depending on whether ξ is 0, a successor ordinal, or a nonzero limit ordinal, though sometimes these distinctions will not matter.

2. Show that a sequence constructed according to this rule will have the desired properties.

2.3 Well-ordering principle

Transfinite induction and transfinite recursion gain additional power when paired with the well-ordering principle, which can be stated as follows.

Theorem 2.3.1 (Well-ordering principle)**.** *For every set X, there is a binary relation $\preceq$ on X such that $(X, \preceq)$ is a well-order.*

We have stated the well-ordering principle as a theorem, and it is indeed a theorem of ZFC. Over the axioms of ZF (which are just the axioms of ZFC without the axiom of choice), it turns out that the well-ordering principle is *equivalent* to the axiom of choice, so one could just as well think of it as an alternative formulation of the axiom of choice.

Since the ordinal numbers are themselves well-ordered, we know that, for every *cardinal* number κ, there is a *minimal* ordinal of cardinality κ. In practice, we identify the cardinal κ with this ordinal, which we will also refer to as κ. A key property of this ordinal κ is the following:

> Every proper initial segment of κ has cardinality strictly less than κ.

This is useful enough in practice that it is worth it to state a more refined version of the well-ordering principle.

Theorem 2.3.2 (Well-ordering principle, version 2)**.** *Suppose that X is a set and $\kappa = |X|$. Then there is a sequence $\vec{x} = \langle x_\alpha \mid \alpha < \kappa \rangle$ such that*

- *$X = \{x_\alpha \mid \alpha < \kappa\}$; and*
- *$\vec{x}$ is injective, i.e., for all $\alpha < \beta < \kappa$, we have $x_\alpha \neq x_\beta$.*

2.4 Applications of transfinite recursion to Euclidean space

In this section, we apply the tools of transfinite recursion to construct interesting objects in Euclidean space, focusing in particular on $\mathbb{R}^2$ and $\mathbb{R}^3$. This will involve transfinite recursions of length $|\mathbb{R}|$. We denote the cardinality of $\mathbb{R}$ by $\mathfrak{c}$; sometimes this cardinal is simply referred to as "the continuum". As you may know, the precise value of $\mathfrak{c}$ is not determined by the axioms of ZFC. It could be $\aleph_1$, $\aleph_2$, or more generally any cardinal κ such that the cofinality of κ is uncountable. Note that

$$\mathfrak{c} = |\mathbb{R}| = |\mathbb{R}^2| = |\mathbb{R}^3| = \ldots = |\mathbb{R}^\omega|.$$

Our first example, due to Mazurkiewicz, establishes the existence of a so-called *two-point set*.

Theorem 2.4.1. *There is a subset A of $\mathbb{R}^2$ such that every straight line in $\mathbb{R}^2$ intersects A in exactly two points.*

Proof. Let $\mathcal{L}$ be the set of all lines in $\mathbb{R}^2$. We first claim that $|\mathcal{L}| = \mathfrak{c}$. Here's one way to see that. First, there are *at least* $\mathfrak{c}$-many lines, since, for example, for every real number r, the equation $y = r$ describes a unique horizontal line in $\mathbb{R}^2$. Thus, $|\mathcal{L}| \geq \mathfrak{c}$. On the other hand, to see that $|\mathcal{L}| \leq \mathfrak{c}$, note that, to specify a line in $\mathbb{R}^2$, it suffices to specify two distinct points on the line. There are only $\mathfrak{c} \times \mathfrak{c} = \mathfrak{c}$-many ways of choosing two points in $\mathbb{R}^2$. Thus, $|\mathcal{L}| \leq \mathfrak{c}$.

Using the well-ordering principle, we can fix an injective sequence $\langle \ell_\alpha \mid \alpha < \mathfrak{c} \rangle$ of lines in $\mathbb{R}^2$ such that every element of $\mathcal{L}$ is equal to ℓ_α for some $\alpha < \mathfrak{c}$. We will recursively construct a sequence $\langle A_\alpha \mid \alpha < \mathfrak{c} \rangle$ satisfying the recursion requirements that, for every $\beta < \mathfrak{c}$:

1. A_β is a subset of $\mathbb{R}^2$ of size at most 2;
2. $\bigcup_{\alpha \leq \beta} A_\alpha$ does not contain any three points that lie on the same line;
3. $\bigcup_{\alpha \leq \beta} A_\alpha$ contains exactly two points on the line ℓ_β.

If we can succeed in this construction, then the set $A = \bigcup_{\alpha < \mathfrak{c}} A_\alpha$ will be as required by the theorem. Let us now describe the recursive construction.

Fix an ordinal $\beta < \mathfrak{c}$ and suppose that we have constructed $\langle A_\alpha \mid \alpha < \beta \rangle$ that satisfies the recursion requirements so far. The following describes how to choose a set A_β to continue the construction.

Let $B = \bigcup_{\alpha < \beta} A_\alpha$, i.e., B is the set of points that we have chosen so far. Let $\mathcal{G}$ be the set of all lines passing through two points of B. Note that

$$|\mathcal{G}| \leq |B| \times |B| \leq |\beta| \times |\beta| < \mathfrak{c}.$$

When choosing A_β, we must be careful not to add any new points that are on lines in $\mathcal{G}$ to satisfy requirement (2) above.

Consider the line ℓ_β. We must make sure that $\bigcup_{\alpha \leq \beta} A_\beta$ contains exactly two points on ℓ_β to satisfy requirement (3) above. If B already contains two points from ℓ_β, then we can simply let $A_\beta = \emptyset$ and move on to the next step. If B contains either 0 or 1 points from ℓ_β, then notice that $\ell_\beta \notin \mathcal{G}$, and therefore every line in $\mathcal{G}$ intersects ℓ_β in at most one point. Since $|\mathcal{G}| < \mathfrak{c}$ and the number of points on ℓ_β is exactly $\mathfrak{c}$, we know that $|\ell_\beta \setminus \bigcup \mathcal{G}| = \beth$, i.e., there are $\mathfrak{c}$-many points on ℓ_β that are not on any of the lines in $\mathcal{G}$.

If B contains 0 points from ℓ_β, then let A_β consist of precisely 2 points from $\ell_\beta \setminus \bigcup \mathcal{G}$, and if B contains 1 point from ℓ_β, then let A_β consist of precisely 1 point from $\ell_\beta \setminus \bigcup \mathcal{G}$. This completes the description of stage β of the construction; one can check that we have maintained the recursion requirements (1) – (3). Thus, this completes the construction and the proof of the theorem. □

The next results concern "circles" in Euclidean space. These are probably what you intuitively expect them to be. By "circle" we mean the boundary of the circle, not its interior. We consider only nontrivial circles, i.e., circles whose radius is strictly positive. In $\mathbb{R}^2$, one can specify a circle by fixing real numbers x_0 and y_0 and a radius $r > 0$; the circle is then the set of all points $(x, y) \in \mathbb{R}^2$ such that $(x - x_0)^2 + (y - y_0)^2 = r^2$. One can do something similar, but more complicated, in $\mathbb{R}^3$: one can specify a circle by first specifying a plane

in $\mathbb{R}^3$ and then specifying a circle in that plane in the same way as we did in $\mathbb{R}^2$. However, for what we want to discuss here, these formal descriptions are not necessary and may even get in the way of intuition. The two basic facts we will need about circles are the following:

Fact 2.4.2. *Suppose that a, b, and c are any three points in $\mathbb{R}^2$ or $\mathbb{R}^3$ that are not all on the same line. Then there is a unique circle that contains all three points.*

Fact 2.4.3. *If C_0 and C_1 are two distinct circles in $\mathbb{R}^2$ or $\mathbb{R}^3$, then C_0 and C_1 intersect in at most two points.*

First, we have an exercise giving a variant on Theorem 2.4.1.

Exercise 2.4.4. There is a subset A of $\mathbb{R}^2$ such that every circle in $\mathbb{R}^2$ intersects A in exactly three points.

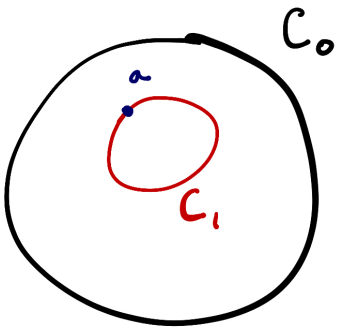
The next example concerns covering Euclidean space by pairwise disjoint circles. Let us say precisely what we mean by this. If $\mathcal{C}$ is a set of circles (in either $\mathbb{R}^2$ or $\mathbb{R}^3$), then we say that $\mathcal{C}$ is *pairwise disjoint* if, for all distinct $C_0, C_1 \in \mathcal{C}$, we have $C_0 \cap C_1 = \emptyset$. In other words, $\mathcal{C}$ is pairwise disjoint if no two distinct element of $\mathcal{C}$ intersect each other.

We say that a pairwise disjoint set $\mathcal{C}$ of circles *covers* $\mathbb{R}^2$ (or $\mathbb{R}^3$) if every element of $\mathbb{R}^2$ (or $\mathbb{R}^3$) is in an element of $\mathcal{C}$. In other words, $\mathcal{C}$ covers $\mathbb{R}^2$ (or $\mathbb{R}^3$) if $\bigcup \mathcal{C} = \mathbb{R}^2$ (or $\bigcup \mathcal{C} = \mathbb{R}^3$). Note that, since $\mathcal{C}$ is pairwise disjoint, if $\mathcal{C}$ covers $\mathbb{R}^2$ or $\mathbb{R}^3$, then every point is in *exactly* one element of $\mathcal{C}$.

We are interested in the question of whether Euclidean spaces can be covered by pairwise disjoint sets of circles and, if they can, what further requirements we can place on these circles. We first show that this is impossible for $\mathbb{R}^2$.

Theorem 2.4.5. *$\mathbb{R}^2$ cannot be covered by a pairwise disjoint set of circles.*

Proof. The key observation about $\mathbb{R}^2$ is the following: every circle in $\mathbb{R}^2$ divides the rest of the plane into a region *inside* the circle and a region outside the circle. If C_0 is a circle and a is a point *inside* of C_0, then any circle C_1 containing a that is disjoint from C_0 must itself lie entirely inside of C_1 (see picture below).



Now suppose for the sake of contradiction that $\mathcal{C}$ is a pairwise disjoint set of circles that covers $\mathbb{R}^2$. Simultaneously recursively define sequences $\langle C_n \mid n < \omega \rangle$ and $\langle a_n \mid n < \omega \rangle$ as follows:

- C_0 is an arbitrary element of $\mathcal{C}$;
- for each $n < \omega$, a_n is the *center* of the circle C_n;
- for each $n < \omega$, C_{n+1} is the unique element of $\mathcal{C}$ that passes through a_n.

In other words, C_0 is an arbitrary element of $\mathcal{C}$, C_1 is the unique element of $\mathcal{C}$ that passes through the center of C_0, C_2 is the unique element of $\mathcal{C}$ that passes through the center of C_1, and so on. By the observation above, for each $n < \omega$, the circle C_{n+1} lies entirely inside of C_n. Moreover, since C_{n+1} passes through the *center* of C_n, the radius of C_{n+1} must be less than half the radius of C_n. For all $n < \omega$, let r_n denote the radius of C_n. We have shown that

$$r_{n+1} < \mathfrak{r}_n 2$$

for all n, and hence the radii $\langle r_n \mid n < \omega \rangle$ converge to 0. Therefore, the centers $\langle a_n \mid n < \omega \rangle$ of the circles $\langle C_n \mid n < \omega \rangle$ converge to a single limit point; call this limit point b.

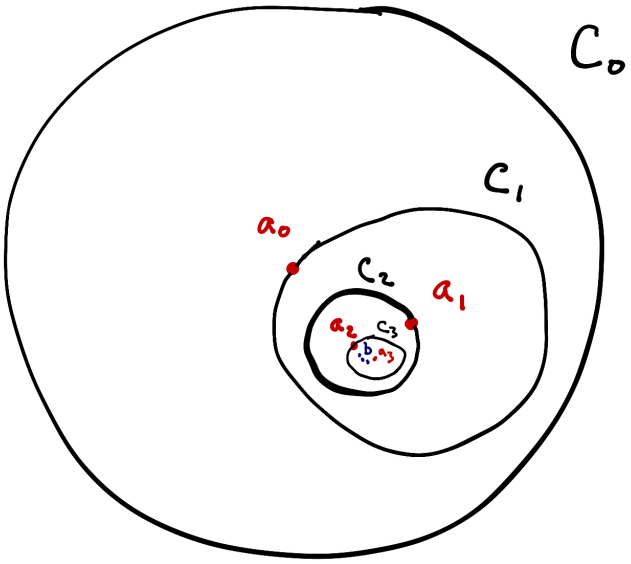


Figure 2.1: The centers $\langle a_n \mid n < \omega \rangle$ of the circles converging to a limit point b.

Notice that b must lie on the *inside* of C_n for every $n < \omega$.

We are assuming that $\mathcal{C}$ covers $\mathbb{R}^2$. We can therefore find a circle $C^* \in \mathcal{C}$ such that $b \in C^*$. Since b is *inside* C_n for all $n < \omega$, we know that C^* cannot be equal to C_n for any $n < \omega$. Let r^* be the radius of C^*. Since the radii $\langle r_n \mid n < \omega \rangle$ converge to 0, we can fix an $n < \omega$ such that $r_n < r^*$. But now we know the following two things:

1. C^* contains a point on the inside of C_n, namely b.

2. The radius of C^*, r^*, is larger than the radius of C_n, r_n. Therefore, C^* cannot be entirely contained in the inside of C_n.

It follows from the two items above that C^* contains points both inside and outside C_n and therefore it must intersect C_n:

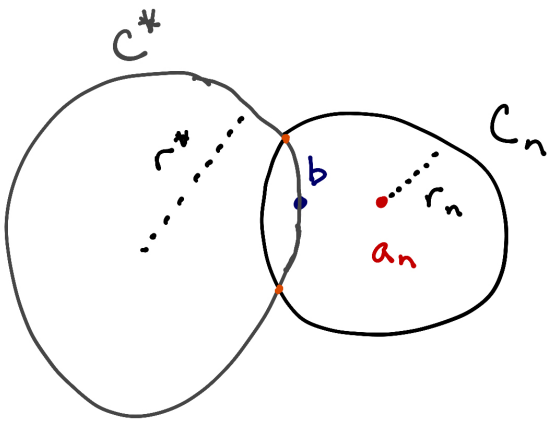


Figure 2.2: C^* contains points both inside and outside C_n, so they must intersect.

However, C^* and C_n are distinct elements of $\mathcal{C}$, which was supposed to be a pairwise disjoint family. This is a contradiction, thus proving the theorem. □

However, perhaps surprising, we now show that $\mathbb{R}^3$ *can* be covered by a pairwise disjoint set of circles. The key difference between $\mathbb{R}^3$ and $\mathbb{R}^2$ with respect to this problem is that, in $\mathbb{R}^3$, unlike in $\mathbb{R}^2$, a circle no longer divides the rest of the space into "inside" and "outside", and this gives us much more freedom to construct interesting sets of circles. For instance, we can have two disjoint circles that are *linked*, like successive rings in a chain.

We will prove, in fact, not only that $\mathbb{R}^3$ can be covered by a pairwise disjoint set of circles, but that all of the circles in this set can be required to have any specified radius (we will construct such a set containing only circles of radius 1).

Theorem 2.4.6. *There is a pairwise disjoint family $\mathcal{C}$ of circles in $\mathbb{R}^3$ such that*

1. *every circle in $\mathcal{C}$ has radius 1; and*
2. *$\mathcal{C}$ covers $\mathbb{R}^3$.*

Proof. Let $\langle a_\alpha \mid \alpha < \mathfrak{c} \rangle$ be an injective sequence of points in $\mathbb{R}^3$ such that every point in $\mathbb{R}^3$ is equal to a_α for some $\alpha < \mathfrak{c}$.

We will recursive construct a sequence $\langle C_\alpha \mid \alpha < \mathfrak{c} \rangle$ satisfying the recursion requirements that, for every $\beta < \mathfrak{c}$:

1. C_β is either the empty set or a circle in $\mathbb{R}^3$ of radius 1;
2. for all $\alpha < \beta$, we have $C_\alpha \cap C_\beta = \emptyset$;

3. $a_\beta \in \bigcup_{\alpha \leq \beta} C_\beta$.

If we can succeed in this construction, then the set

$$\mathcal{C} = \{C_\alpha \mid \alpha < \mathfrak{c} \text{ and } C_\alpha \text{ is a circle in } \mathbb{R}^3\}$$

is as required the theorem. Let us now describe the recursive construction.

Fix an ordinal $\beta < \mathfrak{c}$ and suppose that we have constructed $\langle C_\alpha \mid \alpha < \beta \rangle$ that satisfies the recursion requirements so far. The following describes how to choose C_β to continue the construction.

Consider the point a_β. If there is $\alpha < \beta$ such that $a_\beta \in C_\alpha$, then we can simply let $C_\beta = \emptyset$ and move on to the next step. Otherwise, to satisfy requirements (1) and (3), we need to choose C_β to be a circle in $\mathbb{R}^3$ of radius 1 that passes through x_β. To satisfy requirement (2), we must make sure that C_β is disjoint from C_α for all $\alpha < \beta$.

Let $\mathcal{B} = \{C_\alpha \mid \alpha < \beta \text{ and } C_\alpha \neq \emptyset\}$. In other words, $\mathcal{B}$ is the set of all circles chosen so far. Note that, for each $C_\alpha \in \mathcal{B}$, there is a unique plane P_α containing C_α. Moreover, there are precisely $\mathfrak{c}$-many planes that pass through the point a_β. Therefore, since $|\mathcal{B}| \leq |\beta| < \mathfrak{c}$, we can find a plane P^* passing through a_β such that, for every $C_\alpha \in \mathcal{B}$, P^* does not contain C_α.

Now note that, if P is a plane and C is a circle that is not contained in P, then C intersects P in at most two points. Let $Q = \bigcup_{\alpha<\beta} P^* \cap C_\alpha$, i.e., Q is the set of points in P^* that are in C_α for some $\alpha < \beta$. By the previous paragraph, $P^* \cap C_\alpha$ has size at most two for every $\alpha < \beta$. Therefore, we have $|Q| \leq |\beta| \times 2 < \mathfrak{c}$.

Let $\mathcal{D}$ be the set of circles C such that

- C passes through a_β;
- C is contained in P^*;
- C has radius 1.

We would like to choose an element of $\mathcal{D}$ to be our circle C_β. The following is left as an exercise:

Exercise 2.4.7. $|\mathcal{D}| = \mathfrak{c}$.

We need to require that C_β is disjoint from C_α for all $\alpha < \beta$. Since we are going to choose C_β to be contained in P^*, this amounts to choosing C_β so that it is disjoint from Q. Let us call a circle $C \in \mathcal{D}$ *bad* if $C \cap Q \neq \emptyset$. Let $\mathcal{D}^-$ be the set of bad elements of $\mathcal{D}$. For each $C \in \mathcal{D}^-$, choose $q_C \in C \cap Q$.

Our goal is to show that $\mathcal{D} \setminus \mathcal{D}^- \neq \emptyset$. The following is also left as an exercise:

Exercise 2.4.8. If u and v are two distinct points in a plane P, then there are at most two circles that are contained in P, pass through both u and v, and have radius 1.

By the exercise, for each $q \in Q$, there are at most *two* circles $C \in \mathcal{D}^-$ such that $q_C = q$. Since $|Q| < \mathfrak{c}$, it follows that

$$|\mathcal{D}^-| \leq |Q| \times 2 < \mathfrak{c}.$$

Since $|\mathcal{D}| = \mathfrak{c}$, we know that $\mathcal{D}$ contains circles that are not bad, so we can choose C_β to be any element of $\mathcal{D}$ that is not bad. This completes stage β of the construction. By our construction, we know that that:

- C_β is a circle of radius 1 passing through a_β;
- $C_\beta \cap C_\alpha = \emptyset$ for all $\alpha < \beta$,

so we have maintained the recursion requirements. This completes the construction of $\mathcal{C}$ and hence the proof of the theorem. $\square$

Chapter 3

Lecture 3: The axiom of choice and its consequences

The axiom of choice is an incredibly important, useful, and sometimes controversial axiom in set theory. It forms the "C" in "ZFC", which are the standard axioms of set theory. (The "Z" and "F" stand for "Zermelo" and "Fraenkel", respectively. "ZF" denotes the axioms of ZFC without the axiom of choice.) In this lecture, we review the axiom of choice and its equivalent formulations and present a couple basic applications thereof.

3.1 The axiom of choice

Roughly speaking, the axiom of choice asserts that, given any collection of nonempty sets, one can form a new collection by choosing one element from each set. More formally, it can be formulated as follows.

Definition 3.1.1 (Axiom of choice)**.** The *axiom of choice* is the following assertion: Whenever I is a set and $\langle X_i \mid i \in I \rangle$ is such that each X_i is a nonempty set, there is a sequence $\langle y_i \mid i \in I \rangle$ such that, for all $i \in I$, we have $y_i \in X_i$.

The axiom of choice can also be phrased in terms of functions:

> Whenever I is a set and F is a function with domain I such that $F(i)$ is a nonempty set for all $i \in I$, there is a function g with domain I such that $g(i) \in F(i)$ for all $i \in I$.

As we shall see, the axiom of choice is incredibly powerful and is essential to proving a number of important theorems. It can also lead to some counterintuitive consequences, which has led to it being somewhat controversial. Let us note now, though, that, due to a theorem of Gödel, there is no cost in consistency strength in assuming the axiom of choice.

Theorem 3.1.2 (Gödel)**.** *If the axioms of* ZF *are consistent, then so are the axioms of* ZFC*.*

(We refer the reader to any standard set theory textbook for a precise statement of the axioms of ZFC.)

There are a number of statements that are equivalent to the axiom of choice over ZF; we mention here two especially important ones. In fact, we have already seen one of them: the well-ordering principle, which states that every set can be well-ordered:

Definition 3.1.3 (Well-ordering principle)**.** The *well-ordering principle* is the following assertion: Whenever X is a set, there is a binary relation $\preceq$ on X such that $(X, \preceq)$ is a well-order.

The second important statement that is equivalent to the axiom of choice is known as *Zorn's lemma*. To state it properly, we first need a preliminary definition.

Definition 3.1.4. Suppose that $(X, \leq)$ is a partial order (recall Definition 1.1.1).

1. A subset $K \subseteq X$ is called a *chain* if K is linearly ordered by $\leq$, i.e., for all $x, y \in K$, either $x \leq y$ or $y \leq x$.

2. If $K \subseteq X$ and $z \in X$, then we say that z is an *upper bound* for K if $x \leq z$ for all $x \in K$.

We can now state Zorn's lemma.

