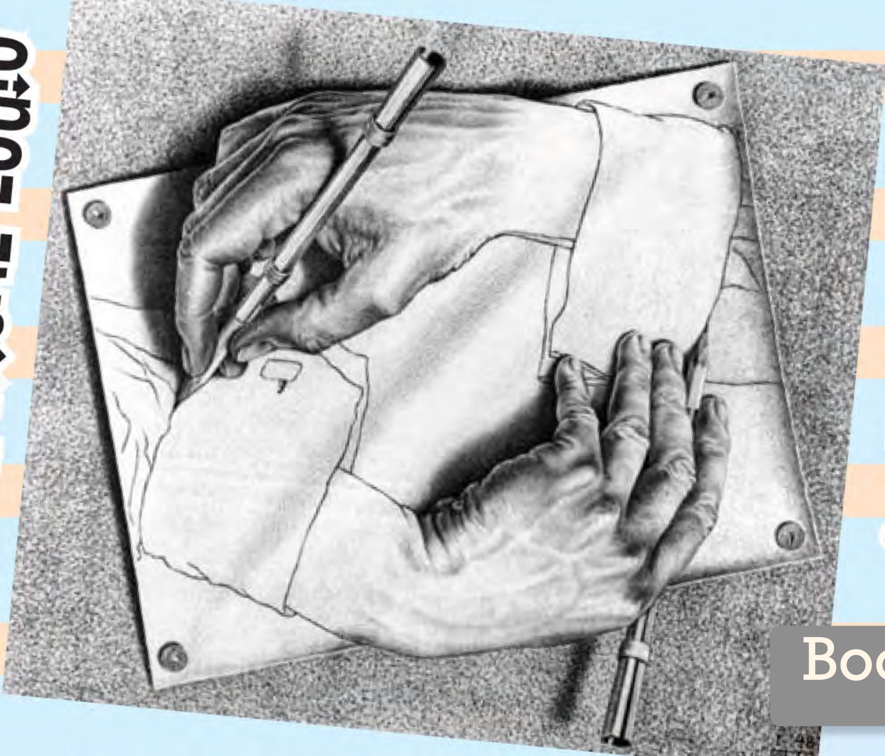
MATHEMATICAL LOGIC & SET THEORY



Book 3

Trivial examples: Fix $x_0 \in X$. Define $\mu(A) = \begin{cases} 0 & \text{if } x_0 \notin A \\ 1 & \text{if } x_0 \in A. \end{cases}$

A <u>measurable cardinal</u> is a uncountable cardinal κ which admits a nontrivial ~~countably additive~~ two-valued measure.

Does such a κ exist? If so then any larger cardinal satisfies this condition.

Given $\kappa < \kappa'$, μ nontrivial countably additive two-valued measure on κ, lift it to one on κ': $\iota : \kappa \to \kappa'$ injection. Define (for $B \subseteq \kappa'$)

$$\mu'(B) = \mu(\iota^{-1}(B)).$$

<u>Theorem</u> (Ulam) If there exists a nontrivial countably additive two-valued measure on an uncountable set X then let X be a smallest example. Then X has a nontrivial κ-additive two-valued measure for all $\kappa \leq |X|$.

μ is κ-additive if

$$\mu\Big(\bigsqcup_{\alpha \in I} A_\alpha\Big) = \sum_{\alpha \in I} \mu(A_\alpha)$$

for every collection of sets $|I| < \kappa$ $(A_\alpha \subseteq X)$.

A <u>measurable cardinal</u> is an uncountable cardinal κ having a κ-additive two-valued measure.

$$[0,1] = \bigsqcup_{\alpha \in [0,1]} \{\alpha\}$$

Do they exist? And who cares?

$$\begin{tikzcd}
 & \underset{\text{open}}{\Sigma^0_1} \arrow[dr, phantom, "\subset"] & & \underset{\text{ctble unions of closed sets}}{\Sigma^0_2} \arrow[dr, phantom, "\subset"] & & \\
\underset{\text{clopen}}{\Delta^0_1} \arrow[ur, phantom, "\subset"] \arrow[dr, phantom, "\subset"] & & \Delta^0_2 \arrow[ur, phantom, "\subset"] \arrow[dr, phantom, "\subset"] & & \Delta^0_3 & \cdots \\
 & \underset{\text{closed}}{\Pi^0_1} \arrow[ur, phantom, "\subset"] & & \underset{\text{ctble intersections of open sets}}{\Pi^0_2} \arrow[ur, phantom, "\subset"] & &
\end{tikzcd}$$

Projective Hierarchy $\underset{\sim}{\Sigma}^1_n$, $\underset{\sim}{\Pi}^1_n$, $\underset{\sim}{\Delta}^1_n = \underset{\sim}{\Sigma}^1_n \cap \underset{\sim}{\Pi}^1_n$

$$\begin{array}{ccccccc} & & \underset{\sim}{\Sigma}^1_1 & & & & \underset{\sim}{\Sigma}^1_2 \\ & \subset & & \supset & & \subset & & \cap \\ \underset{\sim}{\Delta}^1_0 & & & & \underset{\sim}{\Delta}^1_1 = \underset{\sim}{\Sigma}^1_1 \cap \underset{\sim}{\Sigma}^1_1 & & \\ \text{Borel sets} & \cap & & \supset & & \cap & & \subset \\ & & \underset{\sim}{\Pi}^1_1 & & & & \underset{\sim}{\Pi}^1_2 \end{array}$$

