# Solution for Homework 12

Xiangcan Li

January 18, 2021

**Exercise 4.3.1** Verify the claims in the proof of Theorem 4.3.2. Specially, prove that (i) $a \cdot (g_1, \ldots, g_p) = (g_{a+1}, \ldots, g_{a+p})$ defines an action on $\mathbb{Z}_p$ on $G_p$ and (ii) $X = \{(g_1, \ldots, g_p) \in G^p \mid g_1 g_2 \cdots g_p = e\}$ is invariant by $\mathbb{Z}_p$ and hence the $\mathbb{Z}_p$ action on $G^p$ restricts to an action on $X$.

Note that $[0]$ is the identity in the additive group $\mathbb{Z}_p$.

(i) $[0] \cdot (g_1, \ldots, g_p) = (g_{0+1}, \ldots, g_{0+p}) = (g_1, \ldots, g_p)$

(ii) For all $(g_1, \ldots, g_p) \in G^p$ and $[a], [b] \in \mathbb{Z}_p$,

$$\begin{aligned}
[a] \cdot ([b] \cdot (g_1, \ldots, g_p)) &= [a] \cdot (g_{[b]+1}, \ldots, g_{[b]+p}) \\
&= (g_{[a]+[b]+1}, \ldots, g_{[a]+[b]+p}) \\
&= (g_{[a+b]+1}, \ldots, g_{[a+b]+p}) \\
&= [a+b] \cdot (g_1, \ldots, g_p) \\
&= [a \cdot b] \cdot (g_1, \ldots, g_p)
\end{aligned}$$

We conclude $a \cdot (g_1, \ldots, g_p) = (g_{a+1}, \ldots, g_{a+p})$ defines an action on $\mathbb{Z}_p$ on $G_p$.
From Euclidean Algorithm, we have $a = pq + r$ for some $q, r \in \mathbb{Z}$ and $0 \leq r < p$.
We enumerate the congruence class in $\mathbb{Z}_p$.

- When $r = 0$, $[a] = [0]$. Then $\{[a+1], \ldots, [a+p]\} = \{[1], \ldots, [p]\} = \{[0], \ldots, [p-1]\}$

  Then $g_1 \cdots g_p = g_{a+1} \cdots g_{a+p}$.

- When $r \neq 0$, $[a] = [r]$. Then $[a+p-1-r] = [r+p-1-r] = [p-1]$, $[a+p-r] = [p-1+1] = [0]$, $[a+p+1-r] = [1]$ and $[a+p] = [(a+p-r)+r] = [0+r] = [r]$.

  Hence, $\{[a+1], \ldots, [a+p-1-r], [a+p-r], [a+p+1-r] \ldots, [a+p]\} = \{[r+1], \ldots, [p-1], [p], [1] \ldots, [r]\}$.
  Then $\{[1] \ldots, [r], [r+1], \ldots, [p-1], [p]\} = \{[a+p+1-r] \ldots, [a+p], [a+1], \ldots, [a+p-1-r], [a+p-r]\}$.

  Then $g_1 \cdots g_r g_{r+1} \cdots g_{p-1} g_p = g_{a+p+1-r} \cdots g_{a+p} g_{a+1} \cdots g_{a+p-1-r} g_{a+p-r}$. Note that the operation is associative in $G$. Then we have

$$g_1 \cdots g_r g_{r+1} \cdots g_{p-1} g_p = g_{a+1} \cdots g_{a+p-1-r} g_{a+p-r} g_{a+p+1-r} \cdots g_{a+p}.$$

We conclude for both cases, $g_1 \cdots g_p = g_{a+1} \cdots g_{a+p}$. Hence, $g_1 \cdots g_p = e$ if and only if $g_{a+1} \cdots g_{a+p} = e$.

**Exercise 4.3.4** Let $p \geq 2$ be a prime and prove that any group of order $p^2$ is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Let $G$ be a group of order $p^2$.
If there exists an element $g \in G$ of order $p^2$, then $g$ is an generator. By Proposition 3.3.20, $G \cong \mathbb{Z}_{p^2}$.

Assume that there does not exists an element of order $n$, then by Corollary 3.5.7, for some $g \in G$, $|g| \Big| |G|$. Since $|G| = p^2$ and $p$ is a prime, we have either $|g| = 1$ or $|g| = p$.

For $|g| = 1$, suppose for contradiction, $g \neq e$, then since $\langle g \rangle$ must contain $e$ and $g$, $|g| > 1$, which is a contradiction. Hence, $g = e$.

Then for all $g \in G$, $g \neq e$, $|g| = p$.