Definition 3.1.5 (Zorn's lemma)**.** Zorn's lemma is the following assertion: Suppose that $(X, \leq)$ is a nonempty partial order such that every chain $K \subseteq X$ has an upper bound. Then X contains a *maximal* element, i.e., there is $y \in X$ such that, for all $z \in X$, we have $y \not< z$.

The following theorem establishes the equivalence of these three important statements. Recall that, if T is a set of axioms and φ and ψ are two statements in the language of T, then we say that φ and ψ are *equivalent* over T if one can prove ψ from $\mathsf{T} \cup \{\varphi\}$ *and* one can prove φ from $\mathsf{T} \cup \{\psi\}$.

We leave its proof as an exercise.

Theorem 3.1.6. *Over the axioms of* ZF*, the following are equivalent:*

1. *the axiom of choice;*

2. *the well-ordering principle;*

3. *Zorn's lemma.*

We say some applications of the well-ordering principle in the previous lecture. We now present two further applications, one using the axiom of choice directly, and the other using Zorn's lemma. Both are related to the general mathematical problem of measuring the *size* of mathematical objects.

3.2 A non-measurable set of real numbers

This section concerns the general task of measuring the size of sets of real numbers. One could of course measure each set of real numbers by its cardinality, but this does not really match with our geometric intuition about $\mathbb{R}$. For example, we already have some intuition about what the measures of certain very simple sets of real numbers should be. For instance, it is natural to measure *intervals* of real numbers by their length:

Definition 3.2.1. If $a \leq b$ are real numbers, then

- the *closed interval* $[a, b]$ is the set $\{x \in \mathbb{R} \mid a \leq x \leq b\}$; and
- the *open interval* (a, b) is the set $\{x \in \mathbb{R} \mid a < x < b\}$.

If I equals either $[a, b]$ or (a, b), then we say that I is an *interval* with endpoints a and b. The *length* of $[a, b]$ (or (a, b)) is denoted $\ell([a, b])$ and is equal to $b - a$.

One can also define intervals with endpoints at $\pm\infty$. For example, if $b \in \mathbb{R}$, then $(-\infty, b] = \{x \in \mathbb{R} \mid x \leq b\}$, or $(b, \infty) = \{x \in \mathbb{R} \mid b < x\}$. The length of such intervals is defined to be ∞.

One can straightforwardly extend this method of measuring sets of real numbers to other simple sets, such as disjoint unions of intervals. For example, it makes sense to say that the measure of the set $[0, 1] \cup (2, 2.5)$ should be $1 + 0.5 = 1.5$. Or, suppose that $\langle I_n \mid n \in \mathbb{N} \rangle$ is a sequence of pairwise disjoint intervals such that, for all $n \in \mathbb{N}$, we have $\ell(I_n) = 1/2^n$. Then it would make sense to say that the measure of the union $\bigcup_{n \in \mathbb{N}} I_n$ should be

$$\sum_{n=0}^{\infty} 1/2^n = 1 + 1/2 + 1/4 + 1/8 + \ldots = 2.$$

It is natural now to ask whether this method of measurement can be extended to measure the size of *all* subsets of $\mathbb{R}$. Of course, in order for this question to make sense, we must ask that this notion of measure satisfies certain nice properties that we would expect to hold of functions that measure the size of sets of real numbers. We extract these properties in the following definition.

Definition 3.2.2. Suppose that $m : \mathscr{P}(\mathbb{R}) \to [0, \infty]$ (i.e., m assigns to every subset $X \subseteq \mathbb{R}$ a measure $m(X)$ that is either a non-negative real number or ∞). We say that m is a *nice measure* if it satisfies the following properties:

1. If $a \leq b$ are real numbers and I is an interval with endpoints a and b, then $m(I) = b - a$.
2. (Monotonicity) If $X \subseteq Y$ are subsets of $\mathbb{R}$, then $m(X) \leq m(Y)$.
3. (Translation invariance) If $X \subseteq \mathbb{R}$ and $a \in \mathbb{R}$, then $m(X) = m(a + X)$, where $a + X$ denotes the set $\{a + x \mid x \in X\}$. In other words, the measure of a set X should not change if we simply shift it horizontally on the number line.

4. (Countable additivity) If $\mathcal{F}$ is a finite or countably infinite collection of pairwise disjoint subsets of $\mathbb{R}$, then

$$m\left(\bigcup \mathcal{F}\right) = \sum_{X \in \mathcal{F}} m(X).$$

In other words, if $\langle X_n \mid n \in \mathbb{N} \rangle$ is a sequence of pairwise disjoint subsets of $\mathbb{R}$ and $X = \bigcup_{n \in \mathbb{N}} X_n$, then

$$m(X) = \sum_{n \in \mathbb{N}} m(X_n) = m(X_0) + m(X_1) + m(X_2) + \dots.$$

Perhaps surprisingly, we will now show that, assuming the axioms of ZFC, there are no nice measures. In other words, it is *impossible* to extend the notion of length to measure *all* subsets of $\mathbb{R}$ in a way that comports with our intuitions about how measures of size should behave.

Theorem 3.2.3 (Vitali)**.** *There are no nice measures.*

Proof. Suppose for the sake of contradiction that $m : \mathscr{P}(\mathbb{R}) \to [0, \infty]$ is a nice measure. Recall that $\mathbb{Q}$ denotes the set of *rational* numbers. $\mathbb{Q}$ is a countably infinite set, and it is also dense in $\mathbb{R}$, meaning that every nonempty open interval (a, b) contains an element of $\mathbb{Q}$. Given a real number $a \in \mathbb{R}$, let $a + \mathbb{Q}$ denote the set $\{a + q \mid q \in \mathbb{Q}\}$.

Let $\mathcal{F}$ denote the set $\{a + \mathbb{Q} \mid a \in \mathbb{R}\}$. Notice that there will be distinct real numbers $a \neq b$ such that $a + \mathbb{Q} = b + \mathbb{Q}$; in fact, this will happen if and only if the difference $b - a$ is rational. Since $\mathcal{F}$ is a *set*, if $a \neq b$ and $a + \mathbb{Q} = b + \mathbb{Q}$, then $\mathcal{F}$ does not somehow contain *separate copies* $a + \mathbb{Q}$ and $b + \mathbb{Q}$. Rather, it contains one set that equals both $a + \mathbb{Q}$ and $b + \mathbb{Q}$. Moreover, $\mathcal{F}$ consists of *pairwise disjoint* sets. The verifications of these facts form the following exercise.

Exercise 3.2.4. Suppose that $a, b \in \mathbb{R}$. Prove the following.

1. $(a + \mathbb{Q}) = (b + \mathbb{Q})$ if and only if $b - a \in \mathbb{Q}$.
2. If $(a + \mathbb{Q}) \neq (b + \mathbb{Q})$, then $(a + \mathbb{Q}) \cap (b + \mathbb{Q}) = \emptyset$.

Lemma 3.2.5. *For every $a \in \mathbb{R}$, we have $(a + \mathbb{Q}) \cap [0, 1] \neq \emptyset$.*

Proof. Fix $a \in \mathbb{R}$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, we can fix a rational number q in the interval $(-a, -a + 1)$. Then $a + q \in a + \mathbb{Q}$, and we have the following:

- $a + q \geq a + (-a) = 0$;
- $a + q \leq a + (-a + 1) = 1$.

Therefore, $a + q \in (a + \mathbb{Q}) \cap [0, 1]$. □

We can therefore apply the axiom of choice to the family of pairwise disjoint nonempty sets

$$\{(a + \mathbb{Q}) \cap [0, 1] \mid a \in \mathbb{R}\}$$

to find a set $X \subseteq [0,1]$ that contains exactly one point from each element of $\mathcal{F}$. In other words, for each $a \in \mathbb{R}$, there is exactly one element in the intersection $X \cap (a + \mathbb{Q})$.

We will eventually reach a contradiction using the fact that our measure m must assign a value to the set X. We first need a couple of lemmas.

Lemma 3.2.6. *If p and q are two distinct rational numbers, then $(p + X) \cap (q + X) = \emptyset$.*

Proof. Suppose for the sake of contradiction that p and q are distinct rational numbers and $(p+X)\cap(q+X) \neq \emptyset$. Fix a number $a \in (p+X)\cap(q+X)$. Then there are $x_p, x_q \in X$ such that $a = p + x_p = q + x_q$. Since $p \neq q$, we must have $x_p \neq x_q$. But rearranging the equation in the previous sentence yields

$$x_p - x_q = q - p.$$

Since $q - p$ is rational, Exercise 3.2.4 implies that $x_p + \mathbb{Q} = x_p + \mathbb{Q}$. In other words, x_p and x_q are both elements of $x_p + \mathbb{Q}$. This contradicts the fact that $x_p, x_q \in X$ and X contains only one element of $x_p + \mathbb{Q}$. □

Let $C = \mathbb{Q} \cap [-1, 1]$ be the set of all rational numbers between -1 and 1, and let

$$U = \bigcup_{q \in C} (q + X).$$

Lemma 3.2.7. $[0,1] \subseteq U \subseteq [-1,2]$.

Proof. We first show that $[0,1] \subseteq U$. Fix $a \in [0,1]$, and find $b \in X \cap (a + \mathbb{Q})$. Then $q = a - b$ is a rational number. Moreover, since a and b are both in the interval $[0,1]$, we must have $q \in [-1,1]$. But then $a = q + b \in q + X$, and $q + X \subseteq U$, so $a \in U$.

We next show that $U \subseteq [-1,2]$. Fix $a \in U$. Then there is a rational number $q \in [-1,1]$ and a $b \in X$ such that $a = q + b$. Since $b \in [0,1]$, it follows that $a \in [0 - 1, 1 + 1] = [-1,2]$. □

We are now ready to reach our contradiction. By Lemma 3.2.7 and properties (1) and (2) of Definition 3.2.2, we know that

$$1 \leq m(U) \leq 3.$$

Moreover, by Lemma 3.2.6, we know that the family $\{q+X \mid q \in C\}$ is pairwise disjoint. Also, by definition of U, we have $U = \bigcup_{q\in C}(q+X)$. Thus, by property (4) of Definition 3.2.2, we have

$$m(U) = \sum_{q \in C} m(q + X).$$

By property (3) of Definition 3.2.2, we know that $m(q + X) = m(X)$ for all $q \in C$, so

$$m(U) = \sum_{q \in C} m(X).$$

If $m(X) = 0$, then this yields

$$m(U) = \sum_{q \in C} 0 = 0 + 0 + 0 + \ldots = 0,$$

contradicting the fact that $m(U) \geq 1$. On the other hand, if $m(X) > 0$, then we have

$$m(U) = \sum_{q \in C} m(X) = m(X) + m(X) + m(X) + \ldots = \infty,$$

contradicting the fact that $m(U) \leq 3$. In either case, we reach a contradiction, therefore completing the proof of the theorem. □

We end this section by noting that some use of the axiom of choice really is necessary in the proof of Theorem 3.2.3, due to the following theorem of Solovay. In the statement of the theorem, an *inaccessible cardinal* is a (relatively small) example of a *large cardinal* (formally, an inaccessible cardinal is an uncountable, regular, strong limit cardinal). It is not necessary to understand precisely what it is; we only emphasize that the theory

"ZFC + there exists an inaccessible cardinal"

is considered to be a relatively mild extension of ZFC.

Theorem 3.2.8 (Solovay)**.** *Suppose that the theory*

"ZFC + *there exists an inaccessible cardinal*"

is consistent. Then so is the theory "ZF + *there exists a nice measure*"*.*

3.3 Nonprincipal ultrafilters

Recall that, given a set X, the *power set* of X, denoted $\mathscr{P}(X)$, is defined to be the set of all subsets of X, i.e.,

$$\mathscr{P}(X) = \{Z \mid Z \subseteq X\}.$$

Recall also that, if X is a set and $Y \subseteq X$, then $X \setminus Y$ is called the *complement of* Y *in* X, and

$$X \setminus Y = \{x \in X \mid x \notin Y\}.$$

In particular, $X \setminus Y$ satisfies:

- $Y \cup (X \setminus Y) = X$;
- $Y \cap (X \setminus Y) = \emptyset$.

Given a nonempty set X, a *filter* over X can be thought of as a way of specifying what it means to be a "large" subset of X. Formally, it is defined as follows.

Definition 3.3.1. Suppose that X is a nonempty set. A *filter* over X is a set $\mathcal{F} \subseteq \mathscr{P}(X)$ with the following properties:

1. $X \in \mathcal{F}$ and $\emptyset \notin \mathcal{F}$;

2. for all $Y, Z \in \mathscr{P}(X)$, if $Y \subseteq Z$ and $Y \in \mathcal{F}$, then $Z \in \mathcal{F}$;
3. for all $Y, Z \in \mathscr{P}(X)$, if $Y \in \mathcal{F}$ and $Z \in \mathcal{F}$, then $Y \cap Z \in \mathcal{F}$.

Requirements (1)–(3) in Definition 3.3.1 should make intuitive sense if you think of elements of a filter $\mathcal{F}$ over X as being "large" subsets of X. Namely:

1. Requirement (1) says that the entire set X is large and the empty set is not large.
2. Requirement (2) says that, if Y is large and $Z \supseteq Y$, then Z should also be large.
3. Requirement (3) says that if Y and Z are both large, then their intersection $Y \cap Z$ is large.

Exercise 3.3.2. Suppose that X is an infinite set, and let

$$\mathcal{F} = \{Y \subseteq X \mid X \setminus Y \text{ is finite}\}.$$

In other words, $\mathcal{F}$ consists of all subsets of X that contain all but finitely many elements of X. Prove that $\mathcal{F}$ is a filter over X. This filter is called the *cofinite filter over* X, or sometimes the *Fréchet filter over* X.

Note that, if $\mathcal{F}$ is a filter over a set X and $Y \subseteq X$, then it cannot be the case that both Y and $X \setminus Y$ are in $\mathcal{F}$: if it were the case, then requirement (3) of Definition 3.3.1 would imply that $Y \cap (X \setminus Y) \in \mathcal{F}$, i.e., $\emptyset \in \mathcal{F}$, contradicting requirement (1) of Definition 3.3.1. Thus, $\mathcal{F}$ can contain at most one of Y and $X \setminus Y$. If $\mathcal{F}$ contains precisely one of these sets for *every* $Y \subseteq X$, then we call it an *ultrafilter*.

Definition 3.3.3. Suppose that X is a nonempty set. A set $\mathcal{U} \subseteq \mathscr{P}(X)$ is called an *ultrafilter* over X if

- $\mathcal{U}$ is a filter over X;
- for all $Y \in \mathscr{P}(X)$, either $Y \in \mathcal{U}$ or $X \setminus Y \in \mathcal{U}$.

It is easy to describe certain ultrafilteres:

Exercise 3.3.4. Suppose that X is a nonempty set and $x \in X$. Let

$$\mathcal{U} = \{Y \in \mathscr{P}(X) \mid x \in Y\}.$$

Prove that $\mathcal{U}$ is an ultrafilter over X.

Ultrafilters as in Exercise 3.3.4 are called *principal ultrafilters*. More formally:

Definition 3.3.5. Suppose that X is a nonempty set. Then a set $\mathcal{U} \subseteq \mathscr{P}(X)$ is called a *principal ultrafilter over* X if there is $x \in X$ such that

$$\mathcal{U} = \{Y \in \mathscr{P}(X) \mid x \in Y\}.$$

If $\mathcal{U}$ is an ultrafilter over X and $\mathcal{U}$ is *not* a principal ultrafilter over X, then we call it a *nonprincipal ultrafilter over* X.

We have seen that principal ultrafilters exist, so the question naturally arises whether *nonprincipal* ultrafilters exist. It turns out that, if X is a *finite* set, then every ultrafilter over X is *principal*:

Exercise 3.3.6. Suppose that X is a finite nonempty set and $\mathcal{U}$ is an ultrafilter over X. Prove that $\mathcal{U}$ is a principal ultrafilter over X.

In fact, we have the following:

Exercise 3.3.7. Suppose that X is a set and $\mathcal{U}$ is an ultrafilter over $\mathcal{U}$. Then the following are equivalent:

1. $\mathcal{U}$ is a principal ultrafilter;
2. there is a finite set $Y \subseteq X$ such that $Y \in \mathcal{U}$.

However, if X is infinite, then, assuming the axiom of choice holds, we can prove that nonprincipal ultrafilters over X exist. The following theorem, which we prove using the help of Zorn's lemma, is the key.

Theorem 3.3.8. *Suppose that X is a nonempty set and $\mathcal{F}$ is a filter over X. Then there is an ultrafilter $\mathcal{U}$ over X such that $\mathcal{F} \subseteq \mathcal{U}$.*

Proof. Let P be the set of all filters $\mathcal{G}$ over X such that $\mathcal{F} \subseteq \mathcal{G}$. Note that P is nonempty, since we certainly have $\mathcal{F} \in P$. Consider the binary relation $\subseteq$ on $\mathcal{F}$.

Lemma 3.3.9. *$(P, \subseteq)$ is a partial order.*

Proof. We need to verify all three requirements in Definition 1.1.1. They all follow almost immediately from the definition of the subset relation:

- (Reflexive): For all $\mathcal{G} \in P$, we certainly have $\mathcal{G} \subseteq \mathcal{G}$.
- (Transitive): For all $\mathcal{G}_0, \mathcal{G}_1, \mathcal{G}_2 \in P$, if $\mathcal{G}_0 \subseteq \mathcal{G}_1$ and $\mathcal{G}_1 \subseteq \mathcal{G}_2$, then clearly $\mathcal{G}_0 \subseteq \mathcal{G}_2$.
- (Anti-symmetric): For all $\mathcal{G}, \mathcal{H} \in P$, if $\mathcal{G} \subseteq \mathcal{H}$ and $\mathcal{H} \subseteq \mathcal{G}$, then $\mathcal{G} = \mathcal{H}$.

□

We want to apply Zorn's lemma to the partial order $(P, \subseteq)$. We first need to verify that every $\subseteq$-chain in P has an upper bound. This will follow from the next lemma.

Lemma 3.3.10. *Suppose that $K \subseteq P$ is nonempty and linearly ordered by $\subseteq$ (i.e., for all $\mathcal{G}, \mathcal{H} \in K$, either $\mathcal{G} \subseteq \mathcal{H}$ or $\mathcal{H} \subseteq G$. Then*

$$\bigcup K = \{Y \in \mathscr{P}(X) \mid \exists \mathcal{G} \in K \ [X \in \mathcal{G}]\}$$

is an upper bound for K in $(P, \subseteq)$.

Proof. Let $\mathcal{H} = \bigcup K$. It is clear from the definition that $\mathcal{G} \subseteq \mathcal{H}$ for every $\mathcal{G} \in K$, and therefore also $\mathcal{F} \subseteq \mathcal{H}$. We therefore only need to show that $\mathcal{H}$ is a filter over X. We verify requirements (1)–(3) of Definition 3.3.1.

1. For all $\mathcal{G} \in K$, we have $X \in \mathcal{G}$. Therefore, $X \in \mathcal{H}$. Similarly, for all $\mathcal{G} \in K$, we have $\emptyset \notin \mathcal{G}$. Therefore, $\emptyset \notin \mathcal{H}$.

2. Suppose that $Y, Z \in \mathscr{P}(X)$, $Y \subseteq Z$, and $Y \in \mathcal{H}$. Then there is $\mathcal{G} \in K$ such that $Y \in \mathcal{G}$. Since $\mathcal{G}$ is a filter, it follows that $Z \in \mathcal{G}$. By definition of $\mathcal{H}$, we then have $Z \in \mathcal{H}$.

3. Suppose that $Y, Z \in \mathscr{P}(X)$, $Y \in \mathcal{H}$, and $Z \in \mathcal{H}$. Then there are $\mathcal{G}, \mathcal{G}' \in K$ such that $Y \in \mathcal{G}$ and $Z \in \mathcal{G}'$. Since K is linearly ordered, either $\mathcal{G} \subseteq \mathcal{G}'$ or $\mathcal{G}' \subseteq \mathcal{G}$. Without loss of generality, assume that $\mathcal{G} \subseteq \mathcal{G}'$ (the other case is symmetric). Then, since $Y \in \mathcal{G}$, we have $Y \in \mathcal{G}'$. By assumption, $Z \in \mathcal{G}'$, so, since $\mathcal{G}'$ is a filter, we have $Y \cap Z \in \mathcal{G}'$.

Therefore, $\mathcal{H}$ is indeed a filter over X, completing the proof of the lemma. □

We have now shown that $(P, \subseteq)$ satisfies the hypotheses of Zorn's lemma. Apply Zorn's lemma to find a *maximal* filter $\mathcal{G} \in P$, i.e., an element $\mathcal{G} \in P$ such that there does not exist $\mathcal{H} \in P$ such that $\mathcal{G} \subsetneq \mathcal{H}$.

We claim that $\mathcal{G}$ is an ultrafilter. To show this, suppose for the sake of contradiction that it is *not* an ultrafilter. Then there is a set $Y \in \mathscr{P}(X)$ such that $Y \notin \mathcal{G}$ and $X \setminus Y \notin \mathcal{G}$. Note that $Y \neq \emptyset$, since $X \setminus \emptyset = X$ certainly is in $\mathcal{G}$. We claim that we can find a filter $\mathcal{H}$ in P such that $\mathcal{G} \cup \{Y\} \subseteq \mathcal{H}$, which will contradict the maximality of $\mathcal{G}$.

To see this, let

$$\mathcal{H} = \{W \in \mathscr{P}(X) \mid \exists Z \in \mathcal{G}\ [Z \cap Y \subseteq W]\}.$$

Clearly, $\mathcal{G} \subseteq \mathcal{H}$. Moreover, $Y \in \mathcal{H}$, since $X \in \mathcal{G}$ and $X \cap Y = Y$. Therefore, we will be done if we show that $\mathcal{H}$ is a filter over X. We again verify requirements (1)–(3) of Definition 3.3.1.

1. Since $X \in \mathcal{G}$, we have $X \in \mathcal{H}$. To see that $\emptyset \notin \mathcal{H}$, suppose for the sake of contradiction that $\emptyset \in H$. We know that $\emptyset \notin \mathcal{G}$, so there must be $Z \in \mathcal{G}$ such that $Z \cap Y = \emptyset$. But this means that $Z \subseteq (X \setminus Y)$ (Exercise: prove this!). Therefore, since $\mathcal{G}$ is a filter, we must have $(X \setminus Y) \in \mathcal{G}$. But we chose Y so that $(X \setminus Y) \notin \mathcal{G}$, which yields a contradiction. Thus, $\emptyset \notin \mathcal{G}$.

