Topics in Set Theory

March 12, 2019

Contents

0 Introduction

—Lecture 1—

Example classes: 4th Feb, 18th Feb, 4th Mar 330-5pm MR5; fourth class undecided (probably on 15th).

Although the name of this course is *Topics* in Set theory, for all of its history only one topic is discussed. So maybe this course should be called *One Topic in Set Theory*, or probably just *the Continuum Hypothesis*: in this course we'll just solve one problem: the continuum problem, which we've known in the end that the problem is independent from ZFC.

Let's have some background stories first. In the second ICM congress (1900, Paris), Hilbert posed the famous 23 Hilbert questions, with the first one being the Continuum Hypothesis (a hypothesis at that time). The original formulation of CH was:

Any infinite subset of real numbers is either equinumerous to the set of natural numbers, or to the set of real numbers.

We could definitely formulate it better, but that is less important. More modern version of CH would be a short equation

$$2^{\aleph_0} = \aleph_1$$

which seemingly has nothing to do with the previous problem. However, in ZFC these two statements are equivalent:

• if $2^{\aleph_0} > \aleph_1$, in particular, $2^{\aleph_0} \geq \aleph_2$. Since $2^{\aleph_0} \sim \mathbb{R}$, we get an injection $i : \aleph_2 \to \mathbb{R}$. Consider $X := i[\aleph_1] \subseteq \mathbb{R}$. Clearly, $i \upharpoonright \aleph_1$ (i restricted to $\aleph_1$) is a bijection between $\aleph_1$ and X, so $X \sim \aleph_1$; but $\aleph_1$, being uncountable, is not in bijection with natural numbers, and is not in bijection with real numbers. Thus X refutes CH.

If $2^{\aleph_0} = \aleph_1$, let $X \subseteq \mathbb{R}$. Consider $b : 2^{\aleph_0} \to \mathbb{R}$ a bijection. If X is infinite, then $b^{-1}[X] \subseteq 2^{\aleph_0}$. Thus the cardinality of X is either $\aleph_0$ or $\aleph_1$ (which $\sim \mathbb{N}$ and $\mathbb{R}$ respectively). So $2^{\aleph_0} = \aleph_1 \implies$ CH.

In 1938, Gödel proved that ZFC does not prove ¬CH, and in 1961 Cohen proved that ZFC does not prove CH, by methods of *inner models* and *forcing* (sometimes also called *outer models*, which is not incorrect) respectively. The latter has become the most important method in Set theory since then.

From logic (see Part II Logic and Set Theory) we have Gödel's Completeness Theorem: a theory T is consistent iff it has a model. So from the above two statements, it seems that we're going to prove that there are models for ZFC+CH and ZFC+¬CH; but this is obviously not possible because of the incompleteness phenomenon: we know we can't prove the consistency of ZFC (as a result, we can't even prove there is a model of ZFC)! So instead we could only prove the following:

$$Cons(ZFC) \to Cons(ZFC + CH)$$

or equivalently, if $M \vDash ZFC$, then there is $N \vDash ZFC + CH$ (and similar for the other half).

1 Model theory of set theory

1.1 Absoluteness

For a moment, we will assume that we have a model $(M, \in) \vDash ZFC$. Unfortunately this first assumption doesn't make much sense, because model theory is based on set theory and we don't have anything if ZFC is inconsistent. We refer to the canonical objects in M by the usual symbols, e.g. $0, 1, 2, 3, 4, ..., \omega, \omega + 1, ...$

What would an *inner model* be? Take $A \subseteq M$, and consider $(A, \in)$. It is a substructure of $(M, \in)$, because there are no function symbols or constant symbols in the language of set theory. This might be counterintuitive, because we're using symbols like ϕ and $\{\cdot\}$ all the time! However, these are technically not part of language of set theory as they can all be defined without any use of function symbols, i.e. they are just abbreviations. For example, $X = \phi$ abbreviates $\forall w (\neg w \in X)$; $X = \{Y\}$ abbreviates $\forall w (w \in X \iff w = Y)$, and similarly for $\cup$ and $\mathcal{P}$; and also for relation symbols such as $\subseteq$, which abbreviates $\forall w (w \in X \to w \in Y)$. Note that $X = \phi$ is NOT the formula that it looks like; in particular, it is not quantifier free (because it abbreviates $\forall w (\neg w \in X)$)! So we need to take extra care when we do things in this course.

Definition. If φ is a formula in n free variables, we say φ is *upwards absolute* between A and M if for all $a_1, ..., a_n \in A$,

$$(A, \in) \vDash \varphi(a_1, ..., a_n) \implies (M, \in) \vDash \varphi(a_1, ..., a_n)$$

and we say φ is *downwards absolute* between A and M if for all $a_1, ..., a_n \in A$,

$$(M, \in) \vDash \varphi(a_1, ..., a_n) \implies (A, \in) \vDash \varphi(a_1, ..., a_n)$$

and φ is *absolute* between A and M if it is both upwards and downwards absolute.

Observation:
(a) If φ is *quantifier-free*, then φ is absolute between A and M. But this doesn't really help much, because almost nothing is quantifier-free: without quantifiers we can only say things like $A \in B$ and $A = B$, and conjunctions of those; that's pretty much all.
(b) We say that a formula is Σ_1 if it is of the form

$$\exists x_1 ... \exists x_n \varphi(x_1, ..., x_n)$$

where φ is q.f.;
we say a formula is Π_1 if it is of the form

$$\forall x_1 ... \forall x_n \varphi(x_1, ..., x_n)$$

where φ is q.f..
(c) If φ is Π_1, it is downward absolute; if it's Σ_1 then it is upwards absolute. So in particular, note that $X = \phi$ is downward absolute.

—Lecture 2—

As an example, write $0, 1, 2, 3, ...$ for the ordinals in M, and let $A := M \setminus \{1\}$. In A, we have $0, 2$, but no 1; we also have $\{1\}$. If we use $\Phi_0(x)$ to denote the formula $\forall w(\neg w \in x) \iff x = \phi$. Clearly $(M, \in) \vDash \Phi_0(0)$, so by π_1-downwards absoluteness, $(A, \in) \vDash \Phi_0(0)$.

Now, how many elements does $2 = \{0, 1\}$ have? In M we obviously know 2 has 2 elements; but in A, 2 only has one element 0, and $\{1\}$ has no element: $(A, \in) \vDash \Phi_0(\{1\})$! Clearly $(M, \in) \nvDash \Phi_0(\{1\})$, so Φ_0 is not absolute between A and M. As a corollary, we get $(A, \in) \nvDash$ extensionality (we can uniquely specify sets by specifying their elements).

Remark. We could go on, defining formulas $\Phi_1(x), \Phi_2(x)$, etc to analyse which of the elements correspond to the natural numbers in A.

Reminder (from Part II Logic and Set Theory): we say A is *transitive in M* if for all $a \in A$ and $x \in M$ s.t. $(M, \in) \vDash x \in a$, we have $x \in A$. The problem for the above A is that it is not transitive. As long as that is fixed, we have the following:

Proposition. If A is transitive, then Φ_0 is absolute between A and M.

Proof. Since Φ_0 is Π_1, we only need to show upwards absoluteness. Suppose $a \in A$ s.t. $(A, \in) \vDash \Phi_0(a)$, and suppose for contradiction that $a \neq 0$. Then there is some $x \in a$. By transitivity, $x \in A$. But then $\Phi_0(a) : \forall w(w \notin a)$ is not true in $(A, \in)$. $\square$

Similarly, if Φ_n is the formula describing the natural number n, and there is $a \in A$ s.t. $(A, \in) \vDash \Phi_n(a)$, and A is transitive, then $a = n$.

Proposition. If A is transitive in M, then $(A, \in) \vDash$ extensionality.

Proof. Take $a, b \in A$ with $a \neq b$. So by extensionality in $(M, \in)$, find, WLOG some $c \in a \setminus b$. Since $c \in a \in A$, by transitivity $c \in A$. Note that all of these quantifier-free formulas are absolute, so $(A, \in)$ also models them; in particular, $(A, \in) \vDash c \in a, c \notin b$. So a, b do not satisfy the assumptions of extensionality. $\square$

Consider now $A = \omega + 2 = \{0, 1, 2, ..., \omega, \omega + 1\} \subseteq M$. This is clearly transitive subset of M because it's an ordinal. So $(A, \in) \vDash$ extensionality, but clearly it isn't anything like a model of set theory as it is too thin. Consider the formula $x = \mathcal{P}(y)$. Unfortunately, this is not a formula, as $\mathcal{P}$ is undefined. We have to expand it properly:

$$x = \mathcal{P}(y)$$
$$\iff x = \{z; z \subseteq y\}$$
$$\iff \forall w(w \in x \leftrightarrow w \subseteq y)$$
$$\iff \forall w(w \in x \leftrightarrow (\forall v(v \in w \rightarrow v \in y)))$$

In A, what is $\mathcal{P}(\omega)$? We have $(A, \in) \vDash \omega + 1 = \mathcal{P}(\omega)$, which is obviously not what we want for $\mathcal{P}(\omega)$ to be.

Definition. (Bounded quantification)
We first define the notations $\exists v \in w \; \varphi$ to be $\exists v(v \in w \wedge \phi)$, and $\forall v \in w \; \varphi$ to be $\forall v(v \in w \to \phi)$, and we call these quantifiers *bounded*.
Now we say a formula φ is $\triangle_0$ if it is in the smallest set S of formulas with the following properties:
1. All q-f formulas are in S;
2. If $\varphi, \psi \in S$, then so are:

      2a. $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \to \psi$, $\varphi \leftrightarrow \psi$;
      2b. $\neg\varphi$;
      2c. $\exists x \in w \; \varphi$, $\forall v \in w \; \varphi$.

Theorem. If φ is $\triangle_0$ and A is transitive, then φ is absolute between A and M.

Proof. We already know that quantifier free formulas are absolute, and absoluteness is obviously preserved under propositional connectives. The only case left is (2c).
Let's just do $\varphi \to \exists v \in w \; \varphi = \exists v(v \in w \wedge \varphi)$. So suppose φ is absolute. We need to deal with downwards absoluteness: we have $(M, \in) \vDash \exists v \in a\varphi(v, a)$ for some $a \in A$, i.e. $(M, \in) \vDash \exists v(v \in a \wedge (\varphi(v, a))$.
Let's find $m \in M$ s.t. $(M, \in) \vDash m \in a \wedge \varphi(m, a)$.
Now $m \in a \in A$, so $m \in A$. By absoluteness of φ, we get $(A, \in) \vDash m \in a \wedge \varphi(m, a) \implies (A, \in) \vDash \exists v \in a\varphi(v, a)$. $\qquad\square$

Let T be any *set theory*. Then we say that φ is $\triangle_0^T$ if there is a $\triangle_0$ formula ψ s.t. $T \vdash \varphi \leftrightarrow \psi$. So we get, as a corollary:

Corollary. If A is transitive in M, and both $(M, \in)$ and $(A, \in)$ are models of T, then $\triangle_0^T$ formulas are absolute between A and M.
We may also define Σ_1^T formulas to be the formulas that are T-equivalent to $\exists v_1...\exists v_n\psi$ where ψ is $\triangle_0$, and similarly for Π_1^T formulas. So $\Sigma_1^T(\Pi_1^T)$ formulas are upwards(downwards) absolute between A and M respectively.

On Wednesday we will look at what formulas are actually in these classes.

—Lecture 3—

Last time we fixed some *set theory* T, and defined formula classes $\triangle_0^T$, Σ_0^T and Π_1^T. We showed that $\triangle_0^T$ formulas are absolute between A, M if A is transitive and $A, M \vDash T$, and also Σ_1^T and Π_1^T upwards and downwards respectively.

Even if you haven't paid attention you would have realize that we have some 0 and some 1 as subscripts here. So what is Δ_1^T?

Definition. A formula is Δ_1^T if it is both Σ_1^T and Π_1^T.
Note that this definition is only possible upon taking equivalence classes on T, else no formula could be both Σ_1 and Π_1.

Corollary. If A is transitive, $A, M \vDash T$, and ϕ is Δ_1^T, then ϕ is absolute between A and M.

Now we have to think of what a *set theory* is. We have to think of which axioms we're using. Preferably we would have extensionality, and then let's have pairing, union, power set, separation.
We denote this by FST_0 (finite set theory), with the 0 denoting that we don't have foundation yet. We use FST to denote FST_0+foundation(regularity).
Now if we add infinity in, we reach the original version of Zermelo set theory Z_0. However, nowadays we often call $Z = Z_0$+foundation the Zermelo set theory.
For ordinary people these are enough (or far more than enough). But set-theorists realized later that they need replacement; we call this ZF_0 (of course ZF for the version with foundation). And lastly if we add choice in we get ZFC_0 (with foundation we get ZFC).

1.2 Long List of Δ_0^T formulas

Now we find a long list of Δ_0^T formulas. We start with the more trivial ones:
1. $x \in y$;
2. $x = y$;
These two are Δ_0 without T needed.
3. $x \subseteq y$. Apparently this is not a formula: we think it means $\forall w(w \in x \to w \in y)$, which we might abbreviate it as $\forall w \in x(w \in y)$, which is exactly the (2c) in definition of Δ_0. So this is Δ_0 without T as well.
4. $\Phi_0(x) : \forall w(w \notin x) : \iff \forall w(\neg w \in x)$. If you took part II Logic and Set theory, you'll disagree that this is a formula, because $\neg$ is not a thing; but let's not be so parsimonious on the syntax, but write it as $\forall w(w \in x \to \neg x = x)$, so this is also Δ_0 in predicate logic.

We say that an operation $x_1, ..., x_n \to F(x_1, ..., x_n)$ is defined by a formula in class Γ (where Γ is any class of formulas) in the theory T if there is a formula $\Psi \in \Gamma$ s.t.
(1) $T \vdash \forall x_1...\forall x_n \exists y \Psi(x_1, ..., x_n, y)$;
(2) $T \vdash \forall x_1...\forall x_n \forall y, z \ \Psi(x_1, ..., x_n, y) \wedge \Psi(x_1, ..., x_n, z) \to y = z$;
(3) $\Psi(x_1, ..., x_n, y)$ iff $y = F(x_1, ..., x_n)$.
Note that the first two are formal requirements, but the last one is an informal requirement as we haven't defined what F is.

Examples: $x \to \{x\}$, $x, y \to \{x, y\}$ (these are opeartions in FST_0). Note that these are informal because notations like $\{\cdot\}$ are undefined.

Let's now continue our lists:
5. $x \to \{x\}$. We need a formula $\Psi(x, z) \leftrightarrow$ '$z = \{x\}$' $\leftrightarrow \forall w(w \in z \leftrightarrow w = x)$.
This is not Δ_0 yet because we have a $\leftrightarrow$ here. We rewrite it as
$\forall w((w \in z \to w = x) \wedge (w = x \to w \in z))$, but the second part is not Δ_0. So we again rewrite it as
$\exists w \in z(w = w) \wedge \forall w \in z(w \in z \to w = x)$. So this is Δ_0, with some very weak set theory being sufficient.

Similar to 5, we also have

6. $x, y \to \{x, y\}$;

7. $x, y \to x \cup y$;

8. $x, y \to x \cap y$;

9. $x, y \to x \setminus y$;

10. $x, y \to (x, y)$, the ordered pair, where we define it as $\{\{x\}, \{x, y\}\}$. Note that we could apply 5 and 6 (twice) to get this one.

The last one gives us the motivation that if two operations $f, g_1, ..., g_k$ are defined by Δ_0^T-formulas, then so is the operation

$$x_1, ..., x_n \to f(g_1(x_1, ..., x_n), ..., g_k(x_1, ..., x_n))$$

We then naturally have

11. $x \to x \cup \{x\} := S(x)$ (by the previous fact from 5 and 7).

12. $x \to \cup x$; (obvious if we write this fully out)

13. the formula φ describing "x is transitive".

14. the formula describing x is an ordered pair. At first look it looks like this is unbounded , but that's not the case: the quantifiers for the two components of x are bounded by $\cup x$.

15. $a, b \to a \times b$;

16. the formula "x is a binary relation";

17. $x \to \text{dom}(x) := \{y : \exists p \in x (p \text{ is an ordered pairs}, p = (v, w), y = v)\}$;

18. $x \to range(x) := \{y : \exists p \in x (p \text{ is an ordered pair and } p = (v, y))\}$;

19. the formula 'x is a function';

20. the formula 'x is injective';

21. the formula 'x is a function from A to B';

22. the formula 'x is a surjection from A to B';

23. the formula 'x is a bijection from A to B'.

Note that we've only used some very few axioms: union, pairing and some finite version of separation, and nothing more.

Let's also agree on the definition of an ordinal: α is an ordinal if α is a transitive set well-ordered by $\in$. Of course we have to also agree on what being well-ordered means: it's totally ordered + well-founded, i.e. $\forall X (X \subseteq \alpha \to X$ has a $\in$-least element).

Being totally ordered is Δ_0 formula (check); however, the sentence (X, R) being well-founded is not obviously absolute, since the bound for the $\forall Z (Z \subseteq X...)$ quantifier is the power set. We'll talk about absoluteness of well-foundedness on Friday.

However, we don't actually need the general well-foundedness; we only need well-foundedness by $\in$, but that is given by axiom of foundation! So in models with the axiom of foundation, α is an ordinal iff α is transitive and totally ordered by $\in$.

—Lecture 4—

We're still on our list of things that are absolute for transitive models. We ended

with ordinals last time, where we defined that x is an ordinal iff x is transitive and $(x, \in)$ is a well-order. We went into an issue there, because that consists of $(x, \in)$ is a total order, which is fine; but then it also needs $\in$ is a well-founded relation on x, which is only Π_1. The good side is that if T contains the axiom of foundation, then $\Phi_{ord}(x)$ is equivalent to x is transitive and $(x, \in)$ is a total order (as the last part is guaranteed), which is Δ_0^T. Therefore we can expand our list:

24. 'x is an ordinal' is Δ_0^T (for the right choice of T);
This is not as harmless as before, because we actually need T to include the axiom of foundation.
25. 'x is a successor ordinal', which is equivalent to 'x is an ordinal' and $\exists y \in x (y$ is the $\in$-largest element of x);
26. 'x is a limit ordinal';
27. $x = \omega$ (the smallest limit ordinal; similarly, $x = \omega + \omega$, $x = \omega + 1$, $x = \omega + \omega + 1$, $x = \omega^2$, $x = \omega^3$, $x = \omega^\omega$, ...)