Then for arbitrary two nonidentity element $g, h$ in $G$, $|g| = |h| = p$. By Corollary 3.5.8, both $g$ and $h$ are generators.

- $h \in \langle g \rangle$. Note that $|g| = p < \infty$, by Proposition 3.2.6, $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$. Then $h = g^m$ for some $m \in [1, n-1]$. Then $\langle h \rangle = \{g^m, g^{m+1}, g^{m+2}, \ldots, g^{n-1}, e, g, g^2 \ldots, g^{m-1}\}$. Hence, $\langle g \rangle = \langle h \rangle$.
- $h \notin \langle g \rangle$. Suppose for contradiction, $\langle g \rangle \cap \langle h \rangle \neq \{e\}$. Then there exists some element $x \neq e$ such that $x \in \langle g \rangle$ and $x \in \langle h \rangle$. Then $x = g^s = h^t$ for some $s, t \in [1, p-1]$. Without loss of generality, suppose $s \geq t$, then $x^{1-t+1} = g^{s-t+1} = h^{t-t+1} = h$. Hence, $h \in \langle g \rangle$, which is a contradiction. Hence, $\langle g \rangle \cap \langle h \rangle = \{e\}$.

We conclude for any two nonidentity element $g, h \in G$, either $\langle g \rangle = \langle h \rangle$ or $\langle g \rangle \cap \langle h \rangle = \{e\}$.

Hence, we can choose two nonidentity element $g, h \in G$ such that $h \notin \langle g \rangle$. Then we have $\langle g \rangle \cap \langle h \rangle = \{e\}$.

Note that $|\langle g \rangle \langle h \rangle| = p \cdot p = p^2 = |G|$. For $x \in |\langle g \rangle \langle h \rangle|$, $x = g^n h^m$ for some $m, n \in \mathbb{Z}$. Since the operation is closed under $G$, $x \in G$. Then $\langle g \rangle \langle h \rangle \subset G$. Since $G$ is a finite group, $G = \langle g \rangle \langle h \rangle$.

By Corollary 3.2.4, $\langle g \rangle$ and $\langle h \rangle$ are abelian. By Exercise 3.7.1, $G$ is abelian. Then by Exercise 3.3.4, since $\langle g \rangle$ and $\langle h \rangle$ are cyclic subgroups, $\langle g \rangle$ and $\langle h \rangle$ are normal.

By proposition 3,7.1, $G \cong \langle g \rangle \langle h \rangle$. By Proposition 3.3.20, $\langle g \rangle \cong \mathbb{Z}_p$ and $\langle h \rangle \cong \mathbb{Z}_p$. Hence, $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

**Exercise 4.3.6** Prove that any finite abelian group is isomorphic to the direct product of its Sylow subgroups.

By Theorem 1.4.3, $|G|$ has a prime factorization $|G| = p_1^{n_1} \cdots p_k^{n_k}$. By theorem 4.3.6, for each $p_i^{k_i}$, there exists some $K_i < G$ such that $|K_i| = p_i^{k_i}$. By Exercise 3.3.4, since $G$ is an abelian group, every subgroup $K_i$ is normal.

Let $K_1$ be the $p_i$-Sylow subgroup and $K_j$ be the $p_j$-Sylow subgroup. Since $K_i$ and $K_j$ have relatively primes sizes, $K_i \cap K_j = \{e\}$ by Lagrange. Then for any $K_i$, $K_i \cap K_1 K_2 \cdots K_{i-1} K_{i+1} \cdots K_n = \{e\}$. By proposition 3.7.2, $K_1 \cdots K_n \cong K_1 \times \cdots \times K_n$. Hence, $|K_1 \cdots K_n| = |K_1 \times \cdots \times K_n|$.

By Exercise 3.7.3, $K_1 \cdots K_n < G$. Let $gk_1 \cdots k_n g^{-1} \in gK_1 \cdots K_n g^{-1}$. Since $G$ is abelian, $k_1, \cdots, k_n \in K_1, \cdots, K_n \subset G$, we have $gk_1 \cdots k_n g^{-1} = gg^{-1}k_1 \cdots k_n = k_1 \cdots k_n \in K_1 \cdots K_n$. Hence, $gK_1 \cdots K_n g^{-1} \subset K_1 \cdots K_n$. By Lemma 3.3.12, $K_1 \cdots K_n$ is normal.

