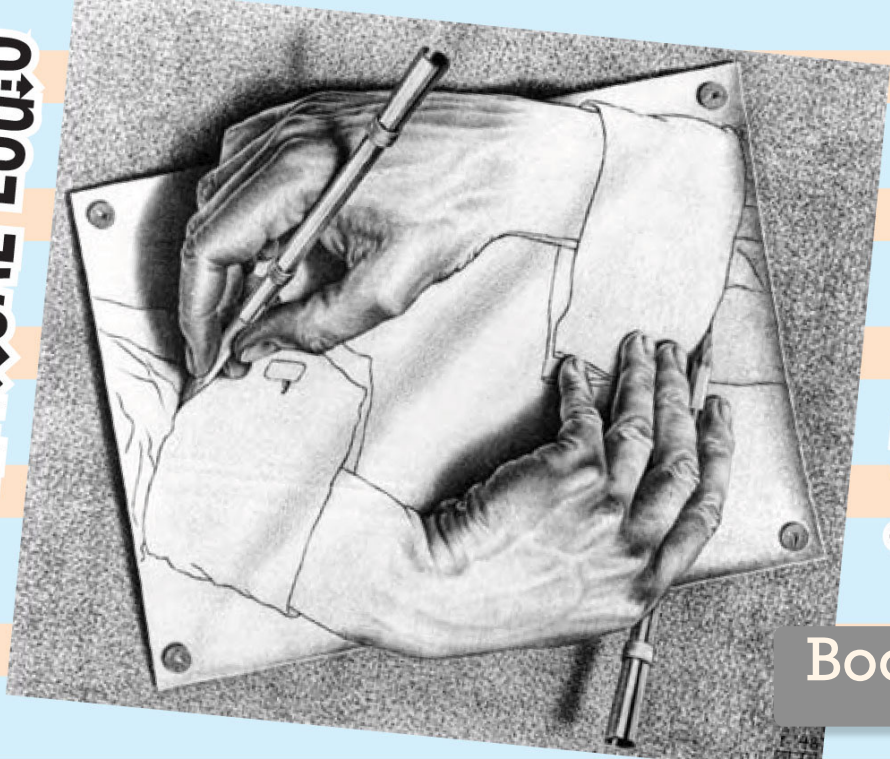


**MATHEMATICAL LOGIC**



**& 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 measurable cardinal is a <sup>uncountable</sup> cardinal  $\kappa$

which admits a nontrivial ~~countably additive~~ two-valued measure.

Does such a  $\kappa$  exist? If so then any larger cardinal satisfies this condition.

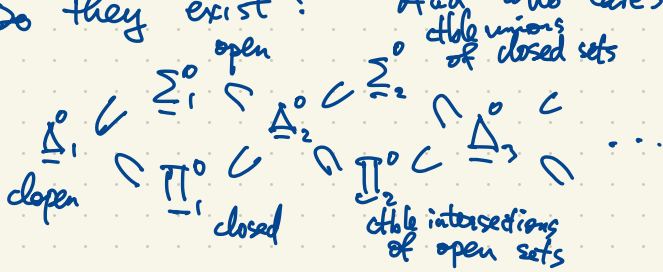
Given  $\kappa < \kappa'$ ,  $\mu$  nontrivial countably additive two-valued measure on  $\kappa$ , lift it to one on  $\kappa'$ .  $i: \kappa \rightarrow \kappa'$  injection. Define (for  $B \subseteq \kappa'$ )

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

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

A measurable cardinal is an uncountable cardinal  $\kappa$  having a  $\kappa$ -additive two-valued measure.

Do they exist? And who cares?



