Modern Algebra

Chapter I. Groups

I.1. Semigroups, Monoids, and Groups—Proofs of Theorems

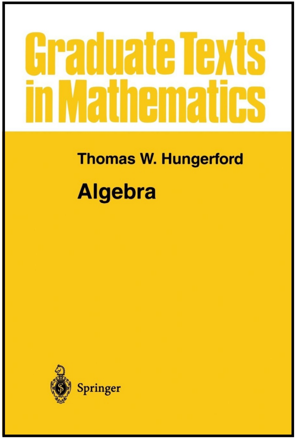

Table of contents

Proposition I.1.4

Proposition I.1.4. Let G be a semigroup. Then G is a group if and only if for all $a, b \in G$ the equations $ax = b$ and $ya = b$ have solutions in G.

Proof. First, if G is a group then a and b have inverses, so $ax = b$ implies $a^{-1}(ax) = a^{-1}b$ and by associativity $(a^{-1}a)x = a^{-1}b$ or $ex = a^{-1}b$ or $x = a^{-1}b$. Similarly $ya = b$ implies that $y = ba^{-1}$. So $ax = b$ and $ya = b$ have solutions in G.

Proposition I.1.4

Proposition I.1.4. Let G be a semigroup. Then G is a group if and only if for all $a, b \in G$ the equations $ax = b$ and $ya = b$ have solutions in G.

Proof. First, if G is a group then a and b have inverses, so $ax = b$ implies $a^{-1}(ax) = a^{-1}b$ and by associativity $(a^{-1}a)x = a^{-1}b$ or $ex = a^{-1}b$ or $x = a^{-1}b$. Similarly $ya = b$ implies that $y = ba^{-1}$. So $ax = b$ and $ya = b$ have solutions in G.

Second, suppose $ax = b$ and $ya = b$ have solutions. By Proposition I.1.3, we need only show that G has a left identity and that each $a \in G$ has a left inverse. Now for all $a \in G$, $ya = a$ has a solution, say $y = e_a$. For any $b \in G$, notice that the equation $ax = b$ has a solution, say $ac = b$. We then have $e_a b = e_a(ac) = (e_a a)c = ac = b$ and so e_a is a left identity for all elements of G, so we denote it as $e_a = e$.

Proposition I.1.4

Proposition I.1.4. Let G be a semigroup. Then G is a group if and only if for all $a, b \in G$ the equations $ax = b$ and $ya = b$ have solutions in G.

Proof. First, if G is a group then a and b have inverses, so $ax = b$ implies $a^{-1}(ax) = a^{-1}b$ and by associativity $(a^{-1}a)x = a^{-1}b$ or $ex = a^{-1}b$ or $x = a^{-1}b$. Similarly $ya = b$ implies that $y = ba^{-1}$. So $ax = b$ and $ya = b$ have solutions in G.

Second, suppose $ax = b$ and $ya = b$ have solutions. By Proposition I.1.3, we need only show that G has a left identity and that each $a \in G$ has a left inverse. Now for all $a \in G$, $ya = a$ has a solution, say $y = e_a$. For any $b \in G$, notice that the equation $ax = b$ has a solution, say $ac = b$. We then have $e_a b = e_a(ac) = (e_a a)c = ac = b$ and so e_a is a left identity for all elements of G, so we denote it as $e_a = e$. Finally, the equation $ya = e$ has solution for all $a \in G$, so each $a \in G$ has a left inverse. Therefore, by Proposition I.1.3, G is a group. □

Proposition I.1.4

Proposition I.1.4. Let G be a semigroup. Then G is a group if and only if for all $a, b \in G$ the equations $ax = b$ and $ya = b$ have solutions in G.

Proof. First, if G is a group then a and b have inverses, so $ax = b$ implies $a^{-1}(ax) = a^{-1}b$ and by associativity $(a^{-1}a)x = a^{-1}b$ or $ex = a^{-1}b$ or $x = a^{-1}b$. Similarly $ya = b$ implies that $y = ba^{-1}$. So $ax = b$ and $ya = b$ have solutions in G.

