Preface

These are solutions for Hungerford's *Algebra* text. Any theorems cited in the exercises or hints will be included.

Contents

Last update: 2025 May 27

Chapter 1

Groups

§ 1.1. Semigroups, Monoids, and Groups

Exercise 1.1.1. Give examples other than those in the text of semigroups and monoids that are not groups.

Exercise 1.1.2. Let G be a group (written additively), S a nonempty set, and $M(S,G)$ the set of all functions $f : S \to G$. Define addition in $M(S,G)$ as follows: $(f+g) : S \to G$ is given by $s \mapsto f(s) + g(s) \in G$. Prove that $M(S,G)$ is a group, which is abelian if G is.

Proof. Clearly $M(S,G)$ is closed under addition defined as above. Assocativity can be seen as follows:

$$\begin{aligned}
[f + (g+h)](s) &= f(s) + (g+h)(s) \\
&= f(s) + [g(s) + h(s)] \\
&= [f(s) + g(s)] + h(s) \quad \text{Since } G \text{ is a group.} \\
&= (f+g)(s) + h(s) \\
&= [(f+g)+h](s).
\end{aligned}$$

Define $\mathbf{0} : S \to G$ by $\mathbf{0}(s) = 0$, the additive identity of G. Then:

$$\begin{aligned}
(f + \mathbf{0})(s) &= f(s) = \mathbf{0}(s) \\
&= f(s) + 0 \\
&= f(s) \\
&= 0 + f(s) \\
&= \mathbf{0}(s) + f(s) \\
&= (\mathbf{0} + f)(s).
\end{aligned}$$

Whence $\mathbf{0} \in M(S,G)$ is the identity element. Given $f \in M(S,G)$, define $f^{-1} : S \to G$ by $s \mapsto -f(s)$. We can see:

$$\begin{aligned}
(f + f^{-1})(s) &= f(s) + f^{-1}(s) \\
&= 0 \\
&= (-f(s)) + f(s) \\
&= f^{-1}(s) + f(s) \\
&= (f^{-1} + f)(s).
\end{aligned}$$

Thus $M(S,G)$ is a group. If G is abelian, then:

$$\begin{aligned}
(f + g)(s) &= f(s) + g(s) \\
&= g(s) + f(s) && \text{Since } G \text{ is abelian.} \\
&= (g + f)(s).
\end{aligned}$$

Thus $M(S,G)$ is an abelian group. □

Exercise 1.1.3. Is it true that a semigroup which has a *left* identity element and in which every element has a *right* inverse is a group?

Proof. No. Consider $G = \{a, e\}$ with a binary operation defined as follows:

$$\begin{aligned}
ea &= a, \\
ae &= e.
\end{aligned}$$

Note that, for any $a, b, c \in G$:

$$\begin{aligned}
a(bc) &= bc = c, \\
(ab)c &= bc = c.
\end{aligned}$$

Thus G is a semigroup. By construction G admits a left identity element and every element admits a right inverse. Note that G is not a group, since $ae = e \neq a$; i.e., G does not admit a right identity. □

Exercise 1.1.4. Write out the multiplication table for the group D_4^*.

Exercise 1.1.5. Prove that the symmetric group on n letters, S_n, has order $n!$.

Proof. Starting at $1 \in S$, there are n different elements which 1 can be mapped to. For $2 \in S$, there are $n - 1$ different elements which 2 can be mapped to (both 1 and 2 cannot be mapped to the same element, otherwise our function is not bijective). This process continues until we reach $n \in S$, which will only have one element which it can be mapped to. Thus there are $n!$ different permutations on the set S; i.e., $|S_n| = n!$. □

Exercise 1.1.6. Write out an addition table for $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$. $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ is called the **Klein four group**.

Proof.

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

□

Exercise 1.1.7. *** If p is prime, then the nonzero elements of $\mathbf{Z}/p\mathbf{Z}$ form a group of order $p-1$ under multiplication. [*Hint:* $[a]_p \neq [0]_p \Rightarrow \gcd(a,p) = 1$; use Introduction, Theorem 6.5] Show that this statement is false if p is not prime.

Proof. Denote the nonzero elements of $\mathbf{Z}/p\mathbf{Z}$ as $\mathbf{Z}/p\mathbf{Z}^*$. Since there are $p-1$ nonzero elements of $\mathbf{Z}/p\mathbf{Z}$, then $|\mathbf{Z}/p\mathbf{Z}^*| = p-1$. Moreover, since $\mathbf{Z}/p\mathbf{Z}$ is a commutative monoid under multiplication by Introduction, Theorem 6.8 and Groups, Theorem 1.5, it must be that multiplication in $\mathbf{Z}/p\mathbf{Z}^*$ is well-defined.

