

Chapter B: Abstract Algebra

Groups

Definition 1.1: Semigroups, Monoids

A non-empty set G equipped with an associative binary operation $G \times G \rightarrow G$ is called a semigroup. For every $a, b, c \in G$, we have

$$a(bc) = (ab)c \quad (1)$$

A *monoid* is a semigroup G which contains a *two-sided identity* element $e \in G$ such that $ae = ea$ for all $a \in G$. (not necessarily unique)

Monoids admit unique two-sided identities.

Lemma 1.1: Monoids: unique identity

Let e and i be two-sided identities for a monoid G , then

Proof.

$$e = ei = i$$



Definition 1.2: Group

A semigroup G is a group if every element $a \in G$ admits a two-sided inverse a^{-1} . (not necessarily unique)

$$aa^{-1} = a^{-1}a = e$$

Proposition 1.1: Properties of Groups (Hungerford: Theorem 1.2)

Let G be a group with identity e , which is unique by lemma 1.1. Then

(i) $c \in G$ and $cc = c$ implies $c = e$.

(ii) Left/Right cancellation:

$$\begin{cases} ab = ac \implies b = c \\ ba = ca \implies b = c \end{cases}$$

(iii) If $a \in G$, its two-sided inverse is unique.

(iv) Let $a \in G$, then the inverse of its two-sided inverse (uniqueness guaranteed by iii), is a itself; or $(a^{-1})^{-1} = a$.

(v) If $a, b \in G$, then the following equations in x, y admit unique solutions

$$\begin{cases} ax = b \\ ya = b \end{cases}$$

Proof of Proposition 1.1.

Proof of Part (i):

$$cc = c \implies (cc)c^{-1} = cc^{-1} \implies c(cc^{-1}) = e \implies ce = c = e$$

Proof of Part (ii): First claim:

$$\begin{aligned} ab = ac &\implies a^{-1}(ab) = a^{-1}(ac) \\ &\implies (a^{-1}a)b = (a^{-1}a)c \implies eb = ec \implies b = c \end{aligned}$$

Second claim is the same, just cancel from the right using $aa^{-1} = e$ and associativity.

Proof of Part (iii): Suppose b and c are two-sided inverse for a , it follows from Part ii that

$$ab = ac \implies b = c = a^{-1}$$

Proof of Part (iv): From Part iii, the two-sided inverses of group elements exist and are unique, and $a^{-1}a = aa^{-1}$ so a is an inverse for a^{-1} , and it is the only inverse.

Proof of Part (v): First equation: write $ax = b = a(a^{-1}b)$, left-cancelling reads $x = a^{-1}b$, uniqueness follows from Part ii. Second equation is similar. ■

Lemma 1.2: Group: equality lemma

For any pair of elements $a, b \in G$, $a = b \iff ab^{-1} = e$.

Proof. (\implies): $a = b \implies ab^{-1} = bb^{-1} = e$. (\impliedby): $ab^{-1} = e \implies a(b^{-1}b) = eb \implies a = eb = b$. ■

Proposition 1.2: Semigroup: upgrade to group (Hungerford Proposition 1.3)

Let G be a semigroup, G is also a group iff both of the conditions below hold

- Existence of a left-identity: there exists $e \in G$ for every $a \in G$, $ea = a$.

- Existence of left-inverses: for every $a \in G$, there exists a $a^{-1} \in G$ with $a^{-1}a = e$, where e is any left-identity element.

Proof. (\Leftarrow) is trivial. Suppose both conditions hold, notice the proof for Proposition 1.1 Part (i) we only used left-cancellation. $cc = c \Rightarrow e$. To prove a^{-1} is also a right-inverse for a , we can force it as follows:

$$(aa^{-1})(aa^{-1}) = a(a^{-1}a)a^{-1} = aea^{-1} = e \Rightarrow aa^{-1} = e$$

and a^{-1} is also a right-inverse, so every element $a \in G$ admits a two-sided inverse denoted by a^{-1} . To show e is also a right-identity for any arbitrary element $a \in G$,

$ae = a(a^{-1}a)$	left inverse
$= (aa^{-1})a$	associativity
$= ea$	right inverse
$= a$	left identity

■

Proposition 1.3: Semigroup: upgrade to group (Hungerford Proposition 1.4)

Let G be a semigroup, G is a group iff for every pair of elements $a, b \in G$, the equations in x and y

$$\begin{cases} ax = b \\ ya = b \end{cases} \quad (2)$$

have solutions (not necessarily unique).

Proof. If G is a group, the existence of the solutions to eq. (2) follow from Proposition 1.1. We will attempt the contrapositive. Suppose G has no left identity, for every $e \in G$ we can always find an element $a \in G$ such that $ea \neq a$, but this is precisely the (first) equation for $a = a$ and $b = a$.

