# Basic Algebra (Solutions)

by Huah Chu

## Exercises (§1.9, p.62)

1. Let $G = (\mathbb{Q}, +, O)$, $K = \mathbb{Z}$. Show that $G/K \simeq$ the group of complex numbers of the form $e^{2\pi i\theta}$, $\theta \in \mathbb{Q}$, under multiplication.

*Proof.* Define a homomorphism $\phi : G \to \{e^{2\pi i\theta} | \theta \in \mathbb{Q}\}$ by $\theta \to e^{2\pi i\theta}$. Then $\ker\phi = K$ and $\phi$ is surjective. $\square$

2. Show that $a \to a^{-1}$ is an automorphism of a group $G$ if and only if $G$ is abelian, and if $G$ is abelian, then $a \to a^k$ is an endomorphism for every $k\mathbb{Z}$.

*Proof.* (1) $\quad \phi : a \to a^{-1}$ is an automorphism
$\Leftrightarrow$ For all $a, b \in G$, $(ab)^{-1} = \phi(ab) = \phi(a)\phi(b) = a^{-1}b^{-1}$.
$\Leftrightarrow$ For all $a, b \in G$, $ab = ba$, that is, $G$ is abelian.

(2) $G$ is abelian. ¿From $(ab)^k = a^k b^k$, we have $a \to a^k$ is an endomorphism. $\square$

3. Determine $\operatorname{Aut} G$ for (i) $G$ an infinite cyclic group, (ii) a cyclic group of order six, (iii) for any finite cyclic group.

*Sol.* (i) Let $G = \langle a \rangle$ be an infinite cyclic group. The generators of $G$ are $a$ and $a^{-1}$. Hence, for $\phi \in \operatorname{Aut} G$, $\phi(a) = a$ or $a^{-1}$. Hence $\operatorname{Aut} G = \{1_G, \phi : a \to a^{-1}\} \simeq \mathbb{Z}/2\mathbb{Z}$.

(ii) Let $G = \langle a | a^6 = 1 \rangle$. The generators of $G$ are $a$ and $a^5$ by exercise 4, §1.5. hence $\operatorname{Aut} G = \{1_G, \phi : a \to a^5\} \simeq \mathbb{Z}/2\mathbb{Z}$.

(iii) Let $G = \langle a \rangle$ by any finite cyclic group with $|G| = n$. Then all generators of $G$ are $a^k$, $(k, n) = 1$. Then $\operatorname{Aut} G$ is the set of all homomorphisms defined by $\phi : a \to a^k$, $(k, n) = 1$.

**Remark.** In the case of (iii), $\operatorname{Aut} G$ is isomorphic to the group of units of the multiplicative monoid $(\mathbb{Z}/n\mathbb{Z}, \cdot)$. Its structure will be determined in Chap. 4, §11. (Thm. 4.19, 4.20).

4. Determine $\operatorname{Aut} S_3$.

*Sol.* We shall show that $\operatorname{Aut} S_3 \simeq S_3$.

Step 1. The elements of $S_3$ are 1, $a = (123)$, $a^2 = (132)$, $b = (12)$, $ab = (13)$, $(a^2b = (23)$. Then we have the relation $ba = a^2b$. Using this relation, the reader can verify that

$$(a^m b^n)(a^p b^q) = a^{m+(n+1)p} b^{n+q}, \ m, p = 0, 1, 2; \ n, q = 0, 1 \qquad (*)$$

easily. Since an automorphism preserves the order of an element, hence, for $\phi \in \operatorname{Aut} G$, $\phi(a) = a^i$ and $\phi(b) = a^j b$ for some $i = 1, 2$, $j = 0, 1, 2$.

Step 2. Define the map $\phi_{ij} : G \to G$ by $\phi_{ij} : \begin{cases} a \to a^i \\ b \to a^j b \end{cases}$, $i = 1, 2$, $j = 0, 1, 2$. Then $\phi_{ij} \in \operatorname{Aut} G$:

We have $\phi_{ij}(a^m) = a^{im}$, $\phi_{ij}(a^m b) = a^{im+j} b$ by the definition of $\phi_{ij}$. Using these, it is easy to see that $\phi_{ij}$ is bijective. Then we check that $\phi_{ij}$ is a homomorphism in the following four cases:

(i) $x = a^m b$, $y = a^n b$. Then $\phi((a^m b)(a^n b)) = \phi(a^{m+2n})$ (by $(*)$) $= a^{i(m+2n)}$. On the other hand, $\phi(a^m b)\phi(a^n b) = a^{im+j} b a^{in+j} b = a^{im+j+2(in+j)} = a^{im+2in+3j} = a^{i(m+2n)}$. The other three cases: (ii) $x = a^m b$, $y = a^n$, (iii) $x = a^m$, $y = a^n b$, and (iv) $x = a^m$, $y = a^n$ are left to the reader.

