

# A solutions manual for Algebra by Thomas W. Hungerford

## Chapter I: Groups - 3. Cyclic Groups

### Exercises

1. Let  $a, b$  be elements of a group  $G$ . Show that  $|a| = |a^{-1}|$ ;  $|ab| = |ba|$ , and  $|a| = |cac^{-1}|$  for all  $c \in G$ .

**Proof.** By Theorem 2.8, the subgroup  $\langle a \rangle$  generated by  $a$  consists of all finite products  $a^n (n \in \mathbb{Z})$ ; thus  $\langle a \rangle = \langle a^{-1} \rangle$ , and so  $|a| = |a^{-1}|$ .

Suppose that  $ab$  has finite order  $m$ . Since

$$\begin{aligned} e &= (ab)^m = abab \cdots ab = a(ba)^{m-1}b \Leftrightarrow \\ (ba)^{m-1} &= a^{-1}eb^{-1} \Leftrightarrow (ba)^{m-1}b = a^{-1} \Leftrightarrow (ba)^m = e, \end{aligned}$$

$|ba| \leq |ab|$ . Conversely, suppose that  $ba$  has finite order. Similarly to the previous, we have  $|ab| \leq |ba|$ , and so  $|ab| = |ba|$ . Thus if one of  $|ab|$  and  $|ba|$  is finite, then the other is finite; otherwise both infinite, and by Theorem 3.2, every infinite cyclic group is isomorphic to the additive group  $\mathbb{Z}$ , so  $|ab| = |ba| = \aleph_0$ . Therefore,  $|ab| = |ba|$ .

By induction,  $(cac^{-1})^m = cac^{-1}cac^{-1} \cdots cac^{-1} = ca^m c^{-1}$  for all  $n \in \mathbb{N}$ . Suppose that  $cac^{-1}$  has finite order  $m$ . Since

$$e = ca^m c^{-1} \Leftrightarrow cec^{-1} = e = a^m,$$

$|a| \leq |cac^{-1}|$ . Conversely, suppose that  $a$  has finite order  $m$ . Since

$$e = a^m \Leftrightarrow c^{-1}c = a^m \Leftrightarrow e = ca^m c^{-1},$$

$|a| \geq |cac^{-1}|$ , and so  $|a| = |cac^{-1}|$ . Thus if one of  $|a|$  and  $|cac^{-1}|$  is finite, then the other is finite; otherwise both infinite, and by Theorem 3.2,  $|a| = |cac^{-1}| = \aleph_0$ . Therefore,  $|a| = |cac^{-1}|$ .  $\square$

2. Let  $G$  be an abelian group containing elements  $a$  and  $b$  of orders  $m$  and  $n$  respectively. Show that  $G$  contains an element whose order is the least common multiple of  $m$  and  $n$ . [*Hint*: first try the case when  $(m, n) = 1$ .]

**Proof.** Write prime factorizations of  $m$  and  $n$  as

$$m = \prod_i p_i^{\alpha_i} \text{ and } n = \prod_i p_i^{\beta_i},$$

and let

$$m' = \prod_{i: \alpha_i \geq \beta_i} p_i^{\alpha_i} \text{ and } n' = \prod_{i: \beta_i > \alpha_i} p_i^{\beta_i} \text{ and } a' = a^{m/m'} \text{ and } b' = b^{n/n'}.$$

Note that  $m'$  divides  $m$ , and  $n'$  divides  $n$ , and  $m'$  and  $n'$  are relatively prime, and  $m'n'$  is the least common multiple of  $m$  and  $n$ . We claim that the order of  $a'$  is  $m'$ . Let  $k$  be the order of  $a'$ . Since  $e = (a')^k = (a^{m/m'})^k = a^{mk/m'}$ ,  $m$  divides  $mk/m'$ , and so  $m'$  divides  $k$ . On the other hand, since  $(a^{m/m'})^{m'} = a^m = e$ ,  $k$  divides  $m'$ . So the order of  $a'$  is  $m'$ . Similarly, the order of  $b'$  is  $n'$ . Now, let the order of  $a'b' = r'$ , we claim that  $r'$  is  $m'n'$ . Since

$$(a'b')^{m'n'} = a^{(m/m')m'n'} b^{(n/n')m'n'} = a^{mn'} b^{nm'} = e,$$

$r'$  divides  $m'n'$ , and since

$$e = (a'b')^{r'} = (a'b')^{r'm'} = a^{r'm'} b^{r'm'} = b^{r'm'} = e,$$

$n'$  divides  $r'm'$ .  $m'$  and  $n'$  are relatively prime, so  $n'$  divides  $r'$ . Similarly,  $m'$  divides  $r'$ ; thus  $m'n'$  divides  $r'$ , and so  $r' = m'n'$ . Therefore,  $G$  contains an element whose order is the least common multiple of  $m$  and  $n$ .  $\square$

3. Let  $G$  be an abelian group of order  $pq$ , with  $(p, q) = 1$ . Assume there exists  $a, b \in G$  such that  $|a| = p$ ,  $|b| = q$  and show that  $G$  is cyclic.

4. If  $f : G \rightarrow H$  is a homomorphism,  $a \in G$ , and  $f(a)$  has finite order in  $H$ , then  $|a|$  is infinite or  $|f(a)|$  divides  $|a|$ .

5. Let  $G$  be a multiplicative group of all nonsingular  $2 \times 2$  matrices with rational entries. Show that  $a = \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix}$  has order 4 and  $b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$  has order 3, but  $ab$  has infinite order. Conversely, show that the additive group  $Z_2 \oplus Z$  contains nonzero elements  $a, b$  of infinite order such that  $a + b$  has finite order.

6. If  $G$  is a cyclic group of order  $n$  and  $k|n$ , then  $G$  has exactly one subgroup of order  $k$ .

7. Let  $p$  be prime and  $H$  a subgroup of  $Z(p^\infty)$  (Exercise 1.10).

(a) Every element of  $Z(p^\infty)$  has finite order  $p^n$  for some  $n \geq 0$ .

(b) If at least one element of  $H$  has order  $p^k$  and no element of  $H$  has order greater than  $p^k$ , then  $H$  is the cyclic subgroup generated by  $1/p^k$ , whence  $H \cong Z_{p^k}$ .

(c) If there is no upper bound on the orders of elements in  $H$ , then  $H = Z(p^\infty)$ ; [see Exercise-I.2].

(d) The only proper subgroups of  $Z(p^\infty)$  are the finite cyclic groups  $C_n = \langle \overline{1/p^n} \rangle (n = 1, 2, \dots)$ . Furthermore,  $\langle 0 \rangle = C_0 \leq C_1 \leq C_2 \leq C_3 \leq \dots$ .

(e) Let  $x_1, x_2, \dots$  be elements of an abelian group  $G$  such that  $|x_1| = p, px_2 = x_1, px_3 = x_2, \dots, px_{n+1} = x_n, \dots$ . The subgroup generated by the  $x_i (i \geq 1)$  is isomorphic to  $Z(p^\infty)$ . [*Hint*: Verify that the map induced by  $x_i \mapsto \overline{1/p^i}$  is a well-defined isomorphism.]

8. A group that has only a finite number of subgroups must be finite.

9. If  $G$  is an abelian group, then the set  $T$  of all elements of  $G$  with finite order is a subgroup of  $G$ . [Compare Exercise 5.]

10. An infinite group is cyclic if and only if it is isomorphic to each of its proper subgroups.