$\underset{\sim}{\Sigma}^1_1 = \{\text{analytic sets in } X\}$ $\qquad$ $A \in \underset{\sim}{\Sigma}^1_1$ iff A is a continuous image of a Borel set under $f: Y \to X$ (f continuous, Y Polish space)

$\underset{\sim}{\Pi}^1_1 = \{\text{coanalytic sets in } X\} = \{\text{complements of analytic sets}\}$

$\underset{\sim}{\Sigma}^1_2 = \{\text{continuous images of coanalytic sets}\}$

If there exist measurable cardinals, then every $\underset{\sim}{\Sigma}^1_2$-set is Lebesgue measureable.

Coming to: an application a large cardinal to the finite world. see

Non-associative algebra : Keis, Quandles, Racks, Shelves, ... (Sam Nelson, Quandles)

A <u>kei</u> is a set S with a binary operation $\triangleright$ satisfying : for all $x, y, z \in S$,

(1) $x \triangleright x = x$ (every element is idempotent)

(2) $(x \triangleright y) \triangleright y = x$ ($x \mapsto x \triangleright y$ is involutory)

(3) $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$ ("$\triangleright$" is right-distributive over itself)

If $(S, \triangleleft)$ satisfies (3), it is a <u>shelf</u> (or <u>self distributive system</u>). If it satisfies (1) and (3), it is a <u>rack</u>.

If $(S, \triangleleft)$ satisfies (1), (3) and (2') it is a <u>quandle</u>.

(2'): For all y, the map $S \to S$, $x \mapsto x \triangleright y$ is injective.

(1) $x \triangleright x = x$

(2) $(x \triangleright y) \triangleright y = x$

(3) $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$

The kei axioms are equivalent to the Reidemeister moves I, II, III.

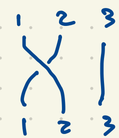
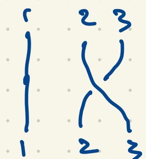
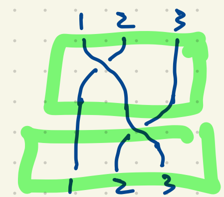
<u>Examples</u>: Fix $c \in \mathbb{R}$ and define $x \triangleright y = cx + (1-c)y$ for $x, y \in \mathbb{R}$. This gives a rack (?) (satisfying (1), (3)). It's a kei if $c = \pm 1$.

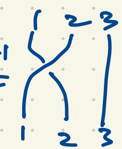
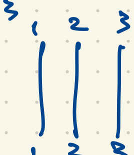
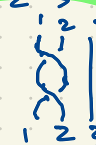
More generally let V be a vector space and $R \in GL(V)$ invertible linear transformation. For $u, v \in V$, $u \triangleright v = Ru + (I - R)v$. This is an Alexander quandle. (Sometimes a kei).

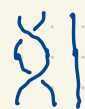
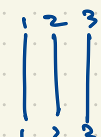
<u>Example</u> Let G be a group (multiplicative). Fix $n \in \mathbb{Z}$. For $a, b \in G$, $a \triangleright b = b^n a b^{-n}$ (n-fold conjugation of a by b). This is a rack, sometimes a quandle.

<u>Example</u> The Braid group B_n

eg. in B_3,

$\sigma =$  , $\tau =$  , $\sigma\tau =$ 

$\sigma^{-1} =$  $\iota =$  $\neq \sigma^2 =$ 

$\sigma\sigma^{-1} =$  $= \iota$ 

$S_n = \mathrm{Sym}\{1, 2, \cdots, n\}$

$|S_n| = n!$

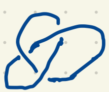
$B_n \twoheadrightarrow S_n$ epimorphism

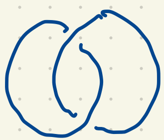
$|B_n| = \aleph_0$.

<u>Kei colorings of braids</u>

Given a braid $\sigma \in B_n$ and a Kei $(K, \triangleright)$ we color the arcs in a braid diagram of σ (i.e. label the arcs using elements of K) such that

This is the same as requiring that if we label the tops of the n strands, the labels on the bottom are independent of the choice of diagram used for the braid σ.





A right shelf satisfies right-distributivity $(x \triangleright y) \triangleright z = (x \triangleright z) \triangleright (y \triangleright z)$

.. left .. .. left - . . . $x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z)$

~~If~~ $(K, \triangleright)$ is left-distributive ~~then~~ $\Longleftrightarrow$ $(K, \triangleleft)$ is right-distributive where $x \triangleleft y = y \triangleright x$ (transpose the "multiplication table")

Switch to studying left shelves. Example found by Richard Laver (set theorist in Boulder)

$A_n = \{1, 2, 3, \cdots, N = 2^n\}$ (integers mod N) Note: 0 is written as N mod N.