1.3 Absoluteness of well-foundedness

If (X, R) is well-founded, we can define a rank function $rk : X \to \alpha$, where α is some ordinal, s.t. rk is order-preserving between (X, R) and $(\alpha, \in)$. This theorem is proved using the right instances of Replacement. In particular, ZF proves:
(X, R) is well-founded $\iff \exists \alpha \exists f$ α is an ordinal, and f is an order-preserving function from (X, R) to $(\alpha, \in)$. RHS is Σ_1^{ZF}, and LHS is Π_1^{ZF}. Thus for sufficiently strong T, (X, R) is well-founded is Δ_1^T and hence absolute for transitive models of T.

We generalize this to concepts defined by transfinite recursion. But first let's recall what it is: let (X, R) be well-founded, let F be 'functional', so for every x there is a unique y s.t. $x = F(y)$. Then there is a unique f with domain X and for all $x \in X$, $f(x) = F(f|IS_R(x))$, where $IS_R(x) = \{z \in x : zRx\}$.

Proposition. Let T be a set theory that is strong enough to prove the transfinite recursion theorem for F. Let F be absolute for transfinite models of T. Let (X, R) be in A. Then f defined by transfinite recursion is absolute between A and M.

Example. Let L be any first-order language whose symbols are all in A. Then the set of L-formulas and the set of L-sentences are in A.
The relation $S \vDash \varphi$ (note that this is not q-f, although it is bounded by S) is defined by recursion, and thus is absolute between A and M.
So: if S is an L-structure, $S \in A$,
$(A, \in) \vDash 'S \vDash \varphi' \iff (M, \in) \vDash 'S \vDash \varphi'$.

Gödel's incompleteness theorem roughly says that, if T is a theory whose set of axioms are recursive enumerable, and its axioms are strong enough to do some arithmetics, then $T \nvdash Cons(T)$ (which is a sentence in L). Examples for T: PA,

Z, ZF, ZFC, ZFC+φ any one additional formula.
In particular, $ZFC^* := ZFC + Cons(ZFC) \nvdash Cons(ZFC + Cons(ZFC))$.

By completeness theorem, $Cons(T) \iff \exists M(M \vDash T)$. Note that LHS is Π_1 and RHS is Σ_1, so completeness theorem tells us that this is a Δ_1 concept. Note also that LHS is a bounded concept, since all quantifiers are bounded (LHS is Δ_0^Z).

Now write β for 'there is a transitive set A s.t. $(A, \in) \vDash ZFC$'. Note that this is stronger than the consistency of ZFC as it also specifies that there is a particular model for it. In particular, we can't prove it even in ZFC^*:

Theorem. If ZFC^* is consistent, then $ZFC^* \nvdash \beta$.

Proof. Let $(M, \in) \vDash ZFC^*$. Suppose $ZFC^* \vdash \beta$. So $(M, \in) \vDash \beta$. So we found a transitive set A in M s.t. $(A, \in)$ is a model of ZFC. By assumption, $(M, \in) \vDash Cons(ZFC)$, so $(A, \in) \vDash Cons(ZFC)$ since $Cons(ZFC)$ is absolute between transitive models. So $(A, \in) \vDash ZFC^*$. So we proved $Cons(ZFC^*)$, contradicting Gödel's incompleteness theorem. $\square$

That means that assuming β is not an obvious assumption, so we need to study under which (natural) assumptions β is true.

1.4 Concrete transitive models of ZFC

So let's investigate transitive models A inside M. The two most basic constructions:
(1) von Neumann hierarchy (cumulative hierarchy);
(2) hereditarily small sets.

(1) is defined as follows by transfinite recursion: $V_0 := \phi$, $V_{\alpha+1} := \mathcal{P}(V_\alpha)$, $V_\lambda := \cup_{\alpha < \lambda} V_\alpha$ for λ being limit ordinals.

Proposition. $\forall \alpha V_\alpha$ is transitive (see Part II Logic and Set Theory). [Induction, with key lemma: if X is transitive, then $\mathcal{P}(X)$ is transitive]

If λ is a limit ordinal, then $V_\lambda \vDash FST$.
If $\lambda > \omega$ and a limit ordinal, then $V_\lambda \vDash Z$.

For (2): let κ be a cardinal. We say X is hereditarily smaller than κ if $|tcl(X)| < \kappa$ (transitive closure).
Let $H_\kappa := \{X : X \text{ is hereditarily smaller than } \kappa\}$. This is obviously transitive.

We'll continue next Monday.

—Lecture 5—

We'll start with V_α today.

We know (if you don't know then I invite you to learn it): if λ is a limit then $V_\lambda \vDash FST$; if further $\lambda > \omega$, then $V_\lambda \vDash Z$. (On example sheet 1. I haven't printed them today, so if you want to try them before Wednesday, find an envelope next to my office at C0.10 from this afternoon).

The critical axiom here is *Replacement*. The test case is $\lambda = \omega + \omega$, which we expect replacement fails. Remember replacement says that if we have a function $F : V_{\omega+\omega} \to V_{\omega+\omega}$ that is definable in $V_{\omega+\omega}$, and $x \in V_{\omega+\omega}$, then $\{F(y) : y \in x\} \in V_{\omega+\omega}$, i.e. image of elements of a set under a function is a set.

The idea is to take $x = \omega$, and define F to be the function that takes $n \to \omega+n$, and $y \to 0$ if $y \notin \omega$. Remember that definable just means that we need a formula that uniques specify the image (see previous notes). Let $Y = \{F(n) : n \in \omega\}$, which needs to be a set if replacement holds. Then Y is a subset of $V_{\omega+\omega}$, so $Y \in V_{\omega+\omega+1}$; but it is not bounded, so it is not in $V_{\omega+\omega}$. This example shows concretely that $V_{\omega+\omega} \vDash \neg Replacement$.

What we needed in this particular example is a function that takes a bounded sequence to an unbounded one. Similarly, if α is any ordinal s.t. there is a definable function $f : \omega \to \alpha$, s.t. the range of f is unbounded in α, then $V_\alpha \vDash \neg Replacement$.

Even more general, if $\beta < \alpha$, and a definable function $f : \beta \to \alpha$ with unbounded range, then $V_\alpha \vDash \neg Replacement$.

Reminder: we call a cardinal κ *regular* if there is no partition $\kappa = \cup_{i \in I} A_i$ s.t. $|I|, |A_i| < \kappa$ for all $i \in I$.
Equivalently, for every $\alpha < \kappa$, there is no unbounded function $f : \alpha \to \kappa$.

We know, for exmaple, that $\aleph_1$ is regular. Moreover, for any α, $\aleph_{\alpha+1}$ is regular. So this gives us the next candidate, $\alpha = \aleph_1$, which replacement cannot fail in the above way. So how does it fail? Note that $\mathcal{P}(\omega) \in V_{\omega+2} \subseteq V_{\omega_1}$. Clearly, there is a surjection $s : \mathcal{P}(\omega) \to \omega_1$. But that means its range is unbounded in ω_1. Thus $V_{\omega_1} \vDash \neg Replacement$ either.
In general, if κ is regular and there is $\lambda < \kappa$ with $|\mathcal{P}(\lambda)| \geq \kappa$, then the same argument shows $V_\kappa \vDash \neg Replacement$.

Definition. A cardinal κ is called *inaccessible* if
(a) κ is regular;
(b) $\forall \lambda < \kappa$, $|\mathcal{P}(\lambda)| < \kappa$.

Side note: Related to the question, 'are there regular limit cardinals'? Under GCH: $\forall \kappa, 2^\kappa = \kappa^+$, we have that κ is inaccessible iff κ is regular limit. This suggests that the above question cannot be answered that easily (we usually call regular limit cardinals *weakly inaccessible*).

Let's assume that $\kappa > \omega$ is inaccessible (because ω is actually inaccessible, which kind of make sense, because *infinity* is the ultimate thing that is not accessible from everything smaller than it).

Lemma. $\forall \lambda < \kappa$, $|V_\lambda| < \kappa$.

Proof. Clearly $|V_\omega| = \aleph_0$, so $|V_\omega| < \kappa$.

By induction, suppose $|V_\lambda| < \kappa$. Then $V_{\lambda+1} = \mathcal{P}(V_\lambda)$. Therefore $|V_{\lambda+1}| = |\mathcal{P}(V_\lambda)| < \kappa$ by (b).

Now let $\lambda < \kappa$ be a limit ordinal. Then $V_\lambda = \cup_{\alpha<\lambda} V_\alpha$. So suppose by contradiction that $|V_\lambda| = \kappa$. But $|V_\alpha| < \kappa$ for all $\alpha < \kappa$, so we can write κ as a union of λ many things of smaller cardinals, contradicting regularity. $\square$

Theorem. If κ is inaccessible, then $V_\kappa \vDash Replacement$.

Proof. We're actually going to something slightly stronger: take any function $F : V_\kappa \to V_\kappa$ (without caring of its definability), and any $x \in V_\kappa$. Note that $V_\kappa = \cup_{\alpha<\kappa} V_\alpha$. So we can find $\alpha \in \kappa$ s.t. $x \in V_\alpha$. Since V_α is transitive, $x \subseteq V_\alpha$. But that means $|x| \le |V_\alpha| < \kappa$ (by lemma). Note that this is exactly what went wrong in V_{ω_1}.

Now consider $X := \{F(y) : y \in x\}$. For each $y \in x$, consider $\rho(F(y)) :=$ the least α s.t. $F(y) \in V_{\alpha+1} \setminus V_\alpha$. By assumption, $\rho(F(y)) < \kappa$. Consider $\{\rho(F(y)) : y \in x\} := R$, then $|R| \le |x| < \kappa$. By regularity, $\alpha := \cup R < \kappa$. But now $\forall y \in x F(y) \in V_{\alpha+1}$. So $X \subseteq V_{\alpha+1}$, so $X \in V_{\alpha+2}$, i.e. $V_\kappa \vDash Replacement$. $\square$

Note that this proves that the existence of inaccessible cardinals cannot be proved from ZFC.

1.5   Inaccessible cardinals

—Lecture 6—

Course webpage:
$https://www.math.uni-hamburg.de/home/loewe/Lent2019/TST\_L19.html$.
Hand in work at the start of example class.

On the example sheet we've seen(or will see) that we write IC for the axiom 'there is an inaccessible cardinal.
We've seen that if κ is inaccessible, then $V_\kappa \vDash ZFC$ (which is a transitive model). So ZFC+IC $\vdash$ 'there is a transitive set that is a model of ZFC', which we have called this β at some point; we've also proved that β is stronger than $Cons(ZFC)$, in the sense that $ZFC + Cons(ZFC) \nvdash \beta$. Therefore $ZFC + Cons(ZFC) \nvdash IC$.

Two model-theoretic reminders (see Part II Logic and Set Theory for both):
(1) Löwenheim-Skolem theorem. We want to formalize this: if $\mathcal{S}$ is any structure in some countable first-order language L, and $X \subseteq S$ is any subset, then there is a *Skolem hull* of X in $\mathcal{S}$, usually written as $\mathcal{H}^{\mathcal{S}}(X)$, with $X \subseteq \mathcal{H}^{\mathcal{S}}(X) \subseteq \mathcal{S}$, s.t.
(a) $\mathcal{H}^{\mathcal{S}}(X) \prec \mathcal{S}$ (elementary subsucture of $\mathcal{S}$);
(b) $|\mathcal{H}^{\mathcal{S}}(X)| \le \max(\aleph_0, |X|)$.
You probably have seen the proof of this theorem, but let's have a sketch again because it's important to see how theorems of this kind are proved.

Proof. (sketch)

Key ingredient – Tarski-Vaught criterion: $Z \subseteq S$ then $Z \prec S$ iff for every φ and all $z_1, ..., z_n$, if $S \vDash \exists \varphi(x, z_1, ..., z_n)$, then $Z \vDash \exists x \varphi(x, z_1, ..., z_n)$.

In order to construct the Skolem hull, we define $Z_1 = Z_0 \cup$ witnesses for all tuples $\varphi_1(z_1, ..., z_n)$ where $z_1, ..., z_n \in Z_0 = X$, and then $Z_{n+1} := Z_n \cup ....$ By induction, each Z_i has the same size. In the end we define $Z := \bigcup_{n \in \mathbb{N}} Z_n$, which will satisfy the Tarski-Vaught criterion. $\qquad\square$

Consequence: work in $ZFC + IC$, $(M, \in) \vDash ZFC + IC$; inside $V_\kappa \subseteq M \vDash ZFC$. Apply L-S theorem to V_κ with $X := \phi$, we find a structure $H := \mathcal{H}^{V_\kappa}(\phi) \prec V_\kappa$, which is countable (since it cannot be finite). So we've found a countable model of ZFC – isn't this a contradiction? Not really, because this H is, in general, not transitive – and it probably shouldn't be – consider the sentence '$\exists x$ s.t. x is the least uncountable cardinal. This is certainly true in V_κ, so it needs to be also true in H; but its only witness in V_κ is $\aleph_1$, so $\aleph_1 \in Z_1 \subseteq H$; so H cannot be transitive since $\aleph_1$ has uncountably many elements.

(2) Mostowski Collapse Theorem. If X is any set, and $R \subseteq X \times X$ s.t. R is well-founded and extensional, then there is a transitive set T s.t. $(T, \in) \cong (X, R)$. Consider $(H, \in) \vDash ZFC$: $\in$ is extensional on H by the axioms of ZFC; $\in$ is well-founded on M, so $\in$ is well-founded on H.

So, let T be the Mostowski collapse of H: T is transitive, $(T, \in) \cong (H, \in)$. So $(T, \in) \vDash ZFC$, and now T is transitive, and since this is a bijection, $|T| = |H| \leq \aleph_0$, so we get a countable transitive model of ZFC!

(some diagrams, where we used T to denote the countable transitive model of ZFC)

Consider $\varphi(x) := x$ is countable: $\exists f(\underbrace{f : x \to \mathbb{N}}_{\Delta_0^{ZFC}}, \underbrace{f \text{ is injective}}_{\Delta_0^{ZFC}})$, which is Σ_1^{ZFC}, so is upwards absolute. But this formula is *not* downwards absolute: if α is an ordinal, $\alpha \in T$, then $V_\kappa \vDash \alpha$ is countable. But since $(T, \in) \vDash ZFC$, there is some $\alpha \in T$ s.t. $(T, \in) \vDash \alpha$ is uncountable, so V_κ and T disagree about the truth value of $\varphi(\alpha)$.

Now consider $\psi(x) : x$ is a cardinal$:= \forall \alpha(\alpha < x \to$ there is no injection from x to $\alpha)$, which is Π_1^{ZFC}, so downwards absolute. In $(T, \in)$, take α least s.t. $(T, \in) \vDash \neg\varphi(\alpha)$. Then $(T, \in) \vDash \alpha$ is a cardinal. Clearly $V_\kappa \vDash \alpha$ is not a cardinal. So ψ is not upwards absolute.

Note that if λ is an uncountable cardinal in V_κ, then $\lambda \notin T$, so the downwards absoluteness of ψ is not very interesting because there aren't many cardinals.

Instead of building $\mathcal{H}^{V_\kappa}(\phi)$, why not build $H^* := \mathcal{H}^{V_\kappa}(\omega_1 + 1)$? Clearly $\omega_1 \in H$ now, and $\omega_1 \subseteq H$ as well, so ω_1 stays the same when we do Mostowski's Collapse; so $\omega_1 \subseteq T^*$ and $\omega_1 \in T^*$ where T^* is the new model obtained after Mostowski's collapse.

Now we have $V_\kappa \vDash \omega_1$ is a cardinal, so by downwards absoluteness, $T^* \vDash \omega_1$ is

a cardinal. However, it might be the case that there are some other cardinals below ω_1, so we can't say $\omega_1 = \aleph_1$.

—Lecture 7—

Remember our goal is to deduce some results about CH. We've decided to go for transitive models of ZFC (as we don't want to be concerned about whether a function is still a function in a submodel). We've looked at 'inner models', and in particular, models of type V_α. We also know that if α is inaccessible, then $V_\alpha \vDash ZFC$. We've also found countable transitive submodel in V_α of ZFC, called T, by Mostowski collapse and L-S theorem.

One problem: this is *not* going to change the truth value of CH: Suppose CH is true in $(M, \in)$, so there's a bijection between $\mathbb{R}$ and ω_1. Similarly, if CH is false then there is no such bijection. An immediate problem is that we don't know what $\mathbb{R}$ is; we might as well replace it by $\mathbb{P}(\mathbb{N})$, which is definitely in $V_{\omega+20}$ (safe enough), while $\omega_1 \in V_{\omega_1+1}$. But that means V_κ knows exactly if there is a bijection (say we can define this in $V_{\omega_1+20} \subseteq V_k$) between $\mathbb{R}$ and ω_1 because it has access to both of the levels, and it could just 'take a look' at it to determine the truth value. So $(M, \in) \vDash CH \iff (V_\kappa, \in) \vDash CH$.
But remember by L-S theorem we got a countable $H \prec V_\kappa$, so $(H, \in) \vDash CH \iff (V_\kappa, \in) \vDash CH$; and Mostowski collapse gives $(T, \in) \cong (H, \in)$, so $(T, \in) \vDash CH \iff (H, \in) \vDash CH$.

Summary: the method of finding countable transitive *elementary* submodels of V_κ is not going to change the value of CH. So let's look at different models.

