Homework 6

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:

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

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. □

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 $\text{Aut}(G)$ 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:

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

$n = 4$: 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:

$$1 \mapsto 1,\;\; x \mapsto x,\;\; x^2 \mapsto x^2 \;\; x^3 \mapsto x^3$$
$$1 \mapsto 1,\;\; x \mapsto x^3,\;\; x^2 \mapsto x^2 \;\; x^3 \mapsto x.$$

$n = 5$: 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:

$$1 \mapsto 1,\;\; x \mapsto x,\;\; x^2 \mapsto x^2 \;\; x^3 \mapsto x^3 \;\; x^4 \mapsto x^4$$
$$1 \mapsto 1,\;\; x \mapsto x^2,\;\; x^2 \mapsto x^4 \;\; x^3 \mapsto x \;\; x^4 \mapsto x^3$$
$$1 \mapsto 1,\;\; x \mapsto x^3,\;\; x^2 \mapsto x \;\; x^3 \mapsto x^4 \;\; x^4 \mapsto x^2$$
$$1 \mapsto 1,\;\; x \mapsto x^4,\;\; x^2 \mapsto x^3 \;\; x^3 \mapsto x^2 \;\; x^4 \mapsto x.$$

$n = 6$: 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:

$$1 \mapsto 1,\;\; x \mapsto x,\;\; x^2 \mapsto x^2 \;\; x^3 \mapsto x^3 \;\; x^4 \mapsto x^4 \;\; x^5 \mapsto x^5$$
$$1 \mapsto 1,\;\; x \mapsto x^5,\;\; x^2 \mapsto x^4 \;\; x^3 \mapsto x^3 \;\; x^4 \mapsto x^2 \;\; x^5 \mapsto x.$$

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. 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 $g_1, g_2 \in G$,

$$(g_1g_2)^2 = g_1^2g_2^2 = 1 \Rightarrow g_1g_2g_1g_2 = g_1g_1g_2g_2 \Rightarrow g_2g_1 = g_1g_2.$$

Thus G is abelian. □

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

(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 $K = \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$. 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

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

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

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

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.

Proof. Let G be a group of order 75. A routine application of Sylow's Theorems show that there is exactly one normal 5-Sylow subgroup $P \trianglelefteq G$ such that $|P| = 5^2$. By the classification of groups of order p^2 for primes p, we must have

$$P \cong \mathbb{Z}_{5^2} \text{ or } P \cong \mathbb{Z}_5 \times \mathbb{Z}_5.$$

Furthermore, Cauchy's Theorem guarentees the existence of at least of subgroup Q of order 3. As 3 and 25 are coprime, $P \cap Q = 1$. Thus $|PQ| = |P||Q| = 75 \Rightarrow PQ = G$. Hence

$$G \cong P \rtimes Q \cong P \rtimes \mathbb{Z}_3.$$

Now we must break into two cases:

Case 1: If $P \cong \mathbb{Z}_{5^2}$, then $\mathrm{Aut}(\mathbb{Z}_{25}) \cong (\mathbb{Z}_{25})^\times$. The order is then $\phi(25) = 20$, which 3 *does not* divide. Thus any map

$$\varphi : \mathbb{Z}_3 \to \mathrm{Aut}(P)$$

must be trivial. The semidirect product of $P \rtimes Q$ degenerates to a direct product between $\mathbb{Z}_{25}$ and $\mathbb{Z}_3$. Hence in this case

$$G \cong \mathbb{Z}_{25} \times \mathbb{Z}_3 \cong \mathbb{Z}_{75}.$$

Case 2: Here $\mathrm{Aut}(P) \cong \mathrm{Aut}(\mathbb{Z}_5 \times \mathbb{Z}_5)$ is much more complicated. We can view $\mathbb{Z}_5 \times \mathbb{Z}_5$ as an vector field over $\mathbb{Z}_5$ by endowing it with the obvious scalar product ($1 \cdot p = p$, $2 \cdot p = p + p$, etc.). Then there is an natural isomorphism between $\mathrm{Aut}(\mathbb{Z}_5 \times \mathbb{Z}_5)$ and the invertible matrices $\mathrm{GL}_2(\mathbb{F}_5)$.

