Basic Algebra (Solutions)

by Huah Chu

Exercises (§1.3, p.39)

1. Use a multiplication table for S_3 (exercise 3, §1.2) and the isomorphism $a \to a_L$ (a_L the left translation defined by a) to obtain a subgroup of S_6 isomorphic to S_3.

Sol. We rewrite the elements of S_3 as $1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Then the isomorphism $a \to a_L$ are:

$$\begin{aligned}
1 \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} &= 1, \\
2 \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 3 & 4 \end{pmatrix} &= (1\ 2)(3\ 5)(4\ 6), \\
3 \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{pmatrix} &= (1\ 3)(2\ 4)(5\ 6), \\
4 \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 5 & 1 & 2 \end{pmatrix} &= (1\ 4\ 5)(2\ 3\ 6), \\
5 \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 1 & 4 & 3 \end{pmatrix} &= (1\ 5\ 4)(2\ 6\ 3), \\
6 \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} &= (1\ 6)(2\ 5)(3\ 4).
\end{aligned}$$

2. Show that the two groups in examples 11 and 13 on pages 33 and 34 of "Basic Algebra, vol. 1" are isomorphic. Obtain a subgroup of S_n isomorphic to these groups.

Ans. For the rotation through angle $\frac{2\pi}{n}$ in R_n, we map it into the complex number $z_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ in U_n. This mapping is an isomorphism. The subgroup of S_n generated by $\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$ isomorphic to these groups.

3. Let G be a group. Define the right translation a_R for $a \in G$ as the map $x \to xa$ in G. Show that $G_R = \{a_R\}$ is a transformation group of the set G and $a \to a_R^{-1}$ is an isomorphism of G with G_R.

Proof. The proof is similar to that of Cayley's Theorem. We leave it to the reader. $\square$

4. Is the additive group of integers isomorphic to the additive group of rationals?

Ans. No. Let $\phi : (\mathbb{Z}, +) \to (\mathbb{Q}, +)$ be any homomorphism. Let $\phi(1) = a$. Then $\phi(n) = \phi(1 + \cdots + 1) = na$ for $n \in \mathbb{N}$, and $\phi(-n) = -na$. Write $a = \frac{r}{s}$ with $r, s \in \mathbb{Z}$, $s \neq 0$, $(r, s) = 1$. If p is any prime number and $p \nmid s$, then $\frac{1}{p} \notin \phi(\mathbb{Z})$. Hence ϕ is not onto.

5. Is the additive group of rationals isomorphic to the multiplicative group of non-zero rationals?

Ans. No. Suppose $\eta : (\mathbb{Q}^*, \cdot) \to (\mathbb{Q}, +)$ is an isomorphism. Then

$$\eta(-1) + \eta(-1) = \eta((-1)(-1)) = \eta(1) = 0, \quad \eta(-1) = 0.$$

A contradiction.

Remarks: (1) In fact, $(\mathbb{Q}^*, \cdot)$ has an element of order 2, that is, -1. But none of the elements in $(\mathbb{Q}, +)$ has finite order.

(2) Furthermore, the additive group of rationals is never isomorphic to the multiplicative group of positive rationals since $nX = a$ is solvable for any $n \in \mathbb{N}$, for any $a \in \mathbb{Q}$ and $Y^n = b$ is not always solvable for any $n \in \mathbb{N}$, for and $b \in \mathbb{Q}^+$.

6. In $\mathbb{Z}$ define $a \circ b = a + b - ab$. Show that $(\mathbb{Z}, \circ, 0)$ is a monoid and that the map $a \to 1 - a$ is an isomorphism of the multiplicative monoid $(\mathbb{Z}, \cdot, 1)$ with $(\mathbb{Z}, \circ, 0)$.

Proof. Omitted. $\square$