We must first show that multiplication is closed in $\mathbf{Z}/p\mathbf{Z}^*$. Let $[a]_p, [b]_p \in \mathbf{Z}/p\mathbf{Z}^*$. Suppose that $[ab]_p = [0]_p$. Then $p \mid ab$. Since $[a]_p \in \mathbf{Z}/p\mathbf{Z}^*$, we know that $[a]_p \neq [0]_p$; i.e., $\gcd(a,p) = 1$. By Introduction, Theorem 6.6, it must be the case that $p \mid b$. But this contradicts the fact that $[b]_p \in \mathbf{Z}/p\mathbf{Z}^*$. Thus $[ab]_p \neq [0]_p$, giving that $\mathbf{Z}/p\mathbf{Z}^*$ is closed under multiplication.

Again, since $\mathbf{Z}/p\mathbf{Z}$ is a commutative monoid under multiplication, it must be that multiplication in $\mathbf{Z}/p\mathbf{Z}^*$ is associative. The identity element is $[1]_p \in \mathbf{Z}/p\mathbf{Z}^*$; observe that for any $[a]_p \in \mathbf{Z}/p\mathbf{Z}^*$:

$$\begin{aligned} [a]_p[1]_p &= [a \cdot 1]_p \\ &= [a]_p \\ &= [1 \cdot a]_p \\ &= [1]_p[a]_p. \end{aligned}$$

It remains to show that each element in $\mathbf{Z}/p\mathbf{Z}^*$ has an inverse. Let $[a]_p \in \mathbf{Z}/p\mathbf{Z}^*$ be arbitrary. Then $\gcd(a,p) = 1$. There exists integers r, s so that $ar + ps = 1$. This is equivalent to $ar = ra \equiv 1 \pmod{p}$. We've shown there exists some r such that $[a]_p[r]_p = [ar]_p = [1]_p = [ra]_p = [r]_p[a]_p$. Thus $\mathbf{Z}/p\mathbf{Z}^*$ is a group.

Suppose that m is a composite integer... □

Exercise 1.1.8.

(a) The relation given by $a \sim b \iff a - b \in \mathbf{Z}$ is a congruence relation on the additive group $\mathbf{Q}$ [see Groups, Theorem 1.5].

(b) The set $\mathbf{Q}/\mathbf{Z}$ of equivalence classes is an infinite abelian group.

Proof. (a) Our relation $\sim$ is clearly reflexive: $a - a = 0 \in \mathbf{Z}$, whence $a \sim a$. If $a \sim b$, then $a - b \in \mathbf{Z}$. Since $\mathbf{Z}$ is a group under addition, the additive inverse of $a - b$ exists; i.e., $-(a-b) = b - a \in \mathbf{Z}$. So $b \sim a$, showing that $\sim$ is symmetric. If $a \sim b$ and $b \sim c$, then $a - b \in \mathbf{Z}$ and $b - c \in \mathbf{Z}$. Since addition is closed under $\mathbf{Z}$, $(a-b)+(b-c) = a - c \in \mathbf{Z}$, giving $a \sim c$. Thus $\sim$ is transitive, and altogether it is an equivalence relation. If $a \sim b$ and $c \sim d$, then $a - b \in \mathbf{Z}$ and $c - d \in \mathbf{Z}$. Again by the closure of $\mathbf{Z}$, $(a-b)+(c-d) = (a+c)-(b+d) \in \mathbf{Z}$. Thus $\sim$ is a congruence relation, as we've shown $a + c \sim b + d$.

(b) It is routine to show that all of the group axioms are satisfied by the elements of $\mathbf{Q}/\mathbf{Z}$. Define $f : \mathbf{N} \to \mathbf{Q}/\mathbf{Z}$ by $n \mapsto \overline{\frac{1}{n}}$. Observe that:

$$\begin{aligned} f(n_1) = f(n_2) &\implies \overline{\frac{1}{n_1}} = \overline{\frac{1}{n_2}} \\ &\implies \overline{\frac{1}{n_1}} = \overline{\frac{1}{n_2}} \end{aligned}$$

Define $\pi : \mathbf{Q} \to \mathbf{Q}/\mathbf{Z}$ by $q \mapsto \overline{q}$. □

Exercise 1.1.9. Let p be a fixed prime. Let R_p be the set of all those rational numbers whose denominator is relatively prime to p. Let R^p be the set of rationals whose denominator is a power of p (p^1, $i \geqslant 0$). Prove that both R_p and R^p are abelian groups under ordinary addition of rationals.