$\mu$  is  $\kappa$ -additive if

$$\mu\left(\bigsqcup_{\alpha \in I} A_\alpha\right) = \sum_{\alpha \in I} \mu(A_\alpha) \quad \text{for every collection of } |I| < \kappa \text{ sets } (A_\alpha \subseteq X).$$

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

Projective Hierarchy  $\Sigma'_n, \Pi'_n, \Delta'_n = \Sigma'_n \cap \Pi'_n$

$$\Delta'_0 \subset \Sigma'_1 \supset \Delta'_1 = \Sigma'_1 \cap \Pi'_1 \subset \Sigma'_2 \cap \Pi'_2$$

Borel sets  $\Pi'_1 \supset \Pi'_2 \subset$

$\Sigma'_1 = \{ \text{analytic sets in } X \}$   $A \in \Sigma'_1$  iff  $A$  is a continuous image of a Borel set under  $f: Y \rightarrow X$

$\Pi'_1 = \{ \text{coanalytic sets in } X \} = \{ \text{complements of analytic sets} \}$  ( $f$  continuous,  $Y$  Polish space)

$\Sigma'_2 = \{ \text{continuous images of coanalytic sets} \}$

If there exist measurable cardinals, then every  $\Sigma'_2$ -set is Lebesgue measurable.

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

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

A kei 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  $(S, \triangleright)$  satisfies (3), it is a shelf. If it satisfies (1) and (3), it is a rack.  
(or self-distributive system)

If  $(S, \triangleright)$  satisfies (1), (3) and (2') it is a quandle.

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

Examples: 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).

Example 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.

Example The Braid group  $B_n$   
eg. in  $B_3$ ,

$$S_n = \text{Sym}\{1, 2, \dots, n\}$$

$$|S_n| = n!$$

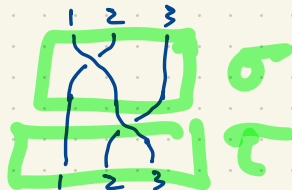
$B_n \rightarrow S_n$  epimorphism

$$|B_n| = \infty$$

$$\sigma = \begin{array}{c} 1 \quad 2 \quad 3 \\ \diagdown \quad | \quad / \\ 1 \quad 2 \quad 3 \end{array}$$

$$\tau = \begin{array}{c} 1 \quad 2 \quad 3 \\ | \quad \diagdown \quad / \\ 1 \quad 2 \quad 3 \end{array}$$

$$\sigma\tau =$$



$$\sigma^{-1} = \begin{array}{c} 1 \quad 2 \quad 3 \\ | \quad / \quad \diagdown \\ 1 \quad 2 \quad 3 \end{array}$$

$$1 = \begin{array}{c} 1 \quad 2 \quad 3 \\ | \quad | \quad | \\ 1 \quad 2 \quad 3 \end{array}$$

$$\neq$$

$$\sigma^2 = \begin{array}{c} 1 \quad 2 \quad 3 \\ \diagdown \quad / \quad | \\ 1 \quad 2 \quad 3 \end{array}$$

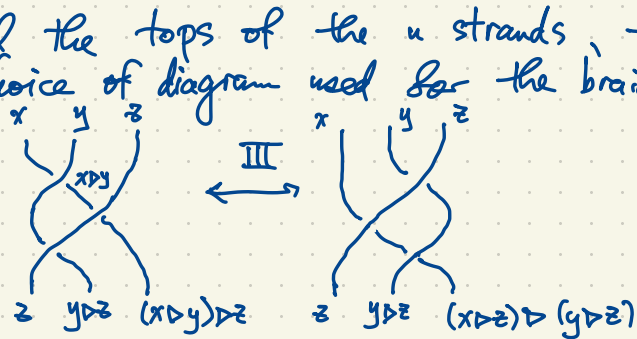
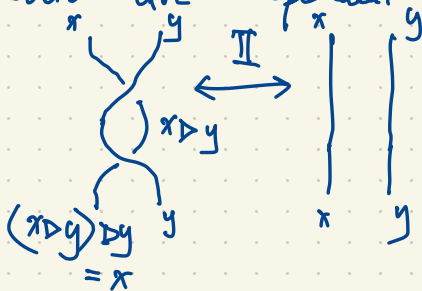
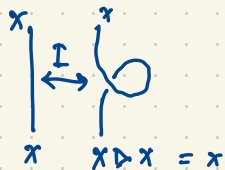
$$\sigma\sigma^{-1} = \begin{array}{c} 1 \quad 2 \quad 3 \\ \diagdown \quad / \quad | \\ 1 \quad 2 \quad 3 \end{array} = 1$$

# Kei colorings of braids

Given a braid  $\sigma \in B_n$  and a Kei  $(K, \triangleright)$  we color the arcs in a braid diagram of  $\sigma$  (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  $\sigma$ .



