Solutions to Artin's Algebra Second Ed

Yue Yu

Contents

Chapter 2

Groups

2.1 Laws of Composition

Exercise 1.1

Proof. For any $a, b, c \in S$, we have

$$(ab)c = ac = a = ab = a(bc),$$

which implies that the law of composition is associative. $\square$

Let a be an arbitrary element in the set for which the law has an identity. Then, we have

$$a = a1 = 1a = 1,$$

which implies that the set must be $\{1\}$.

Exercise 1.2

(1) *Proof.* $la = 1$ and $ar = 1$ imply $l = r = a^{-1}$. $\square$

(2) *Proof.* Suppose that both a' and a'' are the inverses of a. Then $a' = a''$ by part (1) and so the inverse is unique. $\square$

(3) *Proof.* $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$ implies that $(ab)^{-1} = b^{-1}a^{-1}$. $\square$

(4) See Exercise 1.3.

Exercise 1.3

Proof. s has no right inverse because there is no inverse when $n = 1$. However, s has infinitely many left inverses because there are infinitely many mappings sending $n + 1$ to n for $n \in \mathbb{N}$. $\square$

2.2 Groups and Subgroups

Exercise 2.1

Let x be the three-cycle $(1, 2, 3)$ and y be the transposition $(1, 2)$. Then we obtain the following table:

	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	x^2y	xy	1	x^2	x
xy	xy	y	x^2y	x	1	x^2
x^2y	x^2y	xy	y	x^2	x	1

Exercise 2.2

Proof. Denote the subset by T. By definition, every element in T has an inverse. Also, noticing that associativity and the identity follow from those of S, it suffices to prove the closure under composition. Indeed, for any $a, b \in T$, we have $(ab)^{-1} = b^{-1}a^{-1}$, which implies that $ab \in T$. Therefore, T is a group. $\square$

Exercise 2.3

(a) $y = x^{-1}w^{-1}z$.

(b) $xyz = 1$ implies $yz = x^{-1}$ and so $yzx = 1$. However, yxz does not necessarily equal to 1 unless x and z commute.

Exercise 2.4

(a) $H \leq G$.

(b) $H \leq G$.

(c) $H \nleq G$ because there is no inverse for every element in H.

(d) $H \leq G$.

(e) $H \nleq G$ because $H \not\subseteq G$.

Exercise 2.5

Proof. In G, we have $1_H 1_G = 1_H \in H$. Cancelling 1_H on both sides in H, we obtain $1_G = 1_H$. Thus, for any $a \in H$, we have $aa_G^{-1} = 1_G = 1_H = aa_H^{-1}$, which implies that $a_G^{-1} = a_H^{-1}$. $\square$

Exercise 2.6

Proof. We check the four properties in turn.

- **Closure.** For any $a, b \in G^\circ$, we have $a * b = ba \in G$ and so $a * b \in G^\circ$ since $G = G^\circ$.
- **Associativity.** For any $a, b, c \in G^\circ$, we have $(a * b) * c = (ba) * c = cba = (b * c)a = a * (b * c)$.
- **Existence of identity.** The identity is the same as that in G.
- **Existence of inverse.** For any element in G°, the inverse is the same as that in G.

Therefore, $(G^\circ, *)$ is a group. $\square$

2.3 Subgroups of the Additive Group of Integers

Exercise 3.1

By the Euclidean algorithm,

$$\gcd(321, 123) = \gcd(123, 75) = \gcd(75, 48) = \gcd(48, 27) = \gcd(27, 21) = \gcd(21, 6) = \gcd(6, 3) = 3.$$

So $3 = 47 \times 123 - 18 \times 321$.

Exercise 3.2

Proof. Let $d = \gcd(a, b)$. Then $d \mid a + b$ and so $d \mid p$, which implies that $d = 1$ or $d = p$ as p is prime. However, since $a, b > 0$, we have $d < p$. Hence, $d = 1$. $\square$

Exercise 3.3

(a) The greatest common divisor d of $\{a_1, \ldots, a_n\}$ should

- divide $a_1, \ldots, a_n$ and
- for any $c \in \mathbb{N}$ dividing $a_1, \ldots, a_n$, $c \mid d$.

Proof. We prove this by induction.

Denote the gcd of $\{a_1, \ldots, a_m\}$ by d_m, where $m \in \mathbb{N}$. It is clear that the d_2 exists and it is an integer combination of a_1 and a_2 by the Euclidean algorithm. Suppose that d_k exists for some integer $k \geq 2$ and $d_k = \sum_{i=1}^{k} \alpha_i a_i$, where $\alpha_i \in \mathbb{Z}$. Then d_{k+1} exists because $d_{k+1} \mid d_k$ and $d_{k+1} \mid a_{k+1}$. In addition,

$$\begin{aligned} d_{k+1} &= \beta_1 d_k + \beta_2 a_{n+1} && \text{(by the Euclidean algorithm)} \\ &= \beta_1 \sum_{i=1}^{k} \alpha_i a_i + \beta_2 a_{n+1} && \text{(by the inductive hypothesis)} \\ &= \sum_{i=1}^{k} \beta_1 \alpha_i a_i + \beta_2 a_{n+1}, \end{aligned}$$

where $\beta_1, \beta_2 \in \mathbb{Z}$, which proves the assertion by induction. $\square$

(b) *Proof.* Denote the gcd of $\{a_1/d, \ldots, a_n/d\}$ by d'. By part (a), $d = \sum_{i=1}^{n} \alpha_i a_i$ for some $\alpha_i \in \mathbb{Z}$. Dividing both sides by d, we obtain $1 = \sum_{i=1}^{n} \alpha_i (a_i/d)$. Since d' divides $a_1/d, \ldots, a_n/d$, it divides the right-hand side and so it divides 1, which implies that $d' = 1$. $\square$