Exercise 1.1.10. Let p be prime and let $Z(p^\infty)$ be the following subset of the group $\mathbf{Q}/\mathbf{Z}$ (see pg. 27):

$$Z(p^\infty) = \{\overline{a/b} \in \mathbf{Q}/\mathbf{Z} \mid a, b \in \mathbf{Z},\ \ b = p^i \text{ for some } i \geqslant 0\}.$$

Show that $Z(p^\infty)$ is an infinite group under the addition operation of $\mathbf{Q}/\mathbf{Z}$.

Exercise 1.1.11. The following conditions on a group G are equivalent:

(i) G is abelian;

(ii) $(ab)^2 = a^2b^2$ for all $a, b \in G$;

(iii) $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$;

(iv) $(ab)^n = a^nb^n$ for all $n \in \mathbf{Z}$ and all $a, b \in G$;

(v) $(ab)^n = a^nb^n$ for three consecutive integers n and all $a, b \in G$;

Show that $(v) \Rightarrow (i)$ is false if "three" is replaced by "two."

Exercise 1.1.12. If G is a group, $a, b \in G$ and $bab^{-1} = a^r$ for some $r \in \mathbf{N}$, then $b^j ab^{-j} = a^{r^j}$ for all $j \in \mathbf{N}$.

Exercise 1.1.13. If $a^2 = e$ for all elements a of a group G, then G is abelian.

Exercise 1.1.14. If G is a finite group of even order, then G contains an element $a \neq e$ such that $a^2 = e$.

Exercise 1.1.15. Let G be a nonempty finite set with an associative binary operation such that for all $a, b, c \in G$ $ab = ac \Rightarrow b = c$ and $ba = ca \Rightarrow b = c$. Then G is a group. Show that this conclusion may be false if G is infinite.

Exercise 1.1.16. Let $a_1, a_2, ...$ be a sequence of elements in a semigroup G. Then there exists a unique function $\psi : \mathbf{N}^* \to G$ such that $\psi(1) = a_1$, $\psi(2) = a_1a_2$, $\psi(3) = (a_1a_2)a_3$ and for $n \geqslant 1$, $\psi(n+1) = (\psi(n))a_{n+1}$. Note that $\psi(n)$ is precisely the standard n product $\prod_{i=1}^{n} a_i$. [*Hint:* Applying the Recursion Theorem 6.2 of Introduction with $a = a_1$, $S = G$, and $f_n : G \to G$ given by $x \mapsto xa_{n+2}$ yields a function $\varphi : \mathbf{N} \to G$. Let $\psi = \varphi\theta$, where $\theta : \mathbf{N}^* \to \mathbf{N}$ is given by $k \mapsto k - 1$.]

§ 1.2. Homomorphisms and Subgroups

Exercise 1.2.1. If $f : G \to H$ is a homomorphism of groups, then $f(e_G) = e_H$ and $f(a^{-1}) = f(a)^{-1}$ for all $a \in G$. Show by example that the first conclusion may be false if G, H are monoids that are not groups.

Appendix

Introduction, Theorem 6.5 *If* $a_1, a_2, ..., a_n$ *are integers, not all 0, then* $\gcd(a_1, a_2, ..., a_n)$ *exists. Furthermore there are integers* $k_1, k_2, ..., k_n$ *such that*

$$\gcd(a_1, a_2, ..., a_n) = k_1 a_1 + k_2 a_2 + ... + k_n a_n.$$

Introduction, Theorem 6.6 *If* a *and* b *are relatively prime integers (that is,* $\gcd(a, b) = 1$*) and* $a \mid bc$*, then* $a \mid c$*. If* p *is prime and* $p \mid a_1 a_2 ... a_n$*, then* $p \mid a_i$ *for some* i*.*

Introduction, Theorem 6.8 *Let* $m > 0$ *be an integer and* $a, b, c, d \in \mathbf{Z}$*.*

(i) *Congruence modulo* m *is an equivalence relation on the set of integers* $\mathbf{Z}$*, which has precisely* m *equivalence classes.*

(ii) *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$*, then* $a + c \equiv b + d \pmod{m}$ *and* $ac \equiv bd \pmod{m}$*.*

(iii) *If* $ab \equiv ac \pmod{m}$ *and* a *and* m *are relatively prime, then* $b \equiv c \pmod{m}$*.*

Groups, Theorem 1.5 *Let* $\sim$ *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* $a_i, b_i \in G$*. Then the set* $G/\!\sim$ *of all equivalence classes of* G *under* $\sim$ *is a monoid under the binary operation defined by* $\overline{a}\overline{b} = \overline{ab}$*, where* $\overline{x}$ *denotes the equivalence class of* $x \in G$*. If* G *is an (abelian) group, then so is* $G/\!\sim$*.*