2. Suppose that $W, W' \in \mathscr{P}(X)$, $W \subseteq W'$, and $W \in \mathcal{H}$. We want to show that $W' \in \mathcal{H}$. By the definition of $\mathcal{H}$, there is $Z \in \mathcal{G}$ such that $Z \cap Y \subseteq W$. But then we also have $Z \cap Y \subseteq W'$, and hence $W' \in \mathcal{H}$.

3. Suppose that $W, W' \in \mathscr{P}(X)$, $W \in \mathcal{H}$, and $W' \in \mathcal{H}$. We want to show that $W \cap W' \in \mathcal{H}$. By the definition of $\mathcal{H}$, there are $Z, Z' \in \mathcal{G}$ such that $Z \cap Y \subseteq W$ and $Z' \cap Y \subseteq W'$. Then, since $\mathcal{G}$ is a filter, we have $Z \cap Z' \in \mathcal{G}$. Moreover, we have $(Z \cap Z') \cap Y \subseteq W \cap W'$ (Exercise: prove this!), and hence $W \cap W' \in \mathcal{H}$.

This completes the verification that $\mathcal{H}$ is a filter, and hence $\mathcal{H}$ witnesses that $\mathcal{G}$ is not a maximal element of P, since $\mathcal{G} \subsetneq \mathcal{H}$. This is a contradiction; therefore, $\mathcal{G}$ is indeed an ultrafilter. □

Corollary 3.3.11. *For every infinite set X, there is a nonprincipal ultrafilter over X.*

Proof. Let $\mathcal{F} = \{Y \in \mathscr{P}X \mid X \setminus Y \text{ is finite}\}$ be the cofinite filter over X (see Exercise 3.3.2). By Theorem 3.3.8, we can find an ultrafilter $\mathcal{U}$ over X such that $\mathcal{F} \subseteq \mathcal{U}$.

We claim that $\mathcal{U}$ is a nonprincipal ultrafilter. To see this, suppose for the sake of contradiction that $\mathcal{U}$ is a principal ultrafilter. Then there is $x \in X$ such that

$$\mathcal{U} = \{Y \in \mathscr{P}(X) \mid x \in Y\}.$$

In particular, we have $\{x\} \in \mathcal{U}$. But $X \setminus \{x\} \in \mathcal{F}$, since $X \setminus (X \setminus \{x\}) = \{x\}$ is finite. Thus, $X \setminus \{x\} \in \mathcal{U}$ and $\{x\} \in \mathcal{U}$, so

$$(X \setminus \{x\}) \cap \{x\} = \emptyset \in \mathcal{U},$$

contradicting the fact that $\mathcal{U}$ is a filter over X. Thus, $\mathcal{U}$ is a nonprincipal ultrafilter. □

Just as with the nonexistence of a nice measure, the existence of nonprincipal ultrafilters really does require some use of the axiom of choice.

Theorem 3.3.12 (Feferman)**.** *If* ZFC *is consistent, then so is*

"ZF + *there is no nonprincipal ultrafilter over* $\mathbb{N}$".

Chapter 4

Lecture 4: Voting theory and Arrow's Impossibility Theorem

We are confronted with the following practical problem throughout our lives: a community is trying to decide among a number of alternatives (for example, they may be trying to elect a president, or to decide where to eat lunch). Each individual in the community has their own preferences, but somehow the community needs to combine those preferences to come up with a single choice. If the community is trying to decide between only two alternatives, then there is a natural approach to this: simply choose the alternative that is preferred by the majority of community members (one must decide what to do if there is a tie, but this is a minor issue). However, as soon as the community is confronted with *more* than two alternatives, difficulties start to arise. Consider the following simple example, known as *Condorcet's paradox*.

Example 4.0.1. Suppose that there are three individuals, a, b, and c, trying to choose between three alternatives, x, y, and z. Each individual ranks the alternatives in order of preference, and the results are as follows:

- Individual a: $x < y < z$ (i.e., z is a's first choice, y is their second choice, and z is their third choice);
- Individual b: $y < z < x$;
- Individual c: $z < x < y$.

Now, if alternative x is chosen, then one can argue that y should win instead, since 2 of the 3 individuals (i.e., a and c) prefer y to x. But then, if y is chosen, one can argue that z should win instead, since a and b prefer z to y. And finally, if z is chosen, one can argue that x should win instead, since b and c prefer x to z. There thus seems to be no way to coherently amalgamate the three individual's preferences in a seemingly fair way.

In this lecture, we will be looking at voting systems, i.e., methods for combining individual preferences into a single societal choice. To do this, we need to precisely define our terms.

Suppose that we have a collection of individuals, $\mathcal{V}$, and a collection $\mathcal{X}$ of alternatives that they are trying to decide between ($\mathcal{X}$ could be political candidates, or choices of what to build on a particular piece of land, or places

to eat lunch). For concreteness, we will always assume we are in a situation in which every individual can linearly order the elements of $\mathcal{X}$ according to their preferences. Let $\mathcal{L}$ be the collection of all linear orders of $\mathcal{X}$.

Definition 4.0.2. A *social preference function* is a function $f : \mathcal{V} \to \mathcal{L}$. Such a function can be thought of as recording each individual's preferences regarding the alternatives in $\mathcal{X}$. Let $\mathcal{F}$ denote the set of *all* social preference functions.

If $f : \mathcal{V} \to \mathcal{L}$ is a social preference function, then, for all $a \in \mathcal{V}$, we will denote the linear order associated with $f(a)$ by $<_{f(a)}$. Thus, if, for instance, we have $x, y \in \mathcal{X}$, then $x <_{f(a)} y$ is the assertion that, in the context of the social preference function f, individual a prefers y over x.

Definition 4.0.3. A *voting system* is a function $\sigma : \mathcal{F} \to \mathcal{L}$. A voting system can be thought of as a way of *combining* the preferences of the individuals into a single societal ordering of the alternatives.

If σ is a voting system and f is a social preference function, then the linear order associated with $\sigma(f)$ is denoted by $<_{\sigma(f)}$. Thus, if $x, y \in \mathcal{X}$ and $f \in \mathcal{F}$, then $x <_{\sigma(f)} y$ is the assertion that, if f records the preferences of the individuals in the society, then, when using the voting system σ, the society as a whole prefers y to x.

There are certain natural conditions that we might expect fair voting systems to satisfy. To state them, we need one further definition.

Definition 4.0.4. Suppose that $f, g \in \mathcal{F}$ and $x \neq y$ are elements of $\mathcal{X}$. We say that f and g *agree on* $\{x, y\}$ if, for all $a \in \mathcal{V}$, we have

$$(x <_{f(a)} y) \iff (x <_{g(a)} y).$$

In other words, with regard to the two alternatives x and y, every individual has the same preferences under f as they do under g.

We can now state the three desirable properties of a "fair" voting system:

- (Unanimity) For all $f \in \mathcal{F}$ and all distinct $x, y \in \mathcal{X}$, if $x <_{f(a)} y$ for all $a \in \mathcal{V}$, then $x <_{\sigma(f)} y$. (In other words, if every individual prefers y over x, then the society as a whole should prefer y over x.)
- (Independence) For all $f, g \in \mathcal{F}$ and all distinct $x, y \in \mathcal{X}$, if f and g agree on $\{x, y\}$, then $\sigma(f)$ and $\sigma(g)$ agree on $\{x, y\}$, i.e.,

  $$(x <_{\sigma(f)} y) \iff (x <_{\sigma(g)} y).$$

  (In other words, the societal preference between x and y should only depend on the individuals' relative preferences between x and y; it should not depend on irrelevant third options $z \in \mathcal{X} \setminus \{x, y\}$.)
- (No dictator) There is no single individual $a^* \in \mathcal{V}$ such that, for all $f \in \mathcal{F}$ and all distinct $x, y \in \mathcal{X}$, we have

  $$(x <_{\sigma(f)} y) \iff (x <_{f(a^*)} y).$$

  (In other words, there should not be a single individual who singlehandedly decides the society's preferences.)

Somewhat surprisingly, Kenneth Arrow proved in 1950 that, if the set of individuals $\mathcal{V}$ is nonempty and finite and the set of alternatives $\mathcal{X}$ is finite and contains at least 3 elements, then there are *no* voting systems satisfying all three of these conditions.

Theorem 4.0.5. *Suppose that $\mathcal{V}$ is a nonempty finite set of individuals and $\mathcal{X}$ is a finite set of alternatives with at least 3 elements. If σ is a voting system that satisfies Unanimity and Independence, then it has a dictator.*

If the set $\mathcal{V}$ of individuals is not finite, then Theorem 4.0.5 is no longer true precisely as stated, though we shall see later that a generalization of it is true. In preparation for that, let us introduce a general method for constructing voting systems that satisfy Unanimity and Independence:

Example 4.0.6. Suppose that $\mathcal{U}$ is an ultrafilter over the set $\mathcal{V}$ of individuals. We define a function $\sigma_{\mathcal{U}} : \mathcal{F} \to \mathcal{L}$ as follows. We first make the following two observations.

1. In order to specify an element of $\mathcal{L}$, it is enough to specify, for all distinct $x, y \in \mathcal{X}$, whether $x < y$ or $y < x$.
2. For all $f \in \mathcal{F}$ and all distinct $x, y \in \mathcal{X}$, exactly one of the following sets is in $\mathcal{U}$:
   - $\{a \in \mathcal{V} \mid x <_{f(a)} y\}$;
   - $\{a \in \mathcal{V} \mid y <_{f(a)} x\}$.

Now, for all $f \in \mathcal{F}$ and all distinct, $x, y \in \mathcal{X}$, we set

$$(x <_{\sigma_{\mathcal{U}}(f)} y) \iff (\{a \in \mathcal{V} \mid x <_{f(a)} y\} \in \mathcal{U}).$$

We leave the verification that this describes a voting system (i.e., that $\sigma_{\mathcal{U}}(f) \in \mathcal{L}$ for all $f \in \mathcal{F}$) as an exercise:

Exercise 4.0.7. Prove that, for all $f \in \mathcal{F}$, $\sigma_{\mathcal{U}}(f)$ is a linear order.

We also leave it as an exercise to verify that $\sigma_{\mathcal{U}}$ satisfies Unanimity and Independence:

Exercise 4.0.8. Prove that $\sigma_{\mathcal{U}}$ satisfies Unanimity and Independence.

Finally, $\sigma_{\mathcal{U}}$ has a dictator if and only if $\mathcal{U}$ is a *principal* ultrafilter:

Exercise 4.0.9. Prove that $\sigma_{\mathcal{U}}$ has a dictator if and only if $\mathcal{U}$ is a *principal* ultrafilter.

In light of the previous example, an ultrafilter can be thought of as a "generalized dictator" (Kirman and Sondermann call them "invisible dictators"). If a voting system has a dictator, then one can determine the societal preference between two alternatives x and y just by asking the dictator which one they prefer. In the context of a voting system $\sigma_{\mathcal{U}}$ for a nonprincipla ultrafilter, to determine the societal preference between two alternatives x and y, one only needs to ask which one is preferred by some set of individuals that is in the ultrafilter. With the notion of dictator replaced by this generalized notion of dictator, Theorem 4.0.5 *does* generalize to the case in which the set of individuals and the set of alternatives are allowed to be infinite.

Theorem 4.0.10 (Generalized Arrow's theorem)**.** *Suppose that $\mathcal{V}$ is a nonempty (possibly infinite) set of individuals and $\mathcal{X}$ is a set of alternatives (also possibly infinite) with at least 3 elements. If σ is a voting system that satisfies Unanimity and Independence, then there is an ultrafilter $\mathcal{U}$ over $\mathcal{V}$ such that $\sigma = \sigma_{\mathcal{U}}$.*

Proof. Fix a voting system $\sigma : \mathcal{F} \to \mathcal{L}$ that satisfies Unanimity and Independence. First, if $A \subseteq \mathcal{V}$ is a set of individuals, then let A^c denote $\mathcal{V} \setminus A$, i.e., the set of individuals *not* in A. It will be helpful to introduce the following terminology.

Definition 4.0.11. Suppose that x and y are distinct elements of $\mathcal{X}$ and $A \subseteq \mathcal{V}$. Then we say that A is *almost decisive for* (x, y) if there is a social preference function $f \in \mathcal{F}$ such that

- for all $a \in A$, $x <_{f(a)} y$;
- for all $a \in A^c$, $y <_{f(a)} x$;
- $x <_{\sigma(f)} y$.

In other words, A is elmost decisive for (x, y) if there is $f \in \mathcal{F}$ such that $\sigma(f)$ ranks y above x and A is precisely the set of individuals that rank y above x in f.

We now show in two steps that, because of Unanimity and Independence, almost decisive sets actually satisfy much stronger properties. First, we show that the definition is independent of the choice of $f \in \mathcal{F}$.

Lemma 4.0.12. *Suppose that x and y are distinct elements of $\mathcal{X}$ and $A \subseteq \mathcal{V}$. Then the following are equivalent:*

1. *A is almost decisive for (x, y);*
2. *for* every *$g \in \mathcal{F}$ such that*
   - *for all $a \in A$, $x <_{g(a)} y$; and*
   - *for all $a \in A^c$, $y <_{g(a)} x$;*

   we have $x <_{\sigma(g)} y$.

Proof. Property (2) is stronger than property (1) by definition (Exercise: check this), so it suffices to prove that (1) implies (2). To this end, suppose that A is almost decisive for (x, y), and fix an arbitrary $g \in \mathcal{F}$ such that

- for all $a \in A$, $x <_{g(a)} y$; and
- for all $a \in A^c$, $y <_{g(a)} x$.

We must show that $x <_{\sigma(g)} y$.

By the definition of almost decisive, we can find an $f \in \mathcal{F}$ such that

- for all $a \in A$, $x <_{f(a)} y$;
- for all $a \in A^c$, $y <_{f(a)} x$;

- $x <_{\sigma(f)} y$.

Note that f and g agree on $\{x, y\}$: in both functions, everybody in A prefers y over x and everybody in A^c prefers x over y. Thus, by independence and the fact that $x <_{\sigma(f)} y$, we have $x <_{\sigma(g)} y$, as desired. □

We now introduce a natural strengthening of being almost decisive:

Definition 4.0.13. Suppose that $A \subseteq \mathcal{V}$ and x, y are distinct elements of $\mathcal{X}$. We say that A is *decisive for* (x, y) if, for every $f \in \mathcal{F}$ such that

$$\forall a \in A \; x <_{f(a)} y,$$

we have $x <_{\sigma(f)} y$.

In other words, A is decisive for (x, y) if, whenever everyone in A prefers y over x, society also prefers y over x. In light of Lemma 4.0.12, the difference between being decisive for (x, y) and being almost decisive for (x, y) is that, in the definition of being decisive, it doesn't matter what the preferences of individuals in A^c are. However, in the presence of Unanimity and Independence, the two notions are the same:

Lemma 4.0.14. *Suppose that $A \subseteq \mathcal{V}$ and x, y are distinct elements of $\mathcal{X}$. The following are equivalent:*

1. *A is almost decisive for (x, y);*
2. *A is decisive for (x, y).*

Proof. Property (2) implies property (1) by definition, so it suffices to prove that (1) implies (2). To this end, suppose that A is almost decisive for (x, y). To show that A is decisive for (x, y), fix an $f \in \mathcal{F}$ such that $x <_{f(a)} y$ for all $a \in A$. We must show that $x <_{\sigma(f)} y$.

Since $|\mathcal{X}| > 2$, we can fix an alternative $z \in \mathcal{X}$ such that $z \notin \{x, y\}$. Let $g \in \mathcal{F}$ be a social preference function such that:

- for all $a \in A$, we have $x <_{g(a)} y <_{g(a)} z$; and
- for all $a \in A^c$, we have $y <_{g(a)} z <_{g(a)} x$.

Since A is almost decisive for (x, y), Lemma 4.0.12 implies that $x <_{\sigma(g)} y$. Also, since σ satisfies Unanimity and $y <_{g(a)} z$ for all $a \in \mathcal{V}$, we have $y <_{\sigma(g)} z$. Putting these together yields $x <_{\sigma(g)} z$.

Now return to the function f. We know that $x <_{f(a)} y$ for all $a \in A$, but we do not know the preferences on A^c. Let $B_0 = \{a \in A^c \mid y <_{f(a)} x\}$ and $B_1 = \{a \in A^c \mid x <_{f(a)} y\}$. Let $h \in \mathcal{F}$ be a social preference function such that

- for all $a \in A$, we have $x <_{h(a)} z <_{h(a)} y$;
- for all $a \in B_0$, we have $z <_{h(a)} y <_{h(a)} x$; and
- for all $a \in B_1$, we have $z <_{h(a)} x <_{h(a)} y$.

Now make the following observations:

1. h agrees with g on $\{x, z\}$, and therefore, by Independence, we have $x <_{\sigma(h)} z$;
2. $z <_{h(a)} y$ for all $a \in \mathcal{V}$, so, by Unanimity, we have $z <_{\sigma(h)} y$;
3. by (1) and (2), we have $x <_{\sigma(h)} y$;
4. f agrees with h on $\{x, y\}$, so, again by Independence, $x <_{\sigma(f)} y$, as desired.

□

Finally, we show that if a set is decisive for a single pair (x, y), then it is decisive for *all* pairs (x, y).

Lemma 4.0.15. *Suppose that $A \subseteq \mathcal{V}$. The following are equivalent:*

1. *there are distinct $x, y \in \mathcal{X}$ such that A is decisive for (x, y);*
2. *for* every *pair of distinct $x, y \in \mathcal{X}$, A is decisive for (x, y).*

Proof. Again, (2) implies (1) by definition, so it suffices to prove that (1) implies (2). Assume that (1) holds, and fix distinct $x, y \in \mathcal{X}$ such that A is decisive for (x, y). To prove (2), fix an arbitrary pair u, w of distinct elements of $\mathcal{X}$. We must show that A is decisive for (u, w). To show this, suppose that $f \in \mathcal{F}$ is such that $u <_{f(a)} w$ for all $a \in A$. We must show that $u <_{\sigma(f)} w$.

For simplicity, assume that $\{u, w\} \cap \{x, y\} = \emptyset$, i.e., neither u nor w is equal to either x or y. The argument in which one or both of u and w is in $\{x, y\}$ is similar and left as an exercise.

Let $B_0 = \{a \in A^c \mid w <_{f(a)} u\}$ and $B_1 = \{a \in A^c \mid u <_{f(a)} w\}$. Let $g \in \mathcal{F}$ be such that

- for all $a \in A$, we have $u <_{g(a)} x <_{g(a)} y <_{g(a)} w$;
- for all $a \in B_0$, we have $y <_{g(a)} w <_{g(a)} u <_{g(a)} x$;
- for all $a \in B_1$, we have $u <_{g(a)} x <_{g(a)} y <_{g(a)} w$.

Since A is decisive for (x, y) and $x <_{g(a)} y$ for all $a \in A$, we have $x <_{\sigma(g)} y$. By Unanimity, we have $u <_{\sigma(g)} x$ and $y <_{\sigma(g)} w$. Putting this together yields $u <_{\sigma(g)} w$. But f agrees with g on $\{u, w\}$, so $u <_{\sigma(f)} w$, as desired. □

Let us simply say that a set $A \subseteq \mathcal{V}$ is *decisive* if, for every pair of distinct $x, y \in \mathcal{X}$, A is decisive for (x, y). By the previous Lemmas, A is decisive if and only if there are distinct $x, y \in \mathcal{X}$ such that A is almost decisive for (x, y).

Lemma 4.0.16. *Let $\mathcal{U} = \{A \subseteq \mathcal{V} \mid A \text{ is decisive}\}$. Then $\mathcal{U}$ is an ultrafilter over $\mathcal{V}$.*

Proof. Since σ satisfies Unanimity, we have $\mathcal{V} \in \mathcal{U}$ and $\emptyset \notin \mathcal{U}$. The following exercise shows that $\mathcal{U}$ is closed upwards:

Exercise 4.0.17. Suppose that $A \subseteq B \subseteq \mathcal{V}$ and A is decisive. Then B is decisive.

We next need to show that $\mathcal{U}$ is closed under intersection. To this end, suppose that both A and B are decisive. We must show that $A \cap B$ is decisive. By the previous lemmas, this is equivalent to showing that $A \cap B$ is almost (x, y) decisive for some pair of distinct $x, y \in \mathcal{X}$. Fix arbitrary distinct $x, y \in \mathcal{X}$. To show that $A \cap B$ is almost (x, y) decisive, we must find a function $f \in \mathcal{F}$ such that

1. for all $a \in A \cap B$, we have $x <_{f(a)} y$;
2. for all $a \in (A \cap B)^c$, we have $y <_{f(a)} x$;
3. $x <_{\sigma(f)} y$.

Fix $z \in \mathcal{X}$ with $z \notin \{x, y\}$. Let $f \in \mathcal{F}$ be such that

- for all $a \in A \cap B$, we have $x <_{f(a)} z <_{f(a)} y$;
- for all $a \in A \setminus B$, we have $y <_{f(a)} x <_{f(a)} z$;
- for all $a \in B \setminus A$, we have $z <_{f(a)} y <_{f(a)} x$;
- for all $a \in (A \cup B)^c$, we have $y <_{f(a)} z <_{f(a)} x$.

Note that f satisfies requirements (1) and (2) above. We must show that $x <_{\sigma(f)} y$. First note that, for all $a \in A$, we have $x <_{f(a)} z$. Since A is decisive, this implies that $x <_{\sigma(f)} z$. Next note that, for all $a \in B$, we have $z <_{f(a)} y$. Since B is decisive, this implies that $z <_{\sigma(f)} y$. Putting these two together yields $x <_{\sigma(f)} y$, as desired.

Finally, we need to show that, for all $A \subseteq \mathcal{V}$, either $A \in \mathcal{U}$ or $A^c \in \mathcal{U}$. To this end, let $A \subseteq \mathcal{V}$ be arbitrary. Fix distinct $x, y \in \mathcal{X}$, and let $f \in \mathcal{F}$ be such that

- for all $a \in A$, $x <_{f(a)} y$;
- for all $a \in A^c$, $y <_{f(a)} x$.

Now ask what the societal preference between x and y is given the social preference function f. If $x <_{\sigma(f)} y$, then A is almost decisive for (x, y), and hence $A \in \mathcal{U}$. If $y <_{\sigma(f)} x$, then A^c is almost decisive for (y, x), and hence $A^c \in \mathcal{U}$. □

The final step is now almost immediate:

Lemma 4.0.18. $\sigma = \sigma_{\mathcal{U}}$.

