Chapter B: Abstract Algebra

Groups

Definition 1.1: Semigroups, Monoids

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

$$a(bc) = (ab)c \tag{1}$$

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

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

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 $a \in G$,

$$\begin{aligned} ae &= a(a^{-1}a) && \text{left inverse} \\ &= (aa^{-1})a && \text{associativity} \\ &= ea && \text{right inverse} \\ &= a && \text{left identity} \end{aligned}$$

■

Proposition 1.3: Semigroup: upgrade to group II (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

$$\begin{cases} ax = b \\ ya = b \end{cases} \tag{2}$$

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

$$(\overline{a})(\overline{b}) = \overline{ab} \qquad \text{reads: the product of two classes is the class containing the product of any pair of elements from the two classes} \tag{3}$$

where $\overline{a}$ 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 $\overline{a}$ and $\overline{b}$ be elements of G/R, if $a_1, a_2 \in \overline{a}$, and $b_1, b-2 \in \overline{b}$, by definition of R:

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

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

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

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

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

Homomorphisms

Definition 2.1: Homomorphism

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

$$f(ab) = f(a)f(b) \tag{4}$$

Definition 2.2: Monomorphism

Injective homomorphism.

Definition 2.3: Epimorhpism

Surjective homomorphism.

Definition 2.4: Isomorphism

Bijective homomorphism.

Definition 2.5: Endomorphism

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

Definition 2.6: Automorphism

Bijective endomorphism.

Definition 2.7: Kernel of a homomorphism

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

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

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 $f \in \mathrm{Hom}(G, H)$. 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 $\ker f = \{e_G\}$,

(iv) f is an isomorphism iff there exists a homomorphism $f^{-1} : H \to G$ that is also a two-sided inverse for f. In symbols:

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

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 $f(e_G) = H$ and $e_G \in \operatorname{Ker} f$

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 $\ker f = e_G$. 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 $\{e_G\} \subseteq \ker f$. Suppose $a \in \ker f \subseteq G$, but $e_G \in \ker f$, so $f(a) = f(e_G) = e_H$ forces $a = e_G$, and $\ker f = \{e_G\}$.

Proof of Part (iv): ($\impliedby$) 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 $f^{-1} \in \operatorname{Hom}(H, G)$. 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.

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

■

Definition 2.8: Subgroup $H < G$

Let G be a group. If H is a non-empty subset of G that is closed under group operations, then it is a *subgroup of* G. We write $H < G$.

The *trivial subgroup* of G is $\{e\}$ and consists of one element. H is called a *proper subgroup* if $H \neq G$ and $H \neq \{e\}$.

Proposition 2.2: Hungerford Exercise 9

Let $f \in \operatorname{Hom}(G, H)$, $A < G$ and $B < H$,

(i) $\operatorname{Ker} f$ is a subgroup of G,

(ii) $f(A)$ is a subgroup of H,

(iii) $f^{-1}(B)$ is a subgroup of G.

Subgroups

Proposition 3.1: Subgroup criteria (Hungerford Theorem 2.5)

A non-subset $H \subseteq G$ is a subgroup iff for any a, b in H, $ab^{-1} \in H$.

Proof. ($\Longleftarrow$): Choose $a = b$, then $aa^{-1} = e \in H$ acts as the two-sided identity in H, and $ea^{-1} = a^{-1} \in H$ for every $a \in H$. So H is a subgroup by Proposition 1.2. ($\Longrightarrow$): If H is a subgroup, then Proposition 1.2 tells us $b^{-1} \in H$ for every $b \in H$, hence $ab^{-1} \in H$ for elements $a, b \in H$. ■

Corollary 3.1: Hungerford Corollary 2.6

If G is a group and $\{H_i,\, i \in I\}$ is a nonempty family of subgroups, then their intersection $H \triangleq \cap_{i \in I} H_i$ is again a subgroup in G.

Proof. Let $a, b \in H$, then $ab^{-1} \in H_i$ for every $i \in I$, hence $ab^{-1} \in \cap_{i \in I} H_i = H$, and H is a subgroup by Proposition 3.1. ■

Definition 3.1: Subgroup generated by $A \subseteq G$

Let A be a subset of G, the *subgroup generated by* A is the smallest subgroup $H < G$ that contains A as a subset, denoted by $\langle A \rangle$.

Proposition 3.1 gives us an explicit formula for H,

$$H = \bigcap_{\substack{H_i < G \\ A \subseteq H_i}} H_i$$

If A is finite, and $H = \langle A \rangle$ is said to be *finitely generated.* We also write

$$H = \langle a_1, \ldots, a_n \rangle = \Big\langle \{a_1, \ldots, a_n\} \Big\rangle$$

If A consists of one element, $\{a\} = A$, then $\langle a \rangle = \langle \{a\} \rangle$ is called the *cyclic group generated by* a.