We can determine the order of $\mathrm{GL}_2(\mathbb{F}_5)$ via a counting argument. The linear transformations A of $\mathrm{GL}_2(\mathbb{F}_5)$ are defined by the images of the two basis vectors $(1, 0)$ and $(0, 1)$. For the first basis vector, we can pick any nonzero vector v to be its image, giving $5^2 - 1$ choices. The second basis vector cannot be any of $\{1, v, 2v, 3v, 4v\}$ to ensure that the resulting map is invertible. Thus there as $5^5 - 5$ choices. In total, this gives $(5^2 - 1)(5^2 - 5)$ possible linear transformations. Thus

$$|\mathrm{GL}_2(\mathbb{F}_5)| = |\mathrm{Aut}(\mathbb{Z}_5 \times \mathbb{Z}_5)| = 480.$$

Now we must determine the possible semidirect structures of $P \rtimes Q$ by studying the possible homomorphisms $\varphi : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_5 \times \mathbb{Z}_5)$. Once again, if φ is trivial, then the semidirect product is direct, and we have

$$G \cong \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_3.$$

This classifies all the abelian groups of order 75. (Note that this agrees with the Fundemental Theorem of Abelian Groups.)

Otherwise, $\mathbb{Z}_3$ is mapped to some subgroup of order 3 in $\mathrm{Aut}(\mathbb{Z}_5 \times \mathbb{Z}_5)$. By Caunchy's Theorem, such a subgroup exists. Furthermore, we claim that different choices for φ is this produce isomorphic structures on the semidirct product. Indeed, 3 is a maximal prime of 480, so the 3-Sylow subgroups have order 3. Thus by Sylow's 2nd Theorem, all subgroups of order 3 are conjugate to each other in $\mathrm{Aut}(\mathbb{Z}_5 \times \mathbb{Z}_5)$. Since $\mathbb{Z}_3$ is cyclic, we may apply Problem 6 to deduce that all possible choices of φ produce isomorphic semidirect products. Hence we just have one non-abelian group is this case:

$$G \cong (\mathbb{Z}_5 \times \mathbb{Z}_5) \rtimes \mathbb{Z}_3,$$

where the semidirect product acts via conjugation, so that $\varphi(x)(B) = \varphi(x)B\varphi(x)^{-1}$ (viewing both $\varphi(x)$ and B as matrices in $\mathrm{GL}_2(\mathbb{F}_5)$). It is difficult to find an explicit matrix of order 3, so we'll just stop here. (One must work with the characteristic polynomial and deduce something complicated.)

□

Problem 14. Classify groups of order 60.

Proof. This is a terribly long proof, so I will be leaving out many routine details that do not effect the deeper understanding of the techniques used.

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, then Sylow's 3rd Theorem gives $n_3 \geq 4$. Let Q_1, Q_2, Q_3, Q_4 be four distinct 3-Sylow subgroups of G. Then we can construct PQ_i for each i to obtain four groups of order 15 that intersect only at P. Thus each $PQ_i \cong \mathbb{Z}_{15}$ and also centralize P, so that $C_G(P)$ contains at least $15+10+10+10 = 45$ elements. By Lagrange, $|C_G(P)| \div |G|$ and consequently we may only have $|C_G(P)| = 60$. Thus we conclude that $P \leq Z(G)$.

Now consider G/P, a quotient group of order 12. From the textbook's analysis of this group, we know that either $n_2 = 1$ or $n_3 = 1$. For the sake of contradiction assume that $n_3 = 1$. Then G/P has a normal subgroup of order 3. An cardinaility argument shows that this subgroup must be of the form PQ_i/P, which by the fourth isomorphism theorem we may correspond to PQ_i of G. In fact $PQ_i/P \trianglelefteq G/P$ implies $PQ_i \trianglelefteq G$. Then for any $g \in G$, we have $gPQ_ig^{-1} = PQ_i$. If we break up the conjugate action by doing

$$gPQ_ig^{-1} = gPg^{-1}gQ_ig^{-1} = PgQ_ig^{-1} = PQ_i,$$

it becomes clear that $gQ_ig^{-1} = Q_i$. Hence $Q_i \trianglelefteq G$, which gives contradiction.