1.6 The second construction: Models of hereditarily small sets

Let κ be a regular cardinal (e.g. $\kappa = \omega, \kappa = \omega_1$). Then x is called hereditarily of size $< \kappa$ if $|tcl(x)| < \kappa$, where $tcl(x)$ is the transitive closure of x ($= \bigcup_{n \in \mathbb{N}} t_n(x)$, where $t_0(x) := x$, $t_{n+1}(x) = \bigcup t_n(x)$).
The definition of $tcl(x)$ captures the intuition of 'x has size $< \kappa$, all elements of x have size $< \kappa$, all elements of elements of x have size $< \kappa$, etc.'.

Remark. It's important that κ is regular for the intuition to work: suppose it's not, say let $\kappa = \aleph_\omega$. Now think of a tree that has branches of all finite lengths, where at level n we attach something of cardinality $\aleph_n$ at the node. More formally, define

$$x_n^0 = \aleph_n$$
$$x_n^{k+1} = \{x_n^k\}$$
$$...$$
$$\mathbb{X} := \{x_0^0, x_1^1, x_2^2, ...\}$$

Note that $\mathbb{X}$ is countable, but in the 'tcl' notation above, the cardinality of $t_{n+1}(\mathbb{X})$ is $\aleph_n$, so $tcl(x)$, as the union of them, has cardinality $\aleph_\omega$! The problem

is obviously because we could obtain $\aleph_\omega$ from fewer than $\aleph_\omega$ of smaller than $\aleph_\omega$ things, i.e. $\aleph_\omega$ is not regular.

From now let's forget about those singular κ, but only consider κ regular.

We make a few observations:
1. H_κ is transitive;
2. If $X \subseteq H_\kappa$ and $|X| < \kappa$, then $X \in H_\kappa$ (follows directly from regularity of κ and the definitions).

Example. Let $H_{\aleph_0} := HF$ (hereditarily finite).
We claim that $HF = V_\omega$.

Proof. $V_\omega \subseteq HF$. We need to show $V_n \subseteq HF \forall n$. Clearly $V_0 = \phi \subseteq HF$; if $V_n \subseteq HF$, and $Z \subseteq V_n$, then by observation 2, $Z \in HF$, so $\mathcal{P}(V_n) = V_{n+1} \subseteq HF$.
Now we show $HF \subseteq V_\omega$. Suppose not, so there is $x \in HF \setminus V_\omega$; take such x with minimal rank α, so $x \in V_{\alpha+1} \setminus V_\alpha$. By minimality, if $y \in HF$ with $\rho(y) < \alpha$, then there is $k \in \mathbb{N}$ s.t. $\rho(y) = k$. We know $x \in \mathcal{P}(V_\alpha)$, so $x \subseteq V_\alpha \subseteq HF$. So $x \in HF$, so x is finite. Say $x = \{x_1, ..., x_n\}$. By minimality, each of them is in V_{k_i} for some k_i, so $x \subseteq V_{\max(k_1,...,k_n)+1} \subseteq V_\omega$. $\square$

Example. $H_{\aleph_1} = HC$ (hereditarily countable).
We know:
- $Ord \cap HC = \omega_1$;
- $V_{\omega+2} \setminus HC \neq \phi$;
- $V_{\omega+1} \subseteq HC$.

Which axioms are true in HC? Let's check Pair: say $x, y \in HC$. then $\{x, y\} \subseteq HC$. But $|\{x, y\}| < \aleph_1$, so $\{x, y\} \in HC$.
Separation, foundation, extensionality, union all hold in HC as well quite easily.
Replacement: let F be a function $HC \to HC$, and $x \in HC$. Consider $R := \{F(y); y \in x\}$, which exists in the universe, and we need to check whether it's in R. We know $|R| \leq |x| < \aleph_1$, and $R \subseteq HC$. By observation 2 we immediately get $R \in HC$. So replacement is trivial!
So we know Power Set must be false, or at least not provable in HC, else we've proved the existence of a model of ZFC!

Note that Power Set is trivial in ZFC and it's replacement that is troublesome there, while here it's the other way round.

We know that $\mathbb{N} \in HC$, and we also know that $\mathcal{P}(\mathbb{N}) \notin HC$. But that is not enough to disprove Power Set in HC; we need to show that there is no object in HC such that HC *thinks* that it is the power set of $\mathbb{N}$; more formally, we need to show that for all $A \in HC$, $HC \vDash 'A$ is not a power set of $\mathbb{N}$, i.e. $\exists X (X \subseteq \mathbb{N} \land X \notin A)$.

Fix $A \in HC$, and presume that this might be the HC-powerset of $\mathbb{N}$.
Thus, if $X \subseteq \mathbb{N}$ and $X \in HC$, then $X \in A$. But if $X \subseteq \mathbb{N}$, then $X \subseteq HC$, and $|X| < \aleph_1$, so $X \in HC$.

So if A is any set s.t. $\forall X, X \subseteq \mathbb{N} \land X \in HC \to X \in A)$, then A is uncountable, so $A \notin HC$. Contradiction. Thus $HC \vDash \neg PowerSet$.

—Lecture 8—

We've not been doing very useful things so far since what we've done was basically proving that many things are not useful. Even worse, the thing that we're going to do now is the most pointless of all as it's almost identical to some problems in the example sheet.

We knew H_κ is a model of all of ZFC without power set if κ is regular.

Proposition. If κ is a strong limit (cannot be reached by taking power set), then $H_\kappa \vDash PowerSet$.

Proof. We'll show: if $x \in H_\kappa$, then $\mathcal{P}(x) \in H_\kappa$. This is much stronger than the Power Set axiom.
Certainly $tcl(\mathcal{P}(x)) = \mathcal{P}(x) \cup tcl(x)$. Now $|tcl(x)| < \kappa$ since $x \in H_\kappa$, and $|\mathcal{P}(x)| < \kappa$ as well since κ is a strong limit. So together we know $|tcl(\mathcal{P}(x))| < \kappa$, so $\mathcal{P}(x) \in H_\kappa$. $\qquad\square$

General idea: build inner models using *definability* properties. But the problem is: definability is not definable. This sounds like a typical joke from logicians, but it's actually a theorem.

Theorem. (Tarski Undefinability of Truth)
Let $(M, \in) \vDash ZFC$ (we'll just use this, but we'll see in the proof what set theory we actually need). We assume that the language of set theory $L_\in \subseteq M$ (so that sentences and formulas are actually elements of M). Consider the set S of sentences of $L_\in$ and the set U of unary predicates (i.e. $L_\in$-formulas in one free variable).
A *truth predicate* would be a formula $T(x)$ in $L_\in$, so a unary predicate, i.e. $T \in U$, s.t. $(M, \in) \vDash \varphi \iff (M, \in) \vDash T(\varphi)$.
Claim: there can be no such truth predicate.
Before proving this, let's contrast this with the definition of truth we had before. Our previous result says if M is a set, then the concept $(M, \in) \vDash \varphi$ is Δ_0 (because we bound the quantifier by M, which is a set, so in some sense we had to use a parameter M in our previous result, which is not available in our current settings.

Proof. (idea: diagonalisation)
If $\varphi(x) \in U$, then we can ask whether $\varphi(\varphi)$ (which is a sentence, so $\in S$) is true. Let's assume that there is a truth predicate T, and define a unary formula $\delta(x) := \neg T(x(x))$ (the *diagonal*), where $x(x)$ is x applied to x if $x \in U$, and is ϕ otherwise (remember formulas are elements in M). Now apply δ to δ, so $\delta(\delta) \in S$. Now

$$M \vDash \neg T(\delta(\delta)) \iff M \vDash \delta(\delta) \iff M \vDash T(\delta(\delta))$$

by definition of δ and the fact that T was a truth predicate respectively. Contradiction. $\square$

Again, let $M \vDash ZFC$. We say that $x \in M$ is *definable* if there is a formula φ s.t. $\forall y \in M \, x = y \iff M \vDash \varphi(y)$.

We say that a formula D is called a *definition of definability* if $\forall x \in M$, x is definable $\iff M \vDash D(x)$. By now we all know what we should expect next:

Theorem. (undefinability of definability)
There is no formula D that is a definition of definability.

Proof. Assume D is a definition of definability. Consider (informally now)

$$\alpha := \max\{\beta : \beta \text{ is not definable, but} \forall \gamma < \beta \exists \gamma' \, \gamma < \gamma' < \beta \text{ and } \gamma' \text{ is definable}\}$$

which is the supremum of the definable ordinals. This has to exist because there are only countably many formulas, and each formula only specifies at most one ordinal; this has to be uncountable since, say, $\aleph_1$ is definable. This is defined by the formula:
$y = \alpha \leftrightarrow y$ is an ordinal and $\neg D(y)$ and

$$\forall \gamma (\gamma < y \rightarrow \exists \gamma' (\gamma < \gamma' < y \wedge D(\gamma')))$$

This proves that α is definable in the sense of the definition, so $M \vDash D(\alpha)$; but one of the conjuncts in the definition implies $M \vDash \neg D(\alpha)$. Contradiction. $\square$

We now learned that *definability* is not going to work without keeping track of parameters. So we need to define definability with direct reference to what parameters are allowed.

Fix A, and $n \in \mathbb{N}$. We're going to define by recursion what it means to be a definable subset of A^n:
Define $Diag_\in(A, n, i, j) := \{s \in A^n : s_i \in s_j\}$ (read as *diagrams*),
$Diag_=(A, n, i, j) := \{s \in A^n : s_i = s_j\}$,
$Proj(A, R, n) := \{s \in A^n : \exists t \in R(t|_n = s)\}$ (where the formula in the last bracket means t restricted to n) (the intended meaning is for $R \subseteq A^{n+1}$). Now define
$Def(0, A, n) := \{Diag_\in(A, n, i, j) : i, j < n\} \cup \{Diag_=(A, n, i, j) : i, j < n\}$,

$$
\begin{aligned}
Def(k+1, A, n) := Def(k, A, n) &\cup \{R \cap S : R, S \in Def(k, A, n)\} \\
&\cup \{A^n \setminus S : S \in Def(k, A, n)\} \\
&\cup \{Proj(A, R, n) : R \in Def(k, A, n+1)\}
\end{aligned}
$$

(corresponding to conjunctions, negations and existence quantifier). Lastly we define

$$Def(A, n) := \bigcup_{k \in \mathbb{N}} Def(k, A, n)$$

Observe that the definition of $Def(k+1, A, n)$ and $Def(0, A, n)$ are Δ_0 because all of the quantifiers are bounded by A. So the definition of $Def(A, n)$ is a recursive definition based on absolute notions, and thus absolute for transitive models (containing A, of course).

The next thing we are going to do (a bit of preview) is to use $Def(A, n)$ to define the *definable power set*. After that, define a *definable von Neumann hierarchy*. That's what we are going to do on Wednesday.

A reminder that we're going to have an example class this afternoon (330-5pm). I think it's in MR5?

—Lecture 9—

1.7   The constructible universe

Last time we discussed the construction of an inner model $L \subseteq M$ that is based on definability. Problems with definability are conncted to Tarski's Undefinability of Truth; the *definable* fragment of truth is that where we fix the scope of existential quantifiers in advance.
Recall that we defined recursively $Def(A, n)$, which are definable subsets of A^n, where *definable* is interpreted in A.

Lemma. Let $X \subseteq A^n$. If there is a formula φ s.t.

$$(x_1, ..., x_n) \in X \iff (A, \in) \vDash \varphi(x_1, ..., x_n)$$

then $X \in Def(A, n)$.

Proof. Simple induction over complexity of φ. $\qquad\qquad\square$

Lemma. In M, we have that $Def(A, n)$ is countable.
(We even have a concrete surjection $\mathbb{N} \to Def(A, n)$.)

Proof. There are only countably many formulas. $\qquad\qquad\square$

Observation: in the definition of $Def(k, A, n)$, we only used notions absolute for transitive models of ZF. So, since $Def(A, n)$ was defined by recursion over $Def(k, A, n)$, also $Def(A, n)$ is absolute between transitive models.

Our goal is to find a definable power set. However, $Def(A, 1)$ is not a good candidate as it is always countable, so if A is uncountable, then there is $a \in A$ s.t. $\{a\} \notin Def(A, 1)$ by the above lemma.

We define

$$\mathcal{D}(A) := \{X \subseteq A : \exists n \exists s \in A^n \exists R \in Def(A, n+1) s.t. X = \{a \in A : (a, s_0, ..., s_{n-1}) \in R\}\}$$

and we'll call this the *definable power set*.

Observation: If X is informally definable with parameters from A, i.e. $X = \{a \in A : (A, \in) \vDash \varphi(a, p_1, ..., p_n)\}$ for some $p_1, ..., p_n \in A$, then $X \in \mathcal{D}(A)$.

Observation: As $Def(A, n)$ was absolute and the quantifiers in the definition of $\mathcal{D}(A)$ are all bounded, $\mathcal{D}(A)$ is absolute for transitive models.

Proposition. If A is transitive, then $\mathcal{D}(A)$ is transitive.

Proof. Suppose $x \in X \in \mathcal{D}(A)$. Then $x \in X \subseteq A$. So $x \subseteq A$ and $x \in A$ as A is transitive. We can then define x as a subset by the formula $v \in x = \varphi(v)$ (which selects exactly the elements of x, which form x): $x = \{z \in A : (A, \in) \vDash \varphi(z)\}$. $\qquad\square$

Let $L_0 := \phi$,
$L_{\alpha+1} := \mathcal{D}(L_\alpha)$,
$L_\lambda := \bigcup_{\alpha < \lambda} L_\alpha$.

We refer to the class $\bigcup_{\alpha \in Ord} L_\alpha$ as 'L', or *the constructible universe.*

Properties:
(1) If $\alpha \leq \omega$, then $V_\alpha = L_\alpha$.
(2) For every α, L_α is transitive from proposition by induction.
(3) $\alpha \leq \beta \rightarrow L_\alpha \subseteq L_\beta$;
(4) $Ord \cap L_\alpha = \alpha$ (this and (3) are in sheet 2);
(5) If $\alpha \geq \omega$, then $|L_\alpha| = |\alpha|$.

Proof. $\alpha = \omega$: $|L_\omega| = |V_\omega| = \aleph_0 = |\omega|$;
Suppose for all $\beta < \alpha$ we have $|L_\beta| \leq |\beta|$. Show that $|L_\alpha| < |\alpha|^+$:
(a) α is a successor, say $\alpha = \beta + 1$. So $L_\alpha = L_{\beta+1} = \mathcal{D}(L_\beta)$; if we look carefully at the definition, we could get a surjection from $\aleph_0 \times \bigcup_{n \in \mathbb{N}} L_\beta^n$ onto $\mathcal{D}(L_\beta)$; but we assumed α is at least ω, $\aleph_0 \times \bigcup_{n \in \mathbb{N}} L_\beta^n$ has cardinality $|L_\beta|$ as well.
(b) α is a limit. Let $\pi_\beta : \alpha \rightarrow L_\beta$ be a surjection. Then we find surjection from $\alpha \times \alpha \twoheadrightarrow L_\alpha$ by $(\gamma, \gamma') \rightarrow \pi_\gamma(\gamma')$. $\qquad\square$

Note that in the above we've only proved that the cardinality is at most what we wanted; but it is also at least that by property (4).

Now look at $V_{\omega+1}$ and $L_{\omega+1}$. They can't be the same, as the first is uncountable but the second is uncountable. So $L_{\omega+1} \subseteq V_{\omega+1}$, and $V_{\omega+1} \setminus L_{\omega+1} \neq \phi$. However, it is entirely possible that the missing part is collected later when we reach L_{ω_1} or later.

Definition. If x is constructible, $x \in L$, then $\rho_L(x) := \min\{\alpha : x \in L_{\alpha+1}\}$ (an analogue of the rank in V).

Definition. $V = L$ is the axiom of constructibility

$$\forall x \exists \alpha (x \in L_\alpha)$$

Note that this is a concrete sentence in $L_\in$, as L_α can be recursively defined.

Lemma. If M is a transitive set model of $ZFC + (V = L)$, then there is a limit ordinal λ s.t. $M = L_\lambda$.

Note that we haven't shown that such M would exist (as $\neg V = L$ might well be a theorem in ZFC), but we know what it will look like *if* it exists.

We don't really have much time, so we'll present a quick proof here; more details next lecture.

Proof. Consider $\lambda := Ord \cap M$ (remember that M is a set, so λ is indeed a set, so an ordinal). Clearly, λ is a limit ordinal (both are transitive).

We claim that $M = L_\lambda$: suppose $x \in M$, by $V = L$ find $\alpha \in M$ s.t. $(M, \in) \vDash x \in L_\alpha$. L_α was defined by recursion from absolute notions, so $x \in L_\alpha$ is absolute. So $x \in L_\alpha \subseteq L_\lambda$.

Suppose $x \in L_\lambda$, so there is $\alpha < \lambda$ s.t. $x \in L_\alpha$ (this is absolute, so $(M, \in) \vDash x \in L_\alpha$), by choice of λ, $\alpha \in M$. $\qquad \square$

—Lecture 10—

What did we do so far? We defined the constructible universe, and we realized that our definitions were absolute for transitive models: if we write $\Phi(x, \alpha)$ the formula '$x \in L_\alpha$', $\Psi(x, \alpha)$ the formula '$x = L_\alpha$', then both Φ and Ψ are absolute for transitive models of set theory.

We also had the axiom '$V = L$', which is a short hand for $\forall x \exists \alpha\, x \in L_\alpha$.

Proposition. If A is a transitive set model of $ZFC + (V = L)$, then $A = L_\alpha$ where $\alpha = Ord \cap A$.

Proof. '$A \subseteq L_\alpha$': If $x \in A$, then by $(A, \in) \vDash V = L$, find β s.t. $(A, \in) \vDash x \in L_\beta$; by absoluteness, $x \in L_\beta \subseteq L_\alpha$.

