II.2.1

Show that a finite abelian group that is not cyclic contains a subgroup which is isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$ for some prime p.

Proof. Let G be a finite abelian group that is not cyclic. By the Fundamental Theorem of Finite Abelian Groups, we can write G as a direct sum of cyclic groups of prime power order:

$$G \cong \mathbb{Z}_{p_1^{k_1}} \oplus \mathbb{Z}_{p_2^{k_2}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{k_n}}$$

where p_i are primes and k_i are positive integers. Since G is not cyclic we have that the direct sum has at least two cyclic components with the same prime base, i.e., there exist $i \neq j$ such that $p_i = p_j = p$. In this case, the decomposition contains $\mathbb{Z}_{p^a} \oplus \mathbb{Z}_{p^b}$ for some $a, b \geq 1$. So G contains a subgroup isomorphic to $\mathbb{Z}_{p^a} \oplus \mathbb{Z}_{p^b}$. Since $\mathbb{Z}_{p^a}$ and $\mathbb{Z}_{p^b}$ both have subgroups isomorphic to $\mathbb{Z}_p$, we can find a subgroup of G isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Thus, we conclude that any finite abelian group that is not cyclic contains a subgroup isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$ for some prime p. $\square$

II.2.7

A (sub)group in which every element has order a power of a fixed prime p is called a p-(sub)group (*note:* $|0| = 1 = p^0$). Let G be an abelian torsion group.

(a) $G(p)$ is the unique maximum p-subgroup of G (that is, every p-subgroup of G is contained in $G(p)$).

(b) $G = \sum G(p)$, where the sum is over all primes p such that $G(p) \neq 0$.
[*Hint:* If $|u| = p_1^{n_1} \dots p_t^{n_t}$. There exist $c_i \in \mathbb{Z}$ uch that $c_1 m_1 + \cdots + c_t m_t = 1$, whence $u = c_1 m_1 u + \cdots + c_t m_t u$; but $C_i m_i u \in G(p_i)$.]

(c) If H is another abelian torsion group, then $G \cong H$ if and only if $G(p) \cong H(p)$ for all primes p.

(a) *Proof.* Recall that $G(p) = \{u \in G \quad | \quad |u| = p^n \text{ for some } n \geq 0\}$. Suppose, for a contradiction, that there exists a p-subgroup H of G such that $H \not\subseteq G(p)$. Then there exists an element $h \in H$ such that $h \notin G(p)$. This means that the order of h is not a power of p, contradicting the definition of a p-subgroup. Therefore, every p-subgroup of G is contained in $G(p)$, making $G(p)$ the unique maximum p-subgroup of G. $\square$

(b) *Proof.* Let $u \in G$ be an arbitrary element. Since G is a torsion group, the order of u is finite, say $|u| = m$. We can factor m into its prime power decomposition:

$$m = p_1^{n_1} p_2^{n_2} \dots p_t^{n_t}$$

for distinct primes p_i and positive integers n_i. Define $m_i = m/p_i^{n_i}$ for each i. By the Extended Euclidean Algorithm, there exist integers $c_1, c_2, \dots, c_t$ such that:

$$c_1 m_1 + c_2 m_2 + \cdots + c_t m_t = 1$$

Multiplying both sides by u, we have:

$$u = c_1 m_1 u + c_2 m_2 u + \cdots + c_t m_t u$$

Note that each term $c_i m_i u$ has order dividing $p_i^{n_i}$, hence belongs to $G(p_i)$. Therefore, we can express u as a sum of elements from different p-subgroups:

$$u \in G(p_1) + G(p_2) + \cdots + G(p_t)$$

Since u was arbitrary, it follows that:

$$G = \sum_p G(p)$$

where the sum is over all primes p such that $G(p) \neq 0$. $\square$

(c) *Proof.* ($\Rightarrow$) Suppose $G \cong H$. Then there exists an isomorphism $\phi : G \to H$. For any prime p, consider the restriction of ϕ to $G(p)$:

$$\phi|_{G(p)} : G(p) \to H(p)$$

Since ϕ is an isomorphism, it preserves the order of elements. Thus, $\phi|_{G(p)}$ is an isomorphism from $G(p)$ to $H(p)$, implying that $G(p) \cong H(p)$ for all primes p.

