Exercises 16, 17, pp. 138.

Problem 16. Prove that $(\mathbb{Z}/24\mathbb{Z})^\times$ is an elementary abelian group of order 8.

Proof. By the Chinese Remainder Theorem, we have

$$(\mathbb{Z}/24\mathbb{Z})^\times \cong (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times.$$

We know that $(\mathbb{Z}/3\mathbb{Z})^\times \cong \mathbb{Z}_2$. Furthermore, $(\mathbb{Z}/8\mathbb{Z})^\times$ consists of the elements a such that $\gcd(a, 8) = 1$. This give $a = 1, 3, 5, 7$. We can compute their orders directly:

$$\begin{aligned} 1^1 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \mod 8 \\ \Rightarrow |1| = 1 \text{ and } |3| = |5| = |7| = 2. \end{aligned}$$

Thus $(\mathbb{Z}/8\mathbb{Z})^\times$ is a group of order 4 with 3 elements of order 2. The only possible such group is $\mathbb{Z}_2^2$, so

$$(\mathbb{Z}/24\mathbb{Z})^\times \cong \mathbb{Z}_2^2 \times \mathbb{Z}_2 \cong \mathbb{Z}_2^3.$$

Clearly $\mathbb{Z}_2^3$ is an elementary group with $p = 2$ that has order 8 and is abelian. $\square$

Problem 17. Let $\langle G \rangle$ be a cyclic group of order n. For $n = 2, 3, 4, 5, 6$, write out the elements of $\mathrm{Aut}(G)$ explicitly.

Proof. For each case, let x generate the group with $|x| = n$. Notice that we only need to focus on the image of x, as it determines the entire map.

$n = 2$: x can only map to itself. Hence any automorphism must be the identity:

$$1 \mapsto 1, \ \ x \mapsto x.$$

$n = 3$: We can map x to itself or x^2. This gives two maps, which one can easily verify are also homomorphisms:

$$\begin{aligned} 1 \mapsto 1, \ \ x \mapsto x, \ \ x^2 \mapsto x^2 \\ 1 \mapsto 1, \ \ x \mapsto x^2, \ \ x^2 \mapsto x. \end{aligned}$$

$n = 4$: We can map x to itself and x^3, but not x^2 (the map would not be bijective). This again gives two maps, which one can easily verify are also homomorphisms:

$$\begin{aligned} 1 \mapsto 1, \ \ x \mapsto x, \ \ x^2 \mapsto x^2 \ \ x^3 \mapsto x^3 \\ 1 \mapsto 1, \ \ x \mapsto x^3, \ \ x^2 \mapsto x^2 \ \ x^3 \mapsto x. \end{aligned}$$

$n = 5$: We know that $(\mathbb{Z}_5)^\times \cong \mathbb{Z}_4$. Hence there are 4 maps, each corresponding x being mapped to an non-identity element:

$$\begin{gathered} 1 \mapsto 1,\ \ x \mapsto x,\ \ x^2 \mapsto x^2\ \ x^3 \mapsto x^3\ \ x^4 \mapsto x^4 \\ 1 \mapsto 1,\ \ x \mapsto x^2,\ \ x^2 \mapsto x^4\ \ x^3 \mapsto x\ \ x^4 \mapsto x^3 \\ 1 \mapsto 1,\ \ x \mapsto x^3,\ \ x^2 \mapsto x\ \ x^3 \mapsto x^4\ \ x^4 \mapsto x^2 \\ 1 \mapsto 1,\ \ x \mapsto x^4,\ \ x^2 \mapsto x^3\ \ x^3 \mapsto x^2\ \ x^4 \mapsto x. \end{gathered}$$

$n = 6$: If x is mapped to any of x^2, x^3, or x^4, the generated map is not bijective. Hence there are only two possible maps, which we can see are isomorphisms:

$$\begin{gathered} 1 \mapsto 1,\ \ x \mapsto x,\ \ x^2 \mapsto x^2\ \ x^3 \mapsto x^3\ \ x^4 \mapsto x^4\ \ x^5 \mapsto x^5 \\ 1 \mapsto 1,\ \ x \mapsto x^5,\ \ x^2 \mapsto x^4\ \ x^3 \mapsto x^3\ \ x^4 \mapsto x^2\ \ x^5 \mapsto x. \end{gathered}$$

And thus we are done.

□

Exercises 3, 5, 6, 8, 14 pp. 184-187.