'$L_\alpha \subseteq A$': If $x \in L_\alpha$, since $\alpha = Ord \cap A$ and $A \vDash ZFC$, α has to be a limit ordinal. So we can write $L_\alpha = \bigcup_{\beta < \alpha} L_\beta$. So find $\beta < \alpha$ and $x \in L_\beta$. Since $(A, \in) \vDash ZFC$, we know that A thinks 'L_β exists', or slightly more formally, there is X s.t. $(A, \in) \vDash \Psi(X, \beta)$. By absoluteness of Ψ, $\Psi(X, \beta)$ is actually true in the bigger universe M. So $X = L_\beta$. Therefore $L_\beta \in A$. But $x \in L_\beta$ and A is transitive. So $x \in A$. $\qquad \square$

However, as we said last time, we don't really know if there *is* actually a model of $ZFC + (V = L)$, so what we just did seems a bit pointless. Our next major goal shall then be:

Theorem. (Gödel, 1938)
If κ is inaccessible, then $L_\kappa \vDash ZFC + (V = L)$.

Corollary. IC $\implies$ there is a *countable* α s.t. $L_\alpha \vDash ZFC + (V = L)$.

Proof. Take $H := \mathcal{H}^{L_\kappa}(\phi) \prec L_\kappa$, the Skolem hull. H is therefore countable. Then take $T \cong H$ the Mostowski collapse, then $(T, \in) \equiv (L_\kappa, \in)$ (all sentences have the same truth value). Therefore $(T, \in) \vDash ZFC + (V = L)$ is a countable

transitive model; then apply our previous proposition we know $T = L_\alpha$ for some ordinal α. But by a previous property $|L_\alpha| = |\alpha|$, so α has to be countable. $\square$

Contrast this with: If $V_\alpha \vDash ZFC$, then α cannot be countable: if α is countable, then there is a code for a surjection $f : N \twoheadrightarrow \alpha$ in $V_{\omega+1} \subseteq V_\alpha$, so $V_\alpha \vDash$ 'α is countable'; contradiction to $V_\alpha \vDash ZFC$. (some diagram)

Proof. (of theorem)
Extensionality follows from transitivity;
Pair: $x, y \in L_\kappa$, find α s.t. $x, y \in L_\alpha$ s.t. $\{x, y\} \subseteq L_\alpha$. Clearly the formula

$$\varphi(z, x, y) := z = x \lor z = y$$

defines the pair $\{x, y\}$. So by one of our previous lemmas, the pair lies in $\mathcal{D}(L_\alpha) = L_{\alpha+1} \subseteq L_\kappa$.
However, note that our lemma only says that if we have a formula φ, and we interpret it in L_α, then what we get will be in $D(L_\alpha)$. But luckily our φ here is simple enough that it doesn't matter where we interpret it within: its truth value is the same in any model that contains x and y.
The same proof takes care of, say, Union. Let's get to something that's more interesting. How about Power Set? This can't work directly, since there are just not enough elements in $D(L_\alpha)$.
Consider $x \in L_\kappa$. As before, $\alpha < \kappa$, so $x \in L_\alpha$, so $x \subseteq L_\alpha$ by transitivity, so $|x| \le |L_\alpha| < \kappa$ because κ is strongly inaccessible.
Consider $\mathcal{P}(x)$ in M; we know $|\mathcal{P}(x)| = 2^{|x|} < \kappa$ because κ is inaccessible, and $|L_\kappa \cap \mathcal{P}(x)| \le |\mathcal{P}(x)| < \kappa$ (diagram).

Remark. Since $L_\kappa, \mathcal{P}(x)$ are sets in M, $L_\kappa \cap \mathcal{P}(x)$ is a set in V_κ, and it is *definable* in V_κ by the formula

$$z \in L_\kappa \cap \mathcal{P}(x) \iff \Phi(z, \kappa) \land z \subseteq x$$

But that's not good enough to prove that $L_\kappa \cap \mathcal{P}(x) \in L_\kappa$, as we actually need to find an $\alpha < \kappa$ in place of κ in the formula.

For each $z \in L_\kappa \cap \mathcal{P}(x)$, find the L-rank,

$$\alpha_z := \rho_L(z) < \kappa$$

and consider the set

$$\{\alpha_z : z \in L_\kappa \cap \mathcal{P}(x)\} \subseteq \kappa$$

of size $< \kappa$. Then by regularity of κ we know it must be bounded by some $\beta < \kappa$ s.t.

$$\{\alpha_z : z \in L_\kappa \cap \mathcal{P}(x)\} \subseteq \beta$$

So $L_\kappa \cap \mathcal{P}(x) \subset L_\beta$.
Now define

$$P := \{z : (L_\beta, \in) \vDash z \subseteq x\}$$

By our lemma, $P \in \mathcal{D}(L_\beta) = L_{\beta+1} \subseteq L_\kappa$; but $L_\kappa \vDash \forall z(z \in P \iff z \subseteq x)$, so L_κ is a model of the power set axiom. (see diagram)

—Lecture 11—

Example sheet 2 will be in an envelope next to C0.10 this afternoon.
We saw pairing and power set last time. Some of the others will be in the example sheet.

Let's consider separation, a more difficult one. Let $x \in L_\kappa$, φ be a formula, $a_1, ..., a_k \in L_\kappa$.
Separation says that, informally, $\{z \in x : \varphi(z, a_1, ..., a_n)\}$ exists.
More formally, $\{z \in x : L_\kappa \vDash \varphi(z, a_1, ..., a_n)\}$ exists. At first glance we can use the same argument for power set: just find all these z are, and go to the next level and consider $\mathcal{D}$ of it. Let's see how that *stops* working. For each $1 \leq i \leq n$, find $\alpha_i < \kappa$ s.t. $a_i \in L_{\alpha_i}$, and find $\alpha < \kappa$ s.t. $x \in L_\alpha$. Define $\beta := \max\{\alpha, \alpha_1, ..., \alpha_n\}$.
So for any $z \in x$, we have $z, a_1, ..., a_n \in L_\beta$ (by transitivity of L_β). So $\{z \in x : L_\beta \vDash \varphi(z, a_1, ..., a_n)\} \in \mathcal{D}(L_\beta) = L_{\beta+1}$. Apparently this is not necessarily what we want: we have no idea if φ is absolute between L_β and L_κ; in fact we have *some* idea, because this has to work for any φ, so there are definitely some formulas that are not absolute.
So we see the problem is that, in general, $\{z \in x : L_\beta \vDash \varphi(z, a_1, ..., a_n)\} \neq \{z \in x : L_\kappa \vDash \varphi(z, a_1, ..., a_n)\}$.

Note that our choice of β might be a terrible one, as we have no idea what it is; it might even be a successor ordinal. So we have to choose it more carefully.

Consider $\mathcal{H}^{L_\kappa}(L_\beta) \prec L_\kappa$, with cardinality the same as $|L_\beta| = |\beta| < \kappa$; and now consider its Mostowski collapse, $T \cong \mathcal{H}^{L_\kappa}(L_\beta)$, with Mostowski isomorphism $\pi : T \to \mathcal{H}^{L_\kappa}(L_\beta)$. T is transitive, $|T| = |\beta| < \kappa$, and $T \prec L_\kappa$.

[Some model theory recap: we have if $M \cong M'$, $M \vDash \varphi(x_1, ..., x_n) \iff M' \vDash \varphi(\pi(x_1), ..., \pi(x_n))$. $M \equiv M'$ means $M \vDash \varphi \iff M'(\varphi)$ for all sentences φ. Therefore isomorphism implies elementary equivalence. $M \prec M'$ means $M \vDash \varphi(x_1, ..., x_\kappa) \iff M' \vDash \varphi(x_1, ..., x_n)$.]

We then have

$$T \xrightarrow{\quad \pi \quad} \mathcal{H}^{L_\kappa}(L_\beta) \xrightarrow{\quad id \quad} L_\kappa$$

$$\varphi(z, a_1, ..., a_n) \qquad \varphi(\pi(z), \pi(a_1), ..., \pi(a_n)) \qquad \varphi(\pi(z), \pi(a_1), ..., \pi(a_n))$$

We know that the Mostowski collapse is the identity on transitive sets. So, if $X \subseteq L_\kappa$ is transitive, then $\pi|_X = id|_X$. Since L_β *is* transitive, and all $z, a_1, ..., a_n$ are in L_β, we get that $T \vDash \varphi(z, a_1, ..., a_n) \iff L_\kappa \vDash \varphi(z, a_1, ..., a_n)$.

Let's do the 'modified Skolem Hull construction' from sheet 1 q12: let $\alpha_0 := Ord \cap T, \alpha_{n+1}$ is the least γ s.t. L_γ contains L_{α_n} and a witness for each existential statement true with parameters in L_{α_n}. Let $\bar{\alpha} := \bigcup_{n \in \mathbb{N}} \alpha_n$. So

$T \prec L_{\bar{\alpha}}$ with $\bar{\alpha} < \kappa$.

Now define the set via φ over $L_{\bar{\alpha}}$:

$$
\begin{aligned}
L_{\bar{\alpha}+1} = \mathcal{D}(L_{\bar{\alpha}}) \ni &\{z \in x : L_{\bar{\alpha}} \vDash \varphi(z, a_1, ..., a_n)\} \\
=&\{z \in x : T \vDash \varphi(z, a_1, ..., a_n)\} \ (T \prec L_{\bar{\alpha}}) \\
=&\{z \in x : \mathcal{H}^{L_\kappa}(L_\beta) \vDash \varphi(\pi(z), \pi(a_1), ..., \pi(a_n))\} \\
=&\{z \in x : \mathcal{H}^{L_\kappa}(L_\beta) \vDash \varphi(z, a_1, ..., a_n)\} \\
=&\{z \in x : L_\kappa \vDash \varphi(z, a_1, ..., a_n)\}
\end{aligned}
$$

We only showed pairing, power set, and separation. The rest are similar. $\qquad\square$

Theorem. (The Condensation Lemma)
If κ is inaccessible, $x, y \in L_\kappa$, and $y \subseteq x$, then there is $\alpha < \kappa$ with $|\alpha| \le |tcl(x)|$ s.t. $y \in L_\alpha$.

Proof. Consider $y \subseteq x$ and $tcl(x \cup \{y\}) =: t$. Clearly $|t| = |tcl(x)|$. Now consider $T \xrightarrow{\pi} \mathcal{H}^{L_\kappa}(t) \prec L_\kappa$, clearly all these things have the same cardinality. Now we know π is the identity on t, so in particular $\pi(y) = y$, $\forall z \in x \pi(z) = z$, and $\pi(x) = x$.
By our lemma, find β s.t. $T = L_\beta$ (we're now allowed to do this since $L_\kappa \vDash ZFC + (V = L)$, and therefore $L_\beta \equiv L_\kappa \vDash ZFC + (V = L)$).
Now y can be defined over L_β with parameters in L_β, namely viz. y (we know y is in there so we don't actually need to define it).
We just need to check β has the right cardinality: $|\beta| = |L_\beta| = |T| = |tcl(x)|$. $\quad\square$

—Lecture 12—

Today we're going to prove that there is a model of ZFC+CH. This is especially convenient as today we're in the middle of the entire course (the 12th lecture), so we spent exactly half of the course on proving one side of what we wanted.

Recall that last time we had the condensation lemma: if κ is inaccessible. $x, y \in L_\kappa$, $y \subseteq x$, then there is α s.t. $|\alpha| \le |tcl(x)|$ s.t. $y \in L_\alpha$.

Corollary. $x = \mathbb{N}$, $y \subseteq \mathbb{N}$, then there is $\alpha < \omega$ s.t. $y \in L_\alpha$.

Corollary. (1) $\mathcal{P}(\mathbb{N}) \cap L_\kappa \subseteq L_{\omega_1}$.
Observe that $\mathcal{P}(\mathbb{N}) \cap L_\kappa = \mathcal{P}^{L_\kappa}(\mathbb{N})$, where $\mathcal{P}^{L_\kappa}(\mathbb{N})$ referes to the unique $p \in L_\kappa$ s.t. $L_\kappa \vDash p = \mathcal{P}(\mathbb{N})$.
(2) $\mathcal{P}^{L_\kappa}(\mathbb{N}) \subseteq L_{\omega_1}$.
(3) $|\mathcal{P}^{L_\kappa}(\mathbb{N})| \le |L_{\omega_1}| = |\omega_1| = \aleph_1$.
Hence it seems that we're extremely close to having a model of ZFC+CH. However, this ω_1 we're referring to here is, of course, in the model that we're building.
(A 'one-line proof' of the Condensation Lemma:

$$
y \in L_\alpha = T \cong \mathcal{H}^{L_\kappa}(tcl(x) \cup \{y\}) \prec L_\kappa
$$

)

Let's improve this to show $L_\kappa \vDash CH$. The key idea is that $L_\kappa \vDash ZFC$, the condensation lemma itself is a theorem of ZFC(?), so we can just apply condensation lemma inside L_κ.

The problem is that our condensation lemma is a theorem of ZFC+IC instead of ZFC.

Remark. So if you assume ZFC+2IC in M, then this argument gets you that L_κ (where κ should be the second inaccessible cardinal now) is a model of CH, and you're actually done provided that you think 2IC is a reasonable thing to have.

But this feels a bit odd. Let's try to do this without 2IC.

Work in L_κ, we know that $\mathcal{P}^{L_\kappa}(\mathbb{N}) \subseteq L_{\omega_1}$, where ω_1 is the ω_1 in M.
Note that $\omega_1 < \kappa$, so in particular $L_{\omega_1} \subseteq L_\kappa$.

Now we could build $\mathcal{H}^{L_\kappa}(L_{\omega_1}) \prec L_\kappa$, and $\mathcal{P}^{L_\kappa}(\mathbb{N}) \subseteq L_\beta = T \cong \mathcal{H}^{L_\kappa}(L_{\omega_1})$. By the standard argument we know $\beta < \aleph_2 < \kappa$. But now $L_\beta \vDash ZFC + V = L$.

Run the condensation lemma proof for V_κ as M and L_β as L_κ, we then get

$$y \in L_\alpha = T \cong \mathcal{H}^{L_\beta}(\mathbb{N} \cup \{y\}) \prec L_\beta$$

Now the surrounding universe knows that α is countable, so L_κ knows α is countable. So if $\omega_1^{L_\kappa}$ is the ω_1 of L_κ, then $\mathcal{P}^{L_\kappa}(\mathbb{N}) \subseteq L_{\omega_1^{L_\kappa}}$.
So $L_\kappa \vDash 2^{\aleph_0} \leq \aleph_1$, i.e. $L_\kappa \vDash CH$. So we've proved:

Theorem.

$$Cons(ZFC + IC) \implies Cons(ZFC + CH)$$

Remark. (1) The same argument with $x = \lambda$ for some L_κ-cardinal λ gives us $L_\kappa \vDash 2^\lambda \leq \lambda^+$. So GCH holds: $\forall \lambda 2^\lambda = \lambda^+$.
(2) What about the inaccessible cardinal?
(a) If we have a transitive set model of ZFC, we can mimic this proof. Nevertheless we knew it was still stronger than $Cons(ZFC)$.
(b) There is a way of getting around that assumption as well by Lévy Reflection Theorem (see sheet 2): fix in advance some finite list Φ of sentences you wish to preserve, and find sufficiently large α s.t. Φ is absolute for V_α.
Go through all needed absoluteness results and lemmas and theorems, and collect, for each of them, φ, the finite set Φ_φ of axioms of ZFC we needed to prove them. Form $\Phi := \bigcup_{\varphi \text{ is relevant}} \Phi_\varphi$, which is a finite union of finitely many things. Apply Lévy to Φ and run the previous proof to get a model of $\Phi + CH$. Now consider all finite subsets Ψ s.t. $\Phi \subseteq \Psi \subseteq ZFC$, and get models of $\Psi + CH$. Compactness then gives a model of $ZFC + CH$.
(3) Consider

$$L = \bigcup_{\alpha \in Ord} L_\alpha \subseteq M$$

Our proof does not say what axioms hold in L, but using the Lévy reflection theorem, we can prove that if $V \vDash ZFC$, then $L \vDash ZFC + V = L$.

Now let's use this to solve one of the open problems in the 1910s, which follows as an almost trivial consequence of what we've done.

Consider the question about regular limit cardinals. Remember we had notions of regular/singular, successor/limit. We realize that we can prove that every successor cardinal is regular, and we have a lot of singular limit cardinals. So can we get regular limit cardinals?

If we strengthen 'limit'($\forall \lambda < \kappa(\lambda^+ < \kappa)$) to 'strong limit'($\forall \lambda < \kappa(2^\lambda < \kappa)$), then we showed that ZFC cannot prove the existence of regular strong limits (i.e. inaccessible cardinals).

Clearly, ZFC+GCH implies that every limit is a strong limit (because $\lambda^+ = 2^\lambda$). So ZFC+CH gives every regular limit is an inaccessible cardinal.

Proof. Assume that $M \vDash ZFC$ and that $ZFC \vdash$ there are regular limits. Towards a contradiction (with Gödel's incompleteness theorem), prove $M \vDash Cons(ZFC)$.
Consider $L \subset M$, by remark (3), $L \vDash ZFC + GCH$. By assumption, $ZFC \vdash \exists$ regular limit, so $L \vDash ZFC + GCH + (\exists \kappa \ \kappa$ is a regular limit). But ZFC+GCH implies every regular limit is inaccessible, so $L \vDash ZFC + IC$. So $L \vDash \exists \kappa(L_\kappa \vDash ZFC)$, so $L \vDash Cons(ZFC)$; so $M \vDash Cons(ZFC)$ by absoluteness between transitive models. □

2 Construction of the generic model

2.1 Limitation of methods of inner models

—Lecture 13—

Sorry for the forced break on Friday – we'll see if we can manage with 23 lectures; if not we'll have to have an additional one at the end of term.

Last time we gave the impression that we're at a breaking point between the first and the second part of the course (CH and $\neg CH$); but that's not entirely true. Today we'll try to understand the difficulty and limitations of our previous method of inner models.

Definition. If $(M, \in) \vDash ZFC$, $N \subseteq M$, we say that N *is an inner model of M* if:
(a) $(N, \in) \vDash ZFC$;
(b) $Ord \cap N = Ord \cap M$ (not always needed, but this is usually the standard requirement in literature);
(c) N is transitive in M.