Proposition 3.2: Hungerford Theorem 2.8

If G is a group and $A \subseteq G$ is a non-empty subset, the subgroup generated by A is precisely the collection of all finite products (powers included), or

$$\langle A \rangle = \left\{ a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t},\, a_i \in A,\, n_i \in \mathbb{Z} \right\}$$

If $A = \{a\}$, then $\langle A \rangle = \left\{a^k,\ k \in \mathbb{Z}\right\}$.

Proof. Let $W = \left\{a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t},\ a_i \in A,\ n_i \in \mathbb{Z}\right\}$. We first show W is a subgroup of G. Indeed, if $n_1 = n_2 = \cdots = n_t = 0$, then $a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} = e$. And for any $b \in W$,

$$b = a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} \implies b^{-1} = a_t^{-n_t} \cdots a_2^{-n_2} a_1^{-n_1}$$

where each $-n_i \in \mathbb{Z}$, so $b^{-1} \in H$ as well. $\langle A \rangle$ is the smallest subgroup containing A, so $\langle A \rangle \subseteq W$. Conversely, fix an element $b \in W$, so b has the form

$$b = a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t},\ a_i \in A,\ n_i \in \mathbb{Z}$$

and a simple induction will show each $a_i^{n_i} \in \langle A \rangle$ for $1 \le i \le t$, so $b \in \langle A \rangle$ and $\langle A \rangle = W$. ∎

Definition 3.2: Lattice of subgroups

Let $\{H_i\}_{i \in I}$ be a collection of subgroups of G, then

$$\text{glb}\{H_i\} = \bigcap_{i \in I} H_i, \quad \text{lub} = \left\langle \bigcup_{i \in H} H_i \right\rangle$$

The collection of subgroups of G is a *complete lattice*.

Cyclic groups

The proof for the following is straight-forward, the book separates the case into $H = \langle 0 \rangle$ and $H \neq \langle 0 \rangle$, then H contains a non-zero element $h \neq 0$, then $|h| \in \mathbb{N}^+$ is an element in H as well, so H contains a least positive element by invoking the Well Ordering Property. For the second half of the proof, we force $r = 0$ by the Division Algorithm.

Definition 4.1: Order of a subgroup $H < G$

The order of a subgroup H is its cardinality $|H|$.

Definition 4.2: Order of an element $a \in G$

The order of an element $a \in G$ is the order of $|\langle a \rangle|$.

Proposition 4.1: Hungerford Theorem 3.1

Let $\mathbb{Z}$ be equipped with its usual addition operation. Then every subgroup $H < \mathbb{Z}$ is cyclic, either $H = \langle 0 \rangle$ or $H = \langle m \rangle$. With m being the least positive integer in H. If $H \neq \langle 0 \rangle$, then H is infinite.

Proposition 4.2: Hungerford Theorem 3.2

Every infinite cyclic group $G = \langle a \rangle$ is isomorphic to the additive group $\mathbb{Z}$, and every finite cyclic group of order $0 < m < +\infty$ is isomorphic to the additive group $\mathbb{Z}_m$.

Proof of Proposition 4.2. Let $f : \mathbb{Z} \to G$ and $f(k) = a^k$. By Proposition 3.2,

$$G = \left\{ a^k,\ k \in \mathbb{Z} \right\}$$

f is clearly surjective and $f \in \mathrm{Hom}(\mathbb{Z}, G)$ is an easy exercise to verify. The proof splits into two parts

(i) Ker f is trivial: By Proposition 2.1, f is an isomorphism from $\mathbb{Z}$ to G, and $G \cong \mathbb{Z} \implies |G| = |\mathbb{Z}|$.

(ii) Ker f is not trivial: Arguing as in Proposition 4.2, Ker f is a non-trivial subgroup of $\mathbb{Z}$, so it contains a least positive element m, and Ker $f = \langle m \rangle$. m is an element of ker f, so

$$f(m) = a^m = e \implies f(jm) = a^{jm} = \prod_{l=1}^{j} a^m = e,\ j \in \mathbb{Z} \tag{7}$$

Now suppose r and s are integers with $f(r) = f(s)$,

$$\begin{aligned} a^r = a^s &\iff a^{r-s} = e \\ &\iff r - s \in \mathrm{Ker}\, f \\ &\iff r - s \in \langle m \rangle \\ &\iff r \equiv s \mod m \\ &\iff \overline{r} = \overline{s} \end{aligned}$$

where $\overline{r}$ denotes the $\mathbb{Z}_m$ equivalence class of r. Let β be a map from $\mathbb{Z}_m \to G$, such that

$$\beta(\overline{k}) = f(k) = a^k$$

This is well defined, since β is an invariant on each equivalence class, if $r - s$ differ by a multiple of m, then Equation (7) states that $\beta(\overline{r}) = \beta(\overline{s})$. G is finite, as

$$G = \langle a \rangle = \left\{ a^k,\ k \in \mathbb{Z},\ m < k < m \right\}$$

and the kernel of β is trivial, it is an isomorphism and $\mathbb{Z}_m \cong G$.

∎

Cosets

Normal Subgroups

Isomorphism Theorems