Second, suppose $ax = b$ and $ya = b$ have solutions. By Proposition I.1.3, we need only show that G has a left identity and that each $a \in G$ has a left inverse. Now for all $a \in G$, $ya = a$ has a solution, say $y = e_a$. For any $b \in G$, notice that the equation $ax = b$ has a solution, say $ac = b$. We then have $e_a b = e_a(ac) = (e_a a)c = ac = b$ and so e_a is a left identity for all elements of G, so we denote it as $e_a = e$. Finally, the equation $ya = e$ has solution for all $a \in G$, so each $a \in G$ has a left inverse. Therefore, by Proposition I.1.3, G is a group. □

Proposition I.1.5

Theorem I.1.5. Let $R(\sim)$ be an equivalence relation on a monoid G such that $a_1 \sim a_2$ and $b_1 \sim b_2$ imply $a_1 b_1 \sim a_2 b_2$ for all $a_i, b_i \in G$. Such an equivalence relation on G is called a *congruence relation* on G. Then the set G/R of all equivalence classes of G under R is a monoid itself under the binary operation defined by $(\overline{a})(\overline{b}) = \overline{ab}$, where $\overline{x}$ denotes the equivalence class containing x. If G is a group, then so is G/R. If G is abelian, then so is G/R.

Proof. Recall that the equivalence classes of an equivalence relation on a set partition the set. So if $\overline{a}_1 = \overline{a}_2$ and $\overline{b}_1 = \overline{b}_2$ then $a_1 \sim a_2$ and $b_1 \sim b_2$. By hypothesis, $a_1 b_1 \sim a_2 b_2$ and so $\overline{a_1 b_1} = \overline{a_2 b_2}$. So the binary operation on G/R is well defined (i.e., independent of the choice of the representative of the equivalence class in the definition of the binary operation).

Proposition I.1.5

Theorem I.1.5. Let $R(\sim)$ be an equivalence relation on a monoid G such that $a_1 \sim a_2$ and $b_1 \sim b_2$ imply $a_1 b_1 \sim a_2 b_2$ for all $a_i, b_i \in G$. Such an equivalence relation on G is called a *congruence relation* on G. Then the set G/R of all equivalence classes of G under R is a monoid itself under the binary operation defined by $(\overline{a})(\overline{b}) = \overline{ab}$, where $\overline{x}$ denotes the equivalence class containing x. If G is a group, then so is G/R. If G is abelian, then so is G/R.

Proof. Recall that the equivalence classes of an equivalence relation on a set partition the set. So if $\overline{a}_1 = \overline{a}_2$ and $\overline{b}_1 = \overline{b}_2$ then $a_1 \sim a_2$ and $b_1 \sim b_2$. By hypothesis, $a_1 b_1 \sim a_2 b_2$ and so $\overline{a_1 b_1} = \overline{a_2 b_2}$. So the binary operation on G/R is well defined (i.e., independent of the choice of the representative of the equivalence class in the definition of the binary operation).

Proposition I.1.5 (continued 1)

Proof (continued). Since

$$\begin{aligned} \overline{a}(\overline{b}\,\overline{c}) &= \overline{a}(\overline{bc}) \text{ by the definition of } \overline{b}\,\overline{c} \\ &= \overline{a(bc)} \text{ by the definition of } \overline{a}(\overline{bc}) \\ &= \overline{(ab)c} \text{ since associativity holds in } G \\ &= (\overline{ab})\overline{c} \text{ by the definition of } (\overline{ab})\overline{c} \\ &= (\overline{a}\,\overline{b})\overline{c} \text{ by the definition of } \overline{a}\,\overline{b} \end{aligned}$$

then the binary operation is associative and G/R is a semigroup. The identity of G/R is $\overline{e}$ since

$$\begin{aligned} (\overline{a})(\overline{e}) &= (\overline{ae}) \text{ by the definition of } (\overline{a})(\overline{e}) \\ &= \overline{a} \text{ since } e \text{ is a right identity in } G \\ &= (\overline{ea}) \text{ since } e \text{ is a left identity in } G \\ &= (\overline{e})(\overline{a}) \text{ by the definition of } (\overline{e})(\overline{a}) \end{aligned}$$

for all $\overline{a} \in G/R$ and so G/R is a monoid.

