The Lean library file `group.lean` reformulated in ForTheL and pretty-printed

Peter Koepke

June 7, 2019

This file is a ForTheL version of the first half of
`https://github.com/leanprover/lean/blob/master/library/init/algebra/group.lean`
The second half is similar, with additive instead of multiplicative notation.

Preliminaries

Signature 1. *A* type *is a class. Let α stand for a type. Let $a : t$ stand for a is an element of t.*

Semigroups

Signature 2. *A* type with multiplication *is a type. Let α be a type with multiplication and $a, b : \alpha$. $a *^\alpha b$ is an element of α.*

[synonym semigroup/-s]

Definition 1. *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 2. *A* commutative semigroup *is a semigroup α such that for all $a, b : \alpha$ $a *^\alpha b = b *^\alpha a$.*

Definition 3. *A* semigroup with left cancellation *is a semigroup α such that for all $a, b, c : \alpha$ $a *^\alpha b = a *^\alpha c \Rightarrow b = c$.*

Definition 4. *A* semigroup with right cancellation *is a semigroup α such that for all $a, b, c : \alpha$ $a *^\alpha b = c *^\alpha b \Rightarrow a = c$.*

Signature 3. *A* type with one *is a type. Assume α is a type with one. 1^α is an element of α.*

Definition 5. *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 6. *A* commutative monoid *is a monoid that is a commutative semigroup.*

Signature 4. *A* type with inverses *is a type.*

Signature 5. *Assume α is a type with inverses and $a : \alpha$. $a^{-1,\alpha}$ is an element of α.*

0.0.1 Groups

Definition 7. *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 8. *A* commutative group *is a group that is a commutative monoid.*

Lemma 1 (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 2 (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 3 (mul left cancel iff)**.** *Let α be a semigroup with left cancellation. Then for all $a, b, c : \alpha\ a *^\alpha b = a *^\alpha c \leftrightarrow b = c$.*

Lemma 4 (mul right cancel iff)**.** *Let α be a semigroup with right cancellation. Then for all $a, b, c : \alpha\ b *^\alpha a = c *^\alpha a \leftrightarrow b = c$.*

Let α denote a group.

Lemma 5 (inv mul cancel left)**.** *For all $a, b : \alpha\ a^{-1,\alpha} *^\alpha (a *^\alpha b) = b$.*

Lemma 6 (inv mul cancel right)**.** *For all $a, b : \alpha\ a *^\alpha (b^{-1,\alpha} *^\alpha b) = a$.*

Lemma 7 (inv eq of mul eq one)**.** *Let $a, b : \alpha$ and $a *^\alpha b = 1^\alpha$. Then $a^{-1,\alpha} = b$.*

Lemma 8 (one inv)**.** $(1^\alpha)^{-1,\alpha} = 1^\alpha$.

Lemma 9 (inv inv). *Let $a : \alpha$. Then $(a^{-1,\alpha})^{-1,\alpha} = a$.*

Lemma 10 (mul right inv). *Let $a : \alpha$. Then $a *^{\alpha} a^{-1,\alpha} = 1^{\alpha}$.*

Lemma 11 (inv inj). *Let $a, b : \alpha$ and $a^{-1,\alpha} = b^{-1,\alpha}$. Then $a = b$.*

Lemma 12 (group mul left cancel). *Let $a, b, c : \alpha$ and $a *^{\alpha} b = a *^{\alpha} c$. Then $b = c$.*

Lemma 13 (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 14 (mul inv cancel left). *Let $a, b : \alpha$. Then $a *^{\alpha} (a^{-1,\alpha} *^{\alpha} b) = b$.*

Lemma 15 (mul inv cancel right). *Let $a, b : \alpha$. Then $(a *^{\alpha} b) *^{\alpha} b^{-1,\alpha} = a$.*

Lemma 16 (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 17 (eq inv of eq inv). *Let $a, b : \alpha$ and $a = b^{-1,\alpha}$. Then $b = a^{-1,\alpha}$.*

Lemma 18 (eq inv of mul eq one). *Let $a, b : \alpha$ and $a *^{\alpha} b = 1^{\alpha}$. Then $a = b^{-1,\alpha}$.*

Lemma 19 (eq mul inv of mul eq). *Let $a, b, c : \alpha$ and $a *^{\alpha} c = b$. Then $a = b *^{\alpha} c^{-1,\alpha}$.*

Lemma 20 (eq inv mul of mul eq). *Let $a, b, c : \alpha$ and $b *^{\alpha} a = c$. Then $a = b^{-1,\alpha} *^{\alpha} c$.*

Lemma 21 (inv mul eq of eq mul). *Let $a, b, c : \alpha$ and $b = a *^{\alpha} c$. Then $a^{-1,\alpha} *^{\alpha} b = c$.*

Lemma 22 (mul inv eq of eq mul). *Let $a, b, c : \alpha$ and $a = c *^{\alpha} b$. Then $a *^{\alpha} b^{-1,\alpha} = c$.*

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

Lemma 24 (eq mul of inv mul eq). *Let $a, b, c : \alpha$ and $b^{-1,\alpha} *^{\alpha} a = c$. Then $a = b *^{\alpha} c$.*

Lemma 25 (mul eq of eq inv mul)**.** *Let* $a, b, c : \alpha$ *and* $b = a^{-1,\alpha} *^{\alpha} c$. *Then* $a *^{\alpha} b = c$.

Lemma 26 (mul eq of eq mul inv)**.** *let* $a, b, c : \alpha$ *and* $a = c *^{\alpha} b^{-1,\alpha}$. *Then* $a *^{\alpha} b = c$.

Lemma 27 (mul inv)**.** *Let* α *be a commutative group. Let* $a, b : \alpha$. *Then* $(a *^{\alpha} b)^{-1,\alpha} = a^{-1,\alpha} *^{\alpha} b^{-1,\alpha}$.