<u>Theorem</u> There is a unique left shelf on A_n satisfying $a \triangleright 1 = a + 1$. for all $a \in A_n$.

<u>Eg</u>. $n = 2$, $N = 4$, $A = \{1, 2, 3, 4\}$ = integers mod 4

$\triangleright$	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

$4 \triangleright 2 = 4 \triangleright (1 \triangleright 1) = (4 \triangleright 1) \triangleright (4 \triangleright 1) = 1 \triangleright 1 = 2$

$4 \triangleright 3 = 4 \triangleright (2 \triangleright 1) = (4 \triangleright 2) \triangleright (4 \triangleright 1) = 2 \triangleright 1 = 3$

$4 \triangleright 4 = 4 \triangleright (3 \triangleright 1) = (4 \triangleright 3) \triangleright (4 \triangleright 1) = 3 \triangleright 1 = 4$

$3 \triangleright 2 = 3 \triangleright (1 \triangleright 1) = (3 \triangleright 1) \triangleright (3 \triangleright 1) = 4 \triangleright 4 = 4$

$2 \triangleright 2 = 2 \triangleright (1 \triangleright 1) = (2 \triangleright 1) \triangleright (2 \triangleright 1) = 3 \triangleright 3 = 4$

$2 \triangleright 3 = 2 \triangleright (2 \triangleright 1) = (2 \triangleright 2) \triangleright (2 \triangleright 1) = 4 \triangleright 3 = 3$

$2 \triangleright 4 = 2 \triangleright (3 \triangleright 1) = (2 \triangleright 3) \triangleright (2 \triangleright 1) = 3 \triangleright 3 = 4$

$1 \triangleright 2 = 1 \triangleright (1 \triangleright 1) = (1 \triangleright 1) \triangleright (1 \triangleright 1) = 2 \triangleright 2 = 4$

$1 \triangleright 3 = 1 \triangleright (2 \triangleright 1) = (1 \triangleright 2) \triangleright (1 \triangleright 1) = 4 \triangleright 2 = 2$

Fact: The left-distributive law holds in all cases although we haven't checked this here.

A_0	1
1	1

A_1	1	2
1	2	2
2	1	2

A_2	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

A_3	1	2	3	4	5	6	7	8
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

Figure 2: Multiplication tables for the first four Laver tables

<u>Conjecture</u> As $n \to \infty$ $(N \to \infty)$ the period of the first row of the table $\to \infty$.
The conjecture holds if there exist a Laver cardinal (a certain kind of large cardinal). No one knows how to prove this in ZFC.

We have an inverse system of left shelves

$$\cdots \longrightarrow A_4 \longrightarrow A_3 \longrightarrow A_2 \longrightarrow A_1 \longrightarrow A_0$$

Let X be any set and let $M = \{$ injective maps $X \to X \}$.
(1-to-1)
Then M is a monoid under composition. (A group iff X is finite).

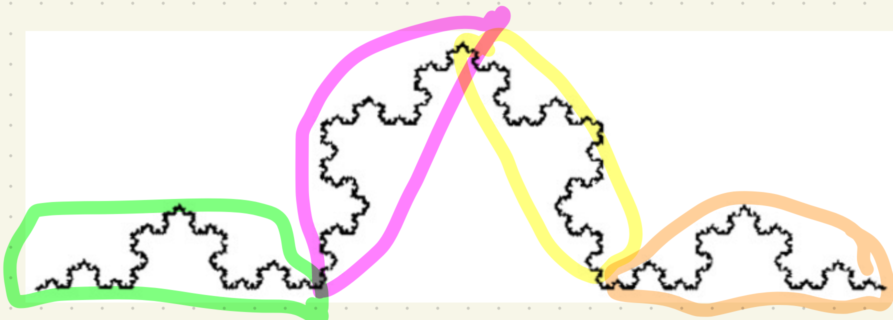
Let A be a set of sentences over some language L, and let $M, N \models A$. (models of A i.e. L-structures which satisfy all the sentences in A)

eg. A: axioms for a ring
L: $+, -, \times$

$\mathbb{Z}, \mathbb{Q} \models A$ and $\mathbb{Z}$ is a submodel of $\mathbb{Q}$ (there is a 1-to-1 map $\mathbb{Z} \xrightarrow{\iota} \mathbb{Q}$ preserving the operations. But $\mathbb{Z}$ is not elementarily embedded in $\mathbb{Q}$ because
(elementary embedded)
there are sentences ϕ over L
such that $\mathbb{Z} \models \phi$, $\mathbb{Q} \models \neg\phi$ (or the other way around) e.g.

eg. $\phi: (\exists x)(\forall y)(\neg(y+y=x))$.

We say $\iota: M \to N$ $(M, N \models A)$ is an elementary embedding if ι is injective and for every sentence ϕ, $\iota(M) \subseteq N$ where $\iota(M)$ is elementarily equivalent to N:
submodel
For all ϕ, $\iota(M) \models \phi$ iff $N \models \phi$.



A portion of the Koch snowflake curve illustrating self-similarity.

