group.lean in ℕaproche

ℕaproche Formalization: Peter Koepke

2021

We give a ForTheL version of the "multiplicative half" of `https://github.com/leanprover/lean/blob/master/library/init/algebra/group.lean` on basic concepts in group theory by J. Avigad and L. de Moura. Whereas the Lean formalization takes place within a sophisticated type system we suggest a simplistic approach in which types are naively viewed as sets.

The purpose of this text is a comparison of the technical approach in Lean with the rather natural input language ForTheL of ℕaproche. ℕaproche allows to introduce new notions like "type with multiplication" or "group" for which further structural components like a multiplication can be introduced and equipped with axioms. Since the mathematics of this text is very basic, ℕaproche can prove most lemmas automatically without explicit proofs. The formalization given here motivates to further use and adapt ℕaproche's soft types for abstract algebraic structures.

0.1 Defining Groups

Lemma 1. Every set is a class.

[synonym type/-s]

Signature 2. A type is a set.

Let α stand for a type. Let $a : t$ stand for a is an element of t.

Signature 3. A type with multiplication is a type.

Signature 4. Let α be a type with multiplication and $a, b : \alpha$. $a *^{\alpha} b$ is an element of α.

[synonym semigroup/-s]

Definition 5. A semigroup is a type with multiplication α such that for all $a, b, c : \alpha$ $(a *^{\alpha} b) *^{\alpha} c = a *^{\alpha} (b *^{\alpha} c)$.

Definition 6. A commutative semigroup is a semigroup α such that for all $a, b : \alpha$ $a *^{\alpha} b = b *^{\alpha} a$.

Definition 7. A semigroup with left cancellation is a semigroup α such that for all $a, b, c : \alpha$ $a *^{\alpha} b = a *^{\alpha} c => b = c$.

Definition 8. A semigroup with right cancellation is a semigroup α such

that for all $a, b, c : \alpha\ a *^{\alpha} b = c *^{\alpha} b => a = c$.

Signature 9. A type with one is a type.

Signature 10. Assume α is a type with one. 1^{α} is an element of α.

Definition 11. A monoid is a semigroup α such that α is a type with one and $\forall a : \alpha 1^{\alpha} *^{\alpha} a = a$ and $\forall a : \alpha a *^{\alpha} 1^{\alpha} = a$.

Definition 12. A commutative monoid is a monoid that is a commutative semigroup.

Signature 13. A type with inverses is a type.

Signature 14. Assume α is a type with inverses and $a : \alpha$. $a^{-1,\alpha}$ is an element of α.

Definition 15. A group is a monoid α such that α is a type with inverses and for all $a : \alpha a^{-1,\alpha} *^{\alpha} a = 1^{\alpha}$.

Definition 16. A commutative group is a group that is a commutative monoid.

1 Term Identities in Groups

We prove a number of simple algebraic consequences of the the group axioms. The formalizations would read even more natural if the dependence on a group α could be made implicit and one could write $a*a^{-1} = 1$ instead of $a*^{\alpha}a^{-1,\alpha} = 1^{\alpha}$. Lean's elaboration mechanism provides this important feature which we would like to implement in ℕaproche as well.

Lemma 17. (mul left comm) Let α be a commutative semigroup. Then for all $a, b, c : \alpha\ a *^{\alpha} (b *^{\alpha} c) = b *^{\alpha} (a *^{\alpha} c)$.

Lemma 18. (mul right comm) Let α be a commutative semigroup. Then for all $a, b, c : \alpha\ a *^{\alpha} (b *^{\alpha} c) = a *^{\alpha} (c *^{\alpha} b)$.

Lemma 19. (mul left cancel iff) Let α be a semigroup with left cancellation. Then for all $a, b, c : \alpha\ a *^{\alpha} b = a *^{\alpha} c <=> b = c$.

Lemma 20. (mul right cancel iff) Let α be a semigroup with right cancellation. Then for all $a, b, c : \alpha\ b *^{\alpha} a = c *^{\alpha} a <=> b = c$.

Let α denote a group.

Lemma 21. (inv mul cancel left) For all $a, b : \alpha\ a^{-1,\alpha} *^{\alpha} (a *^{\alpha} b) = b$.

