

MAU11602
Lecture 29
2026-04-02

ZFC

The usual basis for mathematics since the mid-20th century has been first order logic together with ZFC.

In theory it's classical first order logic with existential presuppositions but in practice it's first order logic without existential presuppositions.

ZFC is a version of set theory. Z is Zermelo and F is Fraenkel, but who is C?

C isn't a person but an axiom, the Axiom of Choice, which can be formulated in many different ways.

Remember the question of when surjective functions have a right inverse? We proved this is true if the domain is countable or if the codomain is finite.

Probably the most intuitive version of the Axiom of Choice is the one saying *every* surjective function has a right inverse.

A function f from A to B is surjective if for every $y \in B$ there's an $x \in A$ such that $f(x) = y$, so why can't we just choose such an x for each y define a function g from B to A by $g(y) = x$?

The Axiom of Choice says we can!

Order relations

In order to state the two main equivalents of the Axiom of Choice we need to discuss order relations.

A *partial order* on a set A is a relation R satisfying:

- Reflexivity: $\forall x. x \in A \rightarrow (x, x) \in R$.
- Antisymmetry: $\forall x. \forall y. (x, y) \in R \wedge (y, x) \in R \rightarrow x = y$.
- Transitivity: $\forall x. \forall y. \forall z. (x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R$.

Reflexivity and Transitivity are the same as for equivalence relations, but Symmetry has been replaced by Antisymmetry.

A *total order* is a partial order such that for all x and y we have $(x, y) \in R$ or $(y, x) \in R$.

A *well ordering* is a total order such that every non-empty subset has a least member, i.e. for every $B \in \mathcal{P}A$ if there is an $x \in B$ then there is an $x \in B$ such that if $y \in B$ then $(x, y) \in R$.

Examples

Consider the set C of cofinite subsets of the natural numbers. We can define a partial order R on C by saying that $(A, B) \in R$ whenever $A \subseteq B$.

R is clearly reflexive, antisymmetric, and transitive. More generally, inclusion defines a reflexive, antisymmetric, and transitive relation on any set of subsets of any set.

R is not a total order on C . For the sets $A = \mathbb{N} \setminus \{0\}$ and $B = \mathbb{N} \setminus \{1\}$ we have neither $A \subseteq B$ nor $B \subseteq A$.

Consider the subset D of C consisting of those sets for which if m is a member then so is n for all $n \geq m$.

We can restrict R to D to get a relation on S on D . More precisely, we set $S = R \cap (D \times D)$.

All the members of D look like $\{m, m + 1, m + 2, \dots\}$ for some m .

Any restriction of a partial order is a partial order and any restriction of a total order is a total order but it can also happen that the restriction of partial order is a total order, and that's what happens here.

Totally ordered subsets of a partially ordered set are called *chains*, so D is a chain in C .

Examples, continued

With C and D as on the previous slide the members of D are each well ordered with respect to the relation \leq , or rather its restriction.

D itself though is not well ordered with respect to the relation S , i.e. the inclusion relation.

In other words, there is no $E \in D$ such that if $F \in D$ then $E \subseteq F$.

For any $E \in D$ there's a proper subset F obtained by removing the least member of E and this F is also in D .

There are subsets of D on which the restriction of S is a well ordering. Finite subsets have this property, and in fact they're the only subsets which do.

More generally, any total order on a finite set is a well ordering.

The example of D and S shows that not every total order on a countable set is a well ordering, but it is still true that every countable set has a well ordering.

The Well Ordering Principle

One equivalent of the Axiom of Choice is the Well Ordering Principle, which says that every set has a well ordering.

There's no guarantee that this well ordering is compatible with any other ordering, total or partial, we might already have.

We saw this with D above. It also applies to the set of reals. The principle implies that there's a well ordering of the reals but it definitely can't be the usual order relation \leq .

Not every non-empty set of reals has a minimum.

By equivalent I mean that if you assume the ZF axioms and the Axiom of Choice you can prove the Well Ordering Principle and if you assume ZF and the Well Ordering Principle you can prove the Axiom of Choice.

Zorn's Lemma

There's another equivalent of the Axiom of Choice, known as Zorn's Lemma, although it's more often taken as an axiom than proved as a lemma.

One form of Zorn's Lemma says that A is a set and R is a partial order on A with the property that every chain in A , i.e. every totally ordered non-empty subset, has a lower bound, then A has a minimal element.

A lower bound for $C \in \mathcal{P}A$ is an $x \in A$ such that if $y \in C$ then $(x, y) \in R$.

This looks like the definition of a least member of C , but the x is not required to be a member of C , just of A .