There are many embeddings of $\mathbb{C}$ in itself. Pick such an embedding $\iota : \mathbb{C} \to \mathbb{C}$.
$\mathbb{C}$, $\iota(\mathbb{C}) \subset \mathbb{C}$ are models of the field axioms A. $\iota(\mathbb{C})$ is an elementary submodel of $\mathbb{C}$ i.e. $\iota : \mathbb{C} \to \mathbb{C}$ is an elementary embedding i.e. $\mathbb{C}$ is an elementary extension of $\iota(\mathbb{C})$.

Note: $\iota : \mathbb{C} \to \mathbb{C}$ preserves $0, 1, +, \times, -$ but not the topology.

For models of ZFC $(L : \in)$ a Laver cardinal is a (inaccessible) cardinal κ such that the V_κ admits an elementary embedding $\iota : V_\kappa \to V_\kappa$ which is not surjective.

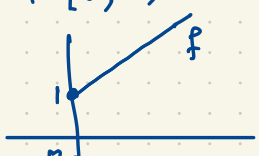
This ι generates a left shelf under the following:

If $f, g : X \to X$ are injective then $f \triangleright g : X \to X$ is

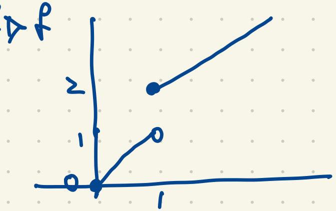
$$(f \triangleright g)(x) = \begin{cases} fgf^{-1}(x) & , \text{ if } x \in f(X) \\ x & , \text{ if } x \notin f(X) \end{cases}$$

$f(X) = \{f(x) : x \in X\} \subset X$

eg. $f : [0, \infty) \to [0, \infty)$, $x \mapsto x+1$



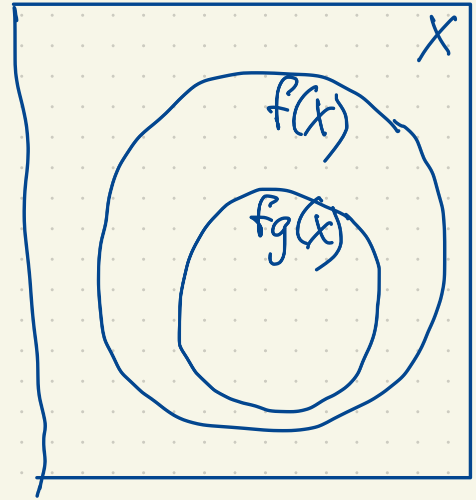
$f \triangleright f$



Why is $\triangleright$ a left shelf?

$((f \triangleright g) \triangleright (f \triangleright h))(x)$

$= (f \triangleright (g \triangleright h))(x)$ Check three cases



If $x \in fg(X)$ then $x = fg(y)$ so

$(g \triangleright h)(x) =$

$\iota : V_\kappa \longrightarrow V_\kappa$ is an elementary embedding but not surjective.

It generates a left shelf under "$\triangleright$". This is the free shelf on one generator $\mathcal{F}_1$

$\mathcal{F}_1 = \{ \iota, \iota \triangleright \iota, (\iota \triangleright \iota) \triangleright \iota, \iota \triangleright (\iota \triangleright \iota), \dots \}$ These combinations of ι under $\triangleright$

are distinct except when required by the left shelf axiom e.g. $(\iota \triangleright \iota) \triangleright (\iota \triangleright \iota) = \iota \triangleright (\iota \triangleright \iota)$

$\mathcal{F}_1$ is a countably infinite left shelf; moreover $\mathcal{F}_1 = \varprojlim A_n$

Let X be an infinite set. A filter on X is a collection $\mathcal{F}$ of subsets of X such that

(i) $\emptyset \notin \mathcal{F}$, $X \in \mathcal{F}$ (Sets in $\mathcal{F}$ are large subsets of X.)

(ii) If $A \in \mathcal{F}$ and $A \subseteq B \subseteq X$ then $B \in \mathcal{F}$.

(iii) If $A, A' \in \mathcal{F}$ then $A \cap A' \in \mathcal{F}$.

By Zorn's lemma, every $\mathcal{F}$ filter extends to an ultrafilter $\mathcal{U} \supseteq \mathcal{F}$ on X which is a filter satisfying

(iv) For all $A \subseteq X$, either A or $X \smallsetminus A$ is in $\mathcal{U}$.

$\mathcal{U}$ gives a two-valued finitely additive probability measure on X.

To get a nonprincipal ultrafilter on X, we start with the Fréchet filter consisting of all cofinite subsets of X (complements of finite subsets of X) and take $\mathcal{U} \supseteq \mathcal{F}$ a maximal filter containing $\mathcal{F}$. $\mathcal{U}$ is nonprincipal: $\mathcal{U}$ contains no finite sets.

We take $\mathcal{U}$ to be a nonprincipal ultrafilter on $\omega = \{0,1,2,3,\dots\}$ and consider the ring $\mathbb{R}^\omega = \{(a_0, a_1, a_2, a_3, \dots) : a_i \in \mathbb{R}\}$ with coordinatewise operations. $\mathbb{R}^\omega$ is a commutative ring with identity, not a field; eg. $(1,0,1,0,\dots)(0,1,0,1,\dots) = (0,0,0,0,\dots) = 0 \in \mathbb{R}^\omega$.