Problem 3. Continue from Example 1. Prove that every element of $G - H$ has order 2. Prove that G is abelian if and only if $h^2 = 1$ for all $h \in H$.

Proof. We prove the statements separately:

Every element of $G-H$ has order 2. Let $g \in G - H$. Then g must be of the form hk for some $h \in H$ and $k \in K$ and *not* of the form $g = h$. Thus we must have $g = hx$. Then $g^2 = hxhx$. The action implies that $xhx^{-1} = xhx = h^{-1}$, therefore $g^2 = hh^{-1} = 1$. Thus $|g| = 2$.

G is abelian $\iff$ $\forall h \in H, h^2 = 1$.

($\Rightarrow$): If G is abelian, then for any $h \in H$, $h(hx) = (hx)h$. Then

$$hhx = hxh \Rightarrow hh = hxhx^{-1} = hxhx = 1 \Rightarrow h^2 = 1.$$

($\Leftarrow$): If $h^2 = 1$ for all $h \in H$, then every element of G has order 2. Then for any $g_1, g_2 \in G$,

$$(g_1 g_2)^2 = g_1^2 g_2^2 = 1 \Rightarrow g_1 g_2 g_1 g_2 = g_1 g_1 g_2 g_2 \Rightarrow g_2 g_1 = g_1 g_2.$$

Thus G is abelian.

□

Problem 5. Let $G = \text{Hol}(\mathbb{Z}_2 \times \mathbb{Z}_2)$.

(a) Prove that $G = H \rtimes K$ where $H = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $K \cong S_3$. Deduce that $|G| = 24$.

(b) Prove that G is isomorphic to S_4.

Proof. We proceed by proving each part:

(a) Let $K = \text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$. If $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_2$ is an isomorphism, then φ must fix $(0,0)$ while permuting $\{(0,1),(1,0),(1,1)\}$. Thus the action of φ on the 3 non-identity elements can be associated with a element of S_3. So we have a map

$$\Phi : \text{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \to S_3.$$

Now, the composition of two maps $\varphi_2 \circ \varphi_1$ will permute the 3 non-identity elements by the composition of the permutations associated with φ_1 and φ_2, so we have

$$\Phi(\varphi_2 \circ \varphi_1) = \Phi(\varphi_1)\Phi(\varphi_2),$$

which shows that Φ is a homomorphism.

Furthermore, clearly two automorphisms $\varphi_1 \neq \varphi_2$ will permute the 3 non-identity elements differently, so Φ is also injective. To see that Φ is surjective, we must show that any permutation of the 3 non-identity elements gives a automorphism of $\mathbb{Z}_2 \times \mathbb{Z}_2$. This is not hard to check directly, but there it is tedious so we shall omit it. Thus Φ is bijective, and hence a isomorphism.

We conclude that $K \cong S_3$. Since $|S_3| = 6$ and $|H \rtimes K| = |H||K|$, we may deduce $|G| = 4 \times 6 = 24$.

(b) Let G act on the 4 left cosets of K, so that we may define the associated homomorphism $G \to S_4$. Note that each left coset may be written as hkK for some $h \in H$ and $k \in K$. Since $kK = K$, we may forget about the factors of k and realize that the 4 cosets are identified by the 4 elements of H.

We want to show that G acts faithfully and conclude that $G \to S_4$ is injective. For any $g \in G$, if $g \cdot hK = hK$ for all left cosets of K, then

$$h^{-1}ghK = K \Rightarrow h^{-1}gh \in K \Rightarrow h^{-1}gh = 1,$$

where the last implication follows from the fact that $h^{-1}gh \in H$ and $H \cap K = 1$. Thus $g = 1$, proving that G acts faithfully and $G \to S_4$ is injective. But $|G| = |S_4| = 24$, so $G \to S_4$ must also be bijective, and therefore an isomorphism.

□

Problem 6. Assume that K is a cyclic group, H is an arbitrary group and φ_1 and φ_2 are homomorphisms from K into $\mathrm{Aut}(H)$ such that $\varphi_1(K)$ and $\varphi_2(K)$ are conjugate subgroups of $\mathrm{Aut}(H)$. If K is infinite assume φ_1 and φ_2 are injective. Prove by constructing an explicit isomorphism that $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K$.

