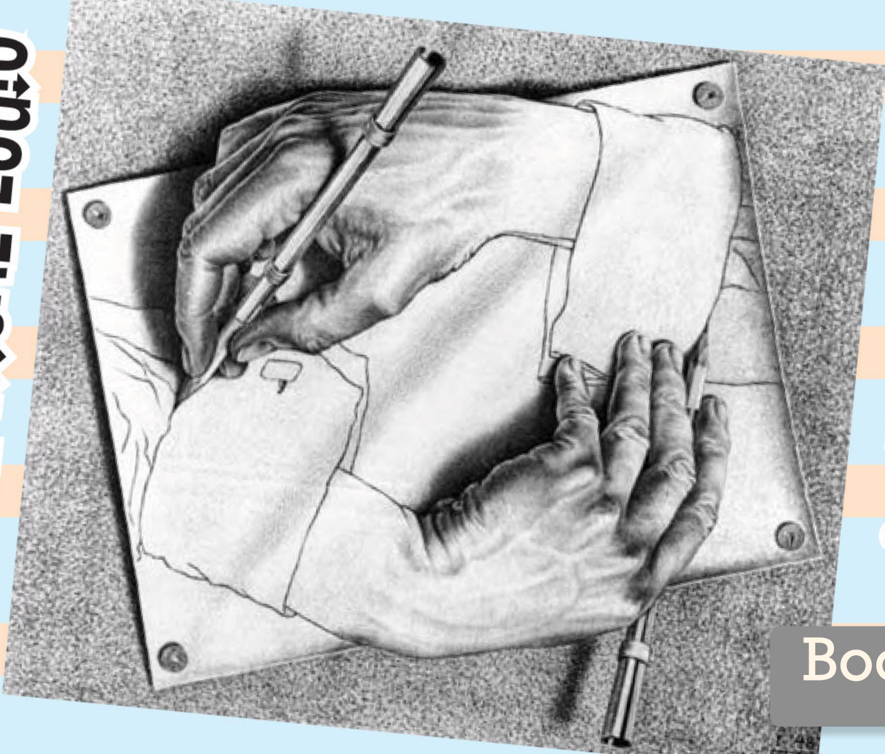
MATHEMATICAL LOGIC & SET THEORY



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 $x, y, z, \ldots$ (symbols)

Special symbols for first order logic: $\exists$, $\forall$, parentheses, $\wedge$, $\vee$, $\neg$, $\rightarrow$, ...

Symbols for constants: $1, \ldots$

Symbols for functions: $*, \ldots$ $\quad x*y$ means $\mu(x,y)$

Symbols for relations: $=$

Axioms of Group Theory:

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

ASSOC: $(\forall x)(\forall y)(\forall z)\ ((x*y)*z = x*(y*z))$

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} = $\{(\forall x)((x*1) = \ldots, \ldots, \ldots\}$ (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?

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

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

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:

$\Sigma \vdash \text{EXP2}$ since $\text{EXP2} \in \Sigma$

$\Sigma \vdash (\text{EXP2} \to (\forall a)(a*a=1))$ (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

$$\text{ORD3}: \underbrace{(\exists x)(\exists y)(\exists z)[(\forall g)((g=x)\vee(g=y)\vee(g=z))}_{\text{"there are at most three elements"}} \wedge \underbrace{\overset{x\neq y}{(\neg(x=y))} \wedge \overset{x\neq z}{(\neg(x=z))} \wedge \overset{y\neq z}{(\neg(y=z))}]}_{\text{"there are at least 3 elements"}}$$

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

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 $Th(\Sigma) = \{\text{statements provable from } \Sigma\} = \{\text{theorems of } \Sigma\}$.