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

$(K, \triangleright)$  is left-distributive  $\iff (K, \triangleleft)$  is right-distributive where

$$x \triangleleft y = y \triangleright x$$

(Transpose the "multiplication table")

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

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

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

Ex.  $n=2, N=4, A = \{1, 2, 3, 4\} = \text{integers mod } 4$

$\triangleright$	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

Conjecture As  $n \rightarrow \infty$  the period of the first row of the table  $\rightarrow \infty$ .  
 The conjecture holds if there exists 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

$$\dots \rightarrow A_4 \rightarrow A_3 \rightarrow A_2 \rightarrow A_1 \rightarrow A_0$$



Let  $X$  be any set and let  $M = \{ \text{injective maps } X \rightarrow X \}$ .

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  $A$

eg.  $A$ : axioms for a ring

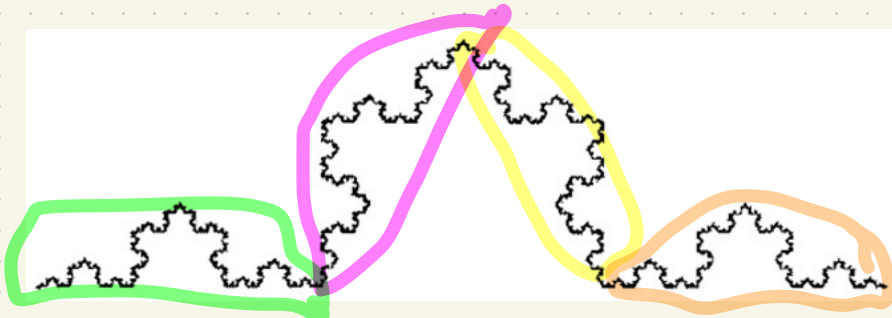
$L$ :  $+, -, \times$

$\mathbb{Z}, \mathbb{Q} \models A$  and  $\mathbb{Z}$  is a submodel of  $\mathbb{Q}$  (there is a 1-to-1 map  $\mathbb{Z} \xrightarrow{1} \mathbb{Q}$  preserving the operations. But  $\mathbb{Z}$  is not elementarily embedded in  $\mathbb{Q}$  because

there are sentences  $\phi$  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  $\iota: M \rightarrow N$  ( $M, N \models A$ ) is an elementary embedding if  $\iota$  is injective and for every sentence  $\phi$ ,  $\iota(M) \subseteq N$  submodel where  $\iota(M)$  is elementarily equivalent to  $N$ . For all  $\phi$ ,  $\iota(M) \models \phi$  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  $\iota: \mathbb{C} \rightarrow \mathbb{C}$ .  $\mathbb{C}$ ,  $\iota(\mathbb{C}) \subset \mathbb{C}$  are models of the field axioms  $\mathcal{A}$ .  $\iota(\mathbb{C})$  is an elementary submodel of  $\mathbb{C}$  i.e.  $\iota: \mathbb{C} \rightarrow \mathbb{C}$  is an elementary embedding i.e.  $\mathbb{C}$  is an elementary extension of  $\iota(\mathbb{C})$ .

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

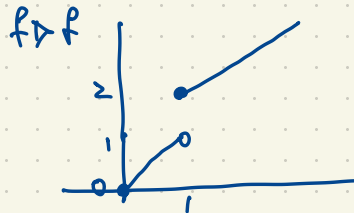
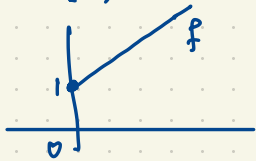
For models of ZFC  $(L: \in)$  a lower cardinal <sup>(inaccessible)</sup> is a cardinal  $\kappa$  such that the  $V_\kappa$  admits an elementary embedding  $\iota: V_\kappa \rightarrow V_\kappa$  which is not surjective. This  $(\iota)$  generates a left shelf under the following:

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

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

$$f(X) = \left\{ \begin{array}{l} f(x) : x \in X \\ \subset X \end{array} \right\}$$

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



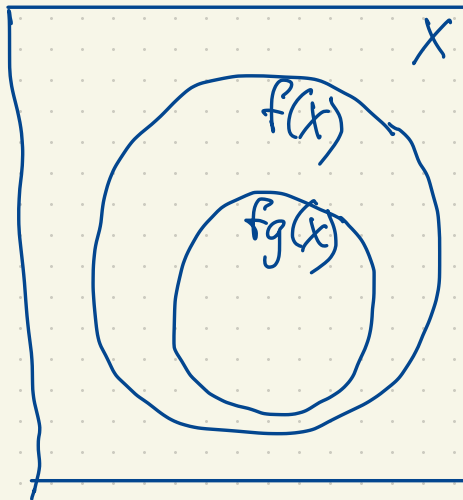
Why is  $\triangleright$  a left shelf?

