Problem 1 (5.2.1)**.** *Find the isomorphism classes of Abelian groups of order 200.*

The isomorphism classes of Abelian groups of order 200 are:

1. $\mathbb{Z}_{200}$
2. $\mathbb{Z}_{40} \times \mathbb{Z}_5$
3. $\mathbb{Z}_{100} \times \mathbb{Z}_2$
4. $\mathbb{Z}_{20} \times \mathbb{Z}_{10}$
5. $\mathbb{Z}_{50} \times \mathbb{Z}_2 \times \mathbb{Z}_2$
6. $\mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$

Problem 2 (5.2.2)**.** *Find the invariant factors and the elementary divisors of the Abelian group*

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5$$

If we combine relative prime numbers and rearrange we get

$$G \cong \mathbb{Z}_{90} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$$

giving us $90, 10, 2$ for the invariant factors.

We can also write G as $G \cong (\mathbb{Z}_2)^3 \times (\mathbb{Z}_6)^5 \times \mathbb{Z}_9$ which gives us the elementary divisors $2^1, 2^1, 2^1, 5^1, 5^1, 3^2$.

Problem 3 (5.2.4)**.**

Proof. Let $S = \{(x_1, \dots, x_p) | x_i \in G, \prod_i x_i = e\}$. The size of S is $|G|^{p-1}$ as the last element must be the inverse of the first $p-1$. Let H be the set of $p-$cycles. Then let H act on S by

$$(x_1, \dots, x_p) \mapsto (x_{\sigma(1)}, \dots, x_{\sigma(p)})$$

Then for an orbit $\mathcal{O}_x$ we have $|\mathcal{O}_x| = \frac{|H|}{\text{Stab}_H(x)}$. Since the size of the orbit needs to divide $|H|$ it will either be of size p or of size 1. The only scenario where it will be of size one is if $x = (x_0, \dots, x_0)$ in which case either $x_0 = e$ or $x_0^p = e$. Since $|S| = \sum |\mathcal{O}_x|$ we have that $|S| = kp + m + 1$ for some k and where m is the number of order p elements. Take the equation modulo p and we get

$$-1 \equiv m \mod p$$

completing the proof. $\square$

Problem 4 (5.3.2)**.** *Let G be a finite group and $N_1, \dots, N_n$ normal subgroups of G such that $G = N_1 \cdots N_n$ and $|G| = |N_1| \cdots |N_n|$. Prove that G is the internal direct product of G.*

Proof. The formula for the order of the product of groups is $|HK| = \frac{|H||K|}{|H \cap K|}$. As such the only way for $|G| = |N_1| \cdots |N_n|$ would be for $N_i \cap N_j = \{e\}$ for $i \neq j$. However this is equivalent to condition 2 of Proposition 5.13. Therefore G is the internal direct product of $N_1, \dots, N_n$. $\square$

Problem 5 (5.5.1)**.** *Let G be a group, H, K subgroups of G, and $H \trianglelefteq G$. Let $\varphi : K \to Aut(H)$ be the homomorphism associated with the conjugate action of K on H. Then the following statements are equivalent:*

1. *$\phi : H \rtimes_\varphi K \to G$ defined by $\phi(h, k) = hk$ is an isomorphism.*
2. *Every element $g \in G$ can be written as $g = hk$ with $h \in H$ and $k \in K$ in a unique way.*
3. *$G = HK$ and $H \cap K = \{e\}$.*

*Proof*1 $\to$ 2: Since ϕ is an isomorphism, and thus surjective for any g there is a pair (h, k) such that $g = hk$. Writing $g = hk$ is unique due to ϕ being injective.

2 $\to$ 3: Since we can write $g = hk$ for any G we know that $G = HK$. To show that $H \cap K = \{e\}$ note that we can write $h = he$ and $k = ek$ for elements of H and K. If $h = k_1k_2$ then it would have two representations $h = he = ek_1k_2$ which would be a contradiction.