Proof. We must show that, for all $f \in \mathcal{F}$ and all distinct $x, y \in \mathcal{X}$, we have

$$(x <_{\sigma(f)} y) \iff (\{a \in \mathcal{V} \mid x <_{f(a)} y\} \in \mathcal{U}).$$

Fix such $f \in \mathcal{F}$ and $x, y \in \mathcal{X}$. Suppose first that $x <_{\sigma(f)} y$. By definition, $\{a \in \mathcal{V} \mid x <_{f(a)} y\}$ is almost decisive for (x, y), and hence is in $\mathcal{U}$, thus proving the left-to-right direction.

For the other direction, suppose that $A = \{a \in \mathcal{V} \mid x <_{f(a)} y\} \in \mathcal{U}$. By the definition of $\mathcal{U}$, this means that A is decisive. By the definition of decisive, this means that $x <_{\sigma(f)} y$. □

□

Notice that if $\mathcal{U}$ is an ultrafilter, then not only is $\mathcal{U}$ closed under pairwise intersection, but it is closed under *finite* intersections, i.e., if $n \in \mathbb{N}$ and $A_0, A_1, \ldots, A_n \in \mathcal{U}$, then $A_0 \cap A_1 \cap \ldots \cap A_n \in \mathcal{U}$. This allows us the following strengthening of Theorem 4.0.10.

Corollary 4.0.19. *Suppose that $\mathcal{V}$ is a nonempty set of individuals and $\mathcal{X}$ is a finite set of alternatives with at least 3 elements. If σ is a voting system that satisfies Unanimity and Independence, then there is an ultrafilter $\mathcal{U}$ over $\mathcal{V}$ such that, for all $f \in \mathcal{F}$, we have*

$$\{a \in \mathcal{V} \mid f(a) = \sigma(f)\} \in \mathcal{U}.$$

In other words, the societal preferences are simply formed by copying the individual preferences of a group of individuals that is in $\mathcal{U}$.

Proof. Apply Theorem 4.0.10 to find an ultrafilter $\mathcal{U}$ over $\mathcal{V}$ such that $\sigma = \sigma_{\mathcal{U}}$. Now fix an arbitrary $f \in \mathcal{F}$. For all distinct $x, y \in \mathcal{X}$, let $A_{x,y}$ be the set of $a \in \mathcal{V}$ such that the preferences of a between x and y agree with the societal preferences, i.e.,

$$A_{x,y} = \{a \in \mathcal{V} \mid (x <_{f(a)} y) \Leftrightarrow (x <_{\sigma(f)} y)\}.$$

Since $\sigma = \sigma_{\mathcal{U}}$, we have $A_{x,y} \in \mathcal{U}$. Since $\mathcal{X}$ is finite, there are only finitely many pairs of distinct $x, y \in \mathcal{X}$. Thus, the set

$$A = \bigcup_{x \neq y \in \mathcal{X}} A_{x,y}$$

is in $\mathcal{U}$. But now one can check that, for all $a \in A$, we have $f(a) = \sigma(f)$. □

Remark 4.0.20. Although models of voters or economic actors with infinitely many individuals or alternatives may not seem realistic, there are cases in which such models may be the best or most useful models for studying actual large economic systems. For instance, in Aumann's paper "Markets with a continuum of traders", he argues that the most natural mathematical model for a market with true "perfect competition" is one in which the number of economic actors equals the cardinality of the set of real numbers.

What the results of this section show us, though, is that there is a limit to the usefulness of studying voting systems with infinitely many actors. One might have hoped that, by moving from finite voting systems to infinite ones, one might be able to avoid the paradoxes of Condorcet and Arrow, but the results of this lecture show that this is not the case.

Chapter 5

Lecture 5: Ultraproducts

In this lecture, we introduce a powerful technique for creating new models out of old models: the ultraproduct construction. In a very rough sense, this construction works as follows: one starts with an indexed family $\langle \mathfrak{A}_i \mid i \in I \rangle$ of models, and then one uses an ultrafilter over I to create a new model $\mathfrak{A}$ by *averaging* the models in $\langle \mathfrak{A}_i \mid i \in I \rangle$. Let us now describe the construction more formally.

For now, fix a first-order language $\mathcal{L}$. The language $\mathcal{L}$ consists of relation symbols, function symbols, and constant symbols. Let $\mathcal{R}$ denote the set of relation symbols in $\mathcal{L}$, $\mathcal{F}$ denote the set of function symbols in $\mathcal{L}$, and $\mathcal{C}$ denote the set of constant symbols in $\mathcal{L}$.

Also fix for now an index set I and, for each $i \in I$, an $\mathcal{L}$-model $\mathfrak{A}_i$. For each $i \in I$, let A_i denote the underlying set of $\mathfrak{A}_i$. For each $i \in I$, each $R \in \mathcal{R}$, each $F \in \mathcal{F}$, and each $c \in \mathcal{C}$, let R_i, F_i, and c_i denote the interpretations of R, F, and c, respectively, in the model $\mathfrak{A}_i$. Recall that

$$\prod_{i \in I} A_i$$

denotes the set of all functions f such that $\mathrm{dom}(f) = I$ and, for all $i \in I$, we have $f(i) \in A_i$.

Finally, fix an ultrafilter U over I.

Definition 5.0.1. For all $f, g \in \prod_{i \in I} A_i$, we say that $f =_U g$ if

$$\{i \in I \mid f(i) = g(i)\} \in U.$$

Proposition 5.0.2. *The relation $=_U$ is an equivalence relation on $\prod_{i \in I} A_i$.*

Proof. We must check that $=_U$ is reflexive, symmetric, and transitive. First, for all $f \in \prod_{i \in I} A_i$, we have $\{i \in I \mid f(i) = f(i)\} = I \in U$, so $=_U$ is reflexive.

To check that $=_U$ is symmetric, fix $f, g \in \prod_{i \in I} A_i$. Then

$$\{i \in I \mid f(i) = g(i)\} = \{i \in I \mid g(i) = f(i)\}$$

and thus, if $f =_U g$, then also $g =_U f$.

Finally, to check transitivity, fix $f, g, h \in \prod_{i \in I} A_i$, and suppose that $f =_U g$ and $g =_U h$. Let

$$X_0 = \{i \in I \mid f(i) = g(i)\} \quad \text{and} \quad X_1 = \{i \in I \mid g(i) = h(i)\}.$$

By the definition of $=_U$, we have $X_0, X_1 \in U$. Therefore, since U is an ultrafilter, we have $X_0 \cap X_1 \in U$. For all $i \in X_0 \cap X_1$, we have $f(i) = g(i)$ and $g(i) = h(i)$, so $f(i) = h(i)$. Therefore,

$$X_0 \cap X_1 \subseteq \{i \in I \mid f(i) = h(i)\}.$$

Since U is an ultrafilter and $X_0 \cap X_1 \in U$, it follows that $\{i \in I \mid f(i) = h(i)\} \in U$, i.e., $f =_U h$. □

Given a function $f \in \prod_{i\in I} A_i$, let $[f]_U$ denote the equivalence class of f under the equivalence relation $=_U$. In other words,

$$[f]_U = \left\{ g \in \prod_{i\in I} A_i \;\middle|\; f =_U g \right\}.$$

We can now describe the ultraproduct construction.

Definition 5.0.3. Given $\langle \mathfrak{A}_i \mid i \in I \rangle$ and U as above, the ultraproduct $\prod_{i\in I} \mathfrak{A}_i/U$ (sometimes denoted $\prod_U \mathfrak{A}_i$ or $\mathfrak{A}_I/U$) is defined as follows:

1. The underlying set of $\prod_{i\in I} \mathfrak{A}_i/U$ is

$$\prod_{i\in I} A_i/U = \left\{ [f]_U \;\middle|\; f \in \prod_{i\in I} A_i \right\}.$$

2. Given $R \in \mathcal{R}$, $F \in \mathcal{F}$, or $c \in \mathcal{C}$, we will let their interpretations in $\prod_{i\in I} \mathfrak{A}_i/U$ be denoted by R_U, F_U, and c_U, respectively. These are defined as follows:

   a) If $n \in \mathbb{N}$, $R \in \mathcal{R}$ is an n-ary relation symbol, and $[f_0]_U, [f_1]_U, \ldots, [f_{n-1}]_U \in \prod_{i\in I} A_i/U$, then we set

   $$([f_0]_U, [f_1]_U, \ldots, [f_{n-1}]_U) \in R_U \iff \{i \in I \mid (f_0(i), f_1(i), \ldots, f_{n-1}(i)) \in R_i\} \in U.$$

   b) If $n \in \mathbb{N}$, $F \in \mathcal{F}$ is an n-ary function symbol, and $[f_0]_U, [f_1]_U, \ldots, [f_{n-1}]_U \in \prod_{i\in I} A_i/U$, then we let

   $$F([f_0]_U, [f_1]_U, \ldots, [f_{n-1}]_U) = [g],$$

   where $g \in \prod_{i\in I} A_i$ is defined by letting

   $$g(i) = F(f_0(i), f_1(i), \ldots, f_{n-1}(i))$$

   for all $i \in I$.

   c) If $c \in \mathcal{C}$ is a constant symbol, then we let $c_U = [f_c]_U$, where $f_c \in \prod_{i\in I} A_i$ is defined by letting

   $$f_c(i) = c_i$$

   for all $i \in I$.

There are some things that should be verified for the above construction to make sense.

Exercise 5.0.4. Prove that the constructions in items (2)(a) and (2)(b) of Definition 5.0.3 is well-defined, i.e., that it does not depend on the choice of representatives from the relevant equivalence classes. More precisely, first suppose that $n \in \mathbb{N}$ and $f_0, f_1, \ldots, f_{n-1}, g_0, g_1, \ldots, g_{n-1} \in \prod_{i \in I} A_i$ are such that $f_i =_U g_i$ for all $i \in I$. Now prove the following:

1. If $R \in \mathcal{R}$ is an n-ary relation symbol, then we have

$$\{i \in I \mid (f_0(i), f_1(i), \ldots, f_{n-1}(i)) \in R_i\} \in U$$

   if and only if

$$\{i \in I \mid (g_0(i), g_1(i), \ldots, g_{n-1}(i)) \in R_i\} \in U.$$

2. If $F \in \mathcal{F}$ is an n-ary function symbol and we define $f^*, g^* \in \prod_{i \in I} A_i$, by letting

$$f^*(i) = F(f_0(i), f_1(i), \ldots, f_{n-1}(i))$$

   and

$$g^*(i) = F(g_0(i), g_1(i), \ldots, g_{n-1}(i))$$

   for all $i \in I$, then we have $f^* =_U g^*$.

Remark 5.0.5. Although we did not use the terminology, we actually saw an example of the ultraproduct in the previous lecture. Recall the setup: we were given a set $\mathcal{V}$ of individuals and a set $\mathcal{X}$ of individuals that they are choosing between. Each individual has a ranking of the alternatives in $\mathcal{X}$; formally, this is a linear order on $\mathcal{X}$. For each $a \in \mathcal{V}$, let $<_a$ denote this order. We saw that one way to combine all of these individual preferences into a societal preference $<^*$ is as follows: fix an ultrafilter U over $\mathcal{V}$ and, for all alternatives $x, y \in \mathcal{X}$, set

$$x <^* y \iff \{a \in \mathcal{V} \mid x <_a y\} \in U.$$

Note that this is precisely the voting system σ_U identified in the previous chapter. Moreover, by looking at Definition 5.0.3, we can see that this corresponds precisely to taking the ultraproduct of the structures $\langle <_a \mid a \in \mathcal{V} \rangle$ by the ultrafilter U (the language here just has a single binary relation, denoted $<$).

5.1 Łos' Theorem

We now present the fundamental theorem of ultraproducts, known as Łos' Theorem. Roughly speaking, this says that the truth of formulas in an ultraproduct reflects the truth of the corresponding formulas in the factors of the ultraproduct.

Theorem 5.1.1. *Suppose that $\mathcal{L}$ is a first-order language, I is a nonempty set, $\langle \mathfrak{A}_i \mid i \in I \rangle$ is a family of $\mathcal{L}$-structures, and U is an ultrafilter over I. Then, for every $\mathcal{L}$-formula φ with n free variables and every n-tuple $([f_0]_U, [f_1]_U, \ldots, [f_{n-1}]_U)$ from $\prod_{i \in I} A_i/U$, the following are equivalent:*

1. $\prod_{i \in I} \mathfrak{A}_i/U \models \varphi([f_0]_U, [f_1]_U, \ldots, [f_{n-1}]_U)$;
2. $\{i \in I \mid \mathfrak{A}_i \models \varphi(f_0(i), f_1(i), \ldots, f_{n-1}(i))\} \in U$.

Proof. The proof is by induction on the complexity of formulas. If φ is an atomic formula, then the equivalence of (1) and (2) follows directly from Definition 5.0.3 (Exercise: check this!).

Suppose now that $\varphi = \psi_0 \wedge \psi_1$ and we have established the theorem for ψ_0 and ψ_1. Then we have

$$\begin{aligned}
&\prod_{i\in I} \mathfrak{A}_i/U \models \varphi([f_0]_U, [f_1]_U, \ldots, [f_{n-1}]_U) \\
&\quad \Longleftrightarrow \prod_{i\in I} \mathfrak{A}_i/U \models \psi_0([f_0]_U, [f_1]_U, \ldots, [f_{n-1}]_U) \text{ and} \\
&\qquad \prod_{i\in I} \mathfrak{A}_i/U \models \psi_1([f_0]_U, [f_1]_U, \ldots, [f_{n-1}]_U) \\
&\quad \Longleftrightarrow \{i \in I \mid \mathfrak{A}_i \models \psi_0(f_0(i), f_1(i), \ldots, f_{n-1}(i))\} \in U \text{ and} \\
&\qquad \{i \in I \mid \mathfrak{A}_i \models \psi_1(f_0(i), f_1(i), \ldots, f_{n-1}(i))\} \in U \\
&\quad \Longleftrightarrow \{i \in I \mid \mathfrak{A}_i \models \varphi(f_0(i), f_1(i), \ldots, f_{n-1}(i))\} \in U.
\end{aligned}$$

The first equivalence in the string above follows from the definition of $\wedge$, the second follows from the induction hypothesis, and third follows from the definition of $\wedge$ together with the fact that U is a filter.

Next, suppose that $\varphi = \neg\psi$ and we have established the theorem for ψ. Then we have

$$\begin{aligned}
&\prod_{i\in I} \mathfrak{A}_i/U \models \varphi([f_0]_U, [f_1]_U, \ldots, [f_{n-1}]_U) \\
&\quad \Longleftrightarrow \prod_{i\in I} \mathfrak{A}_i/U \not\models \psi[f_0]_U, [f_1]_U, \ldots, [f_{n-1}]_U) \\
&\quad \Longleftrightarrow \{i \in I \mid \mathfrak{A}_i \models \psi(f_0(i), f_1(i), \ldots, f_{n-1}(i))\} \notin U \\
&\quad \Longleftrightarrow \{i \in I \mid \mathfrak{A}_i \models \varphi(f_0(i), f_1(i), \ldots, f_{n-1}(i))\} \in U.
\end{aligned}$$

The first equivalence in the string above follows from the definition of $\neg$, the second follows from the induction hypothesis, and the third follows from the definition of $\neg$ together with the fact that U is an ultrafilter and therefore, if a subset of I is not in U, then its complement *is* in U.

Finally, suppose that $\varphi(x_0, \ldots, x_{n-1}) = \exists y \psi(x_0, \ldots, x_{n-1}; y)$ and we have established the theorem for ψ. Let us prove that (1) implies (2). Thus, suppose that

$$\prod_{i\in I} \mathfrak{A}_i/U \models \varphi([f_0]_U, [f_1]_U, \ldots, [f_{n-1}]_U).$$

Since $\varphi = \exists y \psi$, this means that there is $[g]_U \in \prod_{i\in I} A_i/U$ such that

$$\prod_{i\in I} \mathfrak{A}_i/U \models \psi([f_0]_U, [f_1]_U, \ldots, [f_{n-1}]_U; [g]_U).$$

By the induction hypothesis, this implies that the set

$$J = \{i \in I \mid \mathfrak{A}_i \models \psi(f_0(i), f_1(i), \ldots, f_{n-1}(i); g(i))\}$$

is in U. But then, for all $i \in J$, we have

$$\mathfrak{A}_i \models \exists y \psi(f_0(i), f_1(i), \ldots, f_{n-1}(i), y),$$

as witnessed by $y = g(i)$. Since $\varphi = \exists y\psi$, and since $J \in U$, this means that

$$J \subseteq \{i \in I \mid \mathfrak{A}_i \models \varphi(f_0(i), f_1(i), \ldots, f_{n-1}(i))\} \in U,$$

as desired. The proof that (2) implies (1) is essentially obtained by reversing this argument and is left as an exercise.

Since the logical connectives $\vee$ and $\forall$ can be expressed in terms of $\wedge$, $\neg$, and $\exists$, this completes the proof of the theorem. □

Exercise 5.1.2. Complete the proof of Theorem 5.1.1 by proving that (2) implies (1) in the case in which $\varphi(x_0, \ldots, x_{n-1}) = \exists y\psi(x_0, \ldots, x_{n-1}; y)$ and we have established the theorem for ψ.

Łos' Theorem has the following immediate corollary.

Corollary 5.1.3. *Suppose that $\mathcal{L}$ is a first-order language, T is a theory in the language $\mathcal{L}$, I is a nonempty set, U is an ultrafilter over I and, for all $i \in I$, we are given an $\mathcal{L}$-structure $\mathfrak{A}_i$ such that $\mathfrak{A}_i \models T$. Then $\prod_{i\in I} \mathfrak{A}_i/U \models T$.*

Proof. T is a collection of sentences in $\mathcal{L}$ with no free variables. Therefore, for each $\varphi \in T$, by Theorem 5.1.1, we have

$$\prod_{i\in I} \mathfrak{A}_i/U \models \varphi \iff \{i \in I \mid \mathfrak{A}_i \models \varphi\} \in U.$$

But for each $i \in I$, we have $\mathfrak{A}_i \models T$, and hence $\mathfrak{A}_i \models \varphi$. Thus,

$$\{i \in I \mid \mathfrak{A}_i \models \varphi\} = I \in U,$$

and hence $\prod_{i\in I} \mathfrak{A}_i/U \models \varphi$. □

5.2 Ultrapowers

An important special case of the ultraproduct construction is that in which all of the structures $\mathfrak{A}_i$ for $i \in I$ are the *same*. In this case, the ultraproduct is more commonly called an *ultrapower*.

Definition 5.2.1. Suppose that $\mathcal{L}$ is a first-order language, I is a nonempty set, U is an ultrafilter over I, and $\mathfrak{A}$ is an $\mathcal{L}$-structure. Then the *ultrapower of $\mathfrak{A}$ by U*, often denoted $\prod_U \mathfrak{A}$, is defined to be the ultraproduct

$$\prod_{i\in I} \mathfrak{A}_i/U,$$

where, for each $i \in I$, we have $\mathfrak{A}_i = \mathfrak{A}$.

Recall that two $\mathcal{L}$-structures $\mathfrak{A}$ and $\mathfrak{B}$ are said to be *elementarily equivalent*, denoted $\mathfrak{A} \equiv \mathfrak{B}$, if they satisfy the same $\mathcal{L}$-sentences, i.e., for every sentence $\varphi \in \mathcal{L}$, we have

$$\mathfrak{A} \models \varphi \Leftrightarrow \mathfrak{B} \models \varphi.$$

Exercise 5.2.2. Suppose that $\mathcal{L}$ is a first-order language, I is a nonempty set, U is an ultrafilter over I, and $\mathfrak{A}$ is an $\mathcal{L}$-structure. Prove that $\mathfrak{A}$ and $\prod_U \mathfrak{A}$ are elementarily equivalent. (Hint: Use Corollary 5.1.3.)

If $\mathfrak{A}$ is an $\mathcal{L}$-structure, with underlying set A, and U is an ultrafilter over some index set I, then there is a natural embedding of $\mathfrak{A}$ into the ultrapower $\prod_U \mathfrak{A}$. This embedding is denoted $j_U : A \to \prod_U A$, and is defined as follows: For all $a \in A$, let $f_a : I \to A$ be the constant map taking value a, i.e., $f_a(i) = a$ for all $i \in I$. Then set $j_U(a) = [a]_U$.

Exercise 5.2.3. Suppose that $\mathcal{L}$ is a first-order language, $\mathfrak{A}$ is an $\mathcal{L}$-structure, I is a nonempty set, and U is an ultrafilter over I. Prove that the ultrapower embedding $j_U : A \to \prod_U A$ as defined above is an *elementary embedding*. In other words, prove that, for every $\mathcal{L}$-formula φ with n free variables, and for all n-tuples $(a_0, a_1, \ldots, a_{n-1})$ of elements of A, we have

$$\mathfrak{A} \models \varphi(a_0, a_1, \ldots, a_{n-1}) \iff \prod_U \mathfrak{A} \models \varphi(j_U(a_0), j_U(a_1), \ldots, j_U(a_{n-1})).$$

(Hint: Apply Łos' Theorem.)

5.3 Nonstandard numbers

One typical use of the ultraproduct construction is to produce "nonstandard" versions of certain standard mathematical structures. This can be used to prove, for instance, that certain properties that these standard mathematical structures possess cannot be expressed in a first-order way. They way this argument goes is as follows: One fixes a first order language $\mathcal{L}$ and an $\mathcal{L}$-structure $\mathfrak{A}$ such that $\mathfrak{A}$ satisfies a certain property P. One then takes an ultrapower $\prod_U \mathfrak{A}$ and proves that this ultrapower does *not* satisfy property P. Since, by Exercise 5.2.2, $\mathfrak{A}$ and $\prod_U \mathfrak{A}$ are elementarily equivalent, they satisfy the same first-order sentences. Since P is satisfies by $\mathfrak{A}$ but not by $\prod_U \mathfrak{A}$, this shows that P cannot be expressed by a first-order sentence in the language $\mathcal{L}$.

Nonstandard natural numbers

Let $\mathcal{L} = \{+, \cdot, <, 0\}$, where $+$ and $\cdot$ are binary function symbols, $<$ is a binary relation symbol, and 0 is a constant symbol. Let $\mathfrak{A} = (\mathbb{N}, +_{\mathbb{N}}, \cdot_{\mathbb{N}}, <_{\mathbb{N}}, 0_{\mathbb{N}})$, where

- $\mathbb{N}$ is the usual set of natural numbers;
- $+_{\mathbb{N}}$ and $\cdot_{\mathbb{N}}$ are the usual operations of addition and multiplication, respectively, on $\mathbb{N}$;
- $<_{\mathbb{N}}$ is the usual ordering of $\mathbb{N}$;
- $0_{\mathbb{N}}$ is the natural number 0.