($\Leftarrow$) Conversely, suppose that $G(p) \cong H(p)$ for all primes p. By part (b), we have:

$$G = \sum_p G(p) \quad \text{and} \quad H = \sum_p H(p)$$

Since each corresponding p-subgroup is isomorphic, we can construct an isomorphism $\psi : G \to H$ by defining it on each $G(p)$ and extending linearly. Specifically, for each prime p, let $\psi_p : G(p) \to H(p)$ be the isomorphism. Then define:

$$\psi(u) = \sum_p \psi_p(u_p)$$

where $u = \sum_p u_p$ with $u_p \in G(p)$. This map ψ is well-defined and bijective, hence an isomorphism. Therefore, $G \cong H$. $\square$

II.2.9

How many subgroups of order p^2 does the abelian group $\mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^2}$ have?

All subgroups of order p^2 are isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$. We will count the number of subgroups of each type and then sum them to get the total number of subgroups of order p^2.

Subgroups isomorphic to $\mathbb{Z}_{p^2}$:

All of these subgroups are generated by elements $(a, b) \in \mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^2}$ of order p^2. We know that the order of (a, b) is given by $\text{lcm}(|a|, |b|)$. This necessitates that $\text{lcm}(|a|, |b|) = p^2$. Thus we can have the following cases:

(i) $|a| = p^2$ and $|b| = \{1, p, p^2\}$.

(ii) $|a| = p$ and $|b| = p^2$.

(iii) $|a| = 1$ and $|b| = p^2$.

So we can count the number of elements in each case:

(i) The number of elements of order p^2 in $\mathbb{Z}_{p^3}$ is $\phi(p^2) = p^2 - p$.

(ii) The number of elements of order p in $\mathbb{Z}_{p^3}$ is $\phi(p) = p - 1$.

(iii) The number of elements of order 1 in $\mathbb{Z}_{p^3}$ is 1.

(iv) All elements in $\mathbb{Z}_{p^2}$ have order $1, p$, or p^2, so there are p^2 choices for b in case (i).

(v) The number of elements of order p^2 in $\mathbb{Z}_{p^2}$ is $\phi(p^2) = p^2 - p$. Thus, there are $p^2 - p$ choices for b in cases (ii) and (iii).

Since each subgroup $\langle (a, b) \rangle$ has $\phi(p^2) = p^2 - p$ generators, we can count the number of distinct subgroups isomorphic to $\mathbb{Z}_{p^2}$ as follows:

$$\begin{aligned}
\text{Number of subgroups isomorphic to } \mathbb{Z}_{p^2} &= \frac{(p^2 - p)(p^2) + (p-1)(p^2 - p) + 1(p^2 - p)}{p^2 - p} \\
&= p^2 + (p - 1) + 1 \\
&= p^2 + p.
\end{aligned}$$

The division by $p^2 - p$ accounts for the fact that each subgroup has $p^2 - p$ generators.

Subgroups isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$:

To count the number of subgroups isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$, we note that such a subgroup is generated by two elements of order p. The elements of order p in $\mathbb{Z}_{p^3}$ are those of the form kp^2 for $k = 1, 2, \ldots, p-1$, giving us $p - 1$ choices. Then, the elements of order p in $\mathbb{Z}_{p^2}$ are those of the form lp for $l = 1, 2, \ldots, p-1$, giving us another $p - 1$ choices. To form a subgroup isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$, we need to select two linearly independent elements of order p. The number of ways to choose two linearly independent elements is:

$$\binom{p^2 - 1}{2} = \frac{(p^2 - 1)(p^2 - 2)}{2}.$$

Thus, the total number of subgroups isomorphic to $\mathbb{Z}_p \oplus \mathbb{Z}_p$ is $\frac{p^2+p}{2}$. Thus we have that the total number of subgroups of order p^2 in $\mathbb{Z}_{p^3} \oplus \mathbb{Z}_{p^2}$ is $(p^2 + p) + \frac{p(p-1)}{2} = \frac{3}{2}\left(p^2 + p\right)$.

II.4.1

Let G be a group and A a normal abelian subgroup. Show that G/A operates on A by conjugation and obtain a homomorphism $G/A \to \mathrm{Aut}(A)$.

Proof. Let G be a group and A a normal abelian subgroup of G. We want to show that the factor group G/A acts on A by conjugation.