Let's rephrase some things that we've learnt about L. We have the following theorem:

Theorem. (Minimality theorem)
If $M \vDash ZFC + (V = L)$, and N is an inner model, of M, then $N = M$.
In other words, L has no non-trivial inner models.

Proof. We know that $M = \bigcup_{\alpha \in Ord \cap M} L_\alpha^M$ (L_α interpreted in M, which doesn't really matter because of absoluteness); this follows directly from $V = L$ in M. So in order to show $N = M$, it's enough to show $L_\alpha^M \subseteq N$ for all $\alpha \in Ord \cap M$. But $L_\alpha^N \subseteq N$ for $\alpha \in Ord \cap N$, but then by absoluteness $L_\alpha^N = L_\alpha^M$; then by requirement (b) we're done. $\square$

Remark. (1) If we drop (b), we still get that $N = L_\Omega^M$ where $\Omega = Ord \cap N$; so we get a smaller model not because it's *narrower*, but only because it's *shorter*.
(2) We don't need full ZFC for this: similar results hold for considerably weaker theories.

Now, what do we mean by the *technique* of inner models? An application of the technique would mean: we want to show $Cons(ZFC + \varphi)$; start with $M \vDash ZFC + \neg\varphi$; go to an inner model $N \subseteq M$ where $N \vDash ZFC + \varphi$. A limitation would mean that this is not possible (while, not quite; it *is* always possible in some way, say by going to a larger model where φ fails and then going back).

Definition. A *definable inner model* is an $L_\in$-formula φ with one free variable, with the property: if $(M, \in) \vDash ZFC$, then define

$$N := \{x \in M : M \vDash \Phi(x)\}$$

Then we call N an inner model of M.

Of course we have an example, L, in the sense that we can use the formula $\Phi(x) \leftrightarrow \exists\alpha(x \in L_\alpha)$.

Now we can define what we mean by *the consistency of φ can be shown by inner models*.

This means we find an inner model φ s.t. for all $M \vDash ZFC$, and $N := \{x \in M, M \vDash \Phi(x)\}$, then $N \vDash ZFC + \varphi$.

Corollary. There is no inner model proof of the consistency proof of $\neg CH$.

Proof. Suppose otherwise, so let Φ be an inner model that proves $Cons(ZFC + \neg CH)$. Take an arbitrary $M \vDash ZFC$. Build L^M, and form $N^* := \{x \in L^M : L^m \vDash \Phi(x)\}$. By minimality theorem, $N^* = L^M$. So $N^* \vDash \neg CH$ by assumption; but also $N^* \vDash CH$ because it's L. Contradiction. $\qquad\square$

2.2 Basic terminologies of forcing

So instead we consider *outer models*, nowadays more often known as *forcing*.

Let's do some illustration first: let L be the language of arithmetic with symbols $+, \cdot, 0, 1$; let Fld denote the axioms for fields; and let Φ_0 denote the formula specifying a field have characteristic 0; and of course use $Fld_0 := Fld + \Phi_0$ (field of characteristic zero).
From algebra we know each characteristic has a prime field (in this case, $\mathbb{Q}$). The method of inner model here would be (something like) subfields. $\mathbb{Q}$ is minimal in the sense that it has no proper subfields.

Now let's consider something that is true in $\mathbb{Q}$ but might be false somewhere else. Maybe let's have the axiom

$$NSRT := \forall x(x \cdot x \neq 1 + 1)$$

(a great name for the axiom *no square root of two*). Then $\mathbb{Q} \vDash NSRT$. In analogy to the discussion of inner models before, the technique of submodels cannot show $Cons(Fld_0 + \neg NSRT)$. So we instead add some weird $X \notin \mathbb{Q}$ (from the surrounding meta-universe), and *assume* that $X^2 = 2$. Obviously we can't just take $\mathbb{Q} \cup \{X\}$ as that won't satisfy axioms of Fld_0. So we need $X + X, X + X + X, qX, X^3, \ldots$. In algebra we had various techniques that allowed us to do constructions and obtain $\mathbb{Q}(X) \vDash Fld_0 + \neg NSRT$.

We've seen how the above illustration works to prove $Cons(Fld_0 + \neg NSRT)$. Why not just do the same for CH? Assume $M \vDash ZFC + CH$, and further more assume M is countable and transitive (by the usual L-S and then Mostowski collapse trick). So all of its elements are countable, i.e. $\mathbb{R}^M, \aleph_1^M, \aleph_2^M, \ldots$ in M are all countable (in M). So there are lots of (uncountably many) reals not in M.

In particular (since $\aleph_2^M$ is countable (in M) as well, we could have an injection $i : \aleph_2^M \to \mathbb{R}$ s.t. the range of i is completely outside M, i.e. $ran(i) \cap M = \phi$.

Now form: $M(i)$, the smallest ZFC models containing M as a subset, i as an element (let's assume we have some way to do that). Then $M(i) \vDash ZFC + |\mathbb{R}| \geq |\aleph_2^M|$.

This looks really like $\neg CH$; unfortunately, $\neg CH$ would require $|\mathbb{R}| \geq |\aleph_2^{M(i)}|$. Note that the property of being a cardinal is only downward absolute, so both $\aleph_1^M$ and $\aleph_2^M$ might lose the property of being a cardinal when we move to $M(i)$. So we definitely want both of them to be preserved as cardinals: if either of them is not a cardinal then at best we get an unimpressive result that $|\mathbb{R}| \geq |\aleph_1^{M(i)}|$. So we need $\aleph_1^M = \aleph_1^{M(i)}$ and $\aleph_2^M = \aleph_2^{M(i)}$ in order to prove $\neg CH$.

Let's summarize our proof components:
(1) Find a construction of transitive $M(i) \vDash ZFC$;
(2) Preservation theorems for cardinals;
We've only seen one preservation theorem (in sheet 1): $\mathbb{R}^M = \mathbb{R}^N \implies \aleph_1^M = \aleph_1^N$. But this is pointless now, as the whole point of our attempt is to add new reals.
Also, there's no chance that our general attempt above would work for any injection i: if x codes a well-order on $\mathbb{N}$ of order type $\aleph_1^M$, and $i(j) = x$, then $M(i) \vDash \aleph_1^M$ is countable; so we really need to be more careful when specifying which i we want (on lecture 14, a different phrased version: if $x \in ran(i)$, then $X \in M[i]$; if x is a code for the countability of $\aleph_1^M$, then $M[i] \nvDash \aleph_2^{M[i]} = \aleph_2^M$).

—Lecture 14—

Even worse, if such an x can be constructed in ZFC from i, then it will be in $M[i]$. So we need to guarantee that no such objects can be constructed.

Let's introduce some vocabularies. As usual, we call $(\mathbb{P}, \leq, 1)$ a *partial order* (in the theory of forcing, this is sometimes also called a *forcing/forcing partial order*) if $\mathbb{P}$ is a set, $\leq$ is a reflexive, transitive, antisymmetric relation, and 1 is the largest element. Elements of $\mathbb{P}$ are called *conditions*; if $p \leq q$, we say *p is stronger than q*.[1]
As usual, $C \subseteq \mathbb{P}$ is called a *chain* if $(C, \leq)$ is a total order. If $p, q \in \mathbb{P}$, say that p and q are *incompatible* ($p \perp q$) if there is no $r \leq p, r \leq q$.
$A \subseteq \mathbb{P}$ is called *antichain* if $\forall p, q \in A, p \neq q \to p \perp q$.
We say that $\mathbb{P}$ has the countable chain condition (ccc) if every *antichain* in $\mathbb{P}$ is countable.
If $D \subseteq \mathbb{P}$, we say D is *dense* if $\forall p \in \mathbb{P} \, \exists q \in D \, q \leq p$.
If $F \subseteq \mathbb{P}$, we say F is a *filter* if
(a) $\forall p \in F \forall q (q \geq p \to q \in F)$;
(b) $\forall p, q \in F \exists r \in F \, r \leq p, q$.

---

[1] This is the standard convention; in Jerusalem there are attempts to revert the order of partial order, so we have a minimum element 0 and $\geq$ means stronger. Unfortunately, this hasn't helped literature: the group in Jerusalem has considerable size of population, so now there are two opposing set of conventions being used in literature. In particular, if you read a paper, you have to first find out which set of conventions is used before anything could make sense.

We say $\mathbb{P}$ is *splitting* if for all $p \in \mathbb{P}$, $\exists q_1, q_2 \in \mathbb{P}$, $q_1, q_2 \leq p$ and $q_1 \perp q_2$.

If $\mathcal{D}$ is a set of dense sets and $G \subseteq \mathbb{P}$, we say G is $\mathcal{D}$-*generic* if $\forall D \in \mathcal{D}$, $(D \cap G \neq \phi)$.

Example. (1, Cohen forcing)

Let $\mathbb{P} := \{p : p \text{ is a partial function from } \mathbb{N} \text{ to } 2 \text{ with finite domain}\}$. Define $p \leq q \iff p \supseteq q$ (so domain of p covers domain of q and they agree on domain of q). Of course here 1 is the empty function.

If $p \perp q$, then there is $n \in dom(p) \cap dom(q)$ s.t. $p(n) \neq q(n)$.

If F is a filter in $\mathbb{P}$, then $\bigcup F$ is a partial function from $\mathbb{N}$ into 2 (think very carefully).

Consider $D_n := \{p : n \in dom(p)\}$. This is a dense set for every n: given any q, if q is defined on n then it's already in D_n; else we could just define it in n (by any value) and get an element in D_n that is stronger than it. Now define $\mathcal{D} := \{D_n : n \in \mathbb{N}\}$. If F is $\mathcal{D}$-generic, then $\bigcup F : \mathbb{N} \to 2$ is a total function. Note that in this way we could have defined the real numbers.

Example. (2)

Let $\mathbb{P}_X := \{p : p \text{ is a partial function from } \mathbb{N} \text{ to } X \text{ with finite domain}\}$, where X is any set.

As before: if F is a filter, $\bigcup F$ is a partial function; if F is $\mathcal{D}$-generic, $\bigcup F : \mathbb{N} \to X$ is a total function.

Let's add some more dense sets: consider $E_X := \{p : x \in ran(p)\}$ for every $x \in X$ (in some sense the dual to D_n). Let $\mathcal{D}^* := \mathcal{D} \cup \{E_x : x \in X\}$.

Suppose G is $\mathcal{D}^*$-generic filter. So in particular $\bigcup G$ is a total function $\mathbb{N} \to X$. But now for every $x \in X$, $E_x \cap G \neq \phi$. So there's some $p \in G$ with $x \in ran(p)$. So $\bigcup G$ is a surjection $\mathbb{N} \to X$. Therefore G cannot exist for uncountable X.

If M is a transitive model of ZFC, and $\mathbb{P} \in M$ is a partial order, we say that a filter G (not necessarily an element of M) is *generic over M*, if it is $\mathcal{D}$-generic for $\mathcal{D} := \{D \in M : D \text{ is dense in } \mathbb{P}\}$.

Lemma. Suppose $\mathbb{P}$ is splitting, $\mathbb{P} \in M$ and M is a transitive model of ZFC. Suppose G is $\mathbb{P}$-generic filter over M. Then $G \notin M$.

This is exactly what we've seen in example 2 above.

Proof. Suppose $G \in M$. Then $D = \mathbb{P} \setminus G \in M$. We claim that D is dens. Take $p \in \mathbb{P}$ arbitrary. By splitting, find $q_1, q_2 \leq p$, $q_1 \perp q_2$. So q_1, q_2 cannot be both in G because G is a filter. So by definition $G \cap D = G \cap \mathbb{P} \setminus G \neq \phi$, contradiction. $\square$

—Lecture 15—

Last time we had the notion of $\mathbb{P}$ being a filter, being $\mathcal{D}$-generic, being $\mathbb{P}$-generic over M, and being splitting. We also proved a lemma that if M is a transitive model of ZFC, $\mathbb{P} \in M$, G a $\mathbb{P}$-generic filter of M, $\mathbb{P}$ splitting, then $G \notin M$. We looked at two examples (one of them is a special example of another).

Lemma. If $\mathcal{D}$ is countable set of dense sets, $p \in \mathbb{P}$, then there is a $\mathcal{D}$-generic filter G over $\mathbb{P}$ s.t. $p \in G$.

Proof. Let $\mathcal{D} = \{D_n : n \in \mathbb{N}\}$. Define recursively:
• $p_0 := p$;
Suppose $p_0 \geq p_1 \geq ... \geq p_n$ are already defined. By definition, D_n has an element q s.t. $q \in D_n, q \leq p_n$, and set $p_{n+1} := q$.
Now consider $X := \{p_n : n \in \mathbb{N}\} \subseteq \mathbb{P}$. Note that if $p_n, p_k \in X$, then $p_{\max(n,k)} \leq p_n, p_k$. So this does generate a filter

$$G := \{p : \exists n p_n \leq p\}$$

which clearly intersect D_n non-trivially for each n. $\qquad\square$

Corollary. If M is a countable transitive model of set theory, $p \in \mathbb{P} \in M$, then there is a $\mathbb{P}$-generic filter G over M with $p \in G$.

Proof. If $\mathbb{P} \in M$, then $\mathbb{P}$ is countable. Now look at

$$\{D \subseteq \mathbb{P} : D \text{ is dense}, D \in M\} \subseteq \mathcal{P}^M(\mathbb{P})$$

the nth power set of $\mathbb{P}$. So this is countable as well. $\qquad\square$

2.3 Forcing language

Fix M a transitive model of set theory, with a partial order $\mathbb{P}$. Define
• $Name_0(M, \mathbb{P}) = \phi$;
• for $\lambda > 0$, set $Name_\lambda(M, \mathbb{P})$ to be

$\{\tau : \text{ each element of } \tau \text{ is an ordered pair } (\sigma, p), \sigma \in Name_\alpha(M, \mathbb{P}) \text{ for some } \alpha < \lambda, p \in \mathbb{P}\}$

The elements of

$$M^{\mathbb{P}} := \bigcup_{\lambda \in Ord \cap M} Name_\lambda(M, \mathbb{P})$$

are called $\mathbb{P}$-names.

Example. The most basic example is $\mathbb{P} = \{1\}$. We can see that ϕ is a name (at the first level), $\{(\phi, 1)\}$ is a name (which in some sense represents $\{\phi\}$), etc. This results in (an isomorphic copy) of the von Neumann hierarchy inside M.

Example. Another basic example is $\mathbb{P} = \{1, L, R\}$, where $L \leq 1$ and $R \leq 1$. The dense sets are $\{1, L, R\}$ and $\{L, R\}$.
What are filters? Filters are closed upwards and do not contain anything incompatible. There are exactly one pair of incompatible things, namely L, R. So the filters are $\{1\}, \{1, L\}$ and $\{1, R\}$.
What are generic filters? $\{1\}$ doesn't intersect $\{L, R\}$, so only the other two are generic filters.

For names, ϕ is a name at the first level; at the next level we have $(\phi, 1)$, (ϕ, L) and (ϕ, R); at the next level we have $\{(\phi, 1)\}, \{(\phi, L)\}, \{(\phi, R)\}, \{(\phi, 1), (\phi, L)\}, \{(\phi, 1), (\phi, R)\}, \{(\phi, L), (\phi, R)\}, \{(\phi, 1), (\phi, R), (\phi, L)\}$.

Interpretation of names: let $\mathbb{P}, M$ be as before, and let G be $\mathbb{P}$-generic over M (the definition actually makes sense for any $G \subseteq P$).
If $\tau \in Name(M, \mathbb{P})$, we define the G-value of τ

$$val(\tau, G) := \{val(\sigma, G) : \exists p \in G, (\sigma, p) \in \tau\}$$

Using this, we can now define $M[G] := \{val(\tau, G) : \tau \in Name(M, \mathbb{P})\}$.

Observation: if N is a transitive model of ZFC s.t. $M \subseteq N$, and $G \in N$, then $M[G] \subseteq N$. Also note that if we can prove $M[G] \vDash ZFC$, this would then be a minimality theorem.

Back to our previous example 2. We had 8 names there. Let's start with ϕ. What is $val(\phi, G)$? There are no elements of τ, so $val(\phi, G) = \phi$ and is completely independent of what G is. So at least the empty set has the correct name.
If τ is any of the other 7 names, and $(\sigma, p) \in \tau$, then $\sigma = \phi$ by our previous listing. So there are only two possibilities

$$val(\tau, G) = \left\{ \begin{array}{l} \phi \\ \{\phi\} = 1 \end{array} \right.$$

Of course, this now depends on which filter we choose. For convenience we set $\tau_L = \{(\phi, L)\}$ and $\tau_R = \{(\phi, R)\}$. Consider $G_L = \{1, L\}$ and $G_R = \{1, R\}$. Not entirely surprisingly we get

$$val(\tau_L, G_L) = \{\phi\}$$
$$val(\tau_L, G_R) = \phi$$

because $L \in G_L$ but $L \notin G_R$. The case is similar for $val(\tau_R, \cdot)$.
Note that even without specifying the filter, we know $val(\tau_L, G)$ is a subset of $\{\phi\} = 1$. There are only two subsets of 1, namely 0 and 1, and we need to specify the filter to know which one it is.
We see from this example that the name is not unique: in the model built by G_R, both ϕ and τ_L name ϕ. So in particular we cannot say something like 'take *the* name of something'.

Definition. Let $x \in M$. We define the *canonical name for x* by recursion:

$$\check{x} := \{(\check{y}, 1) : y \in x\} \in M$$

Proposition. For any G s.t. $1 \in G$, we have $val(\check{x}, G) = x$ (proof is by $\in$-induction).

Corollary. $M \subseteq M[G]$.

This should tell us what we want next: we want to show $G \in M[G]$. Note that all of the names are elements of M, so we can't do the same for G as it's not an element of M.

—Lecture 16—

Note: there is no canonical name for the generic filter G in M. It would be something like

$$'\check{G}' := \{(\check{p}, 1) : p \in G\}$$

Of course we can define this in the surrounding universe; but it is not a name in M. This 'name' has the property that $'\check{G}' \in N \iff G \in N$.

