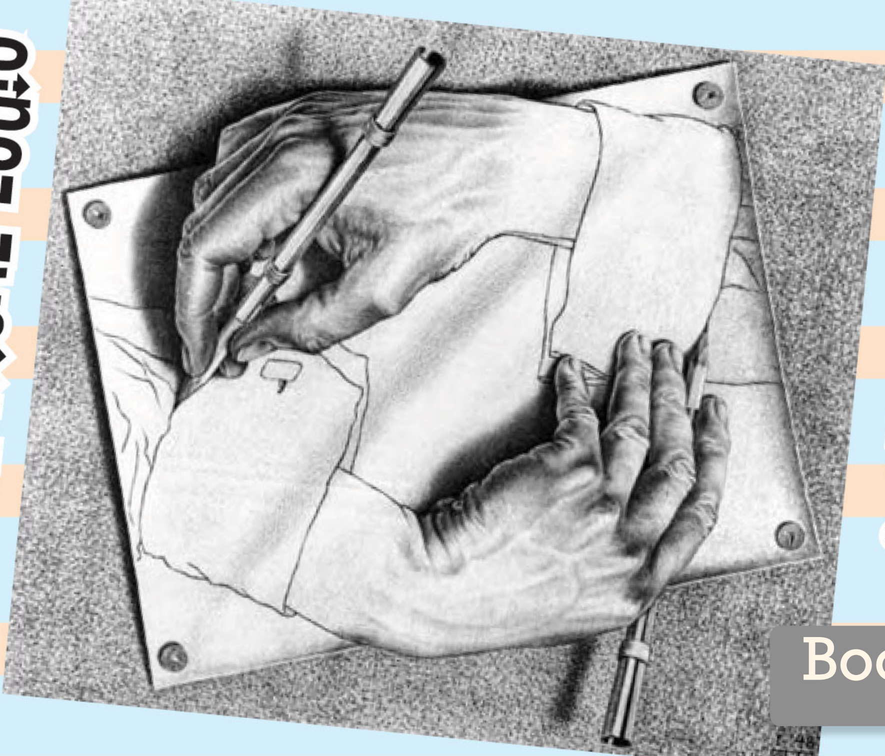
MATHEMATICAL LOGIC & SET THEORY



Book 1

Group Theory: an example of a first-order axiomatic system

An informal proof in group theory

<u>Theorem</u> If G is a (multiplicative) group of exponent 2, then G is abelian.

(G has exponent n if $g^n = 1$ for all $g \in G$.)

(Informal) <u>proof</u>: Let $a, b \in G$. Since $abab = (ab)^2 = 1$, multiplying on the left by "a" and on the right by "b" gives $aababb = a1b$, i.e. $ba = ab$. $\square$

Start with names for variables $x, y, z, \dots$ (symbols)
Special symbols for first order logic: $\exists$, $\forall$, parentheses, $\wedge$, $\vee$, $\neg$, $\rightarrow$, ...
Symbols for constants: $1, \dots$
Symbols for functions: $*, \dots$ $\quad x*y$ means $\mu(x,y)$
Symbols for relations: $=$

Axioms of Group Theory:

ID: $(\forall x)((x*1 = x) \wedge (1*x = x))$

ASSOC: $(\forall x)(\forall y)(\forall z)\ ((x*y)*z = x*(y*z))$ $\quad$ i.e. $\mu(\mu(x,y),z) = \mu(x,\mu(y,z))$

INV: $(\forall x)(\exists y)((x*y = 1) \wedge (y*x = 1))$

We happen to know some groups including C_n (cyclic group of order n), S_n (symmetric group of degree n), ...

GROUPS = {ID, ASSOC, INV} = { $(\forall x)((x*1) =$ ..., ..., ... } (the set consisting of our three axioms of group theory)

S_5 is a group, i.e. $S_5 \models$ GROUPS (S_5 is a <u>model</u> of GROUPS)

ABEL: $(\forall x)(\forall y)\ (x*y = y*x)$

ABEL-GPS = GROUPS $\cup$ {ABEL}. S_5 is a non-abelian group; $S_5 \not\models$ ABEL; $S_5 \not\models$ ABEL-GPS.

A structure has an underlying set of elements, together with an interpretation of all the symbols for constants, functions, and relations.

How do we rewrite our informal proof (above) as a formal proof in first order logic?

