Basic Algebra (Solutions)

by Huah Chu

Exercises (§1.4, p.42)

1. Let A be a monoid, $M(A)$ the monoid of transformations of A into itself, A_L the set of left translations a_L, and A_R the set of right translations a_R. Show that A_L (respectively A_R) is the centralizer of A_R (respectively A_L) in $M(A)$ and that $A_L \cap A_R = \{c_R = c_L | c \in C\}$, C the center of A.

Proof. (1) We show that $A_L = C_{M(A)}(A_R)$. The case of $A_R = C_{M(A)}(A_L)$ is quite similar.

Since $(a_R b_L)(x) = a_R(bx) = (bx)a = b(xa) = b_L(xa) = (b_L a_R)(x)$, hence $A_L \subseteq C_{M(A)}(A_R)$. Given any $\rho \in C_{M(A)}(A_R)$. For all $a \in M$, $a_R \rho = \rho a_R$. In particular, $a_R \rho(1) = \rho a_R(1)$, $\rho(1)a = \rho(1 \cdot a) = \rho(a)$. This means that $\rho = (\rho(1))_L \in A_L$.

(2) $A_L \wedge A_R = \{c_R = c_L | c \in C\}$:

It is clearly that $c_R = c_L$ for $c \in C$. Given any $\rho \in A_L \wedge A_R$, $\rho = a_L$ for some a. Since $\rho \in A_R = C(A_L)$, hence, for all $b \in M$, $a_L b_L(1) = b_L a_L(1)$. Thus $ab = ba$ and $a \in C$. So $\rho \in \{c_L | c \in C\}$. □

2. Show that if $n \geq 3$, then the center of S_n is of order 1.

Proof. Given any $1 \neq \alpha \in S_n$, there exists i such that $\alpha(i) \neq 1$, say $\alpha(i) = j$. Choose $k \neq i, j$ since $n \geq 3$. Take γ be any permutation in S_n such that $\gamma(i) = i$ and $\gamma(j) = k$. Then $\gamma\alpha(i) = \gamma(j) = k$, and $\alpha\gamma(i) = \alpha(i) = j$. Hence $\gamma\alpha \neq \alpha\gamma$ and $\alpha \notin C(S_n)$. □

Remark. For any $\alpha \in S_n$ ($n \geq 3$), we can find $\beta \in S_n$ such that it has the same cycle decomposition as α and $\alpha \neq \beta$ (§1.6). Then there exists γ such that $\gamma\alpha\gamma^{-1} = \beta$ (Ex. 4, §1.6) and $\gamma\alpha \neq \alpha\gamma$.

3. Show that any group in which every a satisfies $a^2 = 1$ is abelian. What if $a^3 = 1$ for every a?

Proof. (1) Note that the condition $a^2 = 1$ implies $a = a^{-1}$ for all $a \in G$. For any $a, b \in G$, since $(ab)^2 = 1$ it follows that $ab = (ab)^{-1}$. But $(ab)^{-1} = b^{-1}a^{-1} = ba$. Hence $ab = ba$.

(2) If $a^3 = 1$ for all $a \in G$, G need not be abelian. We shall use Sylow's Theorem and group extensions to construct a counterexample.

Let G be a finite nonabelian group such that $a^3 = 1$ for all $a \in G$. By Sylow's Theorem (§1.13), $|G| = 3^n$. If $|G| = 9$, G is abelian (§1.12, exercise 6). Hence we assume that $|G| = 27$.

G contains a normal subgroup K of order 9 (exercise 5.2, p.87 in Rotman: The theory of groups, An introduction). K must be elementary abelian, that is, $K = \langle a, b | a^3 = b^3 = 1, ab = ba \rangle$. $G/K \simeq H = \langle h \rangle$ is a cyclic group of order 3. Then G is an extension of K by H (see the Remark after exercise 9, §1.12).

h induces an automorphism α of K. If we use the additive notation for composition of K, then K can be regard as a 2-dimensional vector space over finite field $\mathbb{F}_3$ and α can be represented as a matrix in $M_2(\mathbb{F}_3)$. By suitable changing the basis, assume α has the rational form $\begin{bmatrix} 0 & 1 \\ a & b \end{bmatrix}$ (§3, 10). Since $\alpha^3 = 1$, it is not difficult to show that the only solution is $\alpha = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$.