Now let U be a nonprincipal ultrafilter over ω (we use ω here instead of $\mathbb{N}$ simply to distinguish it from the underlying set of $\mathfrak{A}$). Consider the ultrapower $\prod_U \mathfrak{A}$ and the resulting ultrapower map $j_U : \mathbb{N} \to \prod_U \mathbb{N}$. For each $n \in \mathbb{N}$, let $f_n : \omega \to \mathbb{N}$ be the constant function taking value n. By the definition of j_U, we have $j_U(n) = [f_n]_U$ for all $n \in \mathbb{N}$. Let us prove a few basic facts about this ultrapower. For the first observation, we will need following basic fact about ultrafilters, which we leave as an exercise.

Exercise 5.3.1. Suppose that U is an ultrafilter over a set I. Then, for every natural number n, every set $X \in U$, and every partition $X = X_0 \cup X_1 \cup \ldots \cup X_{n-1}$ of X into n pieces, there is $m < n$ such that $X_m \in U$. (Hint: Prove this by induction on n.)

Proposition 5.3.2. *j_U maps $\mathbb{N}$ onto an initial segment of $\prod_U \mathbb{N}$.*

Proof. It suffices to show that, for all $n \in \mathbb{N}$ and every $f : \omega \to \mathbb{N}$ such that

$$\prod_U \mathfrak{A} \models [f]_U < [f_n]_U,$$

there is $m < n$ such that $f =_U f_m$. To this end, fix such an n and f. Let

$$X = \{i < \omega \mid f(i) < f_n(i) = n\}.$$

By Łos' Theorem and the fact that $\prod_U \mathfrak{A} \models [f]_U < [f_n]_U$, we must have $X \in U$. Now, for all $m < n$, let

$$X_m = \{i \in X \mid f(i) = m\}.$$

Then $X = X_0 \cup X_1 \cup \ldots \cup X_{n-1}$ is a partition of X, so, by Exercise 5.3.1, there is $m < n$ such that $X_m \in U$. But $X_m = \{i < \omega \mid f(i) = m = f_m(i)\}$, so $[f]_U = [f_m]_U$. □

Proposition 5.3.3. *There is $f : \omega \to \mathbb{N}$ such that, for all $n \in \mathbb{N}$, we have $\prod_U \mathfrak{A} \models j_U(n) < [f]_U$.*

Proof. Let $f : \omega \to \mathbb{N}$ be the identity function, i.e., $f(i) = i$ for all $i < \omega$. Now, for all $n \in \mathbb{N}$, we have

$$\{i < \omega \mid f_n(i) < f_i\} = \{i < \omega \mid i > n\} = \{n+1, n+2, n+3, \ldots\}.$$

This set contains all but finitely many elements of ω, so, since U is a nonprincipal ultrafilter, it is an element of U. Thus, we have

$$\prod_U \mathfrak{A} \models j_U(n) < [f]_U.$$

□

It is quite easy to construct many other functions f that satisfy the conclusion of Proposition 5.3.3. In fact, there are $2^{\aleph_0}$-many such functions. Thus, the structure of $\prod_U \mathfrak{A}$ is roughly as follows: at the bottom there is a copy of the standard natural numbers that is equal to $\{j_U(n) \mid n \in \mathbb{N}\}$, and above that is a much larger more complicated structure. The precise properties of this structure are quite interesting, but beyond the scope of this particular lecture. I encourage you to look into it more on your own.

Finally, let us show that the ultrapower $\prod_U \mathfrak{A}$, ordered by its interpretation of $<$, is not well-founded. This will show that the property of $<$ being a well-order cannot be expressed by a first-order sentence in $\mathcal{L}$.

Proposition 5.3.4. *The interpretation of $<$ in $\prod_U \mathfrak{A}$ is not well-founded. In other words, there is a sequence $\langle f_i \mid i < \omega \rangle$ of functions from ω to $\mathbb{N}$ such that, for all $i < \omega$, we have*

$$\prod_U \mathfrak{A} \models [f_{i+1}]_U < [f_i]_U.$$

Proof. For each $i < \omega$, define $f_i : \omega \to \mathbb{N}$ by letting

$$f_i(j) = \begin{cases} 0 & \text{if } j < i \\ j - i & \text{if } j \geq i. \end{cases}$$

We claim that, for all $i < \omega$, we have

$$\prod_U \mathfrak{A} \models [f_{i+1}]_U < [f_i]_U.$$

To see this, fix $i < \omega$. Note that, for all $j > i$, we have

$$f_{i+1}(j) = j - (i+1) = j - i - 1 < j - i = f_i(j).$$

Since U is a nonprincipal ultrafilter, the set $\{j < \omega \mid j > i\}$ is in U. Therefore, $\{j < \omega \mid f_{i+1}(j) < f_i(j)\}$ is in U, so

$$\prod_U \mathfrak{A} \models [f_{i+1}]_U < [f_i]_U,$$

as desired. □

5.4 Nonstandard real numbers

Let $\mathcal{L} = \{+, \cdot, <, 0, 1\}$, where $+$ and $\cdot$ are binary function symbols, $<$ is a binary relation symbol, and 0 and 1 are constant symbols. Let $\mathfrak{A} = (\mathbb{R}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, <_{\mathbb{R}}, 0_{\mathbb{R}}, 1_{\mathbb{R}})$, where

- $\mathbb{R}$ is the usual set of real numbers;
- $+_{\mathbb{R}}$ and $\cdot_{\mathbb{R}}$ are the usual operations of addition and multiplication, respectively, on $\mathbb{R}$;
- $<_{\mathbb{R}}$ is the usual ordering of $\mathbb{R}$;
- $0_{\mathbb{R}}$ is the real number 0 and $1_{\mathbb{R}}$ is the real number 1.

As in the previous section, let U be a nonprincipal ultrafilter over ω and consider the ultrapower $\prod_U \mathfrak{A}$ and the resulting ultrapower map $j_U : \mathbb{R} \to \prod_U \mathbb{R}$. For each real number $r \in \mathbb{R}$, let $f_r : \omega \to \mathbb{R}$ be the constant function taking value r. Then we have $j_U(r) = [f_r]_U$ for all $r \in \mathbb{R}$.

In what follows, if $r \in \mathbb{R}$ and $n \in \mathbb{N}$, then we will let $n * r$ denote the result of adding r to itself n times, i.e.,

$$n * r = \underbrace{r + r + \cdots + r}_{n \text{ times}}.$$

(Note that we are using $*$ for this rather than $\cdot$ because this is being calculated *outside* of the structure $\mathfrak{A}$ rather than internally.) Similarly, given $f : \omega \to \mathbb{R}$ and $n \in \mathbb{N}$, we let

$$n * [f]_U = \underbrace{[f]_U + [f]_U + \cdots + [f]_U}_{n \text{ times}},$$

as calculated in the ultrapower $\prod_U \mathfrak{A}$.

An important property of the standard set of real numbers is that it is *Archimedean*, i.e., for every *positive* real number r, if we add r to itself enough times, it becomes arbitrarily large. More precisely:

Exercise 5.4.1. Prove that $\mathfrak{A}$ is Archimedean, i.e., for all real numbers $a, b > 0$, there is $n \in \mathbb{N}$ such that $n * a > b$.

We will now show, however, that the ultrapower $\prod_U \mathfrak{A}$ is *not* Archimedean. In particular, this will show that the property of being Archimedean cannot be expressed in a first-order way in the language $\mathcal{L}$.

Theorem 5.4.2. *The ultrapower $\prod_U \mathfrak{A}$ is not Archimedean. In other words, there are $f, g : \omega \to \mathbb{R}$ such that*

- $\prod_U \mathfrak{A} \models [f_0]_U < [f]_U \wedge [f_0]_U < [g]_U$*;*
- *for all $n \in \mathbb{N}$, $\prod_U \mathfrak{A} \models n * [f]_U < [g]_U$.*

Proof. First, define $f : \omega \to \mathbb{R}$ by letting $f(i) = 1/(i+1)$ for every $i < \omega$. Let $g = f_1$ be the constant function taking value 1. Note that, for all $i < \omega$, we have $f(i), g(i) > 0$, and hence

$$\prod_U \mathfrak{A} \models [f_0]_U < [f]_U \wedge [f_0]_U < [g]_U.$$

It remains to show that, for all $n \in \mathbb{N}$, we have

$$\prod_U \mathfrak{A} \models n * [f]_U < [g]_U.$$

To this end, fix an arbitrary $n \in \mathbb{N}$. For every $i < \omega$, we have

$$(n * [f]_U)(i) = \underbrace{1/(i+1) + 1/(i+1) + \cdots + 1/(i+1)}_{n \text{ times}} = n/(i+1).$$

Thus, for all $i \geq n$, we have

$$(n * [f]_U)(i) = n/(i+1) < 1 = g(i).$$

Since U is a nonprincipal ultrafilter, the set $\{i < \omega \mid i \geq n\}$ is in U. Therefore, we have

$$\prod_U \mathfrak{A} \models n * [f]_U < [g]_U,$$

as desired. □

The element $[f]_U$ from the proof of the previous theorem is often called an *infinitesimal* element of ultrapower $\prod_U \mathfrak{A}$, since it is greater than 0 but strictly smaller than $j_U(r)$ for every positive $r \in \mathbb{R}$. It can thus be thought of as an *infinitely small* but still positive nonstandard real number. Similarly, there are *infinite* elements of the ultrapower $\prod_U \mathfrak{A}$ that are greater than $j_U(r)$ for every $r \in \mathbb{R}$. For example the function h defined by $h(i) = i$ for all $i < \omega$ is such an infinite element. One of the most interesting applications of the nonstandard real numbers is in providing an alternate foundation for calculus that is in many ways more elegant than the standard foundation. These infinitesimal and infinite nonstandard real numbers play a key role in this theory.

5.5 The compactness theorem

You may have seen other proofs that the notion of *well-order* or the Archimedean property cannot be expressed in a first order way. It is likely that such proofs involved applications of the Compactness Theorem for first-order logic. It is no accident that we were also able to prove them using ultraproducts. In fact, ultraproducts allow us to produce a very elegant proof of the Compactness Theorem itself.

Theorem 5.5.1 (Compactness Theorem for first-order logic)**.** *Suppose that $\mathcal{L}$ is a first-order language and T is a set of $\mathcal{L}$-sentences. Then the following are equivalent:*

1. *T is finitely satisfiable, i.e., for every finite subset $T_0 \subseteq T$, there is an $\mathcal{L}$-structure $\mathfrak{A}$ such that $\mathfrak{A} \models T_0$.*

2. *T is satisfiable, i.e., there is an $\mathcal{L}$-structure $\mathfrak{A}$ such that $\mathfrak{A} \models T$.*

Proof. The direction (2) $\Rightarrow$ (1) is trivial, since if $\mathfrak{A} \models T$, then $\mathfrak{A} \models T_0$ for every finite $T_0 \subseteq T$.

To prove that (1) $\Rightarrow$ (2), assume that T is finitely satisfiable. Let I be the collection of all finite subsets of T. For each $S \in I$, fix an $\mathcal{L}$-structure $\mathfrak{A}_S$ such that $\mathfrak{A}_S \models S$.

For each $S \in I$, let $S^* = \{W \in I \mid S \subseteq W\}$. In other words, S^* is the collection of all finite subsets of T that contain all of the elements of S. Let

$$\mathcal{F} = \{X \in \mathscr{P}(I) \mid \exists S \in I \, [S^* \subseteq X]\}.$$

Exercise 5.5.2. Prove that $\mathcal{F}$ is a filter over I.

By Theorem 3.3.8, we can find an ultrafilter U over I such that $\mathcal{F} \subseteq U$. Now let $\mathfrak{A}$ be the ultraproduct

$$\mathfrak{A} = \prod_{S \in I} \mathfrak{A}_S / U.$$

We claim that $\mathfrak{A} \models T$, i.e., for every sentence $\varphi \in T$, $\mathfrak{A} \models \varphi$. Fix such a sentence φ, and let $S = \{\varphi\}$. Then $S^* \in \mathcal{F} \subseteq U$. Moreover, for every $W \in S^*$, we have $\varphi \in W$, and hence

$$\mathfrak{A}_W \models \varphi.$$

Hence, the set

$$\{W \in I \mid \mathfrak{A}_W \models \varphi\}$$

is in U. By Łos' Theorem, it follows that $\mathfrak{A} \models \varphi$. Hence $\mathfrak{A} \models T$, so T is satisfiable. □

Chapter 6

Lecture 6: Bases in algebraic structures, Part I

In this lecture, we begin to introduce some concepts and structures from algebra. As a framework for their introduction, and as an illustration of some applications of set theory and logic to algebra, we will use the axiom of choice to prove various results about the existence of bases. We begin by studying abelian groups.

Definition 6.0.1. A *group* consists of a nonempty set G and a binary operation "$+$" on G satisfying the following properties:

- (Associativity) For all $x, y, z \in G$, we have $(x + y) + z = x + (y + z)$.
- (Identity element) There exists a unique element $0_G \in G$ such that, for all $x \in G$, we have $x + 0_G = x = 0_G + x$.
- (Inverse elements) For every $x \in G$, there is a unique element $y \in G$ such that $x + y = 0_G = y + x$. This element y is called the *inverse* of x, and is often denoted "$(-x)$".

A group G is called *abelian* if, moreover, it satisfies the following property:

- (Commutativity) For all $x, y \in G$, we have $x + y = y + x$.

Remark 6.0.2. We will often denote a group simply by its underlying set G without explicitly mentioning its binary operation. If clarification is needed, we will sometimes denote the binary operation of G by "$+_G$".

Typically, if G is an arbitrary group that is not necessarily abelian, its binary operation is usually denoted by "$\cdot$" instead of "$+$", the identity element is denoted by "1_G" instead of "0_G" and, given an element $x \in G$, its inverse element is denoted by "x^{-1}" instead of "$(-x)$". The notation we are using here is more typical if G is known to be an abelian group. Since we will be dealing almost exclusively with abelian groups in this course, we will stick with the additive notation.

Example 6.0.3. Let us give some simple examples of groups:

- The set $\mathbb{Z}$ of integers, with the usual operation of addition, is an abelian group.

- The set $\mathbb{Q}$ of rational numbers, with the usual operation of addition, is an abelian group.
- The set $\mathbb{R}$ of real numbers, with the usual operation of addition, is an abelian group.
- The set $\mathbb{R} \setminus \{0\}$ of nonzero real numbers, with the operation of multiplication, is an abelian group.
- The set of all real 2×2 matrices, with the operation of matrix addition, is an abelian group.
- The set of all *invertible* real 2×2 matrices, with the operation of matrix multiplication, is a (nonabelian) group.
- Let X be any set. Then the set of all bijections $f : X \to X$, with the operation of composition of functions (i.e., $f + g = f \circ g$) is a group. It is abelian if $|X| \leq 2$ and nonabelian if $|X| > 2$.

Definition 6.0.4. Suppose that G and H are groups. A function $\pi : G \to H$ is a *group homomorphism* if, for all $x, y \in G$, we have

$$\pi(x +_G y) = \pi(x) +_H \pi(y).$$

A group homomorphism $\pi : G \to H$ is called an *isomorphism* if it is bijective. Two groups G and H are said to be *isomorphic*, denoted $G \cong H$, if there is an isomorphism $\pi : G \to H$.

Exercise 6.0.5. Suppose that $\pi : G \to H$ is a group homomorphism.

1. Prove that $\pi(0_G) = 0_H$.
2. Prove that, for all $x \in G$, $\pi(-x) = -\pi(x)$.
3. Prove that, if π is an isomorphism, then its inverse map $\pi^{-1} : H \to G$ is also a group homomorphism (and hence an isomorphism).

If two groups are isomorphic, then they have the same algebraic structure. They are essentially the same group, except possibly their elements have been renamed. From an algebraic point of view, they are though of as equal.

Definition 6.0.6. If G is an abelian group, $n \in \mathbb{N}$, and $x \in G$, then we let nx denote the result of adding x to itself n times, i.e.,

$$nx = \underbrace{x +_G x +_G \cdots +_G x}_{n \text{ times}}.$$

If $a \in \mathbb{Z}$ is a *negative* integer, so $a = -n$ for some $n \in \mathbb{N}$, then we let ax denote the result of adding $(-x)$ to itself n times, i.e.,

$$(-n)x = n(-x) = \underbrace{(-x) +_G (-x) +_G \cdots +_G (-x)}_{n \text{ times}}.$$

Definition 6.0.7. Let G be an abelian group, and let $E \subseteq G$. We say that E *generates* G if every element of G can be expressed as a finite sum of elements of E, together with their inverses. In other words, E generates G if, for every $x \in G$, there are finitely many elements $e_1, \ldots, e_n \in E$ and integers $a_1, \ldots, a_n \in \mathbb{Z}$ such that

$$x = a_1 e_1 +_G a_2 e_2 +_G \cdots +_G a_n e_n = \sum_{i=1}^{n} a_i e_i.$$

Example 6.0.8.

- The set $\{1\}$ generates the abelian group $(\mathbb{Z}, +)$.
- The set $E = \{1/n \mid n \in \mathbb{N} \setminus \{0\}\}$ generates the abelian group $(\mathbb{Q}, +)$.

Definition 6.0.9. Let G be an abelian group, and let $E \subseteq G$. We say that E is *linearly independent* if, for every finite sequence $\langle e_1, e_2, \ldots, e_n \rangle$ of distinct elements of E and, for every sequence $\langle a_1, a_2, \ldots, a_n \rangle$ of integers, if

$$a_1 e_1 + a_2 e_2 + \cdots + a_n e_n = 0,$$

then $a_1 = a_2 = \cdots = a_n = 0$.

Definition 6.0.10. Let G be an abelian group, and let $E \subseteq G$. We say that E is a *basis* for G is it generates G and is linearly independent. If G has a basis, then G is said to be a *free abelian group.*

Not all abelian groups have bases. In fact, the free abelian groups are quite special in the class of all abelian groups.

Exercise 6.0.11. Suppose that G is an abelian group and $E \subseteq G$. Prove that the following are equivalent:

- E is a basis for G;
- for every $x \in G$, there is a unique finite set $I \subseteq E$ and a unique set $\{a_e \mid e \in I\}$ of nonzero integers such that

$$x = \sum_{e \in I} a_e e.$$

Example 6.0.12.

- We have already seen that $\{1\}$ generates $(\mathbb{Z}, +)$. It is also linearly independent: if a is a nonzero integer, then $a1 = a \neq 0$. Thus, $\{1\}$ is a basis for $\mathbb{Z}$, and hence $\mathbb{Z}$ is a free abelian group.
- We saw above that the set $E = \{1/n \mid n \in \mathbb{N} \setminus \{0\}\}$ generates $(\mathbb{Q}, +)$. However, E is not linearly independent. For example, if $e_1 = 1/1$ and $e_2 = 1/2$, then we have

  $$e_1 - 2e_2 = 0,$$

  thus witnessing that E is not linearly independent. Thus, E is not a basis for $(\mathbb{Q}, +)$. In fact, we will show in the next theorem that $(\mathbb{Q}, +)$ does not have a basis, and thus is not free.

Theorem 6.0.13. *The abelian group $(\mathbb{Q}, +)$ is not free.*

Proof. Suppose for the sake of contradiction that $E \subseteq \mathbb{Q}$ is a basis for $\mathbb{Q}$. Suppose first that E only has one element, i.e., $E = \{e\}$. Then e must be a nonzero rational number, so $e/2$ is a nonzero rational number. Since E is a basis, there must be an integer $a \in \mathbb{Z}$ such that $ae = e/2$. Rearranging this equation algebraically yields $2ae = e$, so $2ae - e = 0$, so $e(2a - 1) = 0$. Since e is nonzero, we must have $2a - 1 = 0$, i.e., $a = 1/2$, contradicting the fact that $a \in \mathbb{Z}$.

Thus, we must have $|E| > 1$. Let e_1, e_2 be two distinct elements of E. Since e_1 and e_2 are nonzero rational numbers, we can express them as

$$e_1 = \frac{p_1}{q_1} \qquad \text{and} \qquad e_2 = \frac{p_2}{q_2}$$

where p_1, p_2, q_1, q_2 are nonzero integers and $q_1, q_2 > 0$. Now let $a_1 = p_2 q_1$ and $a_2 = -p_1 q_2$. Then a_1 and a_2 are nonzero integers, and we have

$$a_1 e_1 + a_2 e_2 = \frac{p_1 p_2 q_1}{q_1} + \frac{-p_1 p_2 q_2}{q_2} = \frac{p_1 p_2 q_1 q_2}{q_1 q_2} + \frac{-p_1 p_2 q_1 q_2}{q_1 q_2} = \frac{p_1 p_2 q_1 q_2 - p_1 p_2 q_1 q_2}{q_1 q_2} = 0,$$

contradicting the fact that E is linearly independent. □

Example 6.0.14. Suppose that n is a positive natural number, and consider the group $\mathbb{Z}^n$, where the operation is pointwise addition. More precisely, given $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in \mathbb{Z}^n$, let

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n).$$

Then $\mathbb{Z}^n$ is a free abelian group. For example, a basis is given by $E = \{e_1, \ldots, e_n\}$ where, for each $1 \leq i \leq n$,

$$e_i = \{0, \ldots, 0, \underbrace{1}_{i}, 0, \ldots, 0\}$$

is the element of $\mathbb{Z}^n$ that is 0 in every coordinate except coordinate i, where it is 1.

Note that the basis of a free abelian group is typically not unique. For example, we saw above that $E_0 = \{(1, 0), (0, 1)\}$ is a basis for $\mathbb{Z}^2$. But the set $E_1 = \{(1, 0), (1, 1)\}$ is also a basis for $\mathbb{Z}^2$ (Exercise: Prove this!).

The next exercise shows that a free abelian group is determined up to isomorphism by the cardinality of its basis.

Exercise 6.0.15.

1. Suppose that G is a free abelian group and E_0 and E_1 are bases for G. Prove that $|E_0| = |E_1|$.

2. Suppose that G and H are free abelian groups, E_G is a basis for G, E_H is a basis for H, and $|E_G| = |E_H|$. Prove that $G \cong H$. (Hint: Let $\sigma : E_G \to E_H$ be a bijection. Now define a function $\pi : G \to H$ as follows. For all $e_1, \ldots, e_n \in E_G$ and all $a_1, \ldots, a_n \in E_H$, set

$$\pi(a_1 e_1 +_G \cdots +_G a_n e_n) = a_1 \sigma(e_1) +_H \cdots +_H a_n \sigma(e_n).$$

Prove that this defines an isomorphism $\pi : G \to H$.)