Proof. Suppose that $\sigma\varphi_1(K)\sigma^{-1} = \varphi_2(K)$. In particular, this can also be seen as the image of an automorphism on $\varphi_2(K)$. Since K is cyclic, any automorphism has the form $k \mapsto k^a$ for some $a \in \mathbb{Z}$. Thus we have $\sigma\varphi_1(k)\sigma^{-1} = \varphi_2(k)^a$ for all $k \in K$.

We claim that the map from $\psi : H \rtimes_{\varphi_1} K \to H \rtimes_{\varphi_2} K$ defined by $(h, k) \mapsto (\sigma(h), k^a)$ is a homomorphism. Indeed, let $(h_1, k_1), (h_2, k_2) \in H \rtimes_{\varphi_1} K$. Then we have,

$$\begin{aligned}
\psi((h_1, k_1) \bullet_{\varphi_1} (h_2, k_2)) &= \psi((h_1\varphi_1(k_1)(h_2), k_1k_2)) \\
&= (\sigma h_1\varphi_1(k_1)(h_2)\sigma^{-1}, (k_1k_2)^a) \\
&= (\sigma h_1\sigma^{-1}\sigma\varphi_1(k_1)(h_2)\sigma^{-1}, k_1^a k_2^a) \\
&= (\sigma h_1\sigma^{-1}\varphi_2(k_1)(h_2)^a, k_1^a k_2^a) \\
&= (\sigma h_1\sigma^{-1}\varphi_2(k_1)(h_2^a), k_1^a k_2^a) \\
&= (\sigma h_1\sigma^{-1}, k_1^a) \bullet_{\varphi_2} (h_2^a, k_2^a) \\
&= (\sigma h_1\sigma^{-1}, k_1^a) \bullet_{\varphi_2} (\sigma h_2\sigma^{-1}, k_2^a) \\
&= \psi(h_1, k_1) \bullet_{\varphi_2} \psi(h_2, k_2).
\end{aligned}$$

Thus ψ is a homomorphism.

Furthermore, we can consider the map $\phi : H \rtimes_{\varphi_2} K \to H \rtimes_{\varphi_1} K$ in the opposite direction given by $\phi((h, k)) = (\sigma^{-1}h\sigma, k^{a^{-1}})$. Since $\sigma^{-1}\varphi_2(K)\sigma = \varphi_1(K)$ and this forms the inverse automorphism which maps $k \mapsto k^{a^{-1}}$, we similarly deduce that ϕ is a homomorphism as well. Now note that

$$\psi \circ \phi((h, k)) = \psi((\sigma^{-1}h\sigma, k^{a^{-1}})) = (\sigma\sigma^{-1}h\sigma\sigma^{-1}, (k^{a^{-1}})^a) = (h, k);$$
$$\phi \circ \psi((h, k)) = \phi((\sigma h\sigma^{-1}, k^a)) = (\sigma^{-1}\sigma h\sigma^{-1}\sigma, (k^a)^{a^{-1}}) = (h, k).$$

So ψ and ϕ are two-sided inverses of each other. Thus ψ is an isomorphism and

$$H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K.$$

□

Problem 8. Construct an non-abelian group of order 75. Classify all groups of order 75.

Problem 14. Classify groups of order 60.

Proof. Let G be a group of order 60, let P be a Sylow 5-subgroup of G and let Q be a Sylow 3-subgroup of G.

(a) If P is not normal in G, then $n_5 > 1$.Proposition 21 in Section 4.5 shows that G is simple. Then Proposition 23 of Section 4.5 shows that $G \cong A_5$.

(b) If $P \trianglelefteq G$ and Q is not normal in G

(c) **TODO**.

$\square$

Exercises 2, 5 pp. 165-167.

Problem 5. Let G be a finite abelian group of type $(n_1, n_2, \ldots, n_t)$. Prove that G contains an element of order m if and only if $m \mid n_1$. Deduce that G is of exponent n_1.

Exercise 15 p. 174.

Problem 15. If A and B are normal subgroups of G such that G/A and G/B are both abelian, prove that $G/A \cap B$ is abelian.

Proof. Let $G' = [G, G]$ be the commutator subgroup of G. By Proposition 7 (4) from the textbook, since both $A, B \trianglelefteq G$ and G/A and G/B are abelian, we have $G' \leq A, B$. Thus $G' \leq A \cap B$, and Proposition 7 (4) once again tells us that $G/(A \cap B)$ must be abelian. $\square$