We have known $\mathrm{Ext}^2_{\mathbb{Z}[H]}(\mathbb{Z}, H) = H^2(H, K)$ and $H^2(H, K) = K^H/NK$ for finite cyclic group H, where $K^H = \{k \in K | \alpha k = k\}$, $NK = \{(1 + \alpha + \alpha^2)k | k \in K\}$. Hence to find all extensions of K by H, it suffices to compute $H^2(H, K)$ first. It is easy to find that $\alpha k = k \Rightarrow k = (x, x)$ for $x \in \mathbb{F}_3$ and $1 + \alpha + \alpha^2 = 0$. Hence $NK = 0$ and $H^2(H, K) = \mathbb{Z}/3\mathbb{Z}$.

We first check the trivial case, that is, semi-direct product of H by K. Since $\begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, we change α to $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ for simplicity. Then $G = \langle a, b, c | a^3 = b^3 = c^3 = 1, ab = ba, ac = ca, bc = cab \rangle$.

Now we check that $x^3 = 1$ for all $x \in G$:

First note that a is in the center of G and from $bc = cab$, we have $cb = a^2bc$, $bcb^2 = ac$ and $c^2bc = ba$. Thus

$$(bc)^3 = b(cb)cbc = ba^2b(ccbc) = ba^2bba = a^3b^3 = 1.$$

The verification of $(bc^2)^3 = (b^2c)^3 = (b^2c^2)^3 = 1$ are similar, and left to the reader. Moreover, since $(ax)^n = a^nx^n$, so $(a^ib^jc^k)^3 = a^{3i}(b^jc^k)^3 = 1$. Hence the result. Thus G is the desired counter-example. □

Remarks: (1) Since $H^2(H, K) \simeq \mathbb{Z}/3\mathbb{Z}$, we can find a nontrivial factor set $f : H \times H \to K$ defined by $f(h, h) = ab$, $f(h^2, h) = f(h, h^2) = 1$, $f(h^2, h^2) = a^2b^2$, and $f(1, x) = f(x, 1) = 1$ for $x \in H$. Let G be the set of all pairs $(k, x) \in K \times H$ with the composition

$$(k, x)(k', y) = (k(xk')f(x, y), xy).$$

Where xk' is defined as follows: (i) If $x = 1$ then $xk' = k'$; (ii) $x = h$, $k' = a^ib^j$ then $xk' = a^{i+j}b^j$; (iii) if $x = h^2$, $k' = a^ib^j$, then $xk' = a^{i+2j}b^j$. Then

$$(1, h)^3 = (1 \cdot (h1) \cdot ab, h^2)(1, h) = (ab, h^2)(1, h) = (ab, 1).$$

Thus $(1, h)$ has order 9, which does not satisfy our condition.

(2) The above discussions also hold for any odd prime p. That is, $G = \langle a, b, c | a^p = b^p = c^p = 1, ab = ba, ca = ac, bc = cab \rangle$ is nonabelian group such that $x^p = 1$ for all $x \in G$.

(3) For the group extensions and cohomology of groups, we refer to J. J. Rotman: The theory of groups; An introduction; or S. MacLane: Homology.

(4) This exercise may be regard as a special case of Burnside's problem: Let G be finitely generated and n is the l.c.m of the orders of elements, is G a finite group? This exercise shows that, if $n = 2$, G is abelian. In fact, if $n = 3$, G is a finite nilpotent group of class ≤ 3. If $n = 4$ or 6, G is a finite group. We refer the reader to B. Huppert: Endlich Gruppen, or M. Hall: The theory of groups, Chap. 18, for more defails.

4. For a given binary composition define a simple product of the sequence of elements $a_1, a_2, \ldots, a_n$ inductively as either $a_1 u$ where u is a simple product of $a_2, \ldots, a_n$ or as va_n where v is a simple product of $a_1, \ldots, a_{n-1}$. Show that any product of $\geq 2^r$ elements can be written as a simple product to r elements (which are themselves products).

Proof. We prove it by induction on r. There is nothing to prove for $r = 1$. Any product of n elements $a_1, \ldots, a_n$, $n = 2^r$, $r > 1$, has the form of $(a_1, \ldots, a_i)(a_{i+1}, \ldots, a_n)$, where $(a_1, \ldots, a_i)$ is a product of $a_1, \ldots, a_i$. Then one of the sequence $\{a_1, \ldots, a_i\}$ and $\{a_{i+1}, \ldots, a_n\}$ has length $\geq 2^{r-1}$, say $\{a_1, \ldots, a_i\}$. By the inductive hypothesis, $(a_1, \ldots, a_i)$ is a simple product of $r - 1$ elements and $(a_1, \ldots, a_i)(a_{i+1}, \ldots, a_n)$ is a simple product of r elements. $\square$

Remark. The condition of $\geq 2^r$ may be refined to $\geq 2^{r-1} + 1$.

The reader may try to give a product of 8 elements which is not a simple product of 4 elements.