Definition 6.0.16. Suppose that G is an abelian group and $H \subseteq G$. We say that H is a *subgroup* of G if $(H, +_H)$ is an abelian group, where $+_H$ denotes the restriction of $+_G$ to H. Concretely, H is a subgroup of G if and only if

- $0_G \in H$;
- for all $x, y \in H$, we have $x +_G y \in H$;
- for all $x \in H$, we have $(-x) \in H$.

Example 6.0.17. For every $m \in \mathbb{N}$, the set

$$\{am \mid a \in \mathbb{Z}\} = \{\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$$

is a subgroup of $(\mathbb{Z}, +)$. We will see in the next theorem that these are the *only* subgroups of $(\mathbb{Z}, +)$.

Theorem 6.0.18. *Suppose that H is a subgroup of $(\mathbb{Z}, +)$. Then there is $m \in \mathbb{N}$ such that $H = \{am \mid a \in \mathbb{Z}\}$.*

Proof. If $H = \{0\}$, then we can take $m = 0$, and we're done. Thus, assume that H contains a nonzero element x. Then, since both x and $-x$ must be in H, it must contain a strictly positive element. Let m be the smallest strictly positive integer in H.

We claim that $H = \{am \mid a \in \mathbb{Z}\}$. First note that, since H is a subgroup, we must have $m + m$, $m + m + m$, $-m$, $-m - m$, etc. all in H. Thus, $H \supseteq \{am \mid a \in \mathbb{Z}\}$. We must show that $H \subseteq \{am \mid a \in \mathbb{Z}\}$. Suppose that there is an element x in H that is not divisible by m. Since both x and $-x$ are in H, we know that H must contain a positive integer y that is not divisible by m. By Euclid's division lemma, we can write y as

$$y = km + r,$$

where $k \in \mathbb{N}$ and $r \in \{1, 2, \ldots, m-1\}$ (r is the *remainder* when y is divided by m). But then both y and km are in H, so $y - km = r$ is in H. But $0 < r < m$, contradicting the fact that m is the smallest positive integer in H. □

We now use the axiom of choice, in particular the well-ordering principle, to prove a very important basic theorem about abelian groups: every subgroup of a free abelian group is itself free.

Theorem 6.0.19. *Suppose that G is a free abelian group. Then every subgroup of H is also a free abelian group.*

Proof. Let E be a basis for G. By the well-ordering principle, we can find a well-ordering of E. In particular, we can express E as $\{e_\alpha \mid \alpha < \kappa\}$ for some cardinal κ.

Now let H be an arbitrary subgroup of G. We must find a basis for H.

For every nonzero element x of H, there is a unique finite set of ordinals $\alpha_1 < \ldots < \alpha_n < \kappa$ and nonzero integers $a_1, \ldots, a_n \in \mathbb{Z}$ such that

$$x = a_1 e_{\alpha_1} + \cdots + a_n e_{\alpha_n}.$$

In such a situation, we let $\#(x)$ denote α_n and $C(x)$ denote a_n, i.e., $\#(x)$ is the largest ordinal appearing as an index of a basis element when writing x as a sum of basis elements, and $C(x)$ is the coefficient of $e_{\#(x)}$ in this expression.

For each $\alpha < \kappa$, let $H_\alpha = \{x \in H \mid \#(x) = \alpha\}$, and let $Z_\alpha = \{0\} \cup \{C(x) \mid x \in H_\alpha\}$.

Lemma 6.0.20. *For each $\alpha < \kappa$, Z_α is a subgroup of $(\mathbb{Z}, +)$.*

Proof. Fix $\alpha < \kappa$. By definition, we have $0 \in Z_\alpha$. Now suppose that $a, b \in Z_\alpha$. We must show that $a+b \in Z_\alpha$. If one of a or b is zero, then we have $a+b \in \{a, b\}$, and we are done. So assume that $a, b \neq 0$. If $a = -b$, then we have $a + b = 0 \in Z_\alpha$, so we are done. Thus, assume that $a \neq -b$. Now, by the definition of Z_α, there are $x, y \in H_\alpha$ such that $x = ae_\alpha + g$ and $y = be_\alpha + h$, where g and h are sums of elements of $\{e_\beta \mid \beta < \alpha\}$. Then $x + y = (a + b)e_\alpha + (g + h)$. By assumption, $(a + b) \neq 0$, and $(g + h)$ is a sum of elements of $\{e_\beta \mid \beta < \alpha\}$. Since H is a subgroup of G, we have $x + y \in H$. Thus, $x + y \in H_\alpha$ and $C(x + y) = (a + b)$, so $a + b \in Z_\alpha$.

Finally, fix $a \in Z_\alpha$. We must show that $-a \in Z_\alpha$. If $a = 0$, then $-a = a$, and we are done. So assume that $a \neq 0$. Then there is $x \in H_\alpha$ such that $x = ae_\alpha + g$, where g is a sum of elements of $\{e_\beta \mid \beta < \alpha\}$. Then $-x = -ae_\alpha - g$. Since H is a subgroup, $-x \in H$. Thus, $-x \in H_\alpha$, and $C(-x) = -a$, so $-a \in Z_\alpha$. □

By Theorem 6.0.18, for each $\alpha < \kappa$, we can fix $m_\alpha \in \mathbb{N}$ such that $Z_\alpha = \{am_\alpha \mid a \in \mathbb{Z}\}$. Let $A = \{\alpha < \kappa \mid n_\alpha > 0\}$. For all $\alpha \in A$, by definition of Z_α, we can choose an element $v_\alpha \in H_\alpha$ such that $C(v_\alpha) = m_\alpha$ (note that making this simultaneous choice of v_α for all $\alpha \in A$ represents another use of the axiom of choice). Let

$$B = \{v_\alpha \mid \alpha \in A\}.$$

We claim that B is a basis for H. Clearly, $B \subseteq H$. We first show that it is linearly independent. To this end, fix ordinals $\alpha_1 < \ldots < \alpha_n$ from A and nonzero integers $a_1, \ldots, a_n$. We must show that $a_1 v_{\alpha_1} + \cdots + a_n v_{\alpha_n} \neq 0$. Notice that the largest index appearing in this sum is α_n, and it only appears in the term $a_n v_{\alpha_n}$. We then know that

$$a_1 v_{\alpha_1} + \cdots + a_n v_{\alpha_n} = a_n m_{\alpha_n} e_{\alpha_n} + g,$$

where g is a sum of elements of $\{e_\beta \mid \beta < \alpha_n\}$. Since $a_n m_{\alpha_n} \neq 0$ and E is linearly independent, it follows that

$$a_1 v_{\alpha_1} + \cdots + a_n v_{\alpha_n} \neq 0.$$

Thus, B is linearly independent.

Finally, we must show that B generates all of H. Suppose for the sake of contradiction that there is an element of H that cannot be expressed as a sum of elements of B. Choose such an $x \in H$ such that $\#(x)$ is minimal, i.e., for all $y \in H$ with $\#(y) < \#(x)$, y *can* be expressed as a sum of elements of B. Let $\alpha = \#(x)$. Then

$$x = C(x)e_\alpha + g,$$

where g is a sum of elements of $\{e_\beta \mid \beta < \alpha\}$ and $C(x) \neq 0$. We know that $C(x) \in Z_\alpha$, so there is a nonzero $a \in \mathbb{Z}$ such that $C(x) = am_\alpha$. Now consider the element $v_\alpha \in B$. We know that

$$v_\alpha = m_\alpha e_\alpha + h,$$

where h is a sum of elements of $\{e_\beta \mid \beta < \alpha\}$. Let $y = x - av_\alpha$. Since both x and v_α are in H, we have $y \in H$. Also,

$$y = x - av_\alpha = am_\alpha e_\alpha + g - am_\alpha e_\alpha - ah = g - ah,$$

so $y = g - ah$, which is a sum of elements of $\{e_\beta \mid \beta < \alpha\}$. In particular, $\#(y) < \alpha$. Thus, by the minimality of $\#(x)$, we know that y can be written as a sum of elements of B. In other words, there are ordinals $\beta_1 < \ldots < \beta_n$ from A and integers $b_1, \ldots, b_n$ such that

$$y = b_1 v_{\beta_1} + \ldots + b_n v_{\beta_n}.$$

But $y = x - av_\alpha$, so

$$x = y + av_\alpha = b_1 v_{\beta_1} + \ldots + b_n v_{\beta_n} + av_\alpha,$$

so we have written x as a sum of elements of B, contradicting our choice of x. Thus, B does generate all of H. It is therefore a basis for H, and hence H is free. $\square$

Chapter 7

Lecture 7: Bases in algebraic structures, Part II

We continue here our exploration of algebraic structures, moving from abelian groups to *fields*, and in particular *algebraically closed fields*.

Definition 7.0.1. A *field* consists of a nonempty set F and two binary relations "$+$" and "$\cdot$" on F satisfying the following properties:

- (Associativity) For all $a, b, c \in F$, we have $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
- (Commutativity) for all $a, b \in F$, we have $a + b = b + a$ and $a \cdot b = b \cdot a$;
- (Identity elements) There are unique and distinct elements $0_F, 1_F \in F$ such that, for all $a \in F$, we have $a + 0_F = a$ and $a \cdot 1_F = a$;
- (Additive inverse) For every $a \in F$, there is a unique $b \in F$ such that $a + b = 0_F$. This element b is denoted "$(-a)$" and is called the *additive inverse* of a;
- (Multiplicative inverse) For every $a \in F$ with $a \neq 0_F$, there is a unique element $b \in F$ such that $a \cdot b = 1_F$. This element b is denoted "a^{-1}" or "$1/a$" and is called the *multiplicative inverse* of a;
- (Distributivity) For all $a, b, c \in F$, we have $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Remark 7.0.2. Note that, if $(F, +, \cdot)$ is a field, then both $(F, +)$ and $(F \setminus \{0_F\}, \cdot)$ are abelian groups, called the *additive group of* F and the *multiplicative group of* F, respectively.

Intuitively, a field is an algebraic structure in which one can add, subtract, multiply, and divide, and in which these operations behave similarly to how they behave in familiar structures, such as the real numbers. If $a, b \in F$, then we will often write $a - b$ instead of $a + (-b)$, and, if $b \neq 0_F$, we will write a/b instead of $a \cdot (b^{-1})$.

Example 7.0.3.
1. $(\mathbb{Q}, +, \cdot)$, the rational numbers with the usual operations, is a field.
2. $(\mathbb{R}, +, \cdot)$, the real numbers with the usual operations, is a field.

3. $(\mathbb{C}, +, \cdot)$, the complex numbers with the usual operations, is a field. Recall that $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, where $i \in \mathbb{C}$ is such that $i^2 = -1$.

4. Let $p \in \mathbb{N}$ be a prime number, and let $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$. Then $(\mathbb{F}_p, +_p, \cdot_p)$ is a field, where $+_p$ and $\cdot_p$ denote addition and multiplication *modulo* p, respectively. For instance, in $\mathbb{F}_5$, we have $3 +_5 4 = 2$, since $3 + 4 = 7 \equiv 2 \mod 5$, and also $3 \cdot_5 4 = 2$, since $3 \cdot 4 = 12 \equiv 2 \mod 5$.

Field homomorphisms and isomorphisms are defined similarly to how they are defined for abelian groups:

Definition 7.0.4. Suppose that F and K are fields. Then a function $\pi : F \to K$ is a *field homomorphism* if

- for all $a, b \in F$, we have $\pi(a +_F b) = \pi(a) +_K \pi(b)$;
- for all $a, b \in F$, we have $\pi(a \cdot_F b) = \pi(a) \cdot_K \pi(b)$;
- $\pi(1_F) = 1_K$.

A *field isomorphism* is a field homomorphism that is a bijection. If there exists a field isomorphism $\pi : F \to K$, then we say that F and K are *isomorphic*, denoted $F \cong K$.

Definition 7.0.5. As in the previous section, if F is a field, n is a natural number, and $a \in F$, then we define na to be the result of adding a to itself n times, i.e.,

$$na = \underbrace{a +_F a +_F \cdots +_F a}_{n \text{ times}}$$

If there is a positive natural number n such that $n1_F = 0_F$, then the least such positive number is called the *characteristic* of F. If there is no such positive natural number, then the characteristic of F is said to be 0.

We can similarly define exponentiation by natural numbers. If n is a natural number and $a \in F$, then we define a^n to be the result of multiplying a by itself n times, i.e.,

$$a^n = \underbrace{a \cdot_F a \cdot_F \cdots \cdot_F a}_{n \text{ times}}.$$

We extend these definitions to negative integers in the usual way: if $n \in \mathbb{N}$ and $a \in F$, then $-na = n(-a)$, and $a^{-n} = (a^{-1})^n$.

Fact 7.0.6. *The characteristic of a field is always either* 0 *or a prime natural number. The characteristics of* $\mathbb{Q}$*,* $\mathbb{R}$*, and* $\mathbb{C}$ *are all* 0*. If* p *is a prime number, then the characteristic of* $\mathbb{F}_p$ *is* p*.*

Definition 7.0.7. Suppose that $(K, +_K, \cdot_K)$ and $(L, +_L, \cdot_L)$ are fields. We say that K is a *subfield* of L if

- $K \subseteq L$;
- $+_K$ is the restriction of $+_L$ to K;
- $\cdot_K$ is the restriction of $\cdot_L$ to K.

In this situation, we also say that L is a *field extension* of K.

In a sense, the definition of a *field* is designed precisely to allow one to solve linear equations: If F is a field, $a, b, c \in F$, and x is a variable, then the equation

$$ax + b = c$$

has a solution in F, i.e., there is a $d \in F$ such that $a \cdot d + b = c$. (This solution d can be calculated to be precisely $\frac{c-b}{a}$, or $(c + (-b)) \cdot a^{-1}$.) This naturally leads to the question of whether one can solve more general polynomial equations.

Definition 7.0.8. Suppose that F is a field. A *polynomial over F in one variable* is an expression of the form

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdot + a_n x^n,$$

where $n \in \mathbb{N}$, x is a variable, and, for all $i \leq n$, we have $a_i \in F$. The *degree* of a polynomial $p(x) = a_0 + a_1 x + a_2 x^2 + \cdot + a_n x^n$ is the largest $k \leq n$ such that $a_k \neq 0_F$.

If $p(x)$ is a polynomial over F, then a *root* of $p(x)$ is an element $b \in F$ such that $p(b) = 0_F$. In other words, if

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdot + a_n x^n,$$

then a *root* of $p(x)$ is a $b \in F$ such that

$$a_0 + a_1 \cdot b + a_2 \cdot b^2 + \cdots + a_n \cdot b^n = 0_F.$$

A polynomial might or might not have any roots in a given field. For example, the polynomial $p(x) = x^2 - 5x + 6$ has two roots in $\mathbb{Q}$, namely $x = 2$ and $x = 3$. On the other hand, the polynomial $q(x) = x^2 + 1$ has no roots in $\mathbb{Q}$, or in $\mathbb{R}$. It does have two roots in $\mathbb{C}$, though, namely $x = i$ and $x = -i$. Questions about whether or not polynomials have roots leads to the important notion of an *algebraically closed field.*

Definition 7.0.9. Suppose that F is a field. We say that F is an *algebraically closed field* if every polynomial over F of degree at least 1 has a root in F.

Example 7.0.10.

1. We have seen through the example of $q(x) = x^2 + 1$ that neither $\mathbb{Q}$ nor $\mathbb{R}$ is algebraically closed.
2. On the other hand, $\mathbb{C}$ *is* an algebraically closed field: this is the statement of the Fundamental Theorem of Algebra.
3. For every prime number p, the field $\mathbb{F}_p$ is not algebraically closed.

We will need various basic facts about fields that we will not have time to formally prove. The first is the following.

Fact 7.0.11. *Suppose that K is a field and $p(x)$ is a polynomial over K of degree n. Then $p(x)$ has at most n distinct roots in K.*

Definition 7.0.12. Suppose that L is a field extension of K (so K is a subfield of L). An element $b \in L$ is called *algebraic over K* if there is a polynomial $p(x)$ over K such that b is a root of p. We say that b is *transcendental over K* if it is not algebraic over K.

Example 7.0.13. Consider $\mathbb{R}$ as a field extension of $\mathbb{Q}$.

1. $\sqrt{2}$ is algebraic over $\mathbb{Q}$, since it is a root of the polynomial $p(x) = x^2 - 2$.
2. π is transcendental over $\mathbb{Q}$: there is no polynomial $p(x)$ over $\mathbb{Q}$ such that π is a root of p. The proof of this fact is quite difficult.

Remark 7.0.14. Although it is quite difficult to prove that any particular real number is transcendental over $\mathbb{Q}$, it is quite easy to see that in fact *most* real numbers are transcendental over $\mathbb{Q}$ just by counting. There are only countably many polynomials with rational coefficients, and each polynomial only has finitely many roots. Therefore, there are only countably many real numbers that are algebraic over $\mathbb{Q}$. Since $\mathbb{R}$ is uncountable, this means that the vast majority of real numbers are transcendental over $\mathbb{Q}$.

Definition 7.0.15. Suppose that L is a field extension of K. We say that L is an *algebraic field extension of* K if every element of L is algebraic over K. We say that L is a *transcendental field extension of* K if there is an element of L that is transcendental over K.

Proposition 7.0.16. *Suppose that L is an algebraic field extension of K. Then $|L| \leq \max\{|K|, \aleph_0\}$.*

Proof. Let $\kappa = \max\{|K|, \aleph_0\}$. There are at most κ-many polynomials over K and, by Fact 7.0.11, every polynomial over K has at most finitely many roots over K. Thus, there are at most κ-many elements of L that are algebraic over K. Since L is algebraic over K, we know that *every* element of L is algebraic over K, so $|L| \leq \kappa$. □

Definition 7.0.17. Suppose that L is a field extension of K. We say that L is an *algebraic closure of* K if

1. L is an algebraic field extension of K; and
2. L is algebraically closed.

Intuitively, an algebraic closure of a field K is the *smallest* algebraically closed field containing K. One can think of constructing it by adding roots to all of the polynomials over K that do not already have roots in K, and then closing under the field operations. To make this precise, we need the following fact, which we will not prove.

Fact 7.0.18. *Suppose that K is a field and $p(x)$ is a polynomial over K. Then there is an algebraic field extension L of K such that there is a root of $p(x)$ in L.*

We will also need the following fact, which we leave as an exercise.

Exercise 7.0.19. If L is an algebraic field extension of K and M is an algebraic field extension of L, then M is an algebraic field extension of K.

We can now use Zorn's Lemma to establish the existence of algebraic closures.

Theorem 7.0.20. *Suppose that K is a field. Then there is exists an algebraic closure of K.*

Proof. Let E be a set such that $E \supset K$ and $|E| > \max\{|K|, \aleph_0\}$. Let P be the set of all fields $(L, +_L, \cdot_L)$ such that

- $L \subseteq E$; and
- $(L, +_L, \cdot_L)$ is an algebraic field extension of K.

Let P be ordered by the field extension relation, i.e., if $(L, +_L, \cdot_L), (M, +_M, \cdot_M) \in P$, then $(L, +_L, \cdot_L) \leq (M, +_M, \cdot_M)$ if and only if $(M, +_M, \cdot_M)$ is a field extension of $(L, +_L, \cdot_L)$.

Exercise 7.0.21. Verify that $(P, \leq)$ is a partial order.

We want to apply Zorn's lemma to $(P, \leq)$, so we must verify that every chain $C \subseteq P$ has an upper bound.

Lemma 7.0.22. *Suppose that $C \subseteq P$ is a chain, i.e., for all $(L, +_L, \cdot_L)$ and $(M, +_M, \cdot_M)$ in C, either L is a subfield of M or M is a subfield of L. Then there is an $(N, +_N, \cdot_N) \in P$ such that $(L, +_L, \cdot_L)$ is a subfield of $(N, +_N, \cdot_N)$ for all $(L, +_L, \cdot_L) \in C$.*

Proof. Let $N = \bigcup\{L \mid (L, +_L, \cdot_L) \in C\}$, and define $+_N$ and $\cdot_N$ to agree with the field relations of the fields in C. In other words, for all $a, b \in N$, find $(L, +_L, \cdot_L) \in C$ such that $b, c \in L$, and set $b +_N c = b +_L c$ and $b \cdot_N c = b \cdot_L c$. Because C is linearly ordered by $\leq$, this is independent of our choice of L.

It is now routine to verify that $(N, +_N, \cdot_N)$ is a field, and hence a field extension of K, and that $N \subseteq E$ (Exercise: Verify this!). To see that N is an algebraic field extension of K, fix an arbitrary $b \in N$. Then $b \in L$ for some $(L, +_L, \cdot_L) \in C$. Since L is an algebraic field extension of K, b is algebraic over K. Thus, N is an algebraic field extension of K.

Finally, the definition of N makes it clear that it is a field extension of every element of C and is thus an upper bound for C. □

Now apply Zorn's lemma to find a maximal element $(L, +_L, \cdot_L)$ of P. We claim that L is an algebraic closure of K. Since $(L, +_L, \cdot_L) \in P$, we know that it is an algebraic field extension of K. It thus remains to show that L is algebraically closed.

Suppose for the sake of contradiction that L is not algebraically closed. Then there is a polynomial $p(x)$ over L that does not have any roots in L. By Fact 7.0.18, we can find an algebraic field extension $(M, +_M, \cdot_M)$ of L such that p has a root in M. Since M is algebraic over L and L is algebraic over K, Exercise 7.0.19 implies that M is algebraic over K. By Proposition 7.0.16, we know that $|M| \leq \max\{|K|, \aleph_0\}$. Since $|E| > \max\{|K|, \aleph_0\}$, we can assume, by renaming elements of $M \setminus L$ if necessary, that $M \subseteq E$. But then $(M, +_M, \cdot_M) \in P$ and $(L, +_L, \cdot_L) \lneq (M, +_M, \cdot_M)$, contradicting the maximality of $(L, +_L, \cdot_L)$. Thus, L is indeed algebraically closed and is hence an algebraic closure of K. □

So far we have been referring to *an* algebraic closure of a field K, but the following fact shows that algebraic closures are unique up to isomorphism, so it is in fact more common to refer to *the* algebraic closure of a field K. We will not give the proof of this fact, but it can also be proved using Zorn's lemma.