Proposition I.1.5 (continued 1)

Proof (continued). Since

$$\begin{aligned}
\overline{a}(\overline{b}\overline{c}) &= \overline{a}(\overline{bc}) \text{ by the definition of } \overline{b}\overline{c} \\
&= \overline{a(bc)} \text{ by the definition of } \overline{a}(\overline{bc}) \\
&= \overline{(ab)c} \text{ since associativity holds in } G \\
&= (\overline{ab})\overline{c} \text{ by the definition of } (\overline{ab})\overline{c} \\
&= (\overline{a}\overline{b})\overline{c} \text{ by the definition of } \overline{a}\overline{b}
\end{aligned}$$

then the binary operation is associative and G/R is a semigroup. The identity of G/R is $\overline{e}$ since

$$\begin{aligned}
(\overline{a})(\overline{e}) &= (\overline{ae}) \text{ by the definition of } (\overline{a})(\overline{e}) \\
&= \overline{a} \text{ since } e \text{ is a right identity in } G \\
&= (\overline{ea}) \text{ since } e \text{ is a left identity in } G \\
&= (\overline{e})(\overline{a}) \text{ by the definition of } (\overline{e})(\overline{a})
\end{aligned}$$

for all $\overline{a} \in G/R$ and so G/R is a monoid.

Proposition I.1.5 (continued 2)

Proof (continued). If G is a group then any $a \in G$ has an inverse $a^{-1} \in G$ and

$$\begin{aligned} (\overline{a^{-1}})(\overline{a}) &= (\overline{a^{-1}a}) \text{ by the definition of } (\overline{a^{-1}})(\overline{a}) \\ &= \overline{e} \text{ since } a^{-1}a = e \text{ in } G \\ &= (\overline{aa^{-1}}) \text{ since } aa^{-1} = e \text{ in } G \\ &= (\overline{a})(\overline{a^{-1}}) \text{ by the definition of } (\overline{a})(\overline{a^{-1}}) \end{aligned}$$

and so G/R is a group. If G is abelian then $ab = ba$ for all $a, b \in G$ and so

$$\begin{aligned} (\overline{a})(\overline{b}) &= (\overline{ab}) \text{ by the definition of } (\overline{a})(\overline{b}) \\ &= (\overline{ba}) \text{ since } ab = ba \text{ in } G \\ &= (\overline{b})(\overline{a}) \text{ by the definition of } (\overline{b})(\overline{a}) \end{aligned}$$

for all $\overline{a}, \overline{b} \in G/R$ and so G/R is abelian. □

Proposition I.1.5 (continued 2)

Proof (continued). If G is a group then any $a \in G$ has an inverse $a^{-1} \in G$ and

$$\begin{aligned} (\overline{a^{-1}})(\overline{a}) &= (\overline{a^{-1}a}) \text{ by the definition of } (\overline{a^{-1}})(\overline{a}) \\ &= \overline{e} \text{ since } a^{-1}a = e \text{ in } G \\ &= (\overline{aa^{-1}}) \text{ since } aa^{-1} = e \text{ in } G \\ &= (\overline{a})(\overline{a^{-1}}) \text{ by the definition of } (\overline{a})(\overline{a^{-1}}) \end{aligned}$$

and so G/R is a group. If G is abelian then $ab = ba$ for all $a, b \in G$ and so

$$\begin{aligned} (\overline{a})(\overline{b}) &= (\overline{ab}) \text{ by the definition of } (\overline{a})(\overline{b}) \\ &= (\overline{ba}) \text{ since } ab = ba \text{ in } G \\ &= (\overline{b})(\overline{a}) \text{ by the definition of } (\overline{b})(\overline{a}) \end{aligned}$$

for all $\overline{a}, \overline{b} \in G/R$ and so G/R is abelian. □

Theorem I.1.6

Theorem I.1.6. Generalized Associative Law.
If G is a semigroup and $a_1, a_2, \ldots, a_n \in G$ then any two meaningful products of $a_1, a_2, \ldots, a_n \in G$ in this order are equal.