Last time we proved that if M is transitive, G is $\mathbb{P}$-generic over M, then $val(\check{x}, G) = x$. (For this, we do not need G to be $\mathbb{P}$-generic, but only $1 \in G$.)

As a consequence, we know $M \subseteq M[G]$.

Definition.

$$\Gamma := \{(\check{p}, p) : p \in \mathbb{P}\}$$

Lemma. $val(\Gamma, G) = G$.

Proof. Suppose $x \in val(\Gamma, G)$. By definition, $x = val(\check{p}, G)$ for some $p \in \mathbb{P}$ with $p \in G$. Then in fact $x = p$. So $x \in G$.

Suppose $x \in G$. Then $(\check{x}, x) \in \Gamma$. But $x \in G$, $x = val(\check{x}, G) \in val(\Gamma, G)$. So $x \in val(\Gamma, G)$. $\square$

Corollary. If M is transitive, then $G \in M[G]$.

Now both elements of M and G are in $M[G]$. But does $M[G]$ satisfy enough set theory?

Lemma. $M[G]$ is transitive.

Proof. To show: $x \in y \in M[G] \implies x \in M[G]$.

$y \in M[G]$ means $\exists \tau \; y = val(\tau, G)$.

$x \in y$ means $\exists \sigma, p, \; p \in G, \; (\sigma, p) \in \tau$ and $x = val(\sigma, G)$. Thus $x \in M[G]$. $\square$

Corollary. $M[G] \vDash$ Extensionality and Foundation.

Let's look at pairing: suppose $x, y \in M[G]$, and τ, σ evaluates to x, y respectively in G ($x = val(\tau, G)$, etc). Construct

$$\mu_{\sigma, \tau} := \{(\sigma, 1), (\tau, 1)\}$$

Now try to evaluate it: 1 is always in the filter G, so

$$val(\mu_{\sigma, \tau}, G) = \{val(\sigma, G), val(\tau, G)\}$$
$$= \{x, y\}$$

So

Proposition. $M[G] \vDash$ Pairing.

We'll stress again that the above name is not unique. For example, we could add any (σ, p) for $p \in G$, or any (μ, q) if $q \notin G$; also the choice of τ and σ is not unique.

On Sheet 3, we'll see Union; so as a corollary, since $\check{\omega} \in M^{\mathbb{P}}$, $val(\check{\omega}, G) = \omega$ we get $M[G] \vDash$ infinity.

Lemma. If $\tau \in M^{\mathbb{P}}$, then

$$\rho(val(\tau, G)) \leq \rho(\tau)$$

where ρ is the rank function.

Proof. Simple induction. $\square$

In particular, there can't be any new ordinals, as any new ordinal cannot have an existing rank. So

Corollary. $Ord \cap M = Ord \cap M[G]$.

How about power set? Let $x \in M[G]$. Take a name $\tau \in M^{\mathbb{P}}$ for it. Why not just take all the first components of elements of τ, and do it the same way as we did for pairing? The problem is that names are not unique; for example we could have $val(\sigma, G) = val(\bar{\sigma}, G)$, where $\bar{\sigma}$ doesn't occur in τ. Now $\{(\bar{\sigma}, p)\}$ *is* name of some subset of x, but we wouldn't know it from looking at τ. It would be nice to be able to talk about whether a name σ is a name for a subset if $val(\tau, G)$ without referring to the precise set-theoretic make-up of τ and σ.

2.4   Forcing Relation

We had *Forcing Language* on the board previously without saying what it actually is, so let's talk about it now. The forcing language is just $L_\in$ augmented with one constant symbol for each $\tau \in M^{\mathbb{P}}$.
If G is $\mathbb{P}$-generic over M, there is a canonical interpretation of $L(M^{\mathbb{P}})$ in $M[G]$

$$M[G] \vDash \varphi(\tau_1, ..., \tau_n) \iff M[G] \vDash \varphi(val(\tau_1, G), ..., val(\tau_n, G))$$

If φ is a sentence of $L(M^{\mathbb{P}})$, and $p \in \mathbb{P}$, then we say $p \Vdash \varphi$ (p forces φ in M): For every $\mathbb{P}$-generic filter G over M s.t. $p \in G$, $M[G] \vDash \varphi$.

Note that this looks to be helpful, but if we look carefully at it, it's entirely not obvious that this relation is even definable in M: we had *for every $\mathbb{P}$-generic filter G over M*, but we knew no such G is in M! However, we have:

Theorem. (Forcing theorem)
The following are equivalent:
(1) $M[G] \vDash \varphi$;
(2) $\exists p \in G(p \Vdash \varphi)$

Theorem. The forcing relation is definable in M, in the sense that:
There is a definable relation $p \Vdash^* \varphi$ s.t. $\forall p, \varphi, \, p \Vdash \varphi \iff p \Vdash^* \varphi$.

—Lecture 17—

Last time we defined what the forcing language $L(M^{\mathbb{P}})$ is and we had a forcing theorem about $M[G] \vDash \varphi$ where φ is a sentence in $L(M^{\mathbb{P}})$. However, there is a small lie here because φ uses G as a parameter, because

$$M[G] \vDash \varphi : \iff M[G] \vDash (val(\tau_1, G), ..., val(\tau_n, G))$$

Technically, the meaning of $M[G] \vDash \varphi$ does not just depend on $M[G]$ but on G as well. So our better notation should be $M[G], G \vDash \varphi$, or $(M, G) \vDash \varphi$.

We then used this to define the forcing relation $p \Vdash \varphi$. Again this is slightly inprecise as the meaning of this depends on the model: we should write $p \Vdash_M \varphi$, which means $\forall G \, p \in G \implies M[G] \vDash \varphi$.

However, $\Vdash$ is a priori not definable in M, since G is not; but we'll show that it is.

We shall give a different definition of a relation $p \Vdash^* \varphi$, which is definable in M, and we'll show that $p \Vdash^* \varphi$ iff $p \Vdash \varphi$.[2]

So let's write down the version of forcing theorem that we're going to prove, which is currently meaningless (as we haven't defined what $\Vdash^*$ is):

Theorem. (Forcing theorem)
Let M be a countable transitive model of set theory, and $\mathbb{P} \in M$. Let φ be a sentence in the forcing language $L(M^{\mathbb{P}})$. Let G be $\mathbb{P}$-generic over M. Then the following are equivalent:
(1) $M[G] \vDash \varphi$;
(2) There is a $p \in G$ s.t. $M \vDash (p \Vdash^* \varphi)$. [3]
Again note that we haven't defined $\Vdash^*$ yet.

Let's prove the equivalence of $\Vdash^*$ and $\Vdash$ from the forcing theorem.

Proposition. Let M be countable transitive model, $\mathbb{P} \in M$, $p \in \mathbb{P}$, φ a sentence of $L(M^{\mathbb{P}})$. Then

$$p \Vdash_M \varphi \iff M \vDash p \Vdash^* \varphi$$

It's a bit weird we're trying to prove something about things we haven't even defined, but of course we had a powerful theorem above.

Proof. Suppose $p \Vdash_M \varphi$. So for every G that is $\mathbb{P}$-generic over M with $p \in G$, we have $M[G] \vDash \varphi$. But now by forcing theorem (1) $\implies$ (2), we can find $q \in G$

---

[2]$\Vdash^*$ and $\Vdash$ are usually called the *syntactic* forcing relation and the *semantic* forcing relation.
[3]Lecturer restated this theorem in different ways for several times and decided on this final version, saying: *If you're wondering why I've been struggling with stating one of the most important theorems, the reason is that there are so many versions of it, and we need the right version for our induction to work later.*

s.t. $M \vDash q \Vdash^* \varphi$.

Let's consider the closure property of $\Vdash$:

(1) if $p \Vdash \varphi$ and $q \leq p$, then $q \Vdash \varphi$ (by property of filter).

(2) If $p \Vdash \varphi$ and $p \Vdash \psi$, then $p \Vdash \varphi \wedge \psi$ (just consider what $\Vdash$ means).

We know that $p, q \in G$, and G is a filter, so there is some $r \in G$ s.t. $r \leq p, q$. By property (1) we know that $r \Vdash \varphi$.

(stuck for a while) Ok, I may have to postpone this until we have actually defined $\Vdash^*$. As you may have noticed I was quite surprised when I realized I could have proved this without defining $\Vdash^*$, but it's good to know now that I was wrong. □

Nevertheless, the above attempt gives us some hints on what properties $\Vdash^*$ need to have: in particular it must make (1) and (2) work.

Definition. We say that D is *dense below p* if $\forall q \leq p \; \exists r \leq q, r \in D$.

Definition. (of $\Vdash^*$)

This will be by simultaneous recursion on the rank of the names involved and the complexity of φ.

Atomic formulas: (1) $\tau_1 \in \tau_2$; (2)$\tau_1 = \tau_2$ (remember these are constants in $L(M^{\mathbb{P}})$, so they are sentences);

(3) for φ, ψ we need to define for $\varphi \wedge \psi$;

(4) for φ we need to define for $\neg\varphi$;

(5) for φ we need for $\exists x \varphi$.

In this setting (1) and (2) are the hardest (after all, they are where the set theory lives in, as (3)-(5) are purely logic). We'll do the easy ones first: For (3) we have no choice due to property (1) in the above failed proof: $p \Vdash^* \varphi \wedge \psi$ iff $p \Vdash^* \varphi$ and $p \Vdash^* \psi$.

(4) $p \Vdash^* \neg\varphi$ iff $\forall q \leq p \; q \nVdash^* \varphi$. So instead of only requiring p to not force φ, we also require that it's not possible to force φ by anything stronger.

(5) $p \Vdash^* \exists x \varphi(x, \tau_1, ..., \tau_n)$ iff

$$\{r : \text{ there is a } \mathbb{P}\text{-name } \sigma \text{ s.t. } r \Vdash^* \varphi(\sigma, \tau_1, ..., \tau_n)\}$$

is dense below p – so for any $q \leq p$, we can extend q to some stronger r s.t. there is a name σ s.t. $r \Vdash^* \varphi(\sigma, \tau_1, ..., \tau_n)$.

These are the logical ones; let's now think about the set-theoretic ones.

(1) $p \Vdash^* \tau_1 \in \tau_2$. Note that this needs to depend on (2) because τ_1 and τ_2 may look very different from set theoretic perspective, but p may force some of the names to be equal. Now we have to be very careful because in defining (2) we may need (1) as well, and we can't do a cyclic definition. This is why we said we would use a simultaneous recursion on rank of names and complexity of φ: define $p \Vdash^* \tau_1 \in \tau_2$ iff

$$\{q : \text{ there is } (\pi, s) \in \tau_2 \text{ s.t. } q \leq s, q \Vdash^* \pi = \tau_1\}$$

is dense below p.

(2) $p \Vdash^* \tau_1 = \tau_2$: now we've already defined (1), if we're going to obtain a model of extensionality then we need to define $=$ in the only possible way as required by (1): $p \Vdash^* \tau_1 = \tau_2$ iff:

(α) for all $(\pi_1, s_1) \in \tau_1$,

$$\{q : q \leq s_1 \rightarrow \exists(\pi_2, s_2) \in \tau_2 \text{ s.t. } q \leq s_2 \text{ and } q \Vdash^* \pi_1 = \pi_2\}$$

is dense below p; and symmetrically,
(β) for all $(\pi_2, s_2) \in \tau_2$,

$$\{q : q \le s_2 \to \exists (\pi_1, s_1) \in \tau_1 \text{ s.t. } q \le s_1 \text{ and } q \Vdash^* \pi_1 = \pi_2\}$$

is dense below p.

Let's justify why this is a proper recursive definition. We start with (2). π_1 and π_2 have strictly lower ranks than τ_1 and τ_2, so (2) on itself is a recursive definition. And then there's no recursion involved in (1) as we've already defined (2), and (1) on itself doesn't depend on $\in$.

You might wonder how absolute these conditions are, because if you look at (1) and (2), of course all of these are bounded by p. So the definition on the atomic formulas are absolute and does not depend on M (?). Obviosuly (3) and (4) doesn't do anything; (5) is slightly trickier as it involves the use of $\mathbb{P}$-names; so if we have a bigger model, we might have more names that change the truth value of the forcing relation. So it's (5) that actually requires us to write things like $M \vDash p \Vdash^* \varphi$; in other words, (5) is the only source of non-absoluteness.

—Lecture 18—

We're going to start the proof of forcing theorem today, and hopefully finish by the end of next lecture.

On ES3 q23, we'll see that
(1) If D is dense below p and $r \le p$, then D is dense below r;
(2) If $\{r : D$ is dense below $r\}$ is dense below p, then D is dense below p.

Lemma. The following are equivalent:
(i) $p \Vdash^* \varphi$;
(ii) $\forall r \le p(r \Vdash^* \varphi)$;
(iii) $\{r : r \Vdash^* \varphi\}$ is dense below p.

Proof. Clearly (ii) $\implies$ (i) and (iii). So we need to show the other two directions.
(i) $\implies$ (ii): Proof by induction on the definition of $\Vdash^*$.
Remember that we had five parts of the recursion. Let's stick with the handout for notation, so we'll use the labelling: (a) $\tau_1 = \tau_2$; (b) $\tau_1 \in \tau_2$; (c) $\wedge$; (d) $\neg$; (e) $\exists$.
If we look at the five parts, we realize that (a),(b) and (e) are all defined by some sets being dense below p, in the sense that we defined $p \Vdash^* \varphi \iff X_\varphi$ is dense below p, where X_φ is some set depending on φ (note that although in defining X_φ we had '$q \le p$', but that's just for convenience, and the resulting set will still be dense below p if we omit the $\le p$ part). But by ES3 q23 we know if $r \le p$ and X_φ is dense below p, then X_φ is dense below r. For (c) and (d) it's obvious that (i) $\implies$ (ii) by definition.
Similarly, (iii) $\implies$ (ii) goes by recursion via (a) - (e) using item (2) of ex.(23) rather than item (1). $\qquad \square$

Corollary. $p \Vdash_M \varphi \iff M \vDash p \Vdash^* \varphi$.
(Assuming FT and lemma)

Proof. Assume $p \Vdash_M \varphi$. So for any G s.t. $p \in G$, $M[G] \vDash \varphi$.

FT gives that $\exists q \in G$ $M \vDash q \Vdash^* \varphi$.

We want to show that $p \Vdash^* \varphi$: by lemma, it suffices to show $D := \{r : r \Vdash^* \varphi\}$ is dense below p.

Fix any $q' \leq p$. Recall that we proved that for countable transitive model M, there is some H with $q' \in H$ and H is a $\mathbb{P}$-generic filter over M. Now $q' \leq p$, we know $p \in H$ as well. So by $p \Vdash_M \varphi$, we know $M[H] \vDash \varphi$.

Apply FT again, we know there is $q'' \in H$ s.t. $M \vDash q'' \Vdash^* \varphi$. But now $q'' \in D \cap H$. Since H is a filter, we find $r \leq q', q''$, $r \in H$. So r witnesses that D is dense below p.

The other direction is easier: assume that $M \vDash p \Vdash^* \varphi$. We want to show that $p \Vdash_M \varphi$. So let G be $\mathbb{P}$-generic over M with $p \in G$. But forcing theorem directly gives that $M[G] \vDash \varphi$. So $p \Vdash_M \varphi$. $\qquad\square$

Proof. (of FT)

Again there's only one way to prove it: $\Vdash^*$ is defined by recursion, so the only way FT could be proved is by doing induction on that recursion.

We'll prove this by induction on

(a) ranks of names,

(b) assumption that $=$ is done,

(c)-(e) complexity of formulas.

We'll do these in the order (c),(d),(e),(b),(a) (increasing difficulty).

Let's write down the induction hypothesis(IH): $M[G] \vDash \varphi \iff \exists p \in G$ $M \vDash p \Vdash^* \varphi$.

(c) assume IH holds for φ and ψ. Assume that $M[G] \vDash \varphi \wedge \psi$. So $M[G] \vDash \varphi$ and $M[G] \vDash \psi$. So by IH, there are $p, q \in G$ s.t. $p \Vdash^* \varphi$ and $q \Vdash^* \varphi$ (we're getting a bit lazy so we'll omit the $M \vDash$). But G is a filter, so $\exists r \leq p, q$ $r \in G$. But by lemma (i) $\implies$ (ii), $r \Vdash^* \varphi$ and $r \Vdash^* \psi$. So $r \Vdash^* \varphi \wedge \psi$.

Conversely, suppose we have a $p \in G$ s.t. $p \Vdash^* \varphi \wedge \psi$. So by definition, $p \Vdash^* \varphi$ and $p \Vdash^* \psi$. But by IH, any G that is a $\mathbb{P}$-generic filter over M will give $M[G] \vDash \varphi$ and $M[G] \vDash \psi$. So $M[G] \vDash \varphi \wedge \psi$.

(d) Let's assume IH for φ. Suppose $M[G] \vDash \neg\varphi$. Consider

$$D := \{p : p \Vdash^* \varphi \text{ or } p \Vdash^* \neg\varphi\}$$

We claim that D is dense, which is quite obvious from definition of $p \Vdash^* \neg\varphi$. So we find some $p \in D \cap G$ (which is non-empty since D is dense and G is $\mathbb{P}$-generic filter). If $p \Vdash^* \neg\varphi$ we're done by FT. So suppose $p \Vdash^* \varphi$. So by IH, $M[G] \vDash \varphi$. But we assumed $M[G] \vDash \neg\varphi$. Contradiction.

Conversely, suppose $p \Vdash^* \neg\varphi$. Suppose for contradiction that $M[G] \vDash \varphi$. So by IH we can find $q \in G$ that $q \Vdash^* \varphi$. But now we find $r \in G$ s.t. $r \leq p, q$. By lemma, $r \Vdash^* \varphi$ because $r \leq q$; but $p \Vdash^* \neg\varphi$, so by definition, $r \nVdash^* \varphi$. Contradiction.

