Modern Algebra I Problem Set 9 Answer Key

Zheheng Xiao

Nov 15, 2023

1 Problem 1

By the classification of finite abelian groups, the isomorphism classes abelian groups of the following orders 27, 200, 605, 720 are:

- Order 27:
  - $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
  - $\mathbb{Z}_3 \times \mathbb{Z}_9$
  - $\mathbb{Z}_{27}$
- Order 200:
  - $\mathbb{Z}_8 \times \mathbb{Z}_{25}$
  - $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{25}$
  - $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$
  - $\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
  - $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
  - $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
- Order 605:
  - $\mathbb{Z}_5 \times \mathbb{Z}_{121}$
  - $\mathbb{Z}_5 \times \mathbb{Z}_{11} \times \mathbb{Z}_{11}$
- Order 720:
  - $\mathbb{Z}_{16} \times \mathbb{Z}_5 \times \mathbb{Z}_9$
  - $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_9$
  - $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_9$
  - $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_9$
  - $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_9$
  - $\mathbb{Z}_{16} \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

- $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
- $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_3$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

2 Problem 2

2.1 Judson Section 13.4 Exercise 6

By the Fundamental theorem of finite abelian groups, we have

$$G \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$$

where $m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, and $p_1, \cdots, p_k$ are primes (not necessarily distinct). Since $n|m$, we can write

$$n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k},$$

where $0 \leq s_i \leq r_i$ for all $1 \leq i \leq k$. For each i, pick $a_i \in \mathbb{Z}_{p_i^{r_i}}$ with order $|a_i| = p_i^{s_i}$. Then the element $a = a_1 a_2 \cdots a_k \in G$ has order $p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} = n$. The subgroup of G generated by a is then a subgroup of order n.

2.2 Judson Section 14.3 Exercise 8

By the Fundamental Theorem of finitely generated abelian group, we know that the groups G, H, K are of the form

$$\begin{aligned} G &\cong \mathbb{Z}^a \times \mathbb{Z}_{{p_1}^{a_1}} \times \mathbb{Z}_{{p_2}^{a_2}} \times \cdots \mathbb{Z}_{{p_n}^{a_n}}, \\ H &\cong \mathbb{Z}^b \times \mathbb{Z}_{{q_1}^{b_1}} \times \mathbb{Z}_{{q_2}^{b_2}} \times \cdots \mathbb{Z}_{{q_k}^{b_k}}, \\ K &\cong \mathbb{Z}^c \times \mathbb{Z}_{{r_1}^{c_1}} \times \mathbb{Z}_{{r_2}^{c_2}} \times \cdots \mathbb{Z}_{{r_l}^{c_l}}, \end{aligned}$$

where the p_i, q_i, r_i's are primes (not necessarily distinct). Since $G \times H \cong G \times K$, we have

$$\mathbb{Z}^{a+b} \times \mathbb{Z}_{{p_1}^{a_1}} \times \cdots \mathbb{Z}_{{p_n}^{a_n}} \times \mathbb{Z}_{{q_1}^{b_1}} \times \cdots \mathbb{Z}_{{q_k}^{b_k}} \cong \mathbb{Z}^{a+c} \times \mathbb{Z}_{{p_1}^{a_1}} \times \cdots \mathbb{Z}_{{p_n}^{a_n}} \times \mathbb{Z}_{{r_1}^{c_1}} \times \cdots \mathbb{Z}_{{r_l}^{c_l}}.$$

Since the Fundamental theorem of finitely generated abelian group provides a unique (up to permutation of terms) representation for a finitely generated abelian group, we must have that $b = c$, and the prime powers $q_1^{b_1}, \cdots, q_k^{b_k}$ match up with $r_1^{c_1}, \cdots r_l^{c_l}$, up to permutation. After reordering of terms, we get $H \cong K$, as desired.

Note that this result is not true for general abelian groups. For example, let $G = \prod_{i=1}^{\infty} \mathbb{Z}$ be a product of infinite copies of $\mathbb{Z}$, $H = \mathbb{Z}$ and $K = \mathbb{Z} \times \mathbb{Z}$. Then we have

$$G \times H \cong \prod_{i=1}^{\infty} \mathbb{Z} \cong G \times K,$$

but $H \ncong K$.

3 Problem 3

For $n = 43, 44$, note that there are two isomorphism classes of $\mathbb{Z}_{44}$: $\mathbb{Z}_4 \times \mathbb{Z}_{11}$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{11}$. For $n = 45$, there are two isomorphism classes of $\mathbb{Z}_{45}$: $\mathbb{Z}_9 \times \mathbb{Z}_5$ and $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. When $n = 46$, there is exactly one isomorphism class of $\mathbb{Z}_{46}$, since $\mathbb{Z}_{46} \cong \mathbb{Z}_2 \times \mathbb{Z}_{23}$, and one isomorphism class of $\mathbb{Z}_{47}$, since 47 is prime. Therefore, the smallest $n > 42$ that satisfies the given condition is $n = 46$.