Now identify two sequences $a = (a_0, a_1, a_2, \dots)$, $b = (b_0, b_1, b_2, \dots)$ if they agree almost everywhere with respect to $\mathcal{U}$ i.e. if $\{i \in \omega : a_i = b_i\} \in \mathcal{U}$.

In the case $a = (1,0,1,0,1,0,\dots)$ we have $a_i = 0$ whenever $i \in \{1,3,5,7,\dots\}$; $b_i = 0$ whenever $i \in \{0,2,4,6,\dots\}$
$b = (0,1,0,1,0,1,\dots)$

If $\{1,3,5,7,\dots\} \in \mathcal{U}$ then $a \sim (0,0,0,0,0,\dots)$ and $b \sim (1,1,1,1,1,\dots)$.

If $\{0,2,4,6,\dots\} \in \mathcal{U}$ then $a \sim (1,1,1,1,1,\dots)$ and $b \sim (0,0,0,0,0,\dots)$.

Identify two sequences in $\mathbb{R}^\omega$ whenever they agree almost everywhere w.r.t. $\mathcal{U}$. Then we get a quotient ring $\mathbb{R}^\omega/\sim \; = {}^*\mathbb{R}$ denoted $\hat{\mathbb{R}}$ in the handout. This is the field of nonstandard reals or hyperreals.

${}^*\mathbb{R}$ has the same first order theory (an ordered field and it's a real closed field, e.g. every poly $f(x) \in {}^*\mathbb{R}[x]$ of odd degree has a root in ${}^*\mathbb{R}$). In fact we have an elementary embedding of $\mathbb{R}$ in ${}^*\mathbb{R}$. The main difference between $\mathbb{R}$ and ${}^*\mathbb{R}$ is that $\mathbb{R}$ has no infinite or infinitesmal elements but ${}^*\mathbb{R}$ does.

The Archimedean property says that if $a > 0$ then $\underbrace{a+a+a+\cdots+a}_{n} = na > 1$ for some n.

$(\forall a)(a>0 \to (a+a>1 \vee a+a+a>1 \vee a+a+a+a>1 \vee \ldots))$

This property is not expressible in the first order theory of fields.

$\mathbb{R}$ satisfies this property, ${}^*\mathbb{R}$ does not.

Eg. $\varepsilon = (1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \cdots) \in \mathbb{R}^\omega$, up to equivalence mod $\mathcal{U}$, defines an infinitesmal in ${}^*\mathbb{R}$.

$n\varepsilon = (n, \frac{n}{2}, \frac{n}{3}, \frac{n}{4}, \cdots) \in \mathbb{R}^\omega$, $n\varepsilon < 1$ since this holds for all but the first n terms of the sequence.

$\frac{1}{\varepsilon} = (1, 2, 3, 4, 5, \cdots) \in \mathbb{R}^\omega$ defines an infinite element of ${}^*\mathbb{R}$.

Every structure M has a enlargement ${}^*M$.

Łoś' Theorem If $M_0, M_1, M_2, \dots \models A$ (statements over a first-order language over L) then the ultraproduct

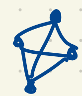
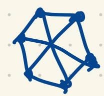
$$\Big(\prod_{i\in\omega} M_i\Big)/\mathcal{U} \models A.$$

Eg. A = axioms for fields, $M_i = \mathbb{R}$ for all i. $\prod_{i\in\omega} M_i = \{(m_0, m_1, m_2, \dots) : m_i \in M_i\}$.

Eg. L = language of a single binary relation '$\sim$'

A = axioms for ordinary graphs of degree 3

A model of A, $\Gamma \models A$, is an ordinary graph of degree 3.

For each $i \in \omega$, take $\Gamma_i \models A$ eg. $\Gamma_0 =$  , $\Gamma_1 =$  , $\Gamma_2, \Gamma_3, \dots$

$$\prod_{i\in\omega} \Gamma_i = \Gamma_0 \times \Gamma_1 \times \Gamma_2 \times \dots = \{(v_0, v_1, v_2, v_3, \dots) : v_i \in \Gamma_i\}$$

$\mathcal{U}$ a nonprincipal ultrafilter on ω i.e. v_i is a vertex in Γ_i.

Now $\Big(\prod_{i\in\omega} \Gamma_i\Big)/\mathcal{U}$ is the set of equiv. classes of sequences $v = (v_0, v_1, v_2, \dots)$.

If $v, w \in \underbrace{\Big(\prod_{i\in\omega} \Gamma_i\Big)/\mathcal{U}}_{\Gamma =}$ then $v \sim w$ iff $v_i \sim w_i$ for almost all i i.e. $\{i \in \omega : v_i \sim w_i\} \in \mathcal{U}$.