(e) Suppose IH for $\varphi(\sigma/x)$, i.e. for any $\sigma \in M^{\mathbb{P}}$, we assume IH hold for the sentence obtained by substituting x with σ. Now suppose $M[G] \vDash \exists x \varphi(x)$. So there is $a \in M[G]$ s.t. $M[G] \vDash (\varphi(a/x))$. But elements of $M[G]$ are just names in $M^{\mathbb{P}}$, so there is $\sigma \in M^{\mathbb{P}}$ s.t. $M[G] \vDash (\sigma/x)$. So by IH, there is $p \in G$ s.t. $M \vDash p \Vdash^* \varphi(\sigma/x)$.

Now let's look at the definition to see what we need to prove. But then we

realized what we've proven is already stronger than definition: we've proved that the set

$$\{r : \exists \sigma \in M^{\mathbb{P}}(r \Vdash^* \varphi(\sigma, ...))\}$$

is not only dense below p, but is actually everything below p. So $p \Vdash^* \exists x \varphi$. This is a very nice point to stop as we've proved exactly half of FT: out of the five cases, we proved the first two and half of the third case. We'll continue next monday to finish the other half.*

—Lecture 19—

We were in the middle of the proof of FT: M is countable transitive model, $\mathbb{P} \in M$, G a $\mathbb{P}$-generic filter over M, φ a $L(M^{\mathbb{P}})$-sentence. The following are equivalent:
(i) $M[G] \vDash \varphi$;
(ii) $\exists p \in G \ M \vDash p \Vdash^* \varphi$.

We had five cases by induction, and we've proved (c),(d) and (e) $\implies$. Let's continue from there:

(e) $\Leftarrow$: Assume that $p \in G$, $p \Vdash^* \exists x \varphi$ (as before, we're suppressing $M \vDash$, but actually this is the only one case that it matters as we've discussed before – (e) is the only source of non-absoluteness. So maybe I should write $M \vDash$ here?). By definition,

$$D := \{r : \text{ there is } \sigma \text{ s.t. } r \Vdash^* \varphi(\sigma/x)\}$$

is dense below p.
We should set IH as: FT holds for each $\varphi(\sigma/x)$ for arbitrary names σ, as we only defined $M[G] \vDash \varphi$ for φ sentences.
Find $r \in D \cap G$ which exists since $p \in G$ and D is dense below p. Fix witness σ to the fact that $r \in D$, i.e. $r \Vdash^* \varphi(\sigma/x)$. By IH, $M[G] \vDash \varphi(\sigma/x)$ (which should actually mean $M[G] \vDash \varphi(val(\sigma, G)/x)$ in the usual model theoretic sense). So $M[G] \vDash \exists x \varphi$.

(b) $\Leftarrow$: Let $p \in G$ s.t. $p \Vdash^* \tau_1 \in \tau_2$. Note that in this case our IH should be FT for $=$ if we look at definition of (b),

$$D := \{q : \exists(\pi, s)\tau_2(q \leq s \wedge q \Vdash^* \pi = \tau_1)\}$$

is dense below p. By the same reason $D \cap G$ is non-empty, so pick $q \in D \cap G$. Fix $(\pi, s) \in \tau_2$ s.t. $q \leq s$ and $q \Vdash^* \pi = \tau_1$. Now

$$q \leq s \implies s \in G \implies val(\pi, G) \in val(\tau_2, G)$$

While

$$q \Vdash^* \pi = \tau_1 \stackrel{IH}{\implies} M[G] \vDash \pi = \tau_1 \implies val(\pi, G) = val(\tau_1, G)$$

So $val(\tau_1, G) \in val(\tau_2, G)$, i.e. $M[G] \vDash \tau_1 \in \tau_2$.

(b) $\implies$: $M[G] \vDash \tau_1 \in \tau_2 \implies val(\tau_1, G) \in val(\tau_2, G)$. Be very careful because this doesn't mean that τ_1 is the first component of some element of τ_2;

what we get from this is only that there is some $(\pi, s) \in \tau_2$ s.t. $s \in G$ and $val(\tau_1, G) = val(\pi, G)$. This gives $M[G] \vDash \tau_1 = \pi$. So by IH we find $r \in G$ s.t. $r \Vdash^* \pi = \tau_1$. Find $p \leq s, r, p \in G$ as it's a filter. Then

$$\{q \leq p : \exists(\bar{\pi}, \bar{s}) \in \tau_2(q \leq \bar{s} \wedge q \Vdash^* \bar{\pi} = \tau_1)\}$$

or even the smaller set

$$\{q \leq p : q \leq s \wedge q \Vdash^* \pi = \tau_1\}$$

is everything below p, so dense below p.

(a) This is the hardest part.
$\Leftarrow$: Fix $p \in G$ s.t. $p \Vdash^* \tau_1 = \tau_2$.
Our IH should be: FT for $=$ with names of lower rank. The form of the definition of $p \Vdash^* \tau_1 = \tau_2$ is symmetric in the sense that if we're using (α) to show that $val(\tau_1, G) \subseteq val(\tau_2, G)$, then (β) shows $val(\tau_2, G) \subseteq val(\tau_1, G)$.
So we'll show $val(\tau_1, G) \subseteq val(\tau_2, G)$.
Fix $x \in val(\tau_1, G)$. Fix a $(\pi_1, s_1) \in \tau_1$ s.t. $s_1 \in G$ and $val(\pi_1, G) = x$.
Now find $r \leq p, s_1$ with $r \in G$. By lemma, r still forces $\tau_1 = \tau_2$, so

$$D := \{q \leq r : q \leq s_1 \to \exists(\pi_2, s_2) \in \tau_2(q \leq s_2 \wedge q \Vdash^* \pi_1 = \pi_2)\}$$

is dense below r.
Find $q \in D \cap G$. $q \leq r$, $r \leq s_1$, so $q \leq s_1$. So the antecedent in the above set of D is true. So we can actually find $(\pi_2, s_2) \in \tau_2$ with $q \leq s_2$ and $q \Vdash^* \pi_1 \in \pi_2$.
Now

$$q \leq s_2 \implies s_2 \in G \implies val(\pi_2, G) \in val(\tau_2, G)$$

and

$$q \Vdash^* \pi_1 = \pi_2 \overset{IH}{\implies} M[G] \vDash \pi_1 = \pi_2 \implies val(\pi_1, G) = val(\pi_2, G)$$

So in the same fashion we get $x = val(\pi_1, G) \in val(\tau_2, G)$. The other half is symmetric.

(a) $\implies$: Assume $M[G] \vDash \tau_1 = \tau_2$. So $val(\tau_1, G) = val(\tau_2, G)$.
Consider the following set

$D := \{r : r \Vdash^* \tau_1 = \tau_2 \text{ (Case 1) or}$
$\qquad \exists(\pi_1, s_1) \in \tau_1(r \leq s_1 \wedge \forall(\pi_2, s_2) \in \tau_2 \forall q(q_2 \leq s_2 \wedge q \Vdash^* \pi_1 = \pi_2) \to q \perp r) \text{ (Case 2) or}$
$\qquad \exists(\pi_2, s_2) \in \tau_2(r \leq s_2 \wedge \forall(\pi_1, s_1) \in \tau_1 \forall q(q_1 \leq s_1 \wedge q \Vdash^* \pi_1 = \pi_2) \to q \perp r) \text{ (Case 3)}\}$

Observation: if $r \in G$, then neither case 2 nor case 3 can hold: by symmetry it's enough to deal with case 2 only: to prove this observation, suppose, towards a contradiction, that $r \in G$ and case 2 holds. Find $(\pi_1, s_1) \in \tau_1$ with the above desired (actually, undesired) properties. Since $r \leq s_1$, $s_1 \in G$. So $val(\pi_1, G) \in val(\tau_1, G) = val(\tau_2, G)$ by our assumption. But then there's some $(\pi_2, s_2) \in \tau_2$ with $s_2 \in G$ and $val(\pi_2, G) = val(\pi_1, G)$ by definition of $\in$.
Now we can use IH on $=$: find $q' \in G$ s.t. $q' \Vdash^* \pi_1 = \pi_2$.
Now find $q \leq r, s_1, s_2, q'$. But now case 2 says that if $q \leq s_2$ and $q \Vdash^* \pi_1 = \pi_2$,

then q has to be incompatible with r; but it isn't. Contradiction.
So we're done if we show that D is dense.
Fix $p \in \mathbb{P}$. If $p \Vdash^* \tau_1 = \tau_2$ then we're done. So assume it doesn't, then we'll find $r \leq p$ for case 2 or 3. Again by symmetry we'll show that if the failure of (α) is the reason for $p \not\Vdash^* \tau_1 = \tau_2$, then we can find r in case 2 in the definition of D. We'll do it on Wednesday because I think we need to do the detail of everything, although it's quite boring.

—Lecture 20—

We're stuck at the end of the proof of FT because the clock is probably 3 minutes faster (so lecture thought he didn't have enough time on Monday). We showed that if $p \in G$, then neither case 2 or 3 can hold. Thus if $p \in G \cap D$, then $p \Vdash^* \tau_1 = \tau_2$.
So we're left to show that D is dense.

Let $p \in \mathbb{P}$ be arbitrary. If $p \Vdash^* \tau_1 = \tau_2$ then we're done. So assume otherwise. We'll show that if (α) from definition of $\Vdash^* \tau_1 = \tau_2$ is violated, then we find $r \leq p$ s.t. Case (2) holds for r. As before the proof is symmetric, so failure of (β) can be done similarly.
So what does it mean for (α) to fail? (α) fails if there is $(\pi_1, s_1) \in \tau_1$ s.t. the set

$$D' := \{q \leq p : q \leq s_1 \to \exists (\pi_2, s_2) \in \tau_2 (q \leq s_2 \wedge q \Vdash^* \pi_1 = \pi_2)\}$$

is *not* dense below p.
Let's fix this $(\pi_1, s_1) \in \tau_1$, and fix $r \leq p$ s.t. D' has no element below r. So for every $q \leq r$,

$$q \leq s_1 \wedge \forall (\pi_2, s_2) \in \tau_2 (q \not\leq s_2 \vee q \not\Vdash^* \pi_1 = \pi_2) \; (***)$$

(just the negation of the implication).
In particular, this holds for r. So we know $r \leq s_1$.
Fix arbitrary $(\pi_2, s_2) \in \tau_2$ and q s.t. (the condition in case 2)

$$q \leq s_2 \wedge q \Vdash^* \pi_1 = \pi_2 \; (4*)$$

Now if q is compatible with r, find $q' \leq r$, q satisfying $(***)$ above. But now

$$q' \not\Vdash^* \pi_1 = \pi_2$$

by $(***)$ and $q \Vdash^* \pi_1 = \pi_2$ by $(4*)$ and $q' \leq q$. Contradiction.
So $q \perp r$, which is exactly what we want to show for Case 2. $\qquad\qquad\square$

We can now prove:

Theorem. (The Generic Model Theorem)
Let M be a countable transitive model of ZFC, $P \in M$, G is $\mathbb{P}$-generic over M, then $M[G] \vDash ZFC$.

Corollary. This shows that $M[G]$ is the minimal transitive model of ZFC with $M \subseteq M[G]$ and $G \in M[G]$.

Observe that if $M = L_\alpha$ for some countable α, and $L_\alpha(G)$ is the relativised L-construction as before, then by minimality of L (or $L(G)$ for models containing G), $M[G] = L_\alpha(G)$.

Proof. (of Generic Model Theorem)
We've already proved extensionality and foundation because $M[G]$ is transitive. We've seen pairing by constructing the name explicitly and proved union also by constructing names in sheet 3.
For infinity, by absoluteness of the formula '$x = \mathbb{N}$', we only need $\mathbb{N} \in M[G]$. But $\mathbb{N} = val(\check{\mathbb{N}}, G)$.
We have four axioms left: separation, replacement, power set, and choice. We'll do replacement and choice in sheet 4, so immediately we only have two left to do (how convenient).

Separation. fix a formula φ and parameters $x_1, ..., x_n \in M[G]$, and $x \in M[G]$ from which we separate. We want to give a name for the set

$$\{z \in x : M[G] \vDash \varphi(z, x_1, ..., x_n)\}$$

Fix names $\tau_1, ..., \tau_n$ for $x_1, ..., x_n$, and σ for x. So we want a name for

$$A := \{z \in val(\sigma, G) : M[G] \vDash \varphi(z, \tau_1, ..., \tau_n)\}$$

But of course we can't use FT directly because the formula to be forced above still contains a free variable z while the forcing relation is only defined for sentences. We need to consider

$$\rho := \{(\pi, p) : p \Vdash^* \pi \in \sigma \wedge \varphi(\pi, \tau_1, ..., \tau_n)\}$$

And we claim that $A = val(\rho, G)$.
$\supseteq$: Suppose $z \in val(\rho, G)$. There is $(\pi, p) \in \rho$ with $p \in G$ and $val(\pi, G) = z$. So $p \Vdash^* \pi \in \sigma \wedge \varphi(\pi, \tau_1, ..., \tau_n)$. By FT, we know

$$M[G] \vDash \pi \in \sigma \wedge \varphi(\pi, \tau_1, ..., \tau_n)$$

which translates to

$$M[G] \vDash z \in x \wedge \varphi(z, x_1, ..., x_n)$$

so $z \in A$.
$\subseteq$: Suppose $z \in A$. So $z \in x$ and $M[G] \vDash \varphi(z, x_1, ..., x_n)(*)$.
Fix π a name for z, so $z = val(\pi, G)$. We know $z \in x$, so FT gives that there is $p \in G$ s.t. $p \Vdash^* \pi \in \sigma$ ($z \in x$ is absolute). FT+$(*)$ gives that there is $q \in G$ s.t. $q \Vdash^* \varphi(\pi, \tau_1, ..., \tau_n)$.
Fix $r \leq p, q$, $r \in G$. Then

$$r \Vdash^* \pi \in \sigma \wedge \varphi(\pi, \tau_1, ..., \tau_n)$$

So by definition $(\pi, r) \in \rho$. But $r \in G$, so $z = val(\pi, G) \in val(\rho, G)$.

Power set. Since we have separation, it's enough to show that

$$\forall x \exists y \forall z (z \subseteq x \rightarrow z \in y)$$

because we can then separate the power set of x as a subset of y.
Fix a name σ for x. Let's write for any name τ:

$$dom(\tau) := \{\tau' : \exists p(\tau', p) \in \tau\}$$

(i.e. just take all the first component, like for functions). We think of names
for subsets of x as names whose domain are subsets of $dom(\sigma)$. Now define

$$\rho_\sigma := \{(\tau, 1) : dom(\tau) \subseteq dom(\sigma)\}$$

which collects every possible subset (plus some additional rubbish because some
of the p might not be in our generic filter G): to prove this, we're proving that
$\forall z(z \subseteq x \to z \in val(\rho_\sigma, G)$. So assume $z \subseteq x$. Fix a name μ for z, so
$val(\mu, G) = z$.
Now define

$$\mu^* := \{(\pi, p) : \pi \in dom(\sigma) \text{ and } p \Vdash^* \pi \in \mu\}$$

By definition, $dom(\mu^*) \subseteq dom(\sigma)$. So $(\mu^*, 1) \in \rho_\sigma$. In particular, $val(\mu^*, G) \in$
$val(\rho_\sigma, G)$. So need to show $val(\mu, G) = val(\mu^*, G)$: $w \in val(\mu, G) \implies$ we can
find $(\pi, p) \in \sigma$ with $p \in G$ s.t. $val(\pi, G) = w$ (since $val(\mu, G) \subseteq val(\sigma, G)$). So
$M[G] \vDash \pi \in \mu$. So by FT, we get some $q \in G$ s.t. $q \Vdash^* \pi \in \mu$. So $(\pi, q) \in \mu^*$.
As $q \in G$, we get $val(\pi, G) \in val(\mu^*, G)$. So $val(\mu, G) \subseteq val(\mu^*, G)$.
Conversely, suppose $w \in val(\mu^*, G)$. So find $(\pi, p) \in \mu^*$, $p \in G$ s.t. $w = val(\pi, G)$. By definition, we get that $p \Vdash^* \pi \in \mu$. By FT, $M[G] \vDash \pi \in \mu$. So
$w = val(\pi, G) \in val(\mu, G)$. $\qquad\square$

—Lecture 21—

As usual the printer didn't print the example sheets, but they're online now
(you can find them in the envelope at the usual place).

As the first step of proving consistency of $\neg CH$, we'll show that $V \neq L$ is
consistent.

Suppose M is a countable transitive model of $ZFC + V = L$. By our work on
L, we know that there is $\alpha < \omega_1$ s.t. $M = L_\alpha$. Take any partial order $\mathbb{P} \in L_\alpha$
that is splitting. By countability, we get G $\mathbb{P}$-generic over M and $G \notin M$ since
$\mathbb{P}$ is splitting. In particular, $M[G] \neq M$.

We claim that $M[G] \vDash V \neq L$: suppose otherwise, then by our previous theorem
we know $M[G] = L_\beta$ for some β. But we proved that M and $M[G]$ have the
same ordinals. So $\beta = \alpha$, i.e. $M = M[G]$. Contradiction.

Let's remind ourselves of the $\mathbb{P}$'s we had. Essentially we only had one so far:

$$\mathbb{P} = Fn(X, Y)$$

the set of partial functions from X to Y with finite domain, where $X, Y \in M$.
We proved that if G is $\mathbb{P}$-generic over M, then $\bigcup G =: f_G : X \to Y$ is surjective.
So if $X = \mathbb{N}$, then $M[G] \vDash Y$ is countable. In particular, if $Y = \aleph_1^M$, which

is clearly uncountable in M, then forcing with $Fn(\mathbb{N}, \aleph_1^M)$ will *collapse* $\aleph_1^M$: $M[G] \vDash \aleph_1^M$ is a countable ordinal.