Define the action of an element $gA \in G/A$ on an element $a \in A$ by:

$$(gA) \cdot a = gag^{-1}$$

for any representative $g \in G$ of the coset gA. Since A is normal in G, the conjugation gag^{-1} is indeed an element of A. To see this defines an action we see that for the identity element $eA \in G/A$, we have:

$$(eA) \cdot a = eae^{-1} = a$$

for all $a \in A$ as well as for any $gA, hA \in G/A$ and $a \in A$, we have:

$$(gA)(hA) \cdot a = (gh)A \cdot a = (gh)a(gh)^{-1} = g(hah^{-1})g^{-1} = gA \cdot (hA \cdot a)$$

Thus, we have shown that G/A acts on A by conjugation.

Next, we define a homomorphism $\varphi : G/A \to \mathrm{Aut}(A)$ by:

$$\varphi(gA)(a) = gag^{-1}$$

for all $a \in A$.

To see that φ is a homomorphism, notice that for any $gA, hA \in G/A$, we have that

$$\varphi((gA)(hA)) = \varphi(gA) \circ \varphi(hA).$$

In fact, for any $a \in A$, we have:

$$\varphi((gA)(hA))(a) = (gh)a(gh)^{-1} = g(hah^{-1})g^{-1} = \varphi(gA)(\varphi(hA)(a)).$$

Thus, we have shown that φ is a homomorphism. Therefore, we conclude that G/A operates on A by conjugation and there exists a homomorphism $\varphi : G/A \to \mathrm{Aut}(A)$. $\square$

II.4.5

If H is a subgroup of G, the factor group $N_G(H)/C_G(H)$ (see Exercise 4) is isomorphic to a subgroup of $\operatorname{Aut}(H)$.

First we prove a lemma:

Lemma 0.1. *Let H be a normal subgroup of the group G. Then G acts by conjugation on H as automorphisms of H. For each $g \in G$, conjugation by g is an automorphism of H. The permutation representation afforded by this action is a homomorphism of G into $\operatorname{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\operatorname{Aut}(H)$.*

Proof. Let φ_g be conjugation by g. Note that since g normalizes A, φ_g maps A to itself. Since conjugation defines an action, we have that $\varphi_1 = 1$ is the identity map on A and $\varphi_a \circ \varphi_b = \varphi_{ab}$ for all $a, b \in G$. So each φ_g gives a bijection from A to itself since it has a two-sided inverse $\varphi_{g^{-1}}$. Each φ_g is a homomorphism since for all $x, y \in A$,

$$\varphi_g(xy) = g(xy)g^{-1} = gx(g^{-1}g)yg^{-1} = (gxg^{-1})(gyg^{-1}) = \varphi_g(x)\varphi_g(y).$$

This shows that conjugation by any fixed element of G defines an automorphism of A. Then we have that the permutation representation $\psi : G \to S_H$ defined by $\psi(g) = \varphi_g$ (which is a homomorphism) has image contained in the subgroup $\operatorname{Aut}(H)$ of S_H. Then,

$$\begin{aligned} \ker\psi &= \{g \in G \quad | \quad \varphi_g = \mathrm{id}\} \\ &= \{g \in G \quad | \quad ghg^{-1} = h \text{ for all } h \in H\} \\ &= C_G(H). \end{aligned}$$

Then, by the First Isomorphism Theorem, we have that $G/C_G(H) \cong \operatorname{Im}\psi \leq \operatorname{Aut}(H)$. □

Now we can prove the problem statement:

Proof. Since we have that H is a normal subgroup of $N_G(H)$, we can apply the lemma with $G = N_G(H)$ to obtain that $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\operatorname{Aut}(H)$. □

II.4.7

Let G be a group and let $\operatorname{In} G$ be the set of all inner automorphisms of G. Show that $\operatorname{In} G$ is a normal subgroup of $\operatorname{Aut} G$.

Proof. Let $\sigma \in \operatorname{Aut} G$ and let $\varphi_g \in \operatorname{In} G$ be an inner automorphism defined by conjugation by $g \in G$. We want to show that $\sigma\varphi_g\sigma^{-1} = \varphi_{\sigma(g)}$. Then we have that for any $x \in G$,

$$\begin{aligned} (\sigma\varphi_g\sigma^{-1})(x) &= \sigma(\varphi_g(\sigma^{-1}(x))) \\ &= \sigma(g\sigma^{-1}(x)g^{-1}) \\ &= \sigma(g)\sigma(\sigma^{-1}(x))\sigma(g^{-1}) \\ &= \sigma(g)x\sigma(g)^{-1} \\ &= \varphi_{\sigma(g)}(x). \end{aligned}$$

So we have that $\sigma \operatorname{In} G\sigma^{-1} \subseteq \operatorname{In} G$. Since σ was arbitrary, we conclude that $\operatorname{In} G$ is a normal subgroup of $\operatorname{Aut} G$. □

II.4.9

If $G/C(G)$ is cyclic, then G is abelian.