3 $\to$ 1: First we will show that $\phi(h, k) = hk$ is a homomorphism. Let $(h_1, k_1), (h_2, k_2) \in H \rtimes_\varphi K$. Then

$$\phi((h_1, k_1)(h_2, k_2)) = \phi(h_1(k_1 \cdot h_2), k_1k_2) = h_1\varphi(k_1)(h_2)k_1k_2 = h_1k_1h_2k_2^{-1}k_1k_2 = h_1k_1h_2k_2 = \phi(h_1, k_1)\phi(h_2, k_2)$$

completing the proof that ϕ is a homomorphism.

We know that ϕ is surjective as $G = HK$ and as such any element $g = hk$ for some $h \in H$ and $k \in K$.

To show that ϕ is injective suppose that $\phi(h, k) = e$. Then $h^{-1} = k$ but since H and K have trivial intersection this means that $h = k = e$. Since the kernel of ϕ is trivial the map ϕ is injective.

Therefore the map ϕ is an isomorphism.

□

Problem 6 (5.5.4)**.** *(a) For any positive integer n, prove that $Aut(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$.*

(b) For any primes $p < q$, if $p|q - 1$, there exists a monomorphism $\varphi : \mathbb{Z}_p \to Aut(\mathbb{Z}_q)$ and $\mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$ is a non-abelian group of order pq.

Proof. (a) Define $\varphi : \mathbb{Z}_n^* \to \mathrm{Aut}(\mathbb{Z}_n)$ as $m \mapsto \phi_m$ where $\phi_m(x) = mx$ with multiplication done modulo n. To show that this is a homomorphism consider $m_1, m_2 \in \mathbb{Z}_n^*$. Then

$$\varphi(m_1m_2) = \phi_{m_1m_2}$$

For any $x \in \mathbb{Z}_n$ we have

$$\phi_{m_1m_2}(x) = (m_1m_2)x = m_1(m_2x) = m_1\phi_{m_2}(x) = \phi_{m_1} \circ \phi_{m_2}(x)$$

Which implies that

$$\varphi(m_1m_2) = \phi_{m_1m_2} = \phi_{m_1} \circ \phi_{m_2} = \varphi(m_1) \circ \varphi(m_2)$$

Therefore the map φ is a homomorphism.

To show it is injective suppose that for $m \in \mathbb{Z}_n^*$ we had $\phi_m(x) = x$ for all $x \in \mathbb{Z}_n$. Then $mx = x$ for all x which would imply that $m = 1$. Therefore the kernel of φ is trivial and as such φ is injective.

Finally to show that it is surjective consider $f \in \mathrm{Aut}(\mathbb{Z}_n)$. Then the generator 1 is sent to $f(1) = m$. Since f is a homomorphism we know that $f(k) = mk \mod n$. Therefore $f = \phi_m$ and φ is surjective.

(b) Since $p|q-1$ we know that $pk+1=q$ for some $k \in \mathbb{Z}^+$. Define a map $\varphi : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$ via $i \mapsto \phi_{2^{ik}}$ where $\phi_{2^{ik}}(x) = 2^{ik}x$. To see that this is a homomorphism let $x \in \mathbb{Z}_q$ and $i, j \in \mathbb{Z}_p$

$$\varphi(i+j)(x) = \phi_{i+j}(x) = 2^{k(i+j)}x = 2^{ki}2^{kj}x = \phi_i \circ \phi_j(x) = \varphi(i) \circ \varphi(j)$$

Therefore φ is a group homomorphism.

To see that it is injective suppose that $\phi_i(x) = x$. Then $2^i x = x$ which implies that $2^i = 1$ and that $i = 0$. Since the kernel is trivial φ is injective.

By definition the group $|\mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$ has order pq. To show that it is not Abelian consider (g, n) and (h, m) where $m \neq n$. Then

$$(g, n)(h, m) = (gh2^{nk}, n+m)$$

and

$$(h, m)(g, n) = (gh2^{mk}, m+n)$$

which are only equal if $m = n$.

$\square$

Problem 7 (5.5.11(book)). *Classify groups of order 28 (there are four isomorphism types).*

The different groups of order 28 are:

1. $\mathbb{Z}_{28}$ cyclic.
2. $\mathbb{Z}_{14} \times \mathbb{Z}_2$ product and abelian.
3. D_{28} Not abelian with 2 elements of order 2.
4. $D_{14} \times \mathbb{Z}_2$ Not abelian and has 3 elements of order 2.