Excursion on forcing a model of CH: Suppose $M \vDash 2^{\aleph_0} = \aleph_2$ and $\mathbb{P} = Fn(\mathbb{N}, \aleph_1^M)$. (diagram)
If $\aleph_1^M$ is no longer a cardinal in $M[G]$, then the original bijection $f : \mathbb{R}^M \to \aleph_2^M$ will be a bijection between $\mathbb{R}^M$ and an ordinal which can be *at best* $\aleph_1^{M[G]}$.

Since $\aleph_1^M < \aleph_1^{M[G]}$, we know $\mathbb{R}^{M[G]} \supsetneq \mathbb{R}^M$ (sheet 1 Q10).

In order to make this into a proof of $M[G] \vDash CH$, we need two things:
(1) $M[G] \vDash \aleph_2^M$ is a cardinal $\implies M[G] \vDash \aleph_2^M = \aleph_1$;
(2) $M[G] \vDash |\mathbb{R}| = |\mathbb{R}^M|$.

But of course we've already proved there is a model for CH, so maybe we don't need to use forcing to force a model; but if we had the two above we get a consistency proof of $ZFC + CH + V \neq L$.

Back to forcing $\neg CH$: instead, take $\mathbb{P} := Fn(\mathbb{N} \times \aleph_2^M, \mathbb{N})$. It's also splitting, and if G is a $\mathbb{P}$-generic filter then it gives a surjection $f_G := \bigcup G : \mathbb{N} \times \aleph_2^M \to \mathbb{N}$. Define in $M[G]$ for $\alpha < \aleph_2^M$,

$$f_\alpha(n) := f(n, \alpha)$$

So f_α is a function $\mathbb{N} \to \mathbb{N}$. We'll show that if $\alpha \neq \beta$, then $f_\alpha \neq f_\beta$. In particular, the map

$$\alpha \to f_\alpha$$

gives an injection from $\aleph_2^M$ to $\mathbb{N}^{\mathbb{N}}$. In particular, $M[G] \vDash |\aleph_2^M| \leq 2^{\aleph_0}$.

Proof of injection. Fix $\alpha \neq \beta$, and define

$$D_{\alpha,\beta} := \{p \in \mathbb{P} : \exists n \in \mathbb{N} \ p(n, \alpha) \neq p(n, \beta)\}$$

We claim that $D_{\alpha,\beta}$ is dense: fix $p \in \mathbb{P}$ arbitrarily. Then $dom(p)$ is finite, so we can find $n \in \mathbb{N}$ s.t. both (n, α) and $(n, \beta) \notin dom(p)$. Now define

$$q := p \cup \{((n, \alpha), 0), ((n, \beta), 1)\}$$

So $q(n, \alpha) \neq q(n, \beta)$. So $q \leq p$ and $q \in D_{\alpha,\beta}$.
So we can find $p \in G \cap D_{\alpha,\beta}$. Then $f_G = \bigcup G$ with $p \in G$, so there is n s.t. $f_G(n, \alpha) \neq f_G(n, \beta)$. So $f_\alpha(n) \neq f_\beta(n)$, i.e. $f_\alpha \neq f_\beta$.

To summarise, if G is $Fn(\mathbb{N} \times \aleph_2^M, \mathbb{N})$-generic over M, then $M[G] \vDash 2^{\aleph_0} \geq |\aleph_2^M|$.

We need, therefore, that $\aleph_1^M = \aleph_1^{M[G]}$ and $\aleph_2^M = \aleph_2^{M[G]}$ in order to get $M[G] \vDash 2^{\aleph} \geq \aleph_2$. So if we could prove that this forcing preserves these two cardinals, then we have constructed a model of $\neg CH$.

Definition. Let M countable transitive model, $\mathbb{P} \in M$. We say that $\mathbb{P}$ *preserves cardinals* if for all α ordinals and all P-generic filters G over M, we have

$$M \vDash \alpha \text{ is a cardinal} \iff M[G] \vDash \alpha \text{ is a cardinal}$$

Note that $\Leftarrow$ is always true since $M \subseteq M[G]$, and the property 'is a cardinal' is Π_1 so downward absolute.

Theorem. If $M \vDash \mathbb{P}$ has the ccc, then $\mathbb{P}$ preserves cardinals.
Remember from Sheet 3 we know if Y is countable, then $\mathbb{P} = Fn(X, Y)$ has the ccc (in ZFC). Certainly $\mathbb{N}$ is countable in any model. So $Fn(\mathbb{N} \times \aleph_2^M, \mathbb{N})$ has ccc in every model M of ZFC.

Putting these together, we get that $\aleph_1^M$ and $\aleph_2^M$ are cardinals in $M[G]$, and nothing else between them can be a cardinal since 'being a cardinal' is Π_1, so $\aleph_1^{M[G]} = \aleph_1^M$ and $\aleph_2^{M[G]} = \aleph_2^M$.

Corollary. With $\mathbb{P}, G, M$ as above, $M[G] \vDash \neg CH$.

Corollary. If M is a countable transitive model of ZFC, then there is $M[G] \vDash ZFC + \neg CH$ countable transitive.

So we now need to prove the theorem above. We'll need a technical lemma:

Lemma. Suppose $M \vDash \mathbb{P}$ has ccc, $A, B \in M$, $f : A \to B$, $f \in M[G]$. Then there is a function $F \in M$ with
(a) $dom(F) = A$;
(b) $\forall a \in A \; F(a) \subseteq B$;
(c) $\forall a \in A \; M \vDash F(a)$ is countable;
(d) $\forall a \in A \; f(a) \in F(a)$.

So in some sense we can *approximate* f by giving some F above and say that $f(a)$ is one of those countably many values in $F(a)$.

Proof of theorem from lemma. Suppose $M \vDash \lambda$ is a cardinal, $M[G] \vDash \lambda$ is not carinal. So $M[G] \vDash \exists \gamma < \lambda \; \exists f$ bijection, $f : \gamma \to \lambda$. Now apply the lemma with $A = \gamma$, $B = \lambda$, $f = f$. We then get an $F \in M$ with those properties. Since f is surjective, $\lambda = \bigcup_{\alpha < \gamma} F(\alpha)$. But $\gamma < \lambda$ and each of $F(\alpha)$ is countable, so $M \vDash |\lambda| \leq |\omega \times \gamma| < \lambda$, contradiction.

So we only need to prove the lemma. We'll do it on Monday.

—Lecture 22—

Remember that our ultimate goal is to prove that CH is independent from ZFC. We had the partial order

$$\mathbb{P} := \{p : p \text{ is a partial function from } \aleph_2^M \times \mathbb{N} \to \mathbb{N}, |dom(p)| < \omega\}$$

We've seen that if G is $\mathbb{P}$-generic over M, then in $M[G]$ there is an injection from $\aleph_2^M$ into $\mathbb{R}$. If $\aleph_1^M = \aleph_1^{M[G]}$ and $\aleph_2^M = \aleph_2^{M[G]}$, then $M[G] \vDash 2^{\aleph_0} \geq \aleph_2$.

We had a theorem that if $M \vDash \mathbb{P}$ has ccc, then $\mathbb{P}$ preserves cardinal. On sheet 3 we actually checked that $M \vDash \mathbb{P}$ has ccc, so we're done if we could prove the theorem. We've also reduced the theorem to the last lemma we stated in the previous lecture.

Proof. (of lemma.)

Fix a name τ for f. Let $\tau : \check{A} \to \check{B}$ be the sentence in the forcing language that expresses 'τ is a function from $\check{A}$ to $\check{B}$'. By FT, we can find $p \in G$ s.t. $p \Vdash \tau : \check{A} \to \check{B}$. We now define

$$F(a) := \{b \in B : \exists q \leq p(q \Vdash \tau(\check{a}) = \check{b}\}$$

where by $\tau(\check{a}) = \check{b}$, we really mean the sentence in the forcing language that expresses 'the value of τ at $\check{a}$ is $\check{b}$'.

Let's now check the properties:

(a) and (b) are trivial by our definition of F. For (d), let $\bar{b} := f(a) \in B$. Then $M[G] \vDash \bar{b} = f(a)$, i.e. $\tau(\check{a}) = \check{\bar{b}}$. By FT we find $q \in G$ s.t. $q \Vdash \tau(\check{a}) = \check{\bar{b}}$. Since G is a filter, we find $q' \leq q, p$, $q' \in G$. But now q' witnesses that $f(a) = \bar{b} \in F(a)$. For (c), if we pick, for each $b \in F(a)$, a q_b witnessing that $b \in F(a)$, i.e. $q_b \Vdash \tau(\check{a}) = \check{b}$, then if $b \neq b'$ then $q_b \perp q_{b'}$. Thus the set

$$\{q_b : b \in F(a)\}$$

is an antichain in $\mathbb{P}$. So we know it's countable in M by ccc. So $F(a)$ is countable in M. $\square$

So in some sense we've achieved the goal of this course. Let's spend some time to spell this out because this is an important moment:

Corollary. If there is a transitive set model of ZFC, then there is:
(a) a transitive set model of $ZFC + CH$;
(b) a transitive set model of $ZFC + \neg CH$.

We're not yet finished because there are still 1.5 lectures to go. A natrual question is to ask: if we have a model of $ZFC + \neg CH$, then what is the size of $2^{\aleph_0}$ in that model (is it $\aleph_2$, or something else)? So far we only knew that $2^{\aleph_0} \geq \aleph_2$ but nothing else. But we will show that if $M \vDash CH$, then $M[G]$ for G $\mathbb{P}$-generic over M for $\mathbb{P} = Fn(\aleph_2^M \times \mathbb{N}, \mathbb{N})$ is a model of $2^{\aleph_0} = \aleph_2$. For this, we need to *count* the names for subsets of $\mathbb{N}$. We've already seen that there's a proper class of them, so we probably shouldn't really count them; but we'll restrict to a set of names that are particularly *nice* and count those.

Definition. A name τ for a subset of $\mathbb{N}$ is called *nice* if for any $n \in \mathbb{N}$ there is an antichain in $A_n \subseteq \mathbb{P}$ s.t.

$$\tau = \{(\check{n}, p) : p \in A_n\}$$

How many nice names are there? This is (sort of) related to the question of how many antichains there are. We know that any antichain is countable, so the number of antichains can be at most $|\mathbb{P}^{\aleph_0}|$, the number of all countable subsets of $\mathbb{P}$. Now $|\mathbb{P}| = \aleph_2$ (think), the above upper bound is actually $\aleph_2^{\aleph_0}$.

What is $\aleph_2^{\aleph_0}$? We have Hausdroff's Formula:

$$\aleph_{\alpha+1}^{\aleph_\beta} = \aleph_{\alpha+1} \cdot \aleph_\alpha^{\aleph_\beta}$$

So

$$\aleph_2^{\aleph_0} = \aleph_2 \cdot \aleph_1^{\aleph_0}$$
$$= \aleph_2 \cdot \aleph_1 \cdot \aleph_0^{\aleph_0}$$
$$= \aleph_2 \cdot 2^{\aleph_0} \stackrel{\text{in } M}{=} \aleph_2 \cdot \aleph_1 = \aleph_2$$

A nice name is essentially a countable collection of antichains, so (running the same argument again) we know there are at most $\aleph_2 = \aleph_2$ nice names.

Theorem. If $x \subseteq \mathbb{N}$ in $M[G]$, then there is a nice name τ s.t.

$$x = val(\tau, G)$$

Proof. Fix a name μ for x. For every $n \in \mathbb{N}$, construct an antichain A_n with the properties
(a) $\forall p \in A_n \ p \Vdash \check{\mu} \in \mu$;
(b) A_n is an antichain;
(c) A_n is maximal w.r.t. (a) and (b).

Now we write

$$\tau := \{(\check{n}, p) : p \in A_n\}$$

which is a nice name. We claim that $M[G] \vDash \tau = \mu$.
$\subseteq$: Let $y \in val(\tau, G)$. So there is some $n \in \mathbb{N}$ s.t. $y = n$. We find $p \in A_n \cap G$ that witnesses $y \in val(\tau, G)$. Since $p \in A_n$, $p \Vdash \check{n} \in \mu$. But p was in G, so $M[G] \vDash n \in val(\mu, G)$.
$\supseteq$: Let $y \in val(\mu, G)$. Since $y = n \in \mathbb{N}$, $y = val(\check{n}, G)$. We know that $(\check{n}, p) \in \tau$ for every $p \in A_n$. If there's a $p \in A_n \cap G$, then $n \in val(\tau, G)$ and we're done. Otherwise, if $A_n \cap G = \phi$ (remember question 24 on sheet 3), there is $q \in G$ s.t. $\forall p \in A_n \ p \perp q$, contradicting the maximality of A_n (in the sense of (c)), as we can still add q into it. $\qquad\square$

So we've shown that $|2^{\aleph_0}|$ can be $\aleph_2$.

3 Example Class 1

3.1 Question 1

The answer to this question really depends on how we formulate the axioms. For example, the pairing axiom

$$\forall x \forall y \exists p \forall z (z \in p \leftrightarrow z = x \vee z = y)$$

is sometimes formulated with the $\leftrightarrow$ changed to $\rightarrow$, but of course they are equivalent with extensionality.

So there is no definite answer to this question; the message I want to convey here is that the axioms really only make sense when you have a set of those.

3.2 Question 2

Note that (a) is not Δ_0, although it is Δ_0 under some first order logic.

3.3 Question 3

(d) if z is a function then $\mathcal{P}(\bigcup\bigcup z)$ is enough to bound the range and domain of the function.

3.4 Question 6

Example given on lecture: $X = \{(x, y) : x < \omega y \in \{0, 1\}\}$;
$R = \{(a, b) : a, b = X, a = (a_1, a_2), b = (b_1, b_2), (b_2 = a_2 \wedge a_1 < b_1) \vee (b_2 > a_2)\}$.
Both of them are in $V_{\omega+1}$, and $(X, R) \in V_{\omega+4}$ or so.

3.5 Question 8

The general case is the fixed point theorem for normal functions. A normal function is a function $F : Ord \rightarrow Ord$ that is
• increasing: $\forall \alpha \; \alpha < F(\alpha)$;
• continuous: $\forall \lambda$ limits, $F(\lambda) = \cup_{\alpha < \lambda} F(\alpha)$.

Define $\gamma_0 := \gamma$, $\gamma_{n+1} := F(\gamma_n)$, $\gamma_\omega := \bigcup_{n \in \mathbb{N}} F(\gamma_n)$. We basically just need to check that the fixed point happens at the third case (so that the cofinality is ω).

3.6   Question 9

(crude notes on board) κ is uncountable and regular. So we know $H_\kappa \vDash ZFC - PowerSet$, $V_\kappa \vDash ZFC - Replacement$. Let $\lambda < \kappa$ be a cardinal. Then $\lambda \in H_\kappa$ and every subset of λ is in H_κ. So $H_\kappa \vDash Powerset \implies P(\lambda) \in H_\kappa$, and $|P(\lambda)| \leq |tcl(P(\lambda))| < \kappa$. So κ is a strong limit.

3.7   Question 10

Remember Hartog's theorem: $\forall x \exists \alpha$ a ordinal s.t. there is no injection from α into X; remember that this is true in ZF.
Let $\Omega := \{R : R$ is a binary relation on $X, (X, R)$ is a well-order$\}$,
$\bar{\Omega} := \{\alpha : \exists R \in \Omega, (\alpha, \in) \cong (X, R)\}$.

Note that this also tells us that, if we have two models of set theory which agree on real numbers, then they agree on the size of $\aleph_1$.

3.8   Question 11

It's worth notice that Φ is not absolute in general (because we need strong limit for inaccessible cardinals).
For the last part just take V_{κ_2}. Also note that the statement holds for any finite number, or even countably many.

We can consider other set theories like $ZFC + \infty IC$: $\forall \alpha \exists \kappa > \alpha$ s.t. κ is inaccessible, or ZFC+ there is a cardinal κ which is inaccessible and $\forall \lambda < \kappa \exists \lambda < \kappa' < \kappa$ s.t. κ' is inaccessible (so κ is an inaccessible limit of inaccessible cardinals).

3.9   Question 12

The idea is almost the same as the one we looked in class: build the Skolem Hull starting from quantifier-free formulas, adding witnesses of existential formulas at each step. By induction we get a countable elementary substructure. Now instead of that, for each step in building the skolem hull we take the V_{α_i} s.t. our structure is contained in V_{α_i}. By regularity of κ we know we won't reach V_κ in the end, say our supremum is α_ω. Note that it's possible that we've hit an inaccessible cardinal en route. So we need to ensure that we go up by at least one level at each stage to ensure that we're actually moving. Then use similar argument as q8.

4 Example Class 2

4.1 Question 15

One major problem is that we can't refer to truth of existential formulas to decide whether we want to add witnesses. This is one of the googlable things so lecturer decided not to spend half an hour on this. This is closely related to q16.

4.2 Question 20

Note that if x is infinite, then $L_0(x) = |x|$, $L_1(x) = \mathcal{D}(x)$ still has cardinality $|x|$, and so on; and at $L_\omega(x)$ still has cardinality $|x| = \aleph_0$.
What if x is not countable? If $|x| = \aleph_1$, we then have $L_0(x) = ... = L_\omega(x) = \aleph_1$, and it keeps this cardinality at $L_{\omega_1}(x)$, and only changes to $\aleph_2$ at $L_{\omega_2}(x)$.

This is instructive enough for question 21.

4.3 Question 22

The given statement is equivalent to $\forall X \in L_\kappa$ s.t. $V \vDash X$ is countable (regularity is downward absolute); $\mathbb{P}^{L_\kappa}(X)$ is also countable. Let $\alpha \in L_\kappa$ be countable (in V), and a cardinal in L_κ. $x \subseteq \omega$ codes a well-ordering of ω of type α. $L(x) \vDash \alpha$ is countable; using the form of condensation lemma we had in q21 we get $L(x) \vDash CH$. So $\aleph_1^{L(x)} = |\mathbb{P}(\omega)|^{L(x)} = |\mathbb{P}(\alpha)|^{L(x)} \geq |\mathbb{P}^{L_\kappa}(\alpha)|^{L(x)}$. LHS is countable, so the last expression is also countable.