Now suppose G has a left identity element (not necessarily unique). Fix $e \in G$ as any left-identity, and suppose there is an element $a \in G$ with no left inverse, so for every $b \in G$, $ba \neq e$. But b is precisely the solution to the (second) equation with parameters $a = a$ and $b = e$. The negation of Proposition 1.2 is precisely the negation of Proposition 1.3, and the proof is complete. ■

Proposition 1.4: Hungerford Theorem 1.5

Let R/\sim be an equivalence relation on a group G , such that it 'preserves' the

group multiplication. More precisely,

$$\begin{cases} a_1 \sim a_2 \\ b_1 \sim b_2 \end{cases} \implies a_1 b_1 \sim a_2 b_2$$

Then the set G/R of all equivalence classes of G under R is a monoid under the binary operation defined by

$$(\bar{a})(\bar{b}) = \overline{ab} \quad \begin{array}{l} \text{reads: the product of two classes is the class} \\ \text{containing the product of any pair} \\ \text{of elements from the two classes} \end{array} \quad (3)$$

where \bar{a} denotes the equivalence class containing a . If G is a group, so is G/R , if G is an abelian group, so is G/R .

Proof. First, notice the binary operation in Equation (3) is well defined. It is independent of the equivalence class representatives chosen, as we have restriction on R that 'forces' the operation on G/R to be well defined. Indeed, let \bar{a} and \bar{b} be elements of G/R , if $a_1, a_2 \in \bar{a}$, and $b_1, b_2 \in \bar{b}$, by definition of R :

$$a_1 \sim a_2 \quad \text{and} \quad b_1 \sim b_2$$

by Equation (3), $a_1 b_1 \sim a_2 b_2 \implies \overline{a_1 b_1} = \overline{a_2 b_2}$.

Associativity is proven similarly, fix $\bar{a}, \bar{b}, \bar{c} \in G/R$, we pass the argument to any of the representatives of the three classes, so

$$(\bar{a}\bar{b})\bar{c} \triangleq \overline{ab\bar{c}} = \overline{(ab)c} = \overline{a(bc)} \triangleq \overline{a\bar{b}c} = \bar{a}(\bar{b}\bar{c})$$

Pass the argument to the representatives, let e denote the identity element in G , it is easily shown that \bar{e} is the identity element in G/R , similarly for two-sided inverses and commutativity of the binary operation. ■

Homomorphisms and Subgroups

Definition 2.1: Homomorphism

Let G and H be semigroups, $f : G \rightarrow H$ is a semi-group *homomorphism* if for all $a, b \in G$,

$$f(ab) = f(a)f(b) \quad (4)$$

Definition 2.2: Monomorphism

Injective homomorphism.

Definition 2.3: Epimorphism

Surjective homomorphism.

Definition 2.4: Isomorphism

Bijjective homomorphism.

Definition 2.5: Endomorphism

Homomorphism for which the domain and codomain (not the range) are equal; i.e $H = G$.

Definition 2.6: Automorphism

Bijjective endomorphism.

Definition 2.7: Kernel of a homomorphism

The kernel of $f \in \text{Hom}(G, H)$ is defined

$$\text{Ker } f = \left\{ a \in G, f(a) = e \in H \right\} \quad (5)$$

as the set of elements in G that get sent to the identity of H .

Proposition 2.1: Hungerford Theorem 2.3

Let G and H be groups and let $f \in \text{Hom}(G, H)$. Denote the identity elements of G and H by e_G and e_H

- (i) $f(e_G) = e_H$,
- (ii) $f(a^{-1}) = (f(a))^{-1}$ for every $a \in G$.
- (iii) f is a monomorphism iff $\text{ker } f = \{e_G\}$,
- (iv) f is an isomorphism iff there exists a homomorphism $f^{-1} : H \rightarrow G$ that is also a two-sided inverse for f . In symbols:

$$f \circ f^{-1} = \text{id}_H \quad \text{and} \quad f^{-1} \circ f = \text{id}_G \quad (6)$$

Proof of Proposition 2.1.

Proof of Part (i): We will use Proposition 1.1 (i). Since $f(e_G) = f(e_G e_G) = f(e_G)f(e_G)$ in H , we see that $f(e_G) = e_H$ and $e_G \in \text{Ker } f$

Proof of Part (ii): Let $a \in G$ be arbitrary, using Part (i), we can 'pass the multiplication' between $f(a)$ and $f(a^{-1})$ into G ,

$$f(a)f(a^{-1}) = f(e_G) = e_H \implies f(a^{-1}) = (f(a))^{-1}$$

Proof of Part (iii): Suppose $\text{ker } f = e_G$. Let $a, b \in G$ such that $f(a) = f(b)$. The equality lemma Lemma 1.2 tells us $(f(a))^{-1} = f(b)$ and $b = a^{-1}$, so $a = b$ by the Lemma again; f is injective.

Conversely, suppose f is injective, Part (i) tell us $\{e_G\} \subseteq \text{ker } f$. Suppose $a \in \text{ker } f \subseteq G$, but $e_G \in \text{ker } f$, so $f(a) = f(e_G) = e_H$ forces ae_G , and $\text{ker } f = \{e_G\}$.

Proof of Part (iv): (\Leftarrow) is trivial since the existence of a (functional) two-sided inverse is equivalent to bijectivity. Suppose f is an isomorphism, and define f^{-1} as its two-sided (functional) inverse, it suffices to show that $f^{-1} \in \text{Hom}(H, G)$. Fix $f(a)$ and $f(b)$ as arbitrary elements in H . We can do this because f is a bijection, so every element in H has a unique 'representative' in G .

$$f^{-1}(f(a)) f^{-1}(f(b)) = ab = f^{-1}(f(ab)) = f^{-1}(f(a)f(b))$$

■