4 Problem 4

(a). The map $\alpha_{a,d} : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_n \times \mathbb{Z}_m$ is defined as

$$\alpha_{a,d}((x, y)) = (ax, dy),$$

for all $(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_m$. Its kernel is the set of (x, y) such that $ax = 0$ in $\mathbb{Z}_n$ and $dy = 0$ in $\mathbb{Z}_m$. Noting that $\gcd(a, n) = \gcd(d, m) = 1$, we conclude that $a = d = 1$; in other words, the kernel of $\alpha_{a,d}$ is trivial, so $\alpha_{a,d}$ is injective. Moreover, since $\gcd(a, n) = \gcd(d, m) = 1$, there exists integers x, y such that $ax = 1$ in $\mathbb{Z}_n$ and $dy = 1$ in $\mathbb{Z}_m$. In particular, we have

$$\alpha_{a,d}(x, 0) = (1, 0), \quad \alpha_{a,d}(0, y) = (0, 1).$$

Since $(1, 0)$ and $(0, 1)$ span the codomain, $\alpha_{a,d}$ is surjective. It remains to check that $\alpha_{a,d}$ is a group homomorphism. Indeed, for $(x_1, y_1), (x_2, y_2) \in \mathbb{Z}_n \times \mathbb{Z}_m$, we have

$$\begin{aligned}
\alpha_{a,d}((x_1, y_1) + (x_2, y_2)) &= \alpha_{a,d}((x_1 + x_2, y_1 + y_2)) \\
&= (a(x_1 + x_2), d(y_1 + y_2)) \\
&= (ax_1, dy_1) + (ax_2, dy_2) \\
&= \alpha_{a,d}((x_1, y_1)) + \alpha_{a,d}((x_2, y_2)).
\end{aligned}$$

(b). Since $\gcd(n, m) = 1$, we may identify $\mathbb{Z}_{nm}$ with $\mathbb{Z}_n \times \mathbb{Z}_m$ via the isomorphism $[x]_{nm} \mapsto ([x]_n, [x]_m)$. From now on, we denote the congruence class $[x]$ by x if the context is clear. Let

$$A_n = \{(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_m : y = 0\}, \tag{1}$$
$$A_m = \{(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_m : x = 0\}. \tag{2}$$

It is clear that A_n, A_m are subgroups of $\mathbb{Z}_n \times \mathbb{Z}_m$ of order n, m, repsectively. We want to show that they are unique subgroups with such order.

Let $(a, b) \in A_n \subset \mathbb{Z}_n \times \mathbb{Z}_m$. Since A_n has order n, we have

$$(0, 0) = n(a, b) = (na, nb) \in \mathbb{Z}_n \times \mathbb{Z}_m,$$

which gives us $nb = 0$ in $\mathbb{Z}_m$. Given that $\gcd(n, m) = 1$, we conclude that $b = 0$ in $\mathbb{Z}_m$. Therefore, A_n must take the form in (1). Similarly, we conclude that A_m must take the form in (2).

Finally, we define a map $f : A_n \times A_m \to \mathbb{Z}_{nm}$ by

$$f((a, 0), (0, b)) = (a, b).$$

One may easily check that f is a bijective group homomorphism, and therefore a group isomorphism.

(c). Let $f : \mathbb{Z}_n \times \mathbb{Z}_m \to \mathbb{Z}_n \times \mathbb{Z}_m$ be an automorphism. Let $f((1,0)) = (a,b)$, $f((0,1)) = (c,d)$. This determines the entire map f. Indeed, since f is a group homomorphism, we have

$$f((x,y)) = f(x(1,0) + y(0,1)) = xf(1,0) + yf(0,1) = (ax + cy, bx + dy),$$

for any $(x,y) \in \mathbb{Z}_n \times \mathbb{Z}_m$. We want to show that $b = c = 0$, and that $\gcd(a,n) = \gcd(d,m) = 1$. Observe that

$$(0,0) = f(0,0) = f(n,0) = nf(1,0) = (na, nb),$$

which tells us that $nb = 0$ in $\mathbb{Z}_m$. Since $\gcd(n,m) = 1$, we have that $b = 0$. By a similar argument, we know that $c = 0$.

Next, suppose for the sake of contradiction that $\gcd(a,n) = k > 1$. Then

$$f(\frac{n}{k}, 0) = \frac{n}{k} f(1,0) = \frac{n}{k}(a,b) = (n \cdot \frac{a}{k}, 0) = (0,0) \in \mathbb{Z}_n \times \mathbb{Z}_m.$$

We then have $f(0,0) = (0,0) = f(\frac{n}{k}, 0)$ and $(\frac{n}{k}, 0) \neq (0,0)$. This contradicts with the surjectivity of f. Hence, we must have $\gcd(a,n) = 1$. By a similar argument, we also have $\gcd(d,m) = 1$. This concludes the proof.

(d). Define $f : \mathbb{Z}_3 \times \mathbb{Z}_9 \to \mathbb{Z}_3 \times \mathbb{Z}_9$ by

$$f(x,y) = (x, 3x + y).$$

The map f is not of the form $\alpha_{a,d}$. We want to show that f is an autmorphism. In particular, we check that

- f is injective: if $f(x,y) = f(x',y')$, then $(x, y+3x) = (x', y+3x)$, so $x = x'$ and $y = y'$.
- f is surjective: for all $(z_1, z_2) \in \mathbb{Z}_3 \times \mathbb{Z}_9$, there exists $(z_1, z_2 - 3z_1) \in \mathbb{Z}_3 \times \mathbb{Z}_9$ such that $f(z_1, z_2 - 3z_1) = (z_1, z_2)$.
- f is a homomorphism: for all $(x,y), (x',y') \in \mathbb{Z}_3 \times \mathbb{Z}_9$, we have

  $$f((x,y)+(x',y')) = f((x+x', y+y')) = (x+x', 3(x+x')+y+y') = (x, 3x+y)+(x', 3x'+y') = f(x,y)+f(x',y').$$

Therefore, f is an automorphism that is not of the form $\alpha_{a,d}$.

(e) Since $M(x,y) = (ax + by, cx + dy)$, the matrix representation of M is

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

and so M is an automorphism if and only if the determinant of M is nonzero, that is, $ad - bc \neq 0$.