Basic Algebra (Solutions)

by Huah Chu

Exercises (§1.2, pp.35–36)

1. Determine $\alpha\beta$, $\beta\alpha$ and α^{-1} in S_5 if

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$$

Ans. $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$, $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 2 & 5 \end{pmatrix}$, $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$.

2. Verify that the permutations

$$1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

form a subgroup of S_3.

Proof. Omitted. □

3. Determine a multiplication table for S_3.

Ans. Let $1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $e = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. The multiplication table is

	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	1	d	e	b	c
b	b	c	1	a	e	d
c	c	b	e	d	1	a
d	d	e	a	1	c	b
e	e	d	c	b	a	1

4. Let G be the set of pairs of real numbers (a, b) with $a \neq 0$ and define: $(a, b)(c, d) = (ac, ad + b)$, $1 = (1, 0)$. Verify that this defines a group.

Sol. (1,0) is the identity element and $\left(\frac{1}{a}, \frac{b}{a}\right)$ is the inverse of (a, b).

5. Let G be the set of transformations of the real linear $\mathbb{R}$ defined by $x \to x' = ax + b$ where a and b are real numbers and $a \neq 0$. Verify that G is a transformation group of $\mathbb{R}$.

Sol. Let $\phi_{(a,b)} : \mathbb{R} \to \mathbb{R}$ is defined by $x \mapsto ax + b$. Then $\phi_{(a,b)} \cdot \phi_{(c,d)} = \phi_{(ac,ad+b)}$. By the above exercise, we find that $G = \{\phi_{(a,b)} | a, b \in R, a \neq 0\}$ is a group.

6. Verify that the set of translations $x \to x' = x + b$ is a subgroup of the group defined in exercise 5.

Sol. Omitted.

7. Show that if an element a of a monid has a right inverse b, that is, $ab = 1$; and a left inverse c, that is, $ca = 1$; then $b = c$, and a is invertible with $a^{-1} = b$. Show that a is invertible with b as inverse if and only if $aba = a$ and $ab^2a = 1$.

Proof. (1) $ab = ca = 1 \Rightarrow b = c$ and $a^{-1} = b$.

Consider cab. $cab = c(ab) = c \cdot 1 = c$; $cab = (ca)b = 1 \cdot b = b$. Hence $b = c$. It follows that $ab = ba = 1$.

(2) $aba = a$ and $ab^2a = 1 \Rightarrow a$ is invertible and $a^{-1} = b$.

¿From $ab^2a = 1$, we have $a(b^2a) = (ab^2)a = 1$. By part (1), we find that a is invertible.

¿From $aba = a$, we get $(aba)a^{-1} = a \cdot a^{-1}$, since a^{-1} exists. Hence $ab = 1$. Now it is clear that $b = a^{-1}$. □

8. Let α be a rotation about the origin in the plane and let ρ be the reflection in the x-axis. Show that $\rho\alpha\rho^{-1} = \alpha^{-1}$.

Let $\alpha : (x, y) \to (x', y')$ where $x' = x\cos\theta - y\sin\theta$, $y' = x\sin\theta + y\cos\theta$ and $\rho : (x, y) \to (x', y')$ where $x' = x$, $y' = -y$. You can check $\rho\alpha\rho^{-1} = \alpha^{-1}$ by direct computation.

9. Let G be a non-vacuous subset of a monoid M. Show that G is a subgroup if and only if every $g \in G$ is invertible in M and $g_1^{-1}g_2 \in G$ for any $g_1, g_2 \in G$.

Proof. We just need to prove the "if part" of the statement.

(1) Take any $g \in G$, then $1 = g^{-1} \cdot g \in G$. Thus G contains the unit.

(2) For any $g \in G$, $g^{-1} = g^{-1} \cdot 1 \in G$. Hence g is invertible in G.

(3) For any $g_1, g_2 \in G$, $g_1g_2 = (g_1^{-1})^{-1} \cdot g_2 \in G$, since $g_1^{-1} \in G$, therefore by the definition of subgroup, G is a subgroup. □

10. Let G be a semigroup having the following properties: (a) G contains a right unit 1_r, that is, an element satisfying $a1_r = a$, $a \in G$, (b) every element $a \in G$ has a right inverse relative to 1_r ($ab = 1_r$). Show that G is a group.

Proof. It suffices to show that, (1) $1_r \cdot a = a$ for all $a \in G$, (2) for all $a \in G$, $ab = 1_r \Rightarrow ba = 1_r$.

We first prove (2): Let $c \in G$ such that $bc = 1_r$. Then $ba = (ba)1_r = (ba)(bc) = b(ab) \cdot c = (b \cdot 1_r)c = bc = 1_r$. Hence (2) follows.

Since $1_r \cdot a = (ab)a = a(ba) = a \cdot 1_r = a$. Hence 1_r is the unit and (1) follows. □

11. Show that in a group, the equations $ax = b$ and $ya = b$ are solvable for any $a, b \in G$. Conversely, show that any semigroup having this property contains a unit and is a group.

Proof. In a group G, the equation $ax = b$ has solution $a^{-1}b$ and $ya = b$ has solution ba^{-1}. Conversely, in a semigroup, $ax = b$ and $ya = b$ are solvable. In particular, $ax = a$ is solvable for some a. Denote the solution by 1_r. For any $b \in G$, there exists y such that $ya = b$ by hypothesis. Then $b1_r = ya1_r = ya = b$, and 1_r is a right unit. Moreover, for any $a \in G$, $ax = 1_r$ are solvable. Thus a has a right inverse relative to 1_r. Now apply the result of Exercise 10. □

12. Show that both cancellation laws hold in a group, that is, $ax = ay \Rightarrow x = y$ and $xa = ya \Rightarrow x = y$. Show that any finite semigroup in which both cancellation laws hold is a group.