Proof. Suppose that $G/C(G)$ is cyclic. Then there exists an element $g \in G$ such that $G/C(G) = \langle gC(G) \rangle$. This means that for any element $x \in G$, there exists an integer n such that:

$$xC(G) = (gC(G))^n = g^n C(G).$$

Therefore, we can write:

$$x = g^n c$$

for some $c \in C(G)$.

Now, consider any two elements $x, y \in G$. We can express them as:

$$x = g^m c_1, \quad y = g^n c_2$$

for some integers m, n and elements $c_1, c_2 \in C(G)$.

Now, we compute the product xy:

$$xy = (g^m c_1)(g^n c_2) = g^{m+n}(c_1 c_2).$$

Since c_1 and c_2 are in the center of G, they commute with all elements of G, including g. Thus, we have:

$$yx = (g^n c_2)(g^m c_1) = g^{n+m}(c_2 c_1) = g^{m+n}(c_1 c_2) = xy.$$

Therefore, for any two elements $x, y \in G$, we have shown that $xy = yx$. This implies that G is abelian. $\square$

Problem 1

Suppose $G = \mathbb{Z} \times (\mathbb{Z}/10\mathbb{Z}) \times (\mathbb{Z}/100\mathbb{Z})$, and H is the subgroup generated by elements $(1, 1, 1), (1, 2, 3)$.

(a) What is the isomorphism class of H? (That is, what is H's standard form, as in Theorem 2.6(ii) or Theorem 2.6(iii)?)

(b) What is the isomorphism class of G/H?

(a) To determine the isomorphism class of H, we first find the relations among the generators $(1, 1, 1)$ and $(1, 2, 3)$. We can represent these generators as rows in a matrix:

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix}$$
$$(\text{Row reduce } M) \sim \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$$

From the row-reduced form, we can express the generators in terms of new generators:

$$H \cong \langle (1, 0, -1), (0, 1, 2) \rangle$$

Since $\langle (1, 0, -1) \rangle \cap \langle (0, 1, 2) \rangle = \{(0, 0, 0)\}$, we have that $H \cong \langle (1, 0, -1) \rangle \oplus \langle (0, 1, 2) \rangle \cong \mathbb{Z} \oplus \mathbb{Z}/50\mathbb{Z}$ as the element $(0, 1, 2)$ has order 50 in G.

(b) To find the isomorphism class of G/H, we use the fact that $G \cong \mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/100\mathbb{Z}$ and $H \cong \mathbb{Z} \oplus \mathbb{Z}/50\mathbb{Z}$. The quotient G/H can be computed by dividing each component of G by the corresponding component of H. Specifically: - The $\mathbb{Z}$ component of G is entirely contained in the $\mathbb{Z}$ component of H, so the quotient of these components is trivial: $\mathbb{Z}/\mathbb{Z} = 0$. - The $\mathbb{Z}/10\mathbb{Z}$ component of G is unaffected by H because H does not contribute anything to this component. Thus, the quotient of this component is $\mathbb{Z}/10\mathbb{Z}$. - The $\mathbb{Z}/100\mathbb{Z}$ component of G is partially "covered" by the $\mathbb{Z}/50\mathbb{Z}$ component of H. The quotient of these components is $\mathbb{Z}/100\mathbb{Z}/\mathbb{Z}/50\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$ because dividing $\mathbb{Z}/100\mathbb{Z}$ by $\mathbb{Z}/50\mathbb{Z}$ reduces the order by a factor of 50.

Combining these results, we have:

$$G/H \cong (\mathbb{Z}/\mathbb{Z}) \oplus (\mathbb{Z}/10\mathbb{Z}/0) \oplus (\mathbb{Z}/100\mathbb{Z}/\mathbb{Z}/50\mathbb{Z}) \cong 0 \oplus \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Simplifying further, we conclude that:

$$G/H \cong \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$