This graph Γ has degree 3. If Γ_i has order $\le n$ for some n then Γ is a graph of order $\le n$. Why? Let θ be the first-order statement that Γ_i has at most n vertices; since $\Gamma_i \models \theta$, $\Gamma := \Big(\prod_{i\in\omega} \Gamma_i\Big)/\mathcal{U} \models \theta$.

You can take the "$*$" operation applied to any standard mathematical object, e.g.

$\mathbb{R} \xrightarrow{*} {}^*\mathbb{R}$, $\quad S \xrightarrow{*} {}^*S \quad ({}^*S = S$ if $|S| < \infty)$.

If $f: \mathbb{R} \to \mathbb{R}$, then ${}^*f: {}^*\mathbb{R} \to {}^*\mathbb{R}$ "enlarges" (extends) f. How do we define ${}^*f(\alpha)$ for $\alpha \in \mathbb{R}^*$? α is represented by $(a_0, a_1, a_2, \dots) \in \mathbb{R}^\omega$.

${}^*f(\alpha)$ is represented by $(f(a_0), f(a_1), f(a_2), \dots) \in \mathbb{R}^\omega$. The equiv. class of this sequence is well-defined in ${}^*\mathbb{R}$.

Suppose $f: \mathbb{R} \to \mathbb{R}$ is differentiable. Classically,

$$f'(a) = \lim_{t \to 0} \frac{f(a+t) - f(a)}{t}.$$

The nonstandard approach:

$$f'(a) = \mathrm{st}\left[\frac{f(a+\varepsilon) - f(\varepsilon)}{\varepsilon}\right] \text{ where } \varepsilon \text{ is an infinitesimal}$$

st: bounded hyperreals to reals. "$\mathrm{st}(\alpha)$" is the standard part of α, i.e. the unique real closest to α (infinitely close).

${}^*\mathbb{R}$ has the order topology which is not metrizable and not separable.

Integrals can be similarly defined in a nonstandard way: if f is Lebesgue integrable then

$$\int_a^b f(t)\,dt = \mathrm{st}\left[\frac{1}{N}\sum_{i=1}^{N} f(a+i\Delta x)\,\Delta x\right] \qquad \Delta x = \frac{b-a}{N}$$

where N is an unbounded hypernatural number

Hypernatural numbers $^*\mathbb{N} = \left(\prod_{i\in\omega}\mathbb{N}\right)/\mathcal{U}$

$\mathbb{N} = \{1, 2, 3, \dots\}$. Sequences $(n_0, n_1, n_2, \dots) \in \mathbb{N}^\omega$ mod $\mathcal{U}$ gives $^*\mathbb{N}$.

$\mathbb{N} \subset {}^*\mathbb{N}$

$^*\mathbb{N}$ looks like

$$|{}^*\mathbb{N}| = |{}^*\mathbb{R}| = |\mathbb{R}| = 2^{\aleph_0}.$$

$$2^{\aleph_0} \overset{?}{\leq} |{}^*\mathbb{N}| \leq |\mathbb{N}^\omega| = \aleph_0^{\aleph_0} = 2^{\aleph_0}$$

Given $\alpha \in (0,1)$ (real) consider the sequence $u_\alpha = (\lceil\alpha\rceil, \lceil 2\alpha\rceil, \lceil 3\alpha\rceil, \lceil 4\alpha\rceil, \dots) \in \mathbb{N}^\omega$

If $\alpha < \beta$ in $(0,1)$ then $u_\alpha < u_\beta$ $\quad u_\alpha \not\equiv u_\beta$ mod $\mathcal{U}$.

An example of an elementary statement about $\mathbb{R}$ that has a (possibly) shorter nonstandard proof than standard proof:

<u>Theorem (Sierpinski)</u> If $a_1, \dots, a_k, b$ are positive reals then

$$\left| \left\{ (n_1, \dots, n_k) \in \mathbb{N}^k : \frac{a_1}{n_1} + \frac{a_2}{n_2} + \cdots + \frac{a_k}{n_k} = b \right\} \right| < \infty .$$

This statement was proved using elementary methods by Sierpinski.

A later nonstandard proof by Ross:

Suppose $S = \{ (a_1, \dots, n_k) \in \mathbb{N}^k : \frac{a_1}{n_1} + \cdots + \frac{a_k}{n_k} = b \}$ is infinite. Then

${}^*S$ contains a solution $(n_1, \dots, n_k)$ where not all $n_i \in \mathbb{N}$ (some n_i's are unbounded);

say $n_1, \dots, n_r \in {}^*\mathbb{N} \setminus \mathbb{N}$; $n_{r+1}, \dots, n_k \in \mathbb{N}$; $1 \le r \le n$. There

$$\underbrace{\frac{a_1}{n_1} + \cdots + \frac{a_r}{n_r}}_{\substack{\text{positive} \\ \text{infinitesimal}}} = \underbrace{b - \frac{a_{r+1}}{n_{r+1}} - \cdots - \frac{a_k}{n_k}}_{\in \mathbb{R} \text{ (bounded)}} ,$$

Contradiction.

We have first-order axioms for group theory.

Axioms for the class of abelian groups:

- axioms of group theory
- $(\forall x)(\forall y)(xy = yx)$

Axioms for class of nonabelian groups

- axioms for group theory
- $(\exists x)(\exists y)(xy \neq yx)$.

