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) $H \not\leq G$ because there is no inverse for every element in H.

(d) $H \leq G$.

(e) $H \not\leq G$ 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, $d = 1$. □

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. □

(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 $d' = 1$. □

2.4 Cyclic Groups

Exercise 4.1

Proof. $ab = aba^7 = a(ba^3)a^4 = a(a^3b)a^4 = a^4ba^4 = a^4(ba^3)a = a^4(a^3b)a = a^7ba = ba$. □

Exercise 4.2

(a) *Proof.* By definition, the nth roots of unity are $\exp\left(\frac{2k\pi i}{n}\right)$, where $k = 0, 1, \ldots, n-1$. Hence, they form the cyclic group $\langle \exp\left(\frac{2\pi i}{n}\right) \rangle$ of order n. □

(b)
$$\prod_{k=0}^{n-1} \exp\left(\frac{2k\pi i}{n}\right) = \exp\left(\sum_{k=0}^{n-1} \frac{2k\pi i}{n}\right) = \exp\left(\frac{(n-1)k\pi i}{n}\right).$$

Exercise 4.3

Proof. Let $|ab| = m$. Then $1 = (ab)^m = a(ba)^{m-1}b$ and so $(ba)^m = 1$. Suppose that there exists some $l \in \mathbb{N}$ smaller than m such that $(ba)^l = 1$. Then by a similar argument, $(ab)^l = 1$, which contradicts that $|ab| = m$. Hence, $|ba| = m = |ab|$. □

Exercise 4.4

We start with the following claim.

Claim. *A cyclic group G has no proper subgroup if and only if $|G|$ is prime.*

Proof. If G is infinite, then $G \cong \mathbb{Z}$ under addition, which has proper subgroups isomorphic to $n\mathbb{Z}$ where $n \in \mathbb{N}$. So G is finite.

Suppose $|G| = p$ where p is prime. Further suppose that $|g^k| = m$ for some positive integer $k < p$. Then $(g^k)^m = (g)^{qp} = 1$ and so $km = qp$. By the fundamental theorem of arithmetic, $m = p$. Since every subgroup of a cyclic group is cyclic, this implies that the order of the cyclic group generated by any element in G is the same as G. Thus, G has no proper subgroup.

Conversely, suppose that $|G|$ is not prime. Then $|G| = ab$ for some integers $a, b > 1$. Then $\langle g^a \rangle$ is a proper subgroup of G, which is a contradiction. So $|G|$ is prime.

Therefore, G has no proper subgroup if and only if $|G|$ is prime. □

Now, we analyze G. Suppose G is generated by at least two elements a, b. Then $\langle a \rangle, \langle b \rangle$ are proper subgroups of G. So G is a cyclic group. Hence, by our claim, $G \cong \mathbb{Z}_p$ where p is prime.

Exercise 4.5

Proof. Let $G = \langle a \rangle$ be a cyclic group and H be a subgroup of G. We may assume that G and H are non-trivial. Pick the smallest $m \in \mathbb{N}$ such that $a^m \in H$. We claim that $H = \langle a^m \rangle$.

To prove this, for any $a^k \in H$, since $k = qm + r$ where $0 \leq r < m$, we have $a^k = a^r \in H$. So $r = 0$ by the minimality of m, which implies that $a^k = (a^m)^q \in \langle a^m \rangle$ and so $H \subseteq \langle a^m \rangle$. On the other hand, for any $(a^m)^n \in \langle a^m \rangle$, $(a^m)^n \in H$ by the closure of H and so $\langle a^m \rangle \subseteq H$. Therefore, $H = \langle a^m \rangle$, which is cyclic. □

Exercise 4.6

(a) There are 2 elements generating the cyclic group of order 6, and 4 elements generating the cyclic groups of order 5 and 8.

(b) We start with the following claim.

Claim. *Let $G = \langle a \rangle$ be a cyclic group of order n. Then a^m generates G if and only if m and n are coprime.*

Proof. Suppose that m and n are coprime. By Bézout's identity, we have $1 = mx + ny$ for some $x, y \in \mathbb{Z}$. So for any $a^k \in G$, $a^k = a^{k(mx+ny)} = (a^m)^{kx} \in \langle a^m \rangle$, which implies that $G \subseteq \langle a^m \rangle$ and so $G = \langle a^m \rangle$. Conversely, suppose that m and n are not coprime. Let $d = \gcd(m, n) > 1$. Then $m = m'd$ and $n = n'd$ for some positive integers $m' < m$ and $n' < n$. So $a^n = a^{n'd} = a^{n'm/m'} = (a^m)^{n'/m'}$. Multiplying both sides by $a^{m'}$, we obtain $(a^m)^{n'} = (a^n)^{m'} = 1$. So $|\langle a^m \rangle| \leq n' < n = |G|$, which is a contradiction since a^m generates G. Therefore, a^m generates G if and only if m and n are coprime. □

Now, by our claim, the number of elements generating the cyclic group $G = \langle a \rangle$ is the number of elements a^k, where $0 < k < n$ and $\gcd(k, n) = 1$.

Exercise 4.7

Proof. Since $(xy)^2 = 1$, we have $yxy = x$ and so $xy = yx$. The result follows from the following table:

	1	x	y	xy
1	1	x	y	xy
x	x	1	xy	y
y	y	xy	1	x
xy	xy	y	x	1

□

Exercise 4.8

To be updated.

Exercise 4.9

There are $\binom{4}{2}$ elements interchanging a single pair of elements, and 3 elements interchanging two pairs of elements. So there are 9 elements of order 2 in total.

Exercise 4.10

Some 2 by 2 matrices should work. However, this is not the case if the group is abelian.

Proof. For any elements a, b of finite order in an abelian group. Suppose $|a| = m$ and $|b| = n$. Then

$$(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = 1,$$

which implies that $|ab|$ is finite. □

Exercise 4.11

(a) *Proof.* Note that every element in S_n is isomorphic to an n by n permutation matrix. Since a permutation matrix is elementary, it can be obtained by applying elementary operations to the identity matrix, in particular, row switching, which proves the assertion. □

(b) *Proof.* The composition of any two transpositions is equal to some three-cycle, which proves the assertion. □