Basic Algebra (Solutions)

by Huah Chu

Exercises (§1.8, p.57)

1. Determine addition tables for $(\mathbb{Z}/\mathbb{Z}3, +)$ and $(\mathbb{Z}/\mathbb{Z}6, +)$. Determine all the subgroups of $(\mathbb{Z}/\mathbb{Z}6, +)$.

Sol. The subgroups of $(\mathbb{Z}/\mathbb{Z}6, +)$ are $\{\bar{0}\}$, $\{\bar{0}, \bar{2}, \bar{4}\}$, $\{\bar{0}, \bar{3}\}$ and $\mathbb{Z}/\mathbb{Z}6$. Addition table for $(\mathbb{Z}/\mathbb{Z}6, +)$:

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

2. Determine a multiplication table for $(\mathbb{Z}/\mathbb{Z}6, \cdot)$.

Sol. Multiplication table for $(\mathbb{Z}/\mathbb{Z}6, \cdot)$:

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

3. Let G be the group of pairs of real numbers (a, b), $a \neq 0$, with the product $(a, b)(c, d) = (ac, ad + b)$ (exercise 4. p.36). Verify that $K = \{(1, b) | b \in \mathbb{R}\}$ is a normal subgroup of G. Show that $G/K \simeq (\mathbb{R}^*, \cdot, 1)$ the multiplicative group of non-zero reals.

Proof. The isomorphism from G/K to $(\mathbb{R}^*, \cdot)$ is $K(a,b) \to a$. All verifications are routine. $\square$

4. Show that any subgroup of index two is normal. Hence prove that A_n is normal in S_n.

Proof. Let H be a subgroup of index two. Its right cosets are $\{H, Hx\}$. If $x \notin H$, its left cosets must be $\{H, xH\}$. Hence $Hx = xH$ for all $x \notin H$, i.e. $x^{-1}Hx \subset H$. For $x \in H$, $x^{-1}Hx \subset H$ holds trivially. Hence H is normal. $\square$

Remark. This exercise is a special case of the following:

Let H be a subgroup a finite group G with index p. If p is the smallest prime dividing $|G|$. Then H is a normal subgroup of G. (See §1.12, exercise 5).

5. Verify that the intersection of any set of normal subgroups of a group is a normal subgroup. Show that if H and K are normal subgroups, then HK is a normal subgroup.

Proof. The second statement follows from $g^{-1}HKg = (g^{-1}Hg)(g^{-1}Kg)$. $\square$

6. Let G_1 and G_2 be simple groups. Determine the normal subgroups of $G_1 \times G_2$.

Proof. In this problem, we use some terminology and some results which will be proved in sections 1.9 and 1.10. Then answer to this problem is the following: (1) When $G_1 \not\simeq G_2$ or $G_1 \simeq G_2 \not\simeq \mathbb{Z}_p$, the only normal subgroups of $G_1 \times G_2$ are $\{1\} \times \{1\}$, $G_1 \times \{1\}$, $\{1\} \times G_2$, and $G_1 \times G_2$; (2) When $G_1 \simeq G_2 \simeq \mathbb{Z}_p$, all the subgroups of $G_1 \times G_2$ are normal, and there are $p+3$ subgroups in $G_1 \times G_2 \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.

Let N be any normal subgroup of $G_1 \times G_2$ with $N \neq G_1 \times G_2$.