Fact 7.0.23. *Suppose that K is a field and that L and M are both algebraic closures of K. Then $L \cong M$.*

The notion of polynomial over a field can be broadened to incorporate more than one variable. Suppose that $n \in \mathbb{N}$ and $\mathcal{X} = \{x_1, \ldots, x_n\}$ is a set of n variables. Then a *monomial* in $\mathcal{X}$ is an expression of the form

$$\prod_{i=1}^{n} x_i^{k_i} = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n},$$

where $k_i \in \mathbb{N}$ for all $1 \leq i \leq n$. For example, if $n = 3$, then the following are all examples of monomials in $\mathcal{X}$:

$$1,\ x_1,\ x_1^2 x_3^5,\ x_1^{10} x_2^3 x_3.$$

Now, if F is a field, then a *polynomial over F, with variables in $\mathcal{X}$*, is an expression of the form

$$p(x_1, \ldots, x_n) = \sum_{i=0}^{m} a_i y_i = a_0 y_0 + \cdots + a_m y_m,$$

where $m \in \mathbb{N}$ and, for each $i \leq m$, $a_i \in F$ and y_i is a monomial in $\mathcal{X}$. For example, if $n = 3$, then the following are examples of polynomials over $\mathbb{Q}$ with variables in $\mathcal{X}$:

$$3 + 2x_1 x_3^2 + \frac{2}{3} x_2^4,\ \frac{1}{2} x_3^6,\ 3 - 4x_1 x_2 + 5x_1 x_3 - 6x_2 x_3.$$

Definition 7.0.24. Suppose that L is a field extension of K and $B \subseteq L$. We say that B is *algebraically independent over K* if, for every finite subset $\{b_1, \ldots, b_n\} \subseteq B$, there is no nonzero polynomial $p(x_1, \ldots, x_n)$ over K such that

$$p(b_1, \ldots, b_n) = 0.$$

Exercise 7.0.25. Suppose that L is a field extension of K and $B \subseteq L$ is algebraically independent over K. Prove that every element of B is transcendental over K.

Example 7.0.26. Consider $\mathbb{R}$ as a field extension of $\mathbb{Q}$, and let $B = \{\pi, 2\sqrt{\pi}\}$. Then each element of B is transcendental over $\mathbb{Q}$, but B is not algebraically independent. To see this, consider the polynomial

$$p(x_1, x_2) = 4x_1 - x_2^2.$$

Then $p(x_1, x_2)$ is a polynomial over $\mathbb{Q}$ and

$$p(\pi, 2\sqrt{\pi}) = 4\pi - (2\sqrt{\pi})^2 = 4\pi - 4\pi = 0.$$

In the other direction, let $B' = \{e^{\sqrt{p}} \mid p \in \mathbb{N} \text{ is prime}\}$. Then B' is algebraically independent over $\mathbb{Q}$ (this follows from the Lindemann-Weierstrass Theorem and is highly nontrivial).

Definition 7.0.27. Suppose that L is a field extension of K. A *transcendence basis for L over K* is a set $B \subseteq L$ that is a maximal algebraically independent set over K, i.e.,

1. B is algebraically independent over K;
2. for all $B' \subseteq L$ such that $B \subsetneq B'$, the set B' is *not* algebraically independent over K.

It is a straightforward application of Zorn's lemma to show that transcendence bases always exist, so we leave it as an exercise:

Exercise 7.0.28. Suppose that L is a field extension of K. Then there exists a transcendence basis for L over K. (Hint: Use Zorn's Lemma.)

If L is a field extension of K, then it turns out that every transcendence basis for L over K has the same cardinality:

Fact 7.0.29. *Suppose that L is a field extension of K and $B_0, B_1 \subseteq L$ are transcendence bases for L over K. Then $|L| = |K|$.*

Definition 7.0.30. Suppose that L is a field extension of K. Then the *transcendence degree of L over K* is defined to be $|B|$, where $B \subseteq L$ is a transcendence basis for L over K.

Example 7.0.31.
1. The set $\{i\}$ is a transcendence basis for $\mathbb{C}$ over $\mathbb{R}$. Thus, the transcendence degree of $\mathbb{C}$ over $\mathbb{R}$ is 1.
2. The transcendence degree of $\mathbb{R}$ over $\mathbb{Q}$ is $2^{\aleph_0}$.

We saw the notion of a basis in the context of free abelian groups in the previous chapter. In that setting, a basis was a maximal linearly independent subset of a free abelian group. Here, maximality could be reformulated in terms of *generating* the abelian group. Something similar can be done here; to state the correct result, we first need some notation.

Definition 7.0.32. Suppose that L is a field extension of K and $S \subseteq L$. Then $K(S)$ denotes the smallest subfield of L that contains both K and S as subsets. Concretely, $K(S)$, is the intersection of all subfields M of L such that $K \cup S \subseteq M$.

$K(S)$ can be thought of as the field extension of K *generated* by S. We can now give an alternative characterization of transcendence bases, which we will not prove:

Fact 7.0.33. *Suppose that L is a field extension of K and $B \subseteq L$ is algebraically independent over K. Then the following are equivalent:*

1. *B is a transcendence basis for L over K;*
2. *L is an algebraic field extension of $K(B)$.*

Chapter 8

Lecture 8: Model theory of algebraically closed fields

In this lecture, we will review some of the basic facts about algebraically closed fields from a model theoretic perspective.

8.1 The theory of algebraically closed fields

The *language* of fields is $\mathcal{L} = \langle +, -, \cdot, 0, 1 \rangle$, where $+$ and $\cdot$ are binary function symbols, $-$ is a unary function symbol, and 0 and 1 are constant symbols. The axioms of fields can then be formally written out as follows (cf. Definition 7.0.1).

1. $\forall a \forall b \forall c (a + (b + c) = (a + b) + c \wedge a \cdot (b \cdot c) = (a \cdot b) \cdot c)$
2. $\forall a \forall b (a + b = b + a \wedge a \cdot b = b \cdot a)$
3. $0 \neq 1 \wedge \forall a (a + 0 = a \wedge a \cdot 1 = a)$
4. $\forall a (a + (-a) = 0 \wedge (\neg (a = 0) \rightarrow \exists b (a \cdot b = 1)))$
5. $\forall a \forall b \forall c (a \cdot (b + c) = (a \cdot b) + (a \cdot c))$

Let T_{fields} be the *theory* of fields, i.e., the set of all first-order sentences in the language $\mathcal{L}$ that can be proven from the axioms of fields. By the soundness and completeness theorems, this is the set of all first-order sentences in $\mathcal{L}$ that are satisfied by all fields.

For every strictly positive natural number n, let ρ_n be the sentence

$$\forall a_0 \forall a_1 \ldots \forall a_{n-1} \exists x \left(a_0 + a_1 \cdot x + \cdots + a_{n-1} \cdot x^{n-1} + x^n = 0 \right).$$

Note that ρ_n can be seen as the assertion that every polynomial of degree n has a root. Let $T_{\text{ACF}} = T_{\text{fields}} \cup \{\rho_n \mid n \in \mathbb{N}_+\}$. Then T_{ACF} is the *theory of algebraically closed fields*.

T_{ACF} is not a complete theory, as it does not specify the *characteristic* of the field. Given a prime number p, let χ_p be the sentence

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} = 0,$$

and let $T_{\mathrm{ACF}_p} = T_{\mathrm{ACF}} \cup \{\chi_p\}$. Let $T_{\mathrm{ACF}_0} = T_{\mathrm{ACF}} \cup \{\neg\chi_p \mid p \text{ is prime}\}$. Then, for p a prime number or $p = 0$, T_{ACF_p} is the *theory of algebraically closed fields of characteristic* p.

8.2 Categoricity

T_{ACF_p} is an extremely nice theory from the model theoretic point of view. We begin by showing that it is *uncountably categorical*.

Definition 8.2.1. Suppose that κ is a cardinal and T is a theory. We say that T is *κ-categorical* if it has exactly one model of cardinality κ up to isomorphism. In other words, T is κ-categorical if

- there is a model M of cardinality κ such that $M \models T$; and
- for all models M and N of cardinality κ such that $M \models T$ and $N \models T$, we have $M \cong N$.

Morley's categoricity theorem is a foundational theorem in model theory, showing that a first-order theory in a countable language is κ-categorical for some uncountable cardinal κ if and only if it is κ-categorical for *all* uncountable cardinals κ.

Theorem 8.2.2 (Morley)**.** *Suppose that T is a first-order theory in a countable language. If there is an uncountable cardinal κ such that T is κ-categorical, then T is λ-categorical for* every *uncountable cardinal λ.*

It turns out that, for each p, T_{ACF_p} is κ-categorical for every uncountable cardinal κ. Let us first give the following useful definition.

Definition 8.2.3. Let F be a field. Then the *prime subfield of F* is the intersection of all of the subfields of F (and therefore the *smallest* subfield of F).

Given a field F, the prime subfield of F can be thought of as the subfield of F generated by 1_F (note that 1_F must be in every subfield of F, and hence in the prime subfield). With this in mind, do the following exercise.

Exercise 8.2.4. Let F be a field of characteristic p. If p is a prime number, then the prime subfield of F is isomorphic to F_p. If $p = 0$, then the prime subfield of F is isomorphic to $\mathbb{Q}$.

Theorem 8.2.5. *Let p be a prime number or $p = 0$, and let κ be an uncountable cardinal. Then T_{ACF_p} is κ-categorical.*

Sketch of proof. A full proof of this theorem would require more algebraic tools than we have, but we provide a sketch of the main ideas. Let K and L be two algebraically closed fields of characteristic p and cardinality κ. Let K_0 and L_0 be their respective prime fields. By Exercise 8.2.4, $K_0 \cong L_0$, and they are either finite or countable.

Let B_K and B_L be transcendence bases for K and L over K_0 and L_0, respectively. By Fact 7.0.33, K is an algebraic field extension of $K_0(B_K)$. Therefore, by Proposition 7.0.16, we must have $|K| \leq \max\{|K_0(B_K)|, \aleph_0\}$.

Since $|K| = \kappa > \aleph_0$, we must have $|K_0(B_K)| = \kappa$. Since K_0 is finite or countable, it follows that $|B_K| = \kappa$. Similar reasoning yields $|B_L| = \kappa$.

We can therefore fix a bijection $f : B_K \to B_L$. Since $K_0 \cong L_0$, we can extend f to an isomorphism $f : K_0(B_K) \to L_0(B_L)$ (this is not entirely trivial, but think about why this is at least plausible). But then we know that K is the algebraic closure of $K_0(B_K)$, and L is the algebraic closure of $L_0(B_L)$. Since $K_0(B_K) \cong L_0(B_L)$, Fact 7.0.23 implies that $K \cong L$. □

Remark 8.2.6. We note that T_{ACF_p} is *not* $\aleph_0$-categorical. The reason the proof of Theorem 8.2.5 does not work if $\kappa = \aleph_0$ is that, if K and L are two countable algebraically closed fields, then they need not have the same transcendence degree over their prime fields; in fact, their transcendence degrees can be any values in the set $\{0, 1, 2, 3, \ldots\} \cup \{\aleph_0\}$. Thus, for instance, we could let K be the algebraic closure of $\mathbb{Q}$, and L be the algebraic closure of $\mathbb{Q}(\pi)$. Then K and L are both countable algebraically closed fields of characteristic 0, but $K \ncong L$.

As a corollary to Theorem 8.2.5, we see that T_{ACF_p} is *complete*, i.e., for every first-order sentence φ in the language $\mathcal{L}$, either $\varphi \in T_{\mathrm{ACF}_p}$ or $\neg\varphi \in T_{\mathrm{ACF}_p}$.

Corollary 8.2.7. *Let p be a prime number or $p = 0$. Then T_{ACF_p} is complete.*

Proof. First note that every algebraically closed field must be infinite. Indeed, if F is a finite field, with its elements enumerated as $\{a_i \mid i < n\}$ for some $n \in \mathbb{N}$, then the polynomial

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

has no roots in F, since $p(b) = 1$ for all $b \in F$.

Now suppose for the sake of contradiction that T_{ACF_p} is not complete. Then there is a sentence φ such that neither φ nor $\neg\varphi$ is in T_{ACF_p}. This means that there are algebraically closed fields K_0 and K_1 of characteristic p such that $K_0 \models \varphi$ and $K_1 \models \neg\varphi$. By the previous paragraph, both K_0 and K_1 are infinite. Let $\kappa = \max\{\aleph_1, |K_0|, |K_1|\}$. By the upward Löwenheim–Skolem theorem, we can find elementary extensions $K_0' \succ K_0$ and $K_1' \succ K_1$ such that $|K_0'| = |K_1'| = \kappa$. By elementarity, we have $K_0' \models \varphi$ and $K_1' \models \neg\varphi$. However, by Theorem 8.2.5, we have $K_0' \cong K_1'$, so they should model exactly the same sentences. This is a contradiction and completes the proof. □

8.3 Other properties

We end this section by mentioning some other nice properties of T_{ACF_p}, without giving proofs.

Definition 8.3.1. A theory T over a language $\mathcal{L}$ is said to be *decidable* if there is an effective method (i.e. a computable function) for determining whether or not an arbitrary sentence in the language $\mathcal{L}$ is a member of T. (This can be made more precise, but because it is not essential for us, we leave things at this level of precision.)

Theorem 8.3.2. *Let p be a prime number or $p = 0$. Then T_{ACF_p} is decidable.*

Definition 8.3.3. A theory T over a language $\mathcal{L}$ is said to have *quantifier elimination* if, for every formula $\varphi(\bar{x})$ over $\mathcal{L}$ (with free variables in $\bar{x}$), there is a formula $\psi(\bar{x})$ over $\mathcal{L}$ with *no quantifiers* such that

$$T \models \forall \bar{x}(\varphi(\bar{x}) \leftrightarrow \psi(\bar{x})).$$

Theorem 8.3.4. *Let p be a prime number or $p = 0$. Then T_{ACF_p} has quantifier elimination.*

Strong minimality and definable linear orders

Definition 8.3.5. Suppose that M is a structure over a language $\mathcal{L}$ and $k \in \mathbb{N}$. We say that a set $X \subseteq M^k$ is *definable* (with parameters) if there is a first order formula $\varphi(x_0, \ldots, x_{j-1}, y_0, \ldots, y_{k-1})$ over $\mathcal{L}$ and a j-tuple $\bar{a} \in M^j$ such that

$$X = \{\bar{b} \in M^k \mid M \models \varphi(\bar{a}, \bar{b}).$$

Example 8.3.6.

1. In the structure $\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1)$, the set of even natural numbers is definable: Let $\varphi(x, y)$ be the formula $\exists z(y = x \cdot z)$. Then the set of even natural numbers is precisely $\{b \in \mathbb{N} \mid \mathcal{N} \models \varphi(2, b)\}$.

2. In the structure $\mathcal{R} = (\mathbb{R}, +, -, \cdot, 0, 1)$ (a field), the set of non-negative real numbers is definable: Let $\varphi(x)$ be the formula $\exists y(y \cdot y = x)$. Then the set of non-negative real numbers is precisely $\{a \in \mathbb{R} \mid \mathcal{R} \models \varphi(a)\}$.

3. In the structure $\mathcal{R}$ from the previous item, the usual ordering $\leq$ of $\mathbb{R}$ is definable (as a subset of $\mathbb{R}^2$: Let $\varphi(x, y)$ be the formula

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

   Then the set of $(a, b) \in \mathbb{R}^2$ such that $a \leq b$ is precisely the set $\{(a, b) \in \mathbb{R}^2 \mid \mathcal{R} \models \varphi(a, b)\}$.

Given a structure M, a *cofinite* subset of M is a subset $X \subseteq M$ such that $M \setminus X$ is finite.

Exercise 8.3.7. Let M be any structure over a language $\mathcal{L}$. Then every finite subset of M is definable, and every cofinite subset of M is definable (with parameters).

Definition 8.3.8. A theory T is *strongly minimal* if, for every model $\mathcal{M} \models T$ with underlying set M, and for every definable subset $X \subseteq M$, X is either finite or cofinite.

Theorem 8.3.9. *Let p be a prime number or $p = 0$. Then T_{ACF_p} is strongly minimal.*

Note that the theory of $(\mathbb{R}, +, -, \cdot, 0, 1)$ (which is a field but not an algebraically closed field), is not strongly minimal. Indeed, we saw above in Example 8.3.6 that the set of all non-negative real numbers is definable, and this set is neither finite nor cofinite.

This turns out to be related to the existence of a definable linear order. We also saw in Example 8.3.6 that there is a linear order of $\mathbb{R}$ that is definable in the structure $(\mathbb{R}, +, -, \cdot, 0, 1)$ (in fact, the natural order of $\mathbb{R}$ is definable).

However, we can use Theorem 8.3.9, and the fact that $\mathbb{C}$ is an uncountable algebraically closed field, to show that there is no linear order of $\mathbb{C}$ that is definable over $(\mathbb{C}, +, -, \cdot, 0, 1)$.

Exercise 8.3.10. Prove that there is no linear order of $\mathbb{C}$ that is definable over the structure $(\mathbb{C}, +, -, \cdot, 0, 1)$. (**Hint:** First show that, if $\preceq$ is a linear order of $\mathbb{C}$, then there is some $a \in \mathbb{C}$ such that both of the sets $\{b \in \mathbb{C} \mid b \prec a\}$ and $\{b \in \mathbb{C} \mid a \prec b\}$ are infinite. Then show that, if $\prec$ were definable and a were such an element, then the set $\{b \in \mathbb{C} \mid a \prec b\}$ is a definable subset of $\mathbb{C}$ that is neither finite nor cofinite, contradicting Theorem 8.3.9.)

Chapter 9

Lecture 9: The Ax–Grothendieck Theorem (Part 1)

Definition 9.0.1. Let K be a field, and let n be a positive natural number. Then a *polynomial map* from K^n to K^n is a map $f : K^n \to K^n$ for which there exist polynomials $p_1(x_1, x_2, \ldots, x_n), p_2(x_1, x_2, \ldots, x_n), \ldots, p_n(x_1, x_2, \ldots, x_n)$, each with variables in $\{x_1, \ldots, x_n\}$ and coefficients in K, such that, for all $(a_1, a_2, \ldots, a_n) \in K^n$, we have

$$f(a_1, a_2, \ldots, a_n) = (p_1(a_1, a_2, \ldots, a_n), p_2(a_1, a_2, \ldots, a_n), \ldots, p_n(a_1, a_2, \ldots, a_n)).$$

Example 9.0.2.

1. The map $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is a polynomial map from $\mathbb{R}$ to $\mathbb{R}$.
2. The map $f : \mathbb{C}^2 \to \mathbb{C}^2$ defined by $f(x, y) = (x^2 + x + y,\ x^2 + y)$ is a polynomial map from $\mathbb{C}^2$ to $\mathbb{C}^2$.

This lecture is devoted to the proof of the following fundamental theorem about polynomial maps between powers of $\mathbb{C}$. The theorem was proven independently by Ax and Grothendieck in the 1960s.

Theorem 9.0.3. *Suppose that n is a positive natural number and $f : \mathbb{C}^n \to \mathbb{C}^n$ is a polynomial map. If f is injective, then f is surjective.*

Remark 9.0.4. We note that the converse of Theorem 9.0.3 does not hold; there are plenty of polynomial maps from $\mathbb{C}^n$ to $\mathbb{C}^n$ that are surjective but not injective. For example, the polynomial map $f : \mathbb{C} \to \mathbb{C}$ defined by $f(x) = x^2$ is not injective since, for instance, $f(1) = f(-1) = 1$, but it is surjective (even though it is not surjective when considered as a map from $\mathbb{R}$ to $\mathbb{R}$.

To see the utility of Theorem 9.0.3, consider the second map in Example 9.0.2, the map $f : \mathbb{C}^2 \to \mathbb{C}^2$ given by $f(x, y) = (x^2 + x + y,\ x^2 + y)$. It is not easy to tell by elementary means whether or not f is surjective. However, one can readily show that it is injective (Exercise: Prove that f is injective.), and then Theorem 9.0.3 yields that it is surjective.

There are two potentially surprising things about the Ax–Grothendieck theorem here. The first is that such a fundamental theorem, about mathematical topics that had been studied already for hundreds of years, was not proven until the 1960s. The second is that it is appearing in a course on applications

of logic and set theory to mathematics. On its face, this theorem has little to do with logic, but, as we will see, the proof of the theorem (at least the one that we present here) makes use of a great number of the logical and model theoretic tools that we have been developing over the previous weeks.

The first observation we make in the path to the proof of Theorem 9.0.3 is that the theorem becomes entirely trivial if, in its statement, one replaces $\mathbb{C}$ by a finite field. In fact, the following stronger statement holds:

Exercise 9.0.5. Suppose that X is a nonempty finite set and $f : X \to X$ is a function. Then f is injective if and only if f is surjective. (Hint: This is simply a reformulation of the Pigeonhole Principle.)

The basic strategy of our proof of Theorem 9.0.3 is now as follows: We know that its analogue holds over finite fields; now use an ultraproduct construction and Łos' Theorem to transfer this fact to infinite fields, and in particular to $\mathbb{C}$. Of course, many details remain to be filled in. We begin by introducing the following fact about finite fields. In what follows, given a field K, we let $\overline{K}$ denote its algebraic closure (so, in particular, given a prime number p, $\overline{F_p}$ is the algebraic closure of the finite field F_p).

Proposition 9.0.6. *Let p be a prime number. Then there is a sequence $\langle F_{p,k} \mid k < \omega \rangle$ of finite fields such that*

1. *$F_{p,0} = F_p$;*
2. *for all $k < \omega$, we have $F_{p,k} \subseteq F_{p,k+1}$;*
3. *$\overline{F_p} = \bigcup_{k<\omega} F_{p,k}$.*

Sketch of proof. A complete proof of this proposition would require some algebraic tools going beyond this course, but we give a sketch of the proof.

First, since F_p is finite, there are only countably many polynomials (in one variable) with coefficients in F_p. Let $\langle q_k \mid k < \omega \rangle$ enumerate all such polynomials. For each $k < \omega$, let S_k denote the set of all roots of q_k in $\overline{F_p}$, i.e.,

$$S_k = \{a \in \overline{F_p} \mid q_k(a) = 0\}.$$

By Fact 7.0.11, each S_k is finite.

We now construct $\langle F_{p,k} \mid k < \omega \rangle$ by recursion on k. First, we let $F_{p,0} = F_p$. Now suppose that $k < \omega$ and we have constructed $F_{p,k}$. In particular, $F_{p,k}$ is a finite field and, for all $j < k$, we have $F_{p,j} \subseteq F_{p,k} \subseteq \overline{F_p}$. Then let $F_{p,k+1} = F_{p,k}(S_k)$. Recall that $F_{p,k}(S_k)$ denotes the intersection of all subfields of $\overline{F_p}$ that contain both $P_{p,k}$ and S_k as subsets. In other words, it is the minimal extension of $P_{p,k}$ containing all elements of S_k.