By Lagrange Theorem,

$$[G : K_1 \cdots K_n] = \frac{|G|}{|K_1 \cdots K_n|} = \frac{|G|}{|K_1| \cdots |K_n|} = 1.$$

Since $G/K_1 \cdots K_n$ forms a partition of $G$ and $|G/K_1 \cdots K_n| = [G : K_1 \cdots K_n] = 1$, $G = K_1 \cdots K_n$. Then $G \cong K_1 \times \cdots \times K_n$.

**Exercise 4.3.8** Let $p \geq 3$ be an odd prime. Prove that any nonabelian group of order $2p$ is isomorphic to the dihedral group $D_p$.

By Example 3.4.8, we have $R_n \rtimes \mathbb{Z}_2 \cong R_n \rtimes \langle j \rangle \cong D_n$, where $R_n$ is a normal cyclic subgroup and $\langle j \rangle < D_n$ is a cyclic subgroup of order 2.

Since $|G| = 2p$, $p > 3$ is an odd prime, we have $p \nmid 2$. By Theorem 4.3.6, there exists a subgroup $K < G$ with $|K| = p$. Then $K$ is a Sylow $p$-subgroup. Then by Theorem 4.3.9, $n_p(G)$ divides $2 = \frac{|G|}{p}$ and $n_p(G) \equiv 1 \mod p$. Since $[2]_p \neq [1]_p$, $n_p(G) = 1$. By Proposition 4.3.10, $K$ is normal.

By Theorem 4.3.6, there exists a subgroup $H < G$ with $|H| = 2$. By Corollary 3.5.8, $H$ is cyclic and $H \cong \mathbb{Z}_2$. Let $H = \{e, h\}$ for some $h \neq e \in G$. Then $h$ is a generator. Then $|h| = 2 \nmid p = |K|$. By Corollary 3.5.7, $h \notin G$. Then $K \cap H = \{e\}$.

By Proposition 3.7.7, $K \rtimes H \cong KH \cong K \rtimes \mathbb{Z}_2$.

By Exercise 3.4.8, $R_p = \{I, r, r^2, r^3 \ldots, r^{\cdot -1}\}$ is a cyclic subgroup generated by $r$ and $|R_p| = p$. Since $p$ is a prime, by Corollary 3.5.8, $R_p \cong \mathbb{Z}_p$. Similarly, since $|K| = p$, $K \cong \mathbb{Z}_p$. Then $K \cong R_p$.

By Exercise 4.3.6, $G \cong K \times H \cong R_p \times \mathbb{Z}_2 \cong D_p$.

**Exercise 5.1.1** Prove that a finite integral domain is a field.

Let $R$ be the finite integral domain, which is also a finite ring.

Let $r \in R$ be an nonzero element in $R$. Then there exists some $m, n \in \mathbb{Z}_n$ such that $r^m = r^n$. Then we have $r^m - r^n = r^n(r^{m-n} - 1) = 0$. Hence, either $r^n = 0$ or $r^{m-n} - 1 = 0$. If $r^n = 0$, then $r = 0$, which is a contradiction. Hence, $r^{m-n} - 1 = 0$.

Note that $m > n$, $m \geq n + 1$ since $m, n \in \mathbb{Z}$. Then $m - n - 1 \geq 0$.

We have $r \cdot r^{m-n-1} = r^{m-n} = 1$. Hence, $r^{m-n-1} \in R$ is an inverse of $r$.

We conclude $R$ is a field.

**Exercise 5.1.4** Prove Lemma 5.1.7:
If $\mathbb{F}$ is a field, then it has no nontrivial ideals. That is, the only ideals in $\mathbb{F}$ are $\{0\}$ and $\mathbb{F}$.
More generally, prove that if $R$ is a commutative ring with 1 and $\mathcal{J} \subset R$ is an ideal containing an invertible element, then $\mathcal{J} = R$.

Suppose $R$ is a commutative ring with 1 and $\mathcal{J} \subset R$ is an ideal containing an invertible element. Then there exists some $a \in \mathcal{J}$ such that $aa^{-1} = 1$ for $a^{-1} \in R$. By definition of the ideal, $aa^{-1} \in \mathcal{J}$. Then $1 \in \mathcal{J}$. Then for all $r \in R$, $r \cdot 1 = r \in \mathcal{J}$. Hence, $R \subset \mathcal{J}$. Hence, $R = \mathcal{J}$.

Since $\mathbb{F}$ is a field, $\mathbb{F}$ is a commutative ring with 1. If the ideal in $\mathbb{F}$ contains an invertible element, then such an ideal is $\mathbb{F}$. If the ideal in $\mathbb{F}$ does not contain an invertible element, such an ideal must be $\{0\}$ since for all $a \in \mathbb{F} - \{0\}$, $a$ has an inverse.