So, for example, all non-positive x are lower bounds for the interval $[0, 1]$, but only 0 is a least member.

Minimal means an $y \in A$ such that if $(x, y) \in R$ then $x = y$.

This is consistent with how we defined minimal members of a set of subsets, if you take the relation to be the inclusion relation.

The usual statement of Zorn's Lemma uses upper bounds and maximal elements but the two versions are equivalent, since for every relation there is a reverse relation.

Banach-Tarski

Zorn's Lemma looks weird and unintuitive but it's the one which usually makes proving theorems easiest.

It even makes it easy to prove things which intuitively should not be true.

A theorem of Banach and Tarski, proved using Zermelo-Fraenkel plus Zorn's Lemma says that there are subsets $A_1, A_2, A_3, A_4, A_5, B_1, B_2, B_3, C_1, C_2, C_3, C_4,$ and C_5 in three dimensional Euclidean space such that

- Each A is disjoint from the other A 's and similarly for the B 's and C 's.
- Each A is congruent to the corresponding C .
- Each B is a ball of radius 1.
- $A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5 = B_1 \cup B_2$.
- $C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 = B_3$.

If you believe bounded subsets of Euclidean space have a finite volume which is additive and invariant under reflections then this should not be possible.

For this and other reasons Zorn's Lemma, and its equivalent forms, the Axiom of Choice and the Well Ordering Principle, are treated with some degree of suspicion.

Countable choice

If we just take Zermelo-Fraenkel set without the Axiom of Choice then there are some standard theorems we can't prove. If we add the full Axiom of Choice then we can prove them, but we can also prove Banach-Tarski and similar monstrosities.

Are there weaker choice axioms which allow us to prove what we want and prevent us from proving what we don't want?

For many purposes the Axiom of Countable Choice is sufficient. It says that f is a surjective function from a set A to a countable set B then it has a right inverse.

The Axiom of Countable Choice follows from the Axiom of Choice because it's the same conclusion with extra hypotheses.

The special cases of AoCC where A is countable or B is finite were already proved without either axiom.

Dependent choice

You can use the Axiom of Countable Choice to make a countable number of choices, but not in a setting where the options for later choices depend on earlier ones, as they often do when constructing sequences.

The Axiom of Dependent Choice, which is weaker than the Axiom of Choice but stronger than the Axiom of Countable Choice, is designed for these situations.

One way to state it is that for any left total relation R on a set A and any $x \in A$ there is an infinite sequence a_0, a_1, \dots such that $a_0 = x$ and $(a_n, a_{n+1}) \in R$.

If R is also right unique, i.e. is a function, then you don't need any choice axiom for this. You also don't need one if A is countable.

There's also an analogue of Zorn's Lemma for this: If every chain of in a partially ordered set is finite then the set has a minimal member.

This is equivalent to the previous version, in the usual sense.

What's different from Zorn's Lemma is that we've replaced having a lower bound with being finite. In general finite chains have a lower bound but sets with a lower bound don't need to be finite.

A reasonable foundation for mathematics

If you want the usual theorems in classical mathematics to be true then a good basis is

- Classical first order logic

Many things can still be proved with intuitionistic logic, but many things can't.

Textbooks present a FOL with existential presuppositions but if you observe mathematicians in their native habitat they really use a FOL without existential presuppositions, mostly unconsciously.

- Zermelo set theory

Within mathematics it hardly matters whether you allow atoms, as Zermelo did, or forbid them, but outside mathematics you want to allow them.

- The Axiom of Replacement

It's rarely needed but often convenient and relies on the same intuition as Separation, which we definitely need.

- The Axiom of Dependent Choice

This is a good compromise between the AoCC, which is not quite powerful enough, and the AoC, which is arguably too powerful and not needed for standard mathematics.

Comments

No reasonable foundation will be semantically or syntactically complete, because of Gödel's theorem (and Rosser's).

We have no proof that this system is consistent. Similar systems have been proved inconsistent in the past, but this one has survived for a century or so now.

Either because it's consistent or because people stopped looking for contradictions. Some mathematicians reject classical logic and only accept intuitionistic logic, or even minimal logic. I'm not going to say you shouldn't, but proving standard theorems is often harder and sometimes impossible if you do.

I mostly discussed intuitionistic and minimal logic because of their connection to computability, not as an alternate foundation for mathematics.

Most mathematicians are happy to accept the full Axiom of Choice, even if it implies things like Banach-Tarski. I'm not going to say you shouldn't, but you mostly don't have to.

I can't think of a good reason for accepting Foundation/Regularity though.