Let $\pi_i : G_1 \times G_2 \to G_i$, $i = 1, 2$, be the projection onto the i-th coordinate. It is straight-forward to verify that $\pi_i(N) < G_i$, $i = 1, 2$. Hence $\pi_i(N) = \{1\}$ or G_i since G_i is simple. It is easy to deduce the followings

$$\begin{cases} \pi_1(N) = \pi_2(N) = \{1\} \Rightarrow N = \{(1,1)\} \\ \pi_1(N) = 1 \ \text{ and } \ \pi_2(N) = G_2 \Rightarrow N = \{1\} \times G_2 \\ \pi_1(N) = G_1 \ \text{ and } \ \pi_2(N) = \{1\} \Rightarrow N = G_1 \times \{1\}. \end{cases}$$

It remains to establish the following:

$$\pi_1(N) = G_1, \ \pi_2(N) = G_2, \ N \neq G_1 \times G_2 \Rightarrow G_1 \simeq G_2 \simeq \mathbb{Z}_p.$$

Step 1. $N \cap (G_1 \times \{1\}) = \{(1,1)\}$, $N \cap (\{1\} \times G_2) = \{(1,1)\}$.

Since N, $G_1 \times \{1\}$ are normal, it follows $N \cap (G_1 \times \{1\}) \lhd (G_1 \times \{1\})$. Thus $N \cap (G_1 \times \{1\}) = \{(1,1)\}$ or $G_1 \times \{1\}$. If $N \cap (G_1 \times \{1\}) = G_1 \times \{1\}$, then $N \supset G_1 \times \{1\}$.

Then $N/G_1 \times \{1\}$ is a normal subgroup of $G_1 \times G_2/G_1 \times \{1\} \simeq G_2$ by Theorem 1.8. (Page 63). Hence $N = G_1 \times G_2$ or $G_1 \times \{1\}$. But $N \neq G_1 \times G_2$ by assumption. If $N = G_1 \times \{1\}$, then $\pi_2(N) \neq G_2$; again a contradiction.

Step 2. For any $h \in G_1$, there is a unique $k \in G_2$ such that $(h, k) \in N$. Similarly for any $k \in G_2$, there is a unique $h \in G_1$ such that $(h, k) \in N$.

For any $h \in G_1$, there is a $k \in G_2$ with $(h, k) \in N$ since $\pi_1(N) = G_1$. Now for the uniqueness: if $(h, k_1), (h, k_2) \in N$, then $(1, k_1k_2^{-1}) = (h, k_1) \cdot (h, k_2)^{-1} \in N$. By Step 1, $(1, k_1k_2^{-1}) \in N \cap (\{1\} \times G_2) = \{(1, 1)\}$. Hence $k_1 = k_2$.

Step 3. For any $h \in G_1$, define $\phi(h) \in G_2$ such that $(h, \phi(h)) \in N$. ϕ is a well-defined homomorphism from G_1 into G_2 by Step 2. Moreover, ϕ is onto by Step 2. Since G_1 is simple, ϕ is one to one. Hence $\phi : G_1 \to G_2$ is an isomorphism.

Step 4. We shall show that G_1 ($\simeq G_2$) is abelian.

For any $h \in G_1$, consider $(h, k) \in N$. For any $g \in G_1$, $(g, 1)^{-1} \cdot (h, k) \cdot (g, 1) \in N$. Hence $(h, k) \in N$. By Step 2, $h = g^{-1}hg$. Thus $gh = hg$ for all $g, h \in G_1$.

Step 5. The only simple abelian groups are $\mathbb{Z}_p$, p, a prime. Choose any nonzero element g. Since G is abelian, $\langle g\rangle$ is normal in G. Since G is simple, $\langle g\rangle = G$. Thus G is cyclic. But $\mathbb{Z}$ and $\mathbb{Z}_n$ (n: a composite number) cannot be simple.

Step 6. Any nontrivial proper subgroup in $\mathbb{Z}_p \times \mathbb{Z}_p$, p, a prime, is cyclic of order p; and there are $p + 1$ such subgroups.

Since $|\mathbb{Z}_p \times \mathbb{Z}_p| = p^2$, any nontrivial subgroup is of order p. Any nonzero element in $\mathbb{Z}_p \times \mathbb{Z}_p$ generates such a subgroup. There are $\frac{p^2-1}{p-1} = p + 1$ such subgroups.

7. Let $\equiv$ be an equivalence relation on a monoid M. Show that $\equiv$ is a congruence if and only if the subset of $M \times M$ defining $\equiv$ (p.10) is a submonoid of $M \times M$.