Step 3. It is easy to see that $\phi_{10} = 1$, $\phi_{11}$ and $\phi_{12}$ have order 3. $\phi_{20}$, $\phi_{21}$ and $\phi_{22}$ have order 2. We define the mapping $\Phi : S_3 \to \operatorname{Aut} S_3$ by $a^i \mapsto \phi_{1i}$, $a^i b \mapsto \phi_{2i}$. The reader can verify that it is an isomorphism.

**Remark.** (1) Since $S_3 = \langle a, b | a^3 = b^2 = 1, ba = a^2 b \rangle$ (See §1.11), to prove that $\phi_{ij}$ is a homomorphism, it is enough to check that $(\phi_{ij}(a))^3 = (\phi_{ij}(b))^2 = 1$, $\phi_{ij}(b)\phi_{ij}(a) = (\phi_{ij}(a))^2(\phi_{ij}(b))$.

(2) In fact, $\operatorname{Aut} S_n \simeq S_n$ for all $n \neq 6$, and $\operatorname{Aut} S_6 / S_6 \simeq \mathbb{Z}/2\mathbb{Z}$, (c.f. I. J. Rotman: The theory of groups, p.132, or B. Huppert Endlich Gruppen I, p.173–177).

(3) For other remark, see the remark after exercise 5.

5. Let $a \in G$, a group, and define the inner automorphism (or conjugation) $I_a$ to be the map $x \to axa^{-1}$ in $G$. Verify that $I_a$ is an automorphism. Show that $a \to I_a$ is a homomorphism of $G$ into $\operatorname{Aut} G$ with kernel the center $C$ of $G$. Hence conclude that $\operatorname{Inn} G \equiv \{I_a | a \in G\}$ is a subgroup of $\operatorname{Aut} G$ with $\operatorname{Inn} G \simeq G/C$. Verify that $\operatorname{Inn} G$ is a normal subgroup of $\operatorname{Aut} G$. $\operatorname{Aut} G / \operatorname{Inn} G$ is called the group of outer automorphisms.

*Proof.* The last statement follows from $\phi I_a \phi^{-1}(b) = I_{\phi(a)}(b)$. We leave all the verifications to the reader. □

**Remark.** A group $G$ is complete in case $C(G') = 1$ and $\operatorname{Aut} G \simeq G$. Exercise 2 in §1.4 and the remark in the above exercise show that $S_n$ is complete for $n \neq 2, 6$.

It can be shown that if $G$ is simple of composite order, then $\mathrm{Aut}(G)$ is complete.

6. Let $G$ be a group, $G_L$ the set of left translations $a_L$, $a \in G$. Show that $G_L \operatorname{Aut} G$ is a group of transformations of the set $G$ and that this contains $G_R$. $G_L \operatorname{Aut} G$ is called the holomorph of $G$ and is denoted as $\operatorname{Hol} G$. Show that if $G$ is finite, then $|\operatorname{Hol} G| = |G||\operatorname{Aut} G|$.

*Proof.* (1) If $g_L \in G_L$, $\phi \in \operatorname{Aut} G$, then $\phi g_L \phi^{-1} = \phi(g)_L$. ¿From this fact, we can prove that $G_L \operatorname{Aut} G$ is a group.

(2) Since $g_L^{-1} g_R(x) = g^{-1}xg = I_{g^{-1}} \in \operatorname{Aut} G$, hence $g_R = g_L I_{g^{-1}}$. And $G_R \subset G_L \operatorname{Aut} G$.

(3) To prove $|\operatorname{Hol} G| = |G||\operatorname{Aut} G|$, it suffices to show that $G_L \cap \operatorname{Aut} G = \{1\}$. Since $g_L(1) = g \neq \phi(1)$ for $\phi \in \operatorname{Aut} G$, $g \neq 1$, the result follows. □

7. Let $G$ be a group such that $\operatorname{Aut} G = 1$. Show that $G$ is abelian and that every element of $G$ satisfies the equation $x^2 = 1$. Show that if $G$ is finite then $|G| = 1$ or 2.