There is no first-order axiomatization of the class of cyclic groups.

Cyclic: $(\exists g)(\forall x)(\exists n \in \mathbb{Z})(x = g^n)$

Not permissible in first order group theory.

If there were a list of axioms A for the theory of cyclic groups then

$\left(\prod_{i \in \omega} C_{i+2}\right) / \mathcal{U}$ is a group of order $2^{\aleph_0}$, not cyclic.

cyclic of order 2

$\left(C_2 \times C_3 \times C_4 \times C_5 \times \cdots\right) / \mathcal{U}$ is not cyclic.

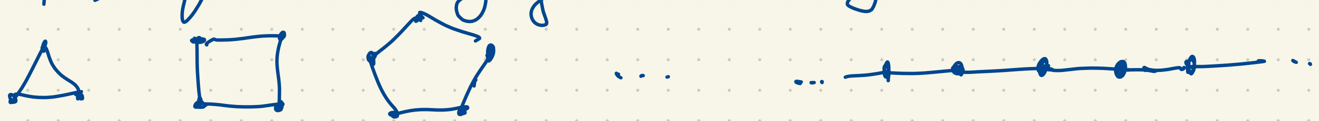
A shorter argument that the class of cyclic groups is not first order axiomatizable:

Suppose A is a collection of statements in first order group theory such that $G \models A$ iff G is a cyclic groups. There exists an infinite model (additive $\mathbb{Z}$) so by the Upward Loewenheim-Skolem Theorem, there exist models of arbitrarily large cardinality. Take any uncountable model $G \models A$; then G is not cyclic.

Let $\mathcal{A}$ be a set of statements in graph theory such that

$\Gamma \models \mathcal{A}$ iff Γ is a graph of degree 2.

Note: this equivalent to saying Γ is a disjoint union of cycles



Let A be the axioms for field theory (over the language $0, 1, +, -, \times$).

$\mathbb{F}_p \models A$ is the field of prime order p; $\overline{\mathbb{F}}_p$ = algebraic closure of $\mathbb{F}_p$

$\overline{\mathbb{F}}_p$ is countably infinite of characteristic p $(\underbrace{1+1+\cdots+1}_{p}=0)$

Let $F = \left(\prod_p \overline{\mathbb{F}}_p\right)/\mathcal{U} = (\overline{\mathbb{F}}_2 \times \overline{\mathbb{F}}_3 \times \overline{\mathbb{F}}_5 \times \overline{\mathbb{F}}_7 \times \cdots)/\mathcal{U}$

Since $\overline{\mathbb{F}}_p \models A$, ($\overline{\mathbb{F}}_p$ is a field) F is a field. What is it? $F \cong \mathbb{C}$.

$F = \left(\prod_{p \text{ prime}} \overline{\mathbb{F}}_p\right)/\mathcal{U}$ is a field of characteristic zero.

It is algebraically closed. (Each $\overline{\mathbb{F}}_p$ is alg. closed as we described in the first month.)

The theory of alg. closed fields of characteristic zero is uncountably categorical.

$|F| = 2^{\aleph_0}$ (look back four pages) so $F \cong \mathbb{C}$.

Now consider $F = \left(\prod_p \mathbb{F}_p\right)/\mathcal{U} = (\mathbb{F}_2 \times \mathbb{F}_3 \times \mathbb{F}_5 \times \mathbb{F}_7 \times \mathbb{F}_{11} \times \cdots)/\mathcal{U}$.

This is a field. It's a subfield of $\mathbb{C}$ (up to isomorphism). It has characteristic zero. $|F| = 2^{\aleph_0}$. $F \ncong \mathbb{C}$ since F has irreducible poly's of every degree. (For every $n \geq 1$, there exists a poly. $f(x) \in F[x]$ of degree n which is irreducible. But so what, $\mathbb{Q}$ also has this property.)

$\mathbb{R}[x]$ has irred. poly's of degree 2 but they all give rise to $\mathbb{C}$:

$\mathbb{R}$ has a unique extension field of degree 2. $\mathbb{Q}$ has infinitely many extension fields of degree 2. $\mathbb{F}_p$ has a <u>unique</u> extension of each degree $n \geq 1$.

F is an uncountable field of char. 0 having a unique extension field of each degree $n \geq 1$.

Take a subset $S \subseteq \mathbb{N}^\omega = \{(n_0, n_1, n_2, \dots) : a_i \in \mathbb{N}\}$. Two players, Alice and Bob, take turns picking elements of $\mathbb{N} = \{1,2,3,4,\dots\}$ starting with Alice, resulting in a *play* $x = (a_0, b_0, a_1, b_1, a_2, b_2, \dots) \in \mathbb{N}^\omega$. If $x \in S$, then A wins. If $x \in \mathbb{N}^\omega - S$, B wins.

Eg. S is the set of eventually constant sequences. This has a winning strategy for Bob.

Eg. S is the set of eventually periodic sequences. Bob's advantage.