Σ = GROUPS $\cup$ {EXP2} where EXP2 : $(\forall x)(x * x = 1)$

ABEL is a theorem in the theory of groups of exponent 2, i.e. $\Sigma \vdash$ ABEL.

A theorem is a sequence of steps

$\Sigma \vdash \square$
$\Sigma \vdash \square$
$\Sigma \vdash \square$
$\vdots$
$\Sigma \vdash \square$

in which every step follows from previous steps by a statement in Σ, or an axiom of first order logic, or a rule of inference.

This is a formal (symbolic) proof!

An outline of a formal proof:

$\Sigma \vdash$ EXP2 since EXP2 $\in \Sigma$

$\Sigma \vdash$ (EXP2 $\rightarrow (\forall a)(a * a = 1))$ (A4) p.86

$\Sigma \vdash (\forall a)(a * a = 1)$ Modus Ponens (R1) p.86

$\vdots$

$\Sigma \vdash (\forall b)(b * b = 1)$

$\vdots$

$\Sigma \vdash (\forall a)(\forall b)((a*b)*(a*b) = 1)$

$\vdots$

$\Sigma \vdash (\forall a)(\forall b)\ ((a*((a*b)*(a*b)) = a*1)$

$\vdots$

$\Sigma \vdash (\forall a)(\forall b)(a*b = b*a)$

RICHARDS BORCHERDS
JOEL DAVID HAMKINS

$$\text{ORD3}: \underbrace{(\exists x)(\exists y)(\exists z)\left[(\forall g)\left((g=x) \vee (g=y) \vee (g=z)\right)\right.}_{\text{"there are at most three elements"}} \wedge \underbrace{(\neg \overbrace{(x=y)}^{x \neq y}) \wedge (\neg(x=z))}_{x \neq z} \wedge \left.(\neg(y=z))\right]$$

$x \neq y$ $\quad x \neq z \quad$ $y \neq z$

"there are at least 3 elements"

ABEL is independent of GROUPS (you cannot either prove or disprove that a general group is abelian). GROUPS $\nvdash$ ABEL and GROUPS $\nvdash$ $\neg$ABEL. This is because $C_3 \models$ GROUPS, $C_3 \models$ ABEL but $S_3 \models$ GROUPS, $S_3 \not\models$ ABEL.

In an arbitrary first-order theory, with axioms Σ, a statement θ is independent of Σ if $\Sigma \nvdash \theta$ and $\Sigma \nvdash \neg\theta$:

Soundness Theorem: If $\Sigma \vdash \theta$ then θ holds in every model of Σ i.e. $M \models \theta$ whenever $M \models \Sigma$.

Completeness Theorem: Converse holds: If θ holds in every model of Σ, then it is provable from Σ i.e. if $M \models \theta$ whenever $M \models \Sigma$, then $\Sigma \vdash \theta$.

Assume Σ is consistent

So: θ is independent of Σ iff there are models of Σ in which θ holds, and models of θ in which θ fails.

Σ is consistent if we cannot prove a contradiction from Σ, ie. $\Sigma \nvdash (\theta \wedge \neg\theta)$ for some θ.

Equivalently, Σ is consistent iff it has a model.

Eg. ABEL is independent of GROUPS.

ORD3 " " " " " " " ".

GROUPS is consistent.

GROUPS $\cup$ {ORD3} is consistent since it has a model. In fact it has a unique model up to isomorphism: the cyclic group C_3 of order 3. The group C_3 (or its theory) is <u>categorical</u>.

GROUPS is not categorial. (There are models, but not a unique model.)

An alternative to INV: $(\forall x)(\exists y)((x*y=1) \wedge (y*x=1))$ is to add a function symbol $\iota(\cdot)$ to the language namely $(\forall x)((x*\iota(x)=1) \wedge (\iota(x)*x=1))$

We already have a binary function symbol $\mu(\cdot,\cdot)$, $\mu(x,y) = x*y$

A <u>theorem</u> of Σ is a statement that can be proved from Σ. A proof is a sequence of statements such....

The <u>theory</u> of Σ is $Th(\Sigma) = \{\text{statements provable from } \Sigma\} = \{\text{theorems of } \Sigma\}$.

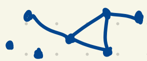
First order theory of graphs has no symbols for constants or functions; there is only one relation symbol $R(\cdot,\cdot)$, for the binary relation of adjacency. We will abbreviate $R(x,y)$ as $x \sim y$.