*Proof.* (1) let $G$ be a group with $\operatorname{Aut} G = 1$. Then $G/C \simeq \operatorname{Inn} G = 1$ where $C$ is the center of $G$ (by exercise 5). Hence $G$ is abelian. If $G$ is abelian, $a \to a^{-1}$ is an automorphism (by exercise 2). The assumption $\operatorname{Aut} G = 1$ implies that $a = a^{-1}$ for all $a$, that is, $a^2 = 1$.

(2) Suppose $|G|$ is finite and $G \neq 1$.

Step 1. We prove that $G$ contains elements $a_1, \dots, a_r$ such that every element of $G$ can be written in a unique way in the form $a - 1^{k_1} \cdots a_r^{k_r}$, $k_i = 0, 1$:

For this purpose, we show that, for all $i$, there exists a normal subgroup $H = \langle a_1, \dots, a_i \rangle$ of $G$ such that every element of $H$ can be written as $a_1^{k_1} \cdots a_r^{k_r}$, $k_i = 0, 1$, uniquely. We prove this statement by induction on $i$. Note that any subgroup of $G$ is normal since $G$ is abelian.

Take any $1 \neq a_1 \in G$, then $\langle a_1 \rangle$ is normal in $G$. Suppose we have $H = \langle a_1 \rangle \times \cdots \times \langle a_i \rangle$. Take any $a_{i+1} \in G - H$. Then $H \cap \langle a_{i+1} \rangle = 1$ since $|\langle a_{i+1} \rangle| = 2$. Because $G$ is abelian any element of $\langle H, a_{i+1} \rangle$ can be written in the form $hb$ with $h \in H$, $b \in \langle a_{i+1} \rangle$. Moreover, the expression is unique: If $h_1 b_1 = h_2 b_2$, then $h_2^{-1} h_1 = b_2 b_1^{-1} \in H \cap \langle a_{i+1} \rangle = 1$ and $h_1 = h_2$, $b_1 = b_2$. Hence the statement.

Step 2. Suppose $n \geq 2$. Define the mapping $\alpha : G \to G$ by $a_1^{k_1} a_2^{k_2} \cdots a_n^{k_n} = a_1^{k_2} a_2^{k_1} a_3^{k_3} \cdots a_n^{k_n}$. Obviously, $\alpha$ is a nontrivial automorphism. This contradicts to the hypothesis $\operatorname{Aut} G = 1$. Thus $n = 1$ and $|G| = 2$.

**Remarks.** (1) We reprove Step 2 in the language of vector space. In Step 1, we have shown that $G$ is abelian and $x^2 = 1$ for all $x$. Regard $G$ as an additive group, then $G$ is a vector space over finite field $\mathbb{Z}/2\mathbb{Z}$ (§4.13) and an automorphism is just a nonsingular linear transformation. Let $\{a_1, \dots, a_n\}$ be a basis of $G$. Suppose $\dim G \geq 2$, then $G$

has a nontrivial nonsingular linear transformation $a_1 \mapsto a_2$, $a_2 \mapsto a_1$, and $a_i \to a_i$, $i > 2$. A contradiction.

(2) When $G$ is an infinite abelian group with $x^2 = 1$ for all $x$, we can still regard $G$ as a vector space over $\mathbb{Z}/2\mathbb{Z}$. In this case, using Zorn's lemma, we can find a base for $G$. Hence it is not difficult to construct a nontrivial nonsingular linear transformation on $G$.

8. Let $\alpha$ be the automorphism of a group $G$ which fixes only the unit of $G(\alpha(a) = a \Rightarrow a = 1)$. Show that $a \to \alpha(a)a^{-1}$ is injective. Hence show that if $G$ is finite, then every element of $G$ has the form $\alpha(a)a^{-1}$.

*Proof.* Let $\alpha$ be a fixed point free automorphism ($\alpha(a) = a \Rightarrow a = 1$). Suppose $\alpha(a)a^{-1} = \alpha(b)b^{-1}$. Then $\alpha(b^{-1}a) = b^{-1}a$. Hence $b^{-1}a$ is fixed by $\alpha$ and $b^{-1}a = 1$. Thus $a \to \alpha(a)a^{-1}$ is injective.

