Formalize The Theory of Group

By Wei Gao

02 Dec 2002

What is Group?

A group is a pair $(G, *)$ where G is a non-empty set and * is binary operation on G which together satisfy :

- closure property
- associativity
- identity property
- inverse property

Formalization in FOL

$T = (L , \Gamma)$

$L = (V, C, F, P)$

- V: a set of individual variables
- C: a set of constant symbols
- F: function symbols
- P: predicate symbols

Γ : Axioms

Formalization Of Group

$\mathrm{T} = (\ \mathrm{L}\ ,\ \ \Gamma\ \ )$

$\mathrm{L} = (\ \mathrm{V}, \{0\}, \{+\ ,\ -\}, \Phi\ )$

Γ : Axioms.

1. $\forall x, y, z.\ (x + y) + z = x + (y + z)$
2. $\forall x.\ (x + 0 = x) \wedge (0 + x = x)$
3. $\forall x.\ (x + (-x) = 0) \wedge ((-x) + x = 0)$

?????

- A subgroup is a subset S of group elements of a group G that satisfies the four group requirements.
- How to define subgroup with the theory of group in FOL?

Simple Type Theory

$T = (L , \Gamma)$

$L = (\mathcal{V}, \mathcal{C}, \tau)$

$\mathcal{V}$: an infinite set of variable symbols

$\mathcal{C}$: a set of constant symbols

τ : a total function $\mathcal{C} \rightarrow \mathcal{T}$

Γ : Axioms

Formalization in STT

$\mathrm{T} = (\ \mathrm{L}\ ,\ \ \Gamma\ \ )$

$\mathrm{L} = (\mathcal{V}\ ,\ \ C = \{0, +, -\},\ \ \tau\ )$

$\tau(0) = l$

$\tau(+) = (l \rightarrow (l \rightarrow l))$

$\tau(-) = (l \rightarrow l)$

Γ : Axioms.

$\forall x : l.\ (x + 0 = x) \wedge (0 + x = x)$

$\forall x : l.\ (x + (-x) = 0) \wedge ((-x) + x = 0)$

$\forall x, y, z : l.\ (x + y) + z = x + (y + z)$

Subgroup

$$C_1 = C \cup \{subgroup\}$$

$$\tau(subgroup) = ((l \to *) \to *)$$

$$\Gamma_1 = \Gamma \cup \{\mathrm{A}\}$$

$$\mathrm{A}: \ subgroup = \lambda s : (l \to *), \ \forall x, y : l.$$

$$(\, s(x) \wedge s(y) \Rightarrow s(x + y)\,) \ \wedge \ (\, s(x) \Rightarrow s(-(x))\,)$$