Axioms of graph theory: two axioms to indicate that our relation is symmetric and irreflexive.

IRREFL: $(\forall x)(\neg(x \sim x))$

SYM: $(\forall x)(\forall y)((x \sim y) \to (y \sim x))$

GRAPHS $= \{$IRREFL, SYM$\}$

 $\models$ GRAPHS  $\not\models$ GRAPHS

MIN7: $(\exists x_1)(\exists x_2)\cdots(\exists x_7)((\neg(x_1 = x_2)) \wedge \cdots \wedge (\neg(x_6 = x_7)))$

"there are at least 7 vertices"

MAX7: $(\exists x_1)(\exists x_2)\cdots(\exists x_7)(\forall y)((y = x_1) \vee \cdots \vee (y = x_7))$

"There are at most 7 vertices"

To say that Γ has exactly 7 vertices, we could write

ORD7: $(\exists x_1)(\exists x_2)\cdots(\exists x_7)\left[((\neg(x_1 = x_2)) \wedge \cdots \wedge (\neg(x_6 = x_7))) \wedge (\forall y)((y = x_1) \vee (y = x_2) \vee \cdots \vee (y = x_7))\right]$

GRAPHS $\cup$ $\{$ORD7$\}$: axioms for graphs with exactly 7 vertices.

Axioms for infinite graphs:

GRAPHS $\cup$ $\{$MIN1, MIN2, MIN3, MIN4, $\ldots\}$

In first order graph theory, we cannot express the condition that a graph is finite.

We can express the condition that a graph has at most 17 vertices.

- - - - - - - - - - - - is infinite.

We cannot express the condition that a graph is countably infinite.

The diameter of a graph is the max. distance between two vertices.

The distance between two vertices is the length of the shortest path between them.

eg. To say that a graph has diameter at most 2 in first order logic:

$$(\forall x)(\forall y)(\neg(x = y)) \to (\underbrace{(x \sim y)}_{\mathrm{dist}(x,y)=1} \vee \underbrace{(\exists z)((x \sim z) \wedge (z \sim y))}_{\mathrm{dist}(x,y) \le 2})$$

Diameter 2:

(diameter at most 2) $\wedge\ (\exists x)(\exists y)(\neg(x \sim y) \wedge \neg(x = y))$

In first order theory, we can express the condition that a graph has diameter 7 or diameter at most 7 but we cannot express the notion that a graph is connected.

Graphs of diameter ≤ 1 (i.e. cliques): $\text{GRAPHS} \cup \{(\forall x)(\forall y)((x=y) \vee (x \sim y))\} = \text{COMPL\_GRPHS}$

has models K_0, K_1, K_2, K_3, K_4, ...

For each cardinality κ (eg. $\kappa = 0, 5, \aleph_0, 2^{\aleph_0}, \ldots$) there is a model $K_\kappa \models \text{COMPL\_GRPHS}$

countably infinite

$|\mathbb{R}| =$ continuum

and any two models of the same cardinality are isomorphic.

$\text{COMPL\_GRPHS} \cup \{\text{ORD4}\}$ has a unique model $K_4 =$  up to isomorphism.

$Th(K_4) = \{$ all statements in graph theory that hold in $K_4 \}$

K_4 (or $Th(K_4)$) is categorical: K_4 is the unique model (up to isomorphism) of

$\text{COMPL\_GRPHS} \cup \{\text{ORD4}\}$ ~~or~~ ~~of~~ $Th(K_4)$

$\text{COMPL\_GRAPHS} \cup \{\text{MIN1}, \text{MIN2}, \ldots\}$ has infinitely many models. But for each cardinality κ, there is only one model (up to isomorphism) of cardinality κ.

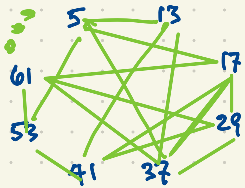
"there are inf. many vertices"

This theory is not categorical but it is κ-categorical.

Consider the graph with countably infinite vertex set $\{5, 13, 17, 29, 37, 41, 53, 61, \dots\}$ (all primes $\equiv 1 \mod 4$).

We say $p \sim q$ if p is a nonsquare mod q (iff q is a nonsquare mod p, by Quadratic Reciprocity).

eg. $5 \sim 13$ (0,1,4 are squares mod 5 but 2,3 are nonsquares mod 5).



Let's call this graph $R \models$ GRAPHS $\cup$ {INF}