Eg. S is any countable collection of sequences, i.e. $S \subseteq \mathbb{N}^\omega$, $|S| = \aleph_0$. Bob has a winning strategy. Enumerate $S = \{s_1, s_2, s_3, \dots\}$. On turn j, Bob chooses any $n \in \mathbb{N}$ which differs from the $2j$-indexed term in s_j.

Eg. S is the set of sequences having no '3,1,4,1,5,9' as subsequence. Alice has a winning strategy.

Eg. S is the set of 'universal' sequences in $\mathbb{N}^\omega$ (sequences containing every finite sequence of natural numbers appears as a consecutive subsequence). Bob can play $2, 2, 2, \dots$ to win.

A *strategy* is a function: $\underbrace{\mathbb{N}^{<\omega}}_{\text{finite strings } (a_0, b_0, \dots)} \to \mathbb{N}$. A strategy for Alice (or Bob) is a *winning strategy* if the player in question is guaranteed to win if they follow that strategy.

a_n or b_n

Axiom of Determinacy (AD): For every $S \subseteq \mathbb{N}^\omega$, either Alice or Bob has a winning strategy for the game G_S.

Theorem (Gale, Stewart) Every open game is determined: either Alice or Bob has a winning strategy.

Topology of $\mathbb{N}^\omega$: $\mathbb{N}$ has the discrete topology : every subset of $\mathbb{N}$ is open.

A basic open set : Given $(x_0, x_1, \cdots, x_{n-1}) \in \mathbb{N}^{<\omega}$, $(x_0, x_1, \cdots, x_{n-1}) \times \mathbb{N}^\omega = \{(x_0, x_1, \cdots, x_{n-1}, x_n, x_{n+1}, \cdots) : x_n, x_{n+1}, x_{n+2}, \cdots \in \mathbb{N}\}$ is a basic open set.

An open set is an arbitrary union of basic open sets.

If $S \subseteq \mathbb{N}^\omega$ is open, then G_S is determined.

The condition that $S \subseteq \mathbb{N}^\omega$ is open means that all winning plays for Alice are determined after a finite number of moves.

An example of an open set is the set of all sequences $(x_0, x_1, x_2, \cdots) \in \mathbb{N}^\omega$ containing any phone number i.e. $x_n = 3077664394$ for some n.

It is $\bigcup_{n=0}^{\infty} U_n$: $U_n = \{(x_0, x_1, \cdots, x_{n-1}, 3077664394, x_{n+1}, x_{n+2}, \cdots) : x_i \in \mathbb{N}\}$

This set is open but not closed : its complement is not open.

Also, if $S \subseteq \mathbb{N}^\omega$ is closed, then G_S. More generally, if $S \subseteq \mathbb{N}^\omega$ is a Borel set, the game G_S is determined.

Consider $S = \{(a_0, b_0, a_1, b_1, \cdots) : a_0 \in \mathbb{N}$ arbitrary, b_n odd, $a_{n+1}+1 = b_n > a_n$ for all $n \geq 1\}$

Alice has a winning strategy.

Typical play: $(\overset{a_0}{1}, \overset{b_0}{48}, \overset{a_1}{47}, \overset{b_1}{46}, \overset{a_2}{45}, \overset{b_2}{44}, \overset{a_3}{43}, \cdots, \overset{a_{23}}{3}, \overset{b_{23}}{2}, \overset{a_{24}}{1})$

Alice has won; this game has value 0 ("0 moves remaining for Alice to win").

$(1, 48, 47, \cdots, 3, 2)$ has value 0.

$(1, 48, 47, \cdots, 4, 3)$ has value 1.

$(1, 48, 47, \cdots, 5, 4)$ " " 1.

⋮

$(1, 48, 47)$ has value 22.

$(1, 48)$ " " "

(1) has value $\omega = \sup\{0, 1, 2, \cdots\}$

$()$ has value $\omega + 1$.

In general, for every position of the game in which Alice has a winning strategy, we assign a value to that position which is an ordinal. '0' means Alice has won already, '1' means 1 move to reach a position of value 0, etc. Some positions will not have any value assigned; these are winning positions for Bob.

The value is defined recursively as follows:

Case I: It's Bob's turn. Position $(a_0, b_0, a_1, b_1, \cdots, a_n)$, $n \geq 0$.

Define the value of $(a_0, b_0, \cdots, a_n)$ to be the sup of the values of $(a_0, b_0, \cdots, a_n, b)$ for $b \in \mathbb{N}$ (if these sequences all have values).

Case II: It's Alice's turn. Position $(a_0, b_0, a_1, b_1, \cdots, a_{n-1}, b_{n-1})$, $n \geq 0$ (ie. $()$ if $n=0$).
This position has value $\alpha+1$ where α is the min value of $(a_0, b_0, a_1, b_1, \ldots, a_{n-1}, b_{n-1}, a)$, $a \in \mathbb{N}$
assuming there exist any such positions of value.

More generally, take any set X and consider games determined by $S \subseteq X^\omega$
(typically $X = \{0,1\}$ or $\mathbb{N}$).

AD is independent of ZF.
AD is inconsistent with AC i.e. $ZF \vdash (AD \to \neg AC)$.