If $|G| < \infty$, by the pigeon hole principle, the mapping is surjective. $\square$

9. Let $G$ and $\alpha$ be as in 8, $G$ finite, and assume $\alpha^2 = 1$. Show that $G$ is abelian of odd order.

*Proof.* (1) For any element $g$ of $G$, $g$ has the form $\alpha(a)a^{-1}$. $\alpha(g) = \alpha(\alpha(a)a^{-1}) = \alpha^2(a)\alpha(a^{-1}) = a\alpha(a)^{-1} = g^{-1}$. Thus $G$ is abelian by exercise 2.

(2) Next we show that $|G|$ is odd. Suppose to the contrary, there is $a \in G$ with order 2 (exercise 13, §1.2). Then $\alpha(a) = a^{-1} = a$, contradicts to the hypothesis about $\alpha$. $\square$

**Remark.** An automorphism $\alpha$ of $G$ is said to be fixed point free if it leaves only the unit fixed. This exercise shows that: if $G$ admits a fixed point free automorphism of order 2, then $G$ is abelian. Some further results are:

Suppose that $G$ admits a fixed point free automorphism $\alpha$ of order $n$. (1) If $n = 3$, then $G$ is nilpotent (for the definition, see Basic Algebra, I, p.243, exercise 6) and $x$ commutes with $\alpha(x)$ for all $x$. (2) If $n$ is a prime, then $G$ is nilpotent (John G. Thompson). (3) $G$ is solvable in general (for the definition, see Basic Algebra, I, p.237). For more details, we refer to D. Gorenstein: Finite groups, chap. 10, pp.333–357 and D. Gorenstein. Finite simple groups.

10. Let $G$ be a finite group, $\alpha$ an automorphism of $G$, and set

$$I = \{g \in G | \alpha(g) = g^{-1}\}.$$

Suppose $|I| > \frac{3}{4}|G|$. Show that $G$ is abelian. If $|I| = \frac{3}{4}|G|$, show that $G$ has an abelian subgroup of index 2.

*Proof.* (1) Let $I = \{g \in G | \alpha(g) = g^{-1}\}$ and $|I| > \frac{3}{4}|G|$. For any $h \in I$, claim: $I \cap h^{-1}I \subset C(h)$. In fact, if $x \in I \cap h^{-1}I$, then $x - h^{-1}g$ with $g, x \in I$. Now $\alpha(h^{-1}g) = (h^{-1}g)^{-1} = g^{-1}h$; on the other hand $\alpha(h^{-1}g) = \alpha(h)^{-1}\alpha(g) = hg^{-1}$. Thus $g^{-1} \in C(h)$. It follows that $g \in C(h)$ and $x = h^{-1}g \in C(h)$ also.

Since $|I| = |h^{-1}I| > \frac{3}{4}|G|$, so $|I \cap h^{-1}I| > \frac{1}{2}|G|$. Thus $C(h)$ is a subgroup of order $> \frac{1}{2}|G|$. Then $C(h) = G$ and $h \in C(G)$, the center of $G$. Because this holds for any $h \in I$, so $|C(G)| \geq \frac{3}{4}|G|$ and $G = C(G)$, $G$ is a abelian.

(2) Suppose $|I| = \frac{3}{4}|G|$. Then $G$ can not be abelian, otherwise, $I$ is a subgroup of $G$. Hence there exists $h \in I - C(G)$. Let $K = I \cap h^{-1}I$, then $K = C(h)$ and $|K| = \frac{1}{2}|G|$, by the proof of (1). Since $[G : K] = 2$, $K$ is normal. The only property remains to prove is that $K$ is abelian.

For any $k = h^{-1}g \in K = C(h)$, then $g \in C(h)$. Thus for $k_1 = h^{-1}g_1$, $k_2 = h^{-1}g_2 \in K$, $g_1g_2 \in C(h) \subset I$. Then $(g_1g_2)^{-1} = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = g_1^{-1}g_2^{-1}$ and $g_1$ commutes with $g_2$. So $k_1$ commutes with $k_2$. $\square$

**Remark.** The reader is urged to find a finite non-abelian group $G$ and its automorphism $\alpha$ such that $|I| = \frac{3}{4}|G|$. In fact let $G = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group and $\alpha$ the inner automorphism determined by $i$. Then $|\{g \in G : \alpha(g) = g^{-1}\}| = 6$.