Proof. Let S be the subset of $M \times M$ defining $\equiv$. Then $(1, 1) \in S$ obviously. The equivalence $\equiv$ is a congruence $\Leftrightarrow$ $a \equiv a'$ and $b \equiv b'$ imply $ab \equiv a'b'$ $\Leftrightarrow$ $(a, b) \in S$ and $(a', b') \in S$ imply $(aa', bb') \in S$ $\Leftrightarrow$ S is a monoid. □

8. Let $\{\equiv_i\}$ be a set of congruences on M. Define the intersection as the intersection of the corresponding subsets of $M \times M$. Verify that this is a congruence on M.

Proof. The reader first verify that it is an equivalence by definition and then apply exercise 7. □

9. Let G_1 and G_2 be subgroups of a group G and let α be the map of $G_1 \times G_2$ into G defined by $\alpha(g_1, g_2) = g_1g_2$. Show that the fiber over g_1g_2 — that is, $\alpha^{-1}(g_1g_2)$ — is the set of pairs $(g_1k, k^{-1}g_2)$ where $k \in K = G_1 \cap G_2$. Hence show that all fibers have the same cardinality, namely, that of K. Use this to show that if G_1 and G_2 are finite then

$$|G_1G_2| = \frac{|G_1||G_2|}{|G_1 \cap G_2|}.$$

Proof. (1) Let $(h_1, h_2) \in \alpha^{-1}(g_1g_2)$, i.e. $h_1h_2 = g_1g_2$. Then $g_1^{-1}h_1 = g_2h_2^{-1} \in G_1 \cap G_2 = K$. Set $k = g^{-1}h_1$. We have $h_1 = g_1k$ and $h_2 = k^{-1}g_2$.

(2) Let α be the map: $G_1 \times G_2 \to G$ defined by $\alpha(g_1, g_2) = g_1g_2$. The image $\alpha(G_1 \times G_2) = G_1G_2$. Then $|G_1 \times G_2| = \sum_{g_1g_2 \in G_1G_2} |\alpha^{-1}(g_1g_2)| = \sum_{g_1g_2 \in G_1G_2} |G_1 \cap G_2| = |G_1G_2||G_1 \cap G_2|$. Hence the result. $\square$

10. Let G be a finite group. A and B non-vacuous subsets of G. Show that $G = AB$ if $|A| + |B| > |G|$.

Proof. Suppose $|A| + |B| > |G|$. For any $g \in G$, let $A^{-1}g \overset{\text{def}}{=} \{a^{-1}g \in G | a \in A\}$. Then $|A^{-1}g| = |A|$. Since $|A^{-1}g| + |B| > |G|$, $A^{-1}g \cap B \neq \emptyset$. Thus $a^{-1}g = b$ for some $a \in A$ and $b \in B$. So $g = ab$. $\square$

11. Let G be a group of order $2k$ where k is odd. Show that G contains a subgroup of index 2.

Proof. Suppose $|G| = 2k$, k is odd. The permutation group G_L of left translations is a subgroup of S_{2k} and isomorphic to G. It suffices to show that G_L contains a subgroup of index 2.

G contains an element a of order 2 by [Chapter 1, §1.2. Exercise 13, p.36] or by Sylow's theorem (p/78). Since $ag \neq g$ for all $g \in G$, a_L has no fixed point in $\{1, 2, \ldots, 2k\}$. Regarding a_L as an element of S_{2k}, its cycle decomposition must be $(12)(34)\cdots(2k-1, 2k)$ by suitable change the notation. α is an odd permutation because k is odd.

Set $H = A_{2k} \cap G_L$. For any odd permutation $\beta \in G_L$, $\beta\alpha^{-1} \in H$. Hence $\beta \in H\alpha$ and $G_L = H \cup H\alpha$. Hence G_L contains the subgroup H of index 2. $\square$