Proof. We use induction to show that for all $n \in \mathbb{N}$, any meaningful product of $a_1, a_2, \ldots, a_n$ is equal to the standard n product $\prod_{i=1}^{n} a_i$. This is easily true for $n = 1$ and $n = 2$. If $n > 2$, then by definition $(a_1 a_2 \cdots a_n) = (a_1 a_2 \cdots a_m)(a_{m+1} a_{m+2} \cdots a_n)$ for some $m < n$.

Theorem I.1.6

Theorem I.1.6. Generalized Associative Law.
If G is a semigroup and $a_1, a_2, \ldots, a_n \in G$ then any two meaningful products of $a_1, a_2, \ldots, a_n \in G$ in this order are equal.

Proof. We use induction to show that for all $n \in \mathbb{N}$, any meaningful product of $a_1, a_2, \ldots, a_n$ is equal to the standard n product $\prod_{i=1}^{n} a_i$. This is easily true for $n = 1$ and $n = 2$. If $n > 2$, then by definition $(a_1 a_2 \cdots a_n) = (a_1 a_2 \cdots a_m)(a_{m+1} a_{m+2} \cdots a_n)$ for some $m < n$. Suppose we have established that $(a_1 a_2 \cdots a_k) = \prod_{i=1}^{k} a_i$ for $k \le n$. Consider $k = n + 1$:

$$(a_1 a_2 \cdots a_{n+1}) = (a_1 a_2 \cdots a_m)(a_{m+1} a_{m+2} \cdots a_{n+1}) \text{ by the definition of meaningful product}$$

Theorem I.1.6

Theorem I.1.6. Generalized Associative Law.
If G is a semigroup and $a_1, a_2, \ldots, a_n \in G$ then any two meaningful products of $a_1, a_2, \ldots, a_n \in G$ in this order are equal.

Proof. We use induction to show that for all $n \in \mathbb{N}$, any meaningful product of $a_1, a_2, \ldots, a_n$ is equal to the standard n product $\prod_{i=1}^{n} a_i$. This is easily true for $n = 1$ and $n = 2$. If $n > 2$, then by definition $(a_1 a_2 \cdots a_n) = (a_1 a_2 \cdots a_m)(a_{m+1} a_{m+2} \cdots a_n)$ for some $m < n$. Suppose we have established that $(a_1 a_2 \cdots a_k) = \prod_{i=1}^{k} a_i$ for $k \leq n$. Consider $k = n + 1$:

$$(a_1 a_2 \cdots a_{n+1}) = (a_1 a_2 \cdots a_m)(a_{m+1} a_{m+2} \cdots a_{n+1}) \text{ by the definition of meaningful product}$$

Theorem I.1.6 (continued 1)

Proof (continued).

$$\begin{aligned}
&= \left(\prod_{i=1}^{m} a_i\right)\left(\prod_{i=1}^{n+1-m} a_{m+i}\right) \text{ by the induction hypothesis} \\
&\qquad\qquad \text{for } k = m \text{ and } k = n+1-m \\
&= \left(\prod_{i=1}^{m} a_i\right)\left(\left(\prod_{i=1}^{n-m} a_{m+i}\right)(a_{n+1})\right) \text{ by the definition} \\
&\qquad\qquad \text{of the standard } n \text{ product} \\
&= \left(\left(\prod_{i=1}^{m} a_i\right)\left(\prod_{i=1}^{n-m} a_{m-i}\right)\right) a_{n+1} \text{ by associativity} \\
&= \left(\prod_{i=1}^{n} a_i\right) a_{n+1} \text{ by the induction hypothesis for } k = n
\end{aligned}$$

Theorem I.1.6 (continued 2)

Theorem I.1.6. Generalized Associative Law.
If G is a semigroup and $a_1, a_2, \ldots, a_n \in G$ then any two meaningful products of $a_1, a_2, \ldots, a_n \in G$ then any two meaningful products of $a_1, a_2, \ldots, a_n$ in this order are equal.

Proof (continued).

$$= \prod_{i=1}^{n+1} a_i \text{ by the definition of standard } n \text{ product.}$$

So the result holds for $k = n + 1$ and hence holds for all $k \in \mathbb{N}$. So any meaningful product of $a_1, a_2, \ldots, a_n$ is equal to the standard n product and hence all meaningful products of $a_1, a_2, \ldots, a_n$ are equal to each other. □