Lemma 22. (inv mul cancel right) For all $a, b : \alpha\ a*^{\alpha}(b^{-1,\alpha}*^{\alpha}b) = a$.

Lemma 23. (inv eq of mul eq one) Let $a, b : \alpha$ and $a *^{\alpha} b = 1^{\alpha}$. Then $a^{-1,\alpha} = b$.

Lemma 24. (one inv) $(1^{\alpha})^{-1,\alpha} = 1^{\alpha}$.

Lemma 25. **(inv inv)** Let $a : \alpha$. Then $(a^{-1,\alpha})^{-1,\alpha} = a$.

Lemma 26. **(mul right inv)** Let $a : \alpha$. Then $a *^\alpha a^{-1,\alpha} = 1^\alpha$.

Lemma 27. **(inv inj)** Let $a, b : \alpha$ and $a^{-1,\alpha} = b^{-1,\alpha}$. Then $a = b$.

Lemma 28. **(group mul left cancel)** Let $a, b, c : \alpha$ and $a *^\alpha b = a *^\alpha c$. Then $b = c$.

Lemma 29. **(group mul right cancel)** Let $a, b, c : \alpha$ and $a *^\alpha b = c *^\alpha b$. Then $a = c$.

Proof. $a = (a *^\alpha b) *^\alpha b^{-1,\alpha} = (c *^\alpha b) *^\alpha b^{-1,\alpha} = c$. □

Lemma 30. **(mul inv cancel left)** Let $a, b : \alpha$. Then $a *^\alpha (a^{-1,\alpha} *^\alpha b) = b$.

Lemma 31. **(mul inv cancel right)** Let $a, b : \alpha$. Then $(a *^\alpha b) *^\alpha b^{-1,\alpha} = a$.

Lemma 32. **(mul inv rev)** Let $a, b : \alpha$. Then $(a *^\alpha b)^{-1,\alpha} = b^{-1,\alpha} *^\alpha a^{-1,\alpha}$.

Proof. $(a *^\alpha b) *^\alpha (b^{-1,\alpha} *^\alpha a^{-1,\alpha}) = 1^\alpha$. □

Lemma 33. **(eq inv of eq inv)** Let $a, b : \alpha$ and $a = b^{-1,\alpha}$. Then $b = a^{-1,\alpha}$.

Lemma 34. **(eq inv of mul eq one)** Let $a, b : \alpha$ and $a *^\alpha b = 1^\alpha$. Then $a = b^{-1,\alpha}$.

Lemma 35. **(eq mul inv of mul eq)** Let $a, b, c : \alpha$ and $a *^\alpha c = b$. Then $a = b *^\alpha c^{-1,\alpha}$.

Lemma 36. **(eq inv mul of mul eq)** Let $a, b, c : \alpha$ and $b *^\alpha a = c$. Then $a = b^{-1,\alpha} *^\alpha c$.

Lemma 37. **(inv mul eq of eq mul)** Let $a, b, c : \alpha$ and $b = a *^\alpha c$. Then $a^{-1,\alpha} *^\alpha b = c$.

Lemma 38. **(mul inv eq of eq mul)** Let $a, b, c : \alpha$ and $a = c *^\alpha b$. Then $a *^\alpha b^{-1,\alpha} = c$.

Lemma 39. **(eq mul of mul inv eq)** Let $a, b, c : \alpha$ and $a *^\alpha c^{-1,\alpha} = b$. Then $a = b *^\alpha c$.

Lemma 40. **(eq mul of inv mul eq)** Let $a, b, c : \alpha$ and $b^{-1,\alpha} *^\alpha a = c$. Then $a = b *^\alpha c$.

Lemma 41. **(mul eq of eq inv mul)** Let $a, b, c : \alpha$ and $b = a^{-1,\alpha} *^\alpha c$. Then $a *^\alpha b = c$.

Lemma 42. **(mul eq of eq mul inv)** let $a, b, c : \alpha$ and $a = c *^\alpha b^{-1,\alpha}$. Then $a *^\alpha b = c$.

Lemma 43. **(mul inv)** Let α be a commutative group. Let $a, b : \alpha$. Then $(a *^\alpha b)^{-1,\alpha} = a^{-1,\alpha} *^\alpha b^{-1,\alpha}$.