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

$$= (f \triangleright (g \triangleright h))(x) \quad \text{check three cases}$$

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

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



$\iota: V_k \rightarrow V_k$  is an elementary embedding but not surjective.

It generates a <sup>left</sup> shelf under " $\triangleright$ ". This is the free shelf on one generator  $\mathfrak{F}_1$ .

$\mathfrak{F}_1 = \{ \iota, \iota \triangleright \iota, (\iota \triangleright \iota) \triangleright \iota, \iota \triangleright (\iota \triangleright \iota), \dots \}$  These combinations of  $\iota$  under  $\triangleright$  are distinct except when required by the left shelf axiom e.g.  $(\iota \triangleright \iota) \triangleright (\iota \triangleright \iota) = \iota \triangleright (\iota \triangleright \iota)$

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

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

Identify two sequences in  $\mathbb{R}^{\omega}$  whenever they agree almost everywhere w.r.t.  $\mathcal{U}$ .  
Then we get a quotient ring  $\mathbb{R}^{\omega}/\mathcal{U} = {}^*\mathbb{R}$  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 infinitesimal elements but  ${}^*\mathbb{R}$  does.

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

$(\forall a)(a > 0 \rightarrow (a+a > 1 \vee a+a+a > 1 \vee a+a+a+a > 1 \vee \dots))$

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

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

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

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

the sequence.

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

Every structure  $M$  has an enlargement  $^*M$ .



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

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

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  $\omega$

i.e.  $v_i$  is a vertex in  $\Gamma_i$ .

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

If  $v, w \in \left( \prod_{i \in \omega} \Gamma_i \right) / \mathcal{U}$  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  $\Gamma$  has degree 3. If  $\Gamma_i$  has order  $\leq n$  for some  $n$  then  $\Gamma$  is a graph of order  $\leq n$ . why? Let  $\theta$  be the first-order statement that  $\Gamma_i$  has at most  $n$  vertices.

Since  $\Gamma_i \models \theta$ ,  $\Gamma := \left( \prod_{i \in \omega} \Gamma_i \right) / \mathcal{U} \models \theta$ .

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

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

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

$f(x)$  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  $f: \mathbb{R} \rightarrow \mathbb{R}$  is differentiable. Classically,

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

The nonstandard approach:

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

st: bounded hyperreals to reals. "st(x)" is the standard part of  $x$ , i.e. the unique real closest to  $x$  (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

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

$$\Delta x = \frac{b-a}{N}$$

where  $N$  is an unbounded hypernatural number

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

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

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

${}^*N$  looks like 

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

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

Given  $\alpha \in (0, 1)$  (real) consider the sequence  $u_\alpha = (\lceil \alpha \rceil, \lceil 2\alpha \rceil, \lceil 3\alpha \rceil, \lceil 4\alpha \rceil, \dots)$   
If  $\alpha < \beta$  in  $(0, 1)$  then  $u_\alpha < u_\beta$   $\in N^\omega$   
 $u_\alpha \not\sim u_\beta \pmod{\mathcal{U}}$



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

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

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

This statement was proved using elementary methods by Sierpinski.

A later nonstandard proof by Ross:

Suppose  $S = \left\{ (n_1, \dots, n_k) \in \mathbb{N}^k : \frac{a_1}{n_1} + \dots + \frac{a_k}{n_k} = b \right\}$  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  $n_1, \dots, n_r \in \mathbb{N}^* - \mathbb{N}$ ;  $n_{r+1}, \dots, n_k \in \mathbb{N}$ ;  $1 \leq r \leq k$ . There

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

positive  
infinitesimal

$\in \mathbb{R}$  (bounded)

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

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