A Quick Introduction to Mathematical Logic

Saeed Salehi

Frontiers Summer School in Mathematics

Equational Logic, 25 August 2021

The First Identity

$$(a+b)^2 = a^2 + 2ab + b^2$$

$(a+b)^2 =$	
$(a+b)(a+b) =$	
$(a+b)a + (a+b)b =$	$x(y+z) = xy + xz$
$a(a+b) + b(a+b) =$	$xy = yx$
$(a^2+ab) + (ba+b^2) =$	
$(a^2+ab) + (ab+b^2) =$	
$a^2 + (ab+ab) + b^2 =$	$x + (y+z) = (x+y) + z$
$a^2 + (1ab + 1ab) + b^2 =$	$1x = x$
$a^2 + 2ab + b^2$	$1 + 1 = 2$

The First Identity, Generalized

$$x \circ (y \circ z) = (x \circ y) \circ z$$

$$x * y = y * x$$

$$x * (y \circ z) = (x * y) \circ (x * z)$$

$$\ell * x = x$$

$$\ell \circ \ell = \Bbbk$$

$$\overline{\overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}}$$

$$(u \circ v) * (u \circ v) = (u * u) \circ [\Bbbk * (u * v)] \circ (v * v)$$

An Example from Algebra & Analysis: $x \cdot 0 = 0$

Lemma

$$\frac{a + c = b + c}{a = b}$$

Proof.

$a + c = b + c$

$(a + c) + (-c) = (b + c) + (-c)$

$a + [c + (-c)] = b + [c + (-c)]$

$a + 0 = b + 0$

$a = b$ ∎

An Example from Algebra & Analysis: $x \cdot 0 = 0$

Theorem

$$x \cdot 0 = 0$$

Proof.

$x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$

$x \cdot 0 = 0 + x \cdot 0$

$x \cdot 0 + x \cdot 0 = 0 + x \cdot 0$

by the lemma

$x \cdot 0 = 0$ ∎

Groups

$$\begin{cases} x*(y*z) = (x*y)*z & \textit{associativity} \\ x*\mathbf{e} = x = \mathbf{e}*x & \textit{idenetity} \\ x*\imath'(x) = \mathbf{e} = \imath'(x)*x & \textit{inverse} \end{cases}$$

Example

- in $\mathbb{Z}$: $* = +$, $\mathbf{e} = 0$, $\imath' = -$. $\langle \mathbb{Z}; +, 0, - \rangle$
- in $\mathbb{Q} - \{0\}$: $* = \times$, $\mathbf{e} = 1$, $\imath'(x) = \frac{1}{x}$. $\langle \mathbb{Q}; \times, 1, 1/x \rangle$
- in $\mathrm{Sym}_{\mathrm{A}}$: $* = \circ$, $\mathbf{e} = \mathbb{I}_{\mathrm{A}}$, $\imath'(f) = f^{-1}$. $\langle \mathrm{Sym}_{\mathrm{A}}; \circ, \mathbb{I}_{\mathrm{A}}, {}^{-1} \rangle$

The 1st Theorem in Group Theory

Theorem

The identity element is unique.

Proof.

We show

$$\frac{\mathbf{e}' * x = x}{\mathbf{e}' = \mathbf{e}}$$

From the assumption and the axiom (definition) of a group

$$\frac{\mathbf{e}' * x = x}{\mathbf{e}' * \mathbf{e} = \mathbf{e}}(x = \mathbf{e})$$

$$\frac{x * \mathbf{e} = x}{\mathbf{e}' * \mathbf{e} = \mathbf{e}'}(x = \mathbf{e}')$$

Therefore, $\mathbf{e}' = \mathbf{e}$. ∎

Equational Logic

$$\frac{}{x \approx x}\ (\textit{Reflexivity})$$

$$\frac{x \approx y}{y \approx x}\ (\textit{Symmetry})$$

$$\frac{x \approx y,\ y \approx z}{x \approx z}\ (\textit{Transitivity})$$

$$\frac{x_1 \approx y_1, \cdots, x_n \approx y_n}{f(x_1 \ldots x_n) \approx f(y_1 \ldots y_n)}\ (\textit{Congruence})$$

$$\frac{x \approx y}{\sigma[x] \approx \sigma[y]}\ (\textit{Substitutivity})$$

Algebraic Structures

A non-empty set with some functions (maybe also constants) that satisfy some equalities. $\mathbb{A} = \langle \mathscr{A}; \mathfrak{f}_1^{\mathbb{A}}, \cdots, \mathfrak{f}_m^{\mathbb{A}} \rangle$.

– if $\mathfrak{f}_i$ is a constant, then $\mathfrak{f}_i^{\mathbb{A}} \in \mathscr{A}$;
– if $\mathfrak{f}_j$ is of arity $k(>0)$, then $\mathfrak{f}_j^{\mathbb{A}} : \mathscr{A}^k \to \mathscr{A}$.

Example

- Groups: $\langle G; *, \mathbf{e}, \boldsymbol{\imath}' \rangle$ — $\langle G; \mathbf{e}^{\mathbb{G}}, \boldsymbol{\imath}'^{\mathbb{G}}, *^{\mathbb{G}} \rangle$
- Rings: $\langle \mathbb{Z}; 0, 1, -, +, \times \rangle$
- Modules:

$\boxed{\text{Universal Algebra}}$

(non-)Algebraic Structures

NOT any $\langle G; *, \mathbf{e}, \boldsymbol{\imath}' \rangle$-structure is a *group*:

- $\langle \mathbb{N}; +, 0, \iota \rangle$ with $\iota(x) = x + 1$
- $\langle \mathbb{Z}; \times, 1, - \rangle$
- $\langle \mathscr{P}(X); -, \emptyset, ^{\complement} \rangle$ ($A^{\complement} = X - A$)

Definition

- Semigroup: $\langle \mathscr{A}; * \rangle$ with associative $*$ ($x*(y*z) = (x*y)*z$)
- Monoid: $\langle \mathscr{A}; *, e \rangle$ with associative $*$ and identity e ($x*e = x$)
- Group: . . . ($x*\boldsymbol{\imath}'(x) = x = \boldsymbol{\imath}'(x)*x$)
- Abelian Group: a group that satisfies also $x*y = y*x$.

Soundness and Completeness

Soundness and Completeness of Equational Logic
in Universal Algebra:

Theorem (Completeness of Equational Logic)

A set of identities $\boldsymbol{\Sigma}$ implies (by the rules of Equational Logic) an identity $\alpha \approx \beta$ if and only if every algebraic structure that satisfies the set $\boldsymbol{\Sigma}$ also satisfies the identity $\alpha \approx \beta$.

Semantic	Syntactic
$\mathbb{A} \vDash \alpha \approx \beta$ $\mathbb{A} \vDash \boldsymbol{\Sigma}$	
$\boldsymbol{\Sigma} \vDash \alpha \approx \beta$	$\boldsymbol{\Sigma} \vdash \alpha \approx \beta$

The 2nd Theorem in Group Theory

Theorem

The inverse element is unique.

Proof.

In a group G, if $ab = e$, then
$a^{-1}(ab) = a^{-1}e$, so
$(a^{-1}a)b = a^{-1}$, thus
$eb = a^{-1}$, therefore
$b = a^{-1}$.

$$\begin{array}{c} u*v=\mathfrak{e} \\ \hline \imath'(u)*(u*v)=\imath'(u)*\mathfrak{e} \\ \hline (\imath'(u)*u)*v=\imath'(u) \\ \hline \mathfrak{e}*v=\imath'(u) \\ \hline v=\imath'(u) \end{array}$$

∎