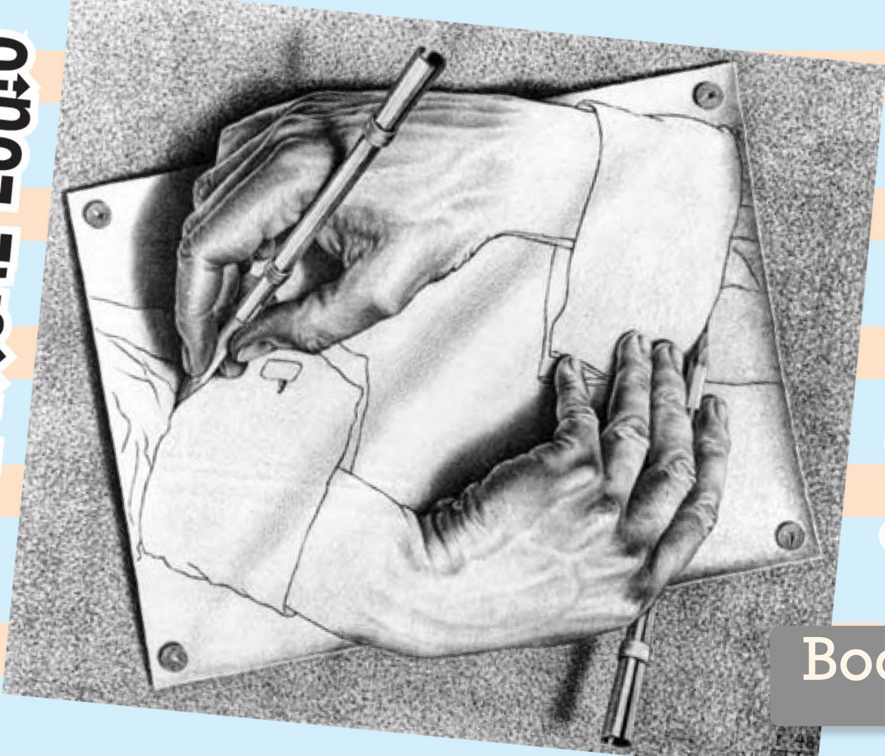
MATHEMATICAL LOGIC & SET THEORY



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: $*, \ldots$ $x*y$ means $\mu(x,y)$

Symbols for relations: $=$

Axioms of Group Theory:

i.e. $\mu(\mu(x,y),z) = \mu(x, \mu(y,z))$

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

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

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?

$\Sigma =$ 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 <u>theorem</u> is a sequence of steps

$$\begin{array}{l} \Sigma \vdash \Box \\ \Sigma \vdash \Box \\ \Sigma \vdash \Box \\ \quad\vdots \\ \Sigma \vdash \Box \end{array}$$

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 $\in \Sigma$

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

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

$\vdots$

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

$\vdots$

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

$\vdots$

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

$\vdots$

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