The one part of this proof that we will not do in full is the verification that $F_{p,k}(S_k)$ is finite. But the idea of the argument is as follows: to form $F_{p,k}(S_k)$, one first adds all of the elements of S_k to $F_{p,k}$, and then closes under the field operations. But both S_k and $F_{p,k}$ are finite, and every element of S_k is algebraic over $F_{p,k}$, so we only need to add finitely many elements to close under all field operations. See any textbook on field theory for a more careful proof of this fact.

It remains to verify item (3) in the statement of the proposition, namely that

$$\overline{F_p} = \bigcup_{k<\omega} F_{p,k}.$$

By construction, we have $F_{p,k} \subseteq \overline{F_p}$ for all $k < \omega$, so the inclusion

$$\overline{F_p} \supseteq \bigcup_{k<\omega} F_{p,k}$$

is immediate. For the reverse inclusion, fix an element $b \in \overline{F_p}$. Since $\overline{F_p}$ is an algebraic extension of F_p, there is a polynomial $q(x)$ over F_p such that $q(b) = 0$. Then there is some $k < \omega$ such that $q = q_k$. But then $b \in S_k$, so, in particular, $b \in F_{p,k+1}$. Thus,

$$\overline{F_p} \subseteq \bigcup_{k<\omega} F_{p,k},$$

completing the proof of the proposition. □

We are now in a position to prove the analogue of Theorem 9.0.3 in which $\mathbb{C}$ is replaced by $\overline{F_p}$ for some prime number p.

Theorem 9.0.7. *Suppose that p is a prime number, n is a positive natural number, and $f : (\overline{F_p})^n \to (\overline{F_p})^n$ is a polynomial map. If f is injective, then f is surjective.*

Proof. Fix polynomials $q_1(x_1, \ldots, x_n), q_2(x_1, \ldots, x_n), \ldots, q_n(x_1, \ldots, x_n)$ such that, for all $(b_1, \ldots, b_n) \in (\overline{F_p})^n$, we have

$$f(b_1, \ldots, b_n) = (q_1(b_1, \ldots, b_n), \ldots, q_n(b_1, \ldots, b_n)).$$

Let S be the set of all coefficients that appear in any of the polynomials $q_1, \ldots, q_n$. In particular, S is a finite subset of $\overline{F_p}$. We want to show that f is surjective. To this end, fix a point $(c_1, \ldots, c_n) \in (\overline{F_p})^n$. We want to show that there exists $(b_1, \ldots, b_n) \in (\overline{F_p})^n$ such that $f(b_1, \ldots, b_n) = (c_1, \ldots c_n)$.

Let $\langle F_{p,k} \mid k < \omega \rangle$ be given by Proposition 9.0.6. In particular, $\langle F_{p,k} \mid k < \omega \rangle$ is a $\subseteq$-increasing sequence of finite fields such that

$$\overline{F_p} = \bigcup_{k<\omega} F_{p,k}.$$

It follows that we can find a sufficiently large $k < \omega$ such that $S \cup \{c_1, \ldots, c_n\} \subseteq F_{p,k}$. Note the following points.

- For each $1 \leq m \leq n$, all of the coeffients of q_m are in $F_{p,k}$, so q_m is a polynomial over $F_{p,k}$. It follows that $f \restriction (F_{p,k})^n$ is a polynomial map from $(F_{p,k})^n$ to $(F_{p,k})^n$.
- Since $f : (\overline{F_p})^n \to (\overline{F_p})^n$ is injective, it follows that $f \restriction (F_{p,k})^n$ is an injective map from $(F_{p,k})^n$ to $(F_{p,k})^n$.

Note that $(F_{p,k})^n$ is a finite set. We can therefore apply Exercise 9.0.5 to conclude that $f \restriction (F_{p,k})^n$ is a surjective map from $(F_{p,k})^n$ to $(F_{p,k})^n$. But we have $(c_1, \ldots, c_n) \in (F_{p,k})^n$, so we can find $(b_1, \ldots, b_n) \in (F_{p,k})^n$ such that $f(b_1, \ldots, b_n) = (c_1, \ldots, c_n)$, as desired. This completes the proof that f is surjective. □

Remark 9.0.8. Let us point out that it was important in the proof of Theorem 9.0.7 that f was a polynomial map, as this allowed us to find a $k < \omega$ such that $f \restriction (F_{p,k})^n$ is a map from $(F_{p,k})^n$ to $(F_{p,k})^n$. If f were simply an arbitrary map, then there would be no guarantee that we could find k such that the range of $f \restriction (F_{p,k})^n$ is contained in $(F_{p,k})^n$.

Chapter 10

Lecture 10: The Ax–Grothendieck Theorem (Part 2)

In this lecture, we complete the proof of the Ax–Grothendieck Theorem (Theorem 9.0.3). This is where we will put into play a significant amount of the logical and model-theoretic machinery that we have developed over the previous weeks.

Let P denote the set of all prime numbers, and let U be a nonprincipal ultrafilter over P. Recall that, for all $p \in P$, $\overline{F_p}$ is the algebraic closure of the finite field F_p; each $\overline{F_p}$ is a countable algebraically closed field of characteristic p.

Let K be the ultraproduct $\prod_{p \in P} \overline{F_p}/U$, considered as a structure in the language of fields. Since each $\overline{F_p}$ is an algebraically closed field, and hence a model of the theory T_{ACF} (recall Chapter 8), Łos' Theorem (Theorem 5.1.1) implies that K is also a model of T_{ACF}, i.e., K is an algebraically closed field.

Remark 10.0.1. Although the fact that K is an algebraically closed field follows directly from Łos' Theorem, it might be instructive to illustrate this fact more concretely.

First, recall what the underlying set of K is. Given functions $f, g \in \prod_{p \in P} \overline{F_p}$, we set $f =_U g$ if

$$\{p \in P \mid f(p) = g(p)\} \in U.$$

This defines an equivalence relation on $\prod_{p \in P} \overline{F_p}$, and the underlying set of K consists of equivalence classes $[f]_U$ of this equivalence relation.

To see that K is a field, we can explicitly define the field operations. Given $[f]_U$ and $[g]_U$ in K, we set $[f]_U + [g]_U = [h]_U$, where $h \in \prod_{p \in P} \overline{F_p}$ is defined by letting $h(p) = f(p) + g(p)$ for all $p \in P$. One can readily check that this is well-defined and specifies an operation that is commutative and associative. We define multiplication in an analogous way.

One can then check that K, with operations thusly defined, satisfies all of the field axioms. For instance, one can check that the additive identity of K (the 0 element) is given by $[c_0]_U$, where $c_0 \in \prod_{p \in P} \overline{F_p}$ is defined by letting $c_0(p) = 0$ for all $p \in P$. Now suppose we want to prove that every element of K

has an additive inverse. Fix an arbitrary element $[f]_U \in K$. Define a function $(-f) \in \prod_{p \in P} \overline{F_p}$ by letting $(-f)(p) = -(f(p))$ for every $p \in P$. Then, for every $p \in P$, we have $f(p)+(-f)(p) = f(p)-f(p) = 0$. Thus, $[f]_U+[(-f)]_U = [c_0]_U$, so $[(-f)]_U$ is the additive inverse to $[f]_U$. The other field axioms are verified in a similar manner.

Finally, let us show that K is algebraically closed. To this end, let $q(x)$ be a polynomial in one variable over K of degree at least one. Then $q(x)$ is of the form $a_0 + a_1x + \cdots + a_nx^n$, where $n \geq 1$ and $a_n \neq 0$. Each a_i is in K, so, for each $i \leq n$, we can fix $f_i \in \prod_{p \in P} \overline{F_p}$ such that $a_i = [f_i]_U$. Since $a_n \neq 0$, we have $f_n \neq_U c_0$. We can therefore fix a set $R \in U$ such that, for all $p \in R$, we have $f_n(p) \neq 0$.

For each $p \in R$, consider the polynomial

$$q_p(x) = f_0(p) + f_1(p)x + \cdots + f_n(p)x^n$$

over $\overline{F_p}$. Since $f_n(p) \neq 0$, $q_p(x)$ has degree $n > 0$. Since $\overline{F_p}$ is algebraically closed, we can fix a root $b_p \in \overline{F_p}$ for $q_p(x)$. Define a function $g \in \prod_{p \in P} \overline{F_p}$ by letting

$$g(p) = \begin{cases} b_p & \text{if } p \in R \\ 0 & \text{if} p \notin R \end{cases}$$

for all $p \in P$. Then, for all $p \in R$, we have $q_p(g(p)) = 0$, i.e.,

$$f_0(p) + f_1(f)g(p) + \cdots + f_n(p)(g(p))^n = 0.$$

Since $R \in U$, Łos' Theorem then implies that, in K, we have

$$[f_0]_U + [f_1]_U[g]_U + \cdots + [f_n]_U([g]_U)^n = [c_0]_U,$$

i.e., $[g]_U$ is a root of $q(x)$ in K. Thus, K is algebraically closed field.

We now know that K is an algebraically closed field. The next natural question is: what is its characteristic?

Proposition 10.0.2. *K has characteristic 0.*

Proof. Recall that, given a prime $p \in P$, we introduced in Chapter 8 a sentence χ_p in the language of fields asserting that a given field has characteristic field. Concretely, χ_p is the simple sentence

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} = 0.$$

Note that, if $p, p' \in P$ and $p \neq p'$, then $\overline{F_{p'}} \models \neg\chi_p$, since the characteristic of $\overline{F_{p'}}$ is p', which is relatively prime to p. Since U is a nonprincipal ultrafilter, we know that, for every $p \in P$, the set $P \setminus \{p\}$ is in U. For every $p' \in P \setminus \{p\}$, we have $\overline{F_{p'}} \models \neg\chi_p$, so, by Łos' Theorem, we have $K \models \neg\chi_p$. It follows that K has characteristic 0. □

The remaining fact about K that we need to ascertain is its cardinality.

Proposition 10.0.3. $|K| = 2^{\aleph_0}$.

Proof. We first show that $|K| \leq 2^{\aleph_0}$. To see this, we calculate the cardinality of $\prod_{p \in P} \overline{F_p}$. Since each $\overline{F_p}$ is countably infinite and P is countably infinite, this product has size $\aleph_0^{\aleph_0} = 2^{\aleph_0}$. Since K consists of equivalence classes of an equivalence relation defined on $\prod_{p \in P} \overline{F_p}$, it follows that

$$|K| \leq \left| \prod_{p \in P} \overline{F_p} \right| = 2^{\aleph_0}.$$

For the other direction, we make use of the following basic set-theoretic claim.

Claim 10.0.4. *There is a sequence of functions*

$$\langle f_\alpha \mid \alpha < 2^{\aleph_0} \rangle$$

from $\mathbb{N}$ *to* $\mathbb{N}$ *such that, for all* $\alpha < \beta < 2^{\aleph_0}$, f_α *and* f_β *are* eventually different, *i.e., there is* $k \in \mathbb{N}$ *such that, for all* $n > k$, *we have* $f_\alpha(n) \neq f_\beta(n)$.

Proof. For each $n \in \mathbb{N}$, let S_n denote the set of sequences of natural numbers of length n or, equivalently, the set of all functions from $\{0, \ldots, n-1\}$ to $\mathbb{N}$. Let $S = \bigcup_{n \in \mathbb{N}} S_n$. Each S_n is countable, so S is also countable. We can therefore fix a bijection $\pi : S \to \mathbb{N}$.

Now let $\langle x_\alpha \mid \alpha < 2^{\aleph_0} \rangle$ be an injective sequence of functions from $\mathbb{N}$ to $\mathbb{N}$ (this exists by the definition of $2^{\aleph_0}$). In particular, for all $\alpha < \beta < 2^{\aleph_0}$, there is some $k \in \mathbb{N}$ such that $x_\alpha(k) \neq x_\beta(k)$. Now for each $\alpha < 2^{\aleph_0}$, define a function $f_\alpha : \mathbb{N} \to \mathbb{N}$ as follows. For each $n \in \mathbb{N}$, note that the restriction $x_\alpha \restriction \{0, \ldots, n-1\}$ is in S_n, and hence in S. Then, for all $n \in \mathbb{N}$, set

$$f_\alpha(n) = \pi(x_\alpha \restriction \{0, \ldots, n-1\}).$$

We claim that this definition satisfies the conclusion of the claim. To this end, fix $\alpha < \beta < 2^{\aleph_0}$. By our choice of x_α and x_β, we can fix $k \in \mathbb{N}$ such that $x_\alpha(k) \neq x_\beta(k)$. But then, for all $n > k$, we have $x_\alpha \restriction \{0, \ldots, n-1\} \neq x_\beta \restriction \{0, \ldots, n-1\}$ and hence, since π is injective, we have

$$f_\alpha(n) = \pi(x_\alpha \restriction \{0, \ldots, n-1\}) \neq \pi(x_\beta \restriction \{0, \ldots, n-1\}) = f_\beta(n).$$

Thus, for all $n > k$, we have $f_\alpha(n) \neq f_\beta(n)$, as desired. □

Fix a sequence $\langle f_\alpha \mid \alpha < 2^{\aleph_0} \rangle$ as in the claim. Let $\langle p_n \mid n \in \mathbb{N} \rangle$ be an increasing enumeration of P and, for each $n \in \mathbb{N}$, let $\langle b^n_\ell \mid \ell \in \mathbb{N} \rangle$ be an injective enumeration of $\overline{F_{p_n}}$. Now, for each $\alpha < 2^{\aleph_0}$, define a function $g_\alpha \in \prod_{p \in P} \overline{F_p}$ by setting, for all $n \in \mathbb{N}$, $g_\alpha(p_n) = b^n_{f_\alpha(n)}$.

Now suppose that we are given a pair $\alpha < \beta < 2^{\aleph_0}$. Fix $k \in \mathbb{N}$ such that, for all $n > k$, we have $f_\alpha(n) \neq f_\beta(n)$. Then, for all $n > k$, we also have $g_\alpha(p_n) \neq g_\beta(p_n)$. Since U is a nonprincipal ultrafilter, we have $\{p_n \mid n > k\} \in U$. Therefore, it follows that $[g_\alpha]_U \neq [g_\beta]_U$. Thus,

$$\langle [g_\alpha]_U \mid \alpha < 2^{\aleph_0} \rangle$$

is an injective sequence of elements of K of length $2^{\aleph_0}$, and hence $|K| \geq 2^{\aleph_0}$.

Putting the two inequalities together, we obtain $|K| = 2^{\aleph_0}$. □

We now know that K is an algebraically closed field of characteristic 0 and cardinality $2^{\aleph_0}$. Moreover, we saw in Theorem 8.2.5 that the theory of algebraically closed fields of characteristic 0, T_{ACF_0}, is uncountably categorical, i.e., if L_0 and L_1 are two algebraically closed fields of characteristic 0 and $|L_0| = |L_1| > \aleph_0$, then $L_0 \cong L_1$. We know that the field $\mathbb{C}$ of complex numbers is an algebraically closed field of characteristic 0 and cardinality $2^{\aleph_0}$. Therefore, we have $K \cong \mathbb{C}$.

It follows that, in order to prove the Ax–Grothendieck Theorem (Theorem 9.0.3), it suffices to prove the theorem with the field K replacing the field $\mathbb{C}$, since the two are, up to isomorphism, *the same field*. More precisely, it suffices to prove the following theorem.

Theorem 10.0.5. *Suppose that n is a positive natural number and $f : K^n \to K^n$ is a polynomial map. If f is injective, then f is surjective.*

Proof. Let $f : K^n \to K^n$ be an injective polynomial map. By the definition of polynomial map, we can fix polynomials

$$q_1(x_1, \ldots, x_n), q_2(x_1, \ldots, x_n), \ldots, q_n(x_1, \ldots, x_n)$$

over K such that, for all $(b_1, \ldots, b_n) \in K^n$, we have

$$f(b_1, \ldots, b_n) = (q_1(b_1, \ldots, b_n), q_2(b_1, \ldots, b_n), \ldots, q_n(b_1, \ldots, b_n)).$$

We now show that, for each i with $1 \leq i \leq n$, and for each $p \in P$, $q_i(x_1, \ldots, x_n)$ induces a polynomial $q_{i,p}(x_1, \ldots, x_n)$ over $\overline{F_p}$.

Fix an i with $1 \leq i \leq n$. Let M_i denote the set of monomials that appear with nonzero coefficients in $q_i(x_1, \ldots, x_n)$ (recall Chapter 7). In particular, for each $y \in M_i$, we can fix an element $a^i_y \in K$ in such a way that

$$q_i(x_1, \ldots, x_n) = \sum_{y \in M_i} a^i_y y.$$

For each $y \in M_i$, fix a function $g^i_y \in \prod_{p \in P} \overline{F_p}$ such that $a^i_y = [g^i_y]_U$. Then define a polynomial $q_{i,p}(x_1, \ldots, x_n)$ over $\overline{F_p}$ by letting

$$q_{i,p}(x_1, \ldots, x_n) = \sum_{y \in M_i} g^i_y(p) y.$$

Exercise 10.0.6. Suppose that $1 \leq i \leq n$ and $g_1, \ldots, g_n, h \in \prod_{p \in P} \overline{F_p}$. Prove that the following are equivalent:

1. $q_i([g_1]_U, \ldots, [g_n]_U) = [h]_U$;
2. the set $\{p \in P \mid q_{i,p}(g_1(p), \ldots, g_n(p)) = h(p)\}$ is in U.

(Hint: Use Łos' Theorem.)

Finally, define a polynomial map $f_p : (\overline{F_p})^n \to (\overline{F_p})^n$ by letting

$$f_p(b_1, \ldots, b_n) = (q_{1,p}(b_1, \ldots, b_n), q_{2,p}(b_1, \ldots, b_n), \ldots, q_{n,p}(b_1, \ldots, b_n))$$

for all $(b_1, \ldots, b_n) \in (\overline{F_p})^n$.

Claim 10.0.7. $\{p \in P \mid f_p \text{ is injective}\} \in U$.

Proof. Suppose for the sake of contradiction that $R = \{p \in P \mid f_p \text{ is } \textit{not} \text{ injective}\}$ is in U. For each $p \in R$, we can then fix two points $(b_{1,p}, \ldots, b_{n,p}) \neq (b'_{1,p}, \ldots, b'_{n,p})$ in $(\overline{F}_p)^n$ such that $f_p(b_{1,p}, \ldots, b_{n,p}) = f_p(b'_{1,p}, \ldots, b'_{n,p})$. Now, for each i with $1 \leq i \leq n$, define two functions $h_i, h'_i \in \prod_{p \in P} \overline{F_p}$ by letting

$$h_i(p) = \begin{cases} b_{i,p} & \text{if } p \in R \\ 0 & \text{if } p \notin R \end{cases}$$

and

$$h'_i(p) = \begin{cases} b'_{i,p} & \text{if } p \in R \\ 0 & \text{if } p \notin R \end{cases}$$

for all $p \in P$.

Subclaim 10.0.8. *There is i with $1 \leq i \leq n$ such that $[h_i]_U \neq [h'_i]_U$.*

Proof. Suppose for the sake of contradiction that $[h_i]_U = [h'_i]_U$ for all i with $1 \leq i \leq n$. Then for each i, the set

$$S_i = \{p \in P \mid h_i(p) = h'_i(p)\}$$

is in U. Let $S = R \cap S_0 \cap S_1 \ldots \cap S_n$. Then $S \in U$. Moreover, for all $p \in S$ and all i with $1 \leq i \leq n$, we have $h_i(p) = h'_i(p)$. Since $p \in R$, this implies $b_{i,p} = b'_{i,p}$. But this contradicts the fact that $(b_{1,p}, \ldots, b_{n,p}) \neq (b'_{1,p}, \ldots, b'_{n,p})$. □

We know that, for all $p \in R$, for all i with $1 \leq i \leq n$, we have

$$q_{i,p}(b_{1,p}, \ldots, b_{n,p}) = q_{i,p}(b'_{1,p}, \ldots, b'_{n,p}),$$

i.e.,

$$q_{i,p}(h_1(p), \ldots, h_n(p)) = q_{i,p}(h'_1(p), \ldots, h'_n(p)).$$

Therefore, by Łos' Theorem (or Exercise 10.0.6), we have

$$q_i([h_1]_U, \ldots, [h_n]_U) = q_i([h'_1]_U, \ldots, [h'_n]_U).$$

(Exercise: Check this!) Since this holds for all $1 \leq i \leq n$, we have

$$f([h_1]_U, \ldots, [h_n]_U) = f([h'_1]_U, \ldots, [h'_n]_U).$$

However, by Subclaim 10.0.8, we have $([h_1]_U, \ldots, [h_n]_U) \neq ([h'_1]_U, \ldots, [h'_n]_U)$, so this contradicts the fact that f is injective. This concludes the proof of the claim. □

Let $J = \{p \in P \mid f_p \text{ is injective}\}$. By the preceding claim, we have $J \in U$. Moreover, by Theorem 9.0.7, for each $p \in J$, the polynomial map $f_p : (\overline{F_p})^n \to (\overline{F_p})^n$ is surjective.

We are now ready to prove that f is surjective. To this end, fix $(c_1, \ldots, c_n) \in K^n$. We must find $(b_1, \ldots, b_n) \in K^n$ such that $f(b_1, \ldots, b_n) = (c_1, \ldots, c_n)$. For each i with $1 \leq i \leq n$, fix a function $h_i \in \prod_{p \in P} \overline{F_p}$ wuch that $[h_i]_U = c_i$.

For each $p \in J$, consider the point $(h_1(p), h_2(p), \ldots, h_n(p)) \in (\overline{F_p})^n$. Since f_p is surjective, we can find a point $(b_{1,p}, b_{2,p}, \ldots, b_{n,p}) \in (\overline{F_p})^n$ such that $f_p(b_{1,p}, \ldots, b_{n,p}) = (h_1(p), h_2(p), \ldots, h_n(p))$.

For each $1 \leq i \leq n$, define a function $g_i^* \in \prod_{p \in P} \overline{F_p}$ by setting

$$g_i^*(p) = \begin{cases} b_{i,p} & \text{if } p \in J \\ 0 & \text{if } p \notin J \end{cases}$$

for all $p \in P$. Now notice that, for all $p \in J$ and all $1 \leq i \leq n$, we have

$$q_{i,p}(b_{1,p}, \ldots, b_{n,p}) = h_i(p),$$

i.e.,

$$q_{i,p}(g_1^*(p), \ldots, g_n^*(p)) = h_i(p).$$

Therefore, by Łos' Theorem (or Exercise 10.0.6), we have

$$q_i([g_1^*]_U, \ldots, [g_n^*]_U) = [h_i]_U = c_i.$$

Since this holds for all $1 \leq i \leq n$, we have

$$f([g_1^*]_U, \ldots, [g_n^*]_U) = (c_1, \ldots, c_n),$$

thus completing the proof that f is surjective. □