Solutions to Exercise #8

(範圍: Groups)

1. Prove (b) of the theorem on page 148 of lecture notes. (10%)

Sol: $f(a) * f(a^{-1}) = f(a \circ a^{-1}) = f(e_G)$.
$f(a^{-1}) * f(a) = f(a^{-1} \circ a) = f(e_G)$.
Therefore, $f(a^{-1}) = [f(a)]^{-1}$.

2. Prove (b) of the theorem on page 159 of lecture notes. (10%)

Sol: $G = \{a^0, a^1, \ldots, a^{n-1}\}$.
Define f: $G \to \mathbf{Z}_n$ by $f(a^m) = [m]$, where $0 \leq m \leq n-1$.
f is one-to-one and onto and $f(a^p \cdot a^q) = f(a^{p+q}) = [p+q] = [p] + [q] = f(a^p) + f(a^q)$.
Hence, f is an isomorphism from G to $\mathbf{Z}_n$, or G is isomorphic to $(\mathbf{Z}_n, +)$.

3. P. 751: 1 (only for (c), (e)). (10%)

Sol: (c) No. The set is not closed under addition.

(e) Yes. The identity is $g(a) = a$ for all $a \in A$ and the inverse of g: $A \to A$ is g^{-1}: $A \to A$.

4. P. 751: 9. (10%)

Sol: (a) $a \cdot a^{-1} = a^{-1} \cdot a = e$. So, a is the inverse of a^{-1}, or $a = (a^{-1})^{-1}$.

(b) $(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot a) \cdot b = b^{-1} \cdot e \cdot b = b^{-1} \cdot b = e$.
$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$.
So, $b^{-1} \cdot a^{-1}$ is the inverse of $a \cdot b$, or $b^{-1} \cdot a^{-1} = (a \cdot b)^{-1}$.

5. P. 756: 6. (20%)

Sol: (a) For $(x_1, y_1), (x_2, y_2) \in \mathbf{Z} \times \mathbf{Z}$, $f((x_1, y_1) \oplus (x_2, y_2)) = f(x_1 + x_2, y_1 + y_2) =$
$(x_1 + x_2) - (y_1 + y_2) = (x_1 - y_1) + (x_2 - y_2) = f(x_1, y_1) + f(x_2, y_2)$.
Therefore, f is a homomorphism.

(b) $f(a, b) = 0 \Leftrightarrow a - b = 0$.
Hence, $f(a, a) = 0$ for all $a \in \mathbf{Z}$.

(c) $f(a, b) = 7 \Leftrightarrow a - b = 7$.

Hence, $f^{-1}(7) = \{(a, a-7) \mid \text{for all } a \in \mathbf{Z}\}$.

(d) $f(a, b) \in E \Leftrightarrow a - b$ is even.

Hence, $f^{-1}(E) = \{(a, b) \mid a, b \in \mathbf{Z} \text{ and } a - b \text{ is even}\}$.

6. P. 756: 15 (only ($\mathbf{Z}_{12}$, +) for (a)). ((a), (b): 10%; (c): 5%)

Sol: (a) $<[a]> = \mathbf{Z}_{12}$ if and only if $\gcd(a, 12) = 1$, as explained below.

(if) $\gcd(a, 12) = 1 \Rightarrow as + 12t = 1$ for some integers s and t

$\Rightarrow [as] = [1]$

$\Rightarrow [a(ks)] = [k]$ for all $0 \le k \le 11$.

(only if) $<[a]> = \mathbf{Z}_{12} \Rightarrow [ap] = [1]$ for some integer p

$\Rightarrow ap = 12q + 1$ for some integer q

$\Rightarrow ap + (12(-q)) = 1$

$\Rightarrow \gcd(a, 12) = 1$.

Therefore, the generators of $\mathbf{Z}_{12}$ are [1], [5], [7], and [11].

(b) (if) For any $b \in G$. Suppose $b = a^r$.

$\gcd(k, n) = 1 \Rightarrow ks + nt = 1$ for some integers s and t

$\Rightarrow b = a^r = a^{r(ks+nt)} = (a^k)^{rs}(a^n)^{rt} = (a^k)^{rs}(e)^{rt} = (a^k)^{rs}$

i.e., b can be generated by a^k.

(only if) $G = <a^k> \Rightarrow a = (a^k)^s$ for some integer s

$\Rightarrow a^{1-ks} = e$

$\Rightarrow 1 - ks = nt$ (or $ks + nt = 1$) for some integer t

$\Rightarrow \gcd(k, n) = 1$.

(c) $|\{k \mid \gcd(k, n) = 1\}| = \phi(n)$ (refer to Example 8.8 on page 394 of Grimaldi's book).

7. P. 758: 4. (10%)

Sol: $H = <[3]> = \{[3i] \mid 0 \le i \le 7\}$.

The cosets determined by H are H, $[1] + H = \{[1+3i] \mid 0 \le i \le 7\}$, and $[2] + H = \{[2+3i] \mid 0 \le i \le 7\}$.

$K = <[4]> = \{[4j] \mid 0 \le j \le 5\}$.

The cosets determined by K are K, $[1] + K = \{[1+4j] \mid 0 \le j \le 5\}$, $[2] + K = \{[2+4j] \mid 0 \le j \le 5\}$, and $[3] + K = \{[3+4j] \mid 0 \le j \le 5\}$.

8. P. 758: 5. (5%)

Sol: According to Lagrange's theorem, $|K|$ divides $|H|$, and $|H|$ divides $|G|$.

Since $66\ (= 2 \times 3 \times 11) < |H| < 660\ (= 2^2 \times 3 \times 5 \times 11)$,

we have $|H| = 2 \times 66 = 132$ or $|H| = 5 \times 66 = 330$.

9. P. 758: 9 (only for (a)). (10%)

Sol: According to Lagrange's Theorem, every proper subgroup H of G has

$|H| = 2$ or p, a prime number.

Suppose that $a \in H$ and $a \neq e$.

If $|H| = 2$, then according to Lagrange's Theorem, $|\langle a \rangle| = 2$, implying $\langle a \rangle = H$.

Similarly, if $|H| = p$, then $\langle a \rangle = H$ as well.