Since $n_3 \neq 1$ we must have instead that $n_2 = 1$. Then the only possible group structure for Q/P is A_4. Again, there is a normal 2-Sylow subgroup of Q/P of the form TP/P, where T is a 2-Sylow subgroup of G. This is due once more to cardinaility arguments. The fourth isomorphism theorem gives $TP \trianglelefteq G$, and thus applying the conjugation argument we see that $T \trianglelefteq G$. Since Q is not normal, we must have $TQ \cong A_4$.

Now with a subgroup of order 12 and P, we can deduce that

$$G \cong P \rtimes TQ \cong \mathbb{Z}_5 \rtimes_\varphi A_4.$$

Consider the possible maps $\varphi : A - 4 \to \operatorname{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_4$. The kernel of φ must be normal in A_4, so it must be equal to 1 or V_4. If $\ker\varphi \cong V_4$, then the image of φ must have order 3, which is impossible due to Lagrange. Hence $\ker\varphi = 1$ and the semidirect product is direct. Thus

$$G \cong \mathbb{Z}_5 \rtimes_\varphi A_4 \cong A_4 \times \mathbb{Z}_5.$$

(c) If $P, Q \trianglelefteq G$, then $PQ \trianglelefteq G$ is a subgroup of order 15 isomorphic to $\mathbb{Z}_{15}$. Let T be a 2-Sylow subgroup of G. We have $G \cong PQ \rtimes T \cong \mathbb{Z}_{15} \rtimes T$. We must find the associated homomorphisms $\varphi : T \to \operatorname{Aut}(\mathbb{Z} - 15) \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. As for T, it must be either $\mathbb{Z}_4$ or $mathbbZ_2 \times \mathbb{Z}_2$. Thus we split into two cases.

Case 1: $T \cong \mathbb{Z}_4$. Let x generate T. We only need do map x to determine the maps $\varphi : T \to \mathbb{Z}_4 \times \mathbb{Z}_2$. If $|\varphi(T)| = 1$, then we have $G = \mathbb{Z}_{15} \times \mathbb{Z}_4$. If $|\varphi(T)| = 2$, then there are 3 possible images: $(0,1), (2,0), (2,1)$. If $|\varphi(G)| = 4$, then there is 2 images: $(1,0)$ and $(1,1)$. (Note here that the images $(3,0)$ and $(3,1)$ are not counted because they give isomorphic representations, but this is too tedious to all write out.)

Hence in this case there are a total of 6 possible isomorphism classes for G.

Case 2: If $T = \mathbb{Z}_2 \times \mathbb{Z}_2$, then we have $(0, 0)$ for the trivial image (giving a abelian group). If the image has order 2, then the differences in how we choose which elements go into the kernel all give the same semidirect structure. Thus only the image matters, of which there are 3 possiblilities: $(2, 0), (0, 1), (2, 1)$. If the image has order 4, then it must map to the unique subgroup generated by $\langle(2, 0)\rangle \times \langle(0, 1)\rangle$. The choice of the mapping again produce the same isomorphism classes of G, so there is only one new group here.

Hence in total, this case produces 5 new isomorphism classes for G.

In total, we have 13 isomorphism classes of G. □

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.

Proof. $(\Rightarrow)$: If $m \mid n_1$, then let $am = n_1$. Consider the element $a \in \mathbb{Z}_{n_1}$. This element clearly has order $n_1/a = m$.

$(\Leftarrow)$: Suppose G contains an element of order m. Let e_i generate $\mathbb{Z}_{n_i}$ for $1 \leq i \leq t$. Then $m = a_1e_1 + \ldots a_te_t$. The order of e_i is n_i, so the order of a_ie_i divides n_i. Furthermore, we know that the order of $a + b$ divides $\mathrm{lcm}(|a|, |b|)$. The lcm of $n_1, \ldots, n_t$ is just n_1, so we may extend the argument to conclude that the order of $m = a_1e_1 + \ldots a_te_t$ divides n_1.

The exponent of G must at most be n_1. Applying our findings above, we deduce that every element of G divides n_1. Thus the exponent of G is also at least n_1. Thus the exponent of G is n_1, as desired. □

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. □