Proof. For the first statement, multiply by a^{-1} on both sides of $ax = ay$ or $xa = ya$. For the second, let S be a finite semigroup in which cancellation laws hold. We shall use exercise 11 to prove that G is a group. It suffices to show that the equations $ax = b$ and $ya = b$ are solvable for $a, b \in G$.

Consider the map $m_a : S \to S$ defined by $m_a(s) = as$. The cancellation law $ax = ay \Rightarrow x = y$ implies that m_a is injective. Since $|S|$ is finite, m_a is surjective by the Pigeon-hole principle. Thus $ax = b$ is solvable. □

13. Show that any finite group of even order contains an element $a \neq 1$ such that $a^2 = 1$.

Proof. Let $S = \{a | a \in G \text{ and } a \neq a^{-1}\}$. $|S|$ is even. Since $|G|$ is even and $1 \in G - S$, hence $G - S \neq \emptyset$ and $|G - S|$ is even. Let $1 \neq b \in G - S$, then $b = b^{-1}$. Thus $b^2 = 1$, $b \neq 1$. □

14. Show that a group G cannot be a union of two proper subgroups.

Proof. Suppose that H_1, H_2 are subgroups of G with $H_i \subsetneq G$. We shall show that $G \supsetneq H_1 \cup H_2$.

Suppose that $G = H_1 \cup H_2$. Choose $a \in G - H_1$. $b \in G - H_2$. Since $G = H_1 \cup H_2$, we find that $a \in H_2$, $a \notin H_1$, $b \in H_1$, $b \notin H_2$. □

Claim: $ab \notin G$, which will lead to a contradiction.

Suppose $ab \in G = H_1 \cup H_2$. It is impossible that $ab \in H_1$ because $ab \in H_1$ implies $a = (ab) \cdot b^{-1} \in H_1$. Similarly $ab \notin H_2$.

15. Let G be a finite set with a binary composition and unit. Show that G is a group if and only if the multiplication table (constructed as for monoids) has the following properties:

(i) every row and every column contains every element of G,

(ii) for every pair of elements $x \neq 1$, $y \neq 1$ of G, let R be any rectangle in the body of the table having 1 as one of its vertices, x a vertex in the same row as 1, y a vertex in the same column as 1, then the fourth vertex of the rectangle depends only on the pair (x, y), and not on the position of 1.

Proof. Let G be a group. Then exercise 11 implies (i). As for (ii), observe the table (1).

	c	d
b	1	y
a	x	z

(1)

We have $bc = 1$, $ac = x$, $bd = y$ and $b = c^{-1}$. Then $z = ad = (ac)(bd) = xy$, which depends only on the pair (x, y).

Conversely, suppose G satisfies (i) and (ii). The condition (i) means that both cancellation laws hold. In virtue of exercise 12, we just need to check the associativity of G.

We give two different arguments to prove this law.

(I) Step 1. For all $a \in G$, there exists a unique a^{-1} such that $aa^{-1} = 1$ by (i).

Step 2. For all $a \in G$, $a^{-1}a = 1$: Comparing right-bottom vertices of the following two rectangles, we have $a^{-1}a = 1$ by (ii).

	1	a
1	1	a
a^{-1}	a^{-1}	$a^{-1}a$

	a^{-1}	1
a	1	a
1	a^{-1}	1

Step 3. For all $a, b \in G$, $a^{-1}(ab) = b$: ¿From the following rectangles.

	1	ab
1	1	ab
a^{-1}	a^{-1}	$a^{-1}(ab)$

	b	bc
b^{-1}	1	c
a	ab	$a(bc)$

Owing to Step 3, the right-top vertex of the second rectangle is equal to c. The assertion is followed from these rectangles.

	1	x
1	1	x
	$\vert$	(A) $\vert$
y	y	yx

	1	x
	1	x
	$\vert$	(B) $\vert$
	y	z

(2)

	1	$(*)$	
1	1	y	v
	$\vert$	$\vert$	$\vert$
$(**)$	$\vert$	1	z
	$\vert$	$\vert$	$\vert$
	x	xy	w

(3)

(II) We first observe the table (2). ¿From the rectangle (A) we see that the right-bottom vertex must be yx.

(α) Suppose one of x, y and z is 1, then $(xy)z = x(yz)$ clearly. Hence we assume that none of x, y and z equal to 1.

(β) In table (3), we find an entry 1 in column $(*)$ (note that 1 may be equal to xy). In the row $(**)$ which 1 lies we find an entry z. In the rectangle $\begin{matrix} y & - & v \\ \vert & & \vert \\ 1 & - & 1 \end{matrix}$, we have $v = yz$ by the above observation. ¿From the rectangle $\begin{matrix} 1 & - & z \\ \vert & & \vert \\ xy & - & w \end{matrix}$, we have $w = (xy)z$. ¿From the rectangle $\begin{matrix} 1 & - & v \\ \vert & & \vert \\ x & - & w \end{matrix}$, we have $w = xv = x(yz)$. Thus $(xy)z = w = x(yz)$, the associative law holds. □

Remark. We can prove that G is a group under the following weaker conditions:

$$\begin{cases} G \text{ is any set (not necessarily finite).} \\ G \text{ has a binary composition with an identity elt. } \forall x \in G, \exists y \in G, \text{ such that } xy = 1. \\ \text{condition (ii).} \end{cases}$$