Problem Set 9
solutions

Problem 1.

(1.1) Show that there exists a nonabelian group of order 63.

Proof. We will show that there exists a nontrivial homomorphism $\rho\colon \mathbb{Z}/9 \to \mathrm{Aut}(\mathbb{Z}/7)$. As a consequence, the semidirect product $\mathbb{Z}/7 \rtimes_\rho \mathbb{Z}/9$ is a nonabelian group.

Since $\mathbb{Z}/9$ is a cyclic group generated by 1, the UMP for cyclic groups says that to any homomorphism $\rho\colon \mathbb{Z}/9 \to \mathrm{Aut}(\mathbb{Z}/7)$ is completely determined by $\alpha = \rho(1)$, and that any $\alpha \in \mathrm{Aut}(\mathbb{Z}/7)$ such that $\alpha^9 = \mathrm{id}$ gives rise to such a homomorphism. Moreover, we showed in Problem Set 8 that each $f \in \mathrm{Aut}(\mathbb{Z}/7)$ corresponds to an element $a \in (\mathbb{Z}/7)^\times$, with $f(i) = ai$.

So consider the automorphism $f\colon \mathbb{Z}/7 \longrightarrow \mathbb{Z}/7$ given by

$$f(i) = 2i.$$

Note that 2 is indeed invertible in $\mathbb{Z}/7$. Moreover, for all $i \in \mathbb{Z}/7$ we have

$$f^3(i) = 2(2(2i)) = 8i = i,$$

so $f^3 = \mathrm{id}$. As a consequence, $f^9 = \mathrm{id}$, and thus by the UMP for cyclic groups there is a homomorphism $\rho\colon \mathbb{Z}/9 \to \mathrm{Aut}(\mathbb{Z}/7)$ with

$$\rho(1) = f.$$

Since $f \neq \mathrm{id}$ this is a nontrivial homomorphism, we conclude that

$$\mathbb{Z}/7 \rtimes_\rho \mathbb{Z}/9$$

is a nonabelian group. $\square$

Alternative proof. Consider $H = \mathbb{Z}/7$ and $K = \mathbb{Z}/9$. If we can find a nontrivial homomorphism $\rho\colon \mathbb{Z}/9 \to \mathrm{Aut}(\mathbb{Z}/7)$, then the semidirect product $H \rtimes_\rho K$ is not abelian.

We also know that

$$\mathrm{Aut}(\mathbb{Z}/7) \cong \mathbb{Z}/6.$$

Since $\mathbb{Z}/9$ is a cyclic group, by the UMP for cyclic groups any homomorphism $\rho\colon \mathbb{Z}/9 \to \mathbb{Z}/6$ is completely determined by $\alpha = \rho(1)$, and any $\alpha \in \mathbb{Z}/6$ such that $9\alpha = 0$ gives rise to such a homomorphism. Thus setting $\alpha = 2$ gives us the homomorphism $\rho\colon \mathbb{Z}/9 \to \mathbb{Z}/6$ with

$$\rho(i) = 2i.$$

Moreover, ρ is nontrivial, since

$$\rho(1) = 2 \neq 0 \text{ in } \mathbb{Z}/6.$$

We conclude that

$$\mathbb{Z}/7 \rtimes_\rho \mathbb{Z}/9$$

is a nonabelian group.

Note: This proof has a big disadvantage: it does not tell us what $\rho(a)(b)$ is for each $a \in \mathbb{Z}/9$ and $b \in \mathbb{Z}/6$, which is important for solving part (b). $\square$

(1.2) Find a presentation for the group you found, with justification.

Proof. To give a presentation for this group, let $x = (1,0)$ and $y = (0,1)$, and note that $\mathbb{Z}/7 \rtimes_\rho \mathbb{Z}/9$ is generated by x and y: indeed, for any $a \in \mathbb{Z}/7$ and $b \in \mathbb{Z}/9$ we have

$$(a,b) = (1,0)^a (0,1)^b = x^a y^b.$$

Note also that

$$x^7 = (7,0) = (0,0) \quad \text{and} \quad y^9 = (0,9) = 0.$$

Moreover,

$$yx = (0,1)(1,0) = (0 + \rho(1)(1), 1 + 0) = (f(1), 1) = (2,1) = x^2 y.$$

We claim that

$$\langle x, y \mid x^7 = e, y^9 = e, yx = x^2 y \rangle$$

is a presentation for $\mathbb{Z}/7 \rtimes_\rho \mathbb{Z}/9$. So let

$$G = \langle u, v \mid u^7 = e, v^9 = e, vu = u^2 v \rangle.$$

By the UMP for presentations, since x and y satisfy

$$x^7 = e, y^9 = e, yx = x^2 y,$$

then there exists a homomorphism $\varphi \colon G \to \mathbb{Z}/7 \rtimes_\rho \mathbb{Z}/9$ given by

$$\varphi(u) = x \quad \text{and} \quad \varphi(v) = y.$$

We showed that x and y generate $\mathbb{Z}/7 \rtimes_\rho \mathbb{Z}/9$, so this homomorphism must be surjective. In particular, $|G| \geqslant |\mathbb{Z}/7 \rtimes_\rho \mathbb{Z}/9| = 7 \cdot 9 = 63$.

On the other hand, in G, any expression involving u and v can be rewritten by replacing $v^2 u$ by uv, so that any element can be written as $u^a v^b$ for some integers a and b. Since $u^7 = e$ and $v^9 = e$, any element in G can then be written as

$$u^a v^b \quad \text{where } 0 \leqslant a \leqslant 6 \text{ and } 0 \leqslant b \leqslant 8.$$

There are $9 \cdot 7 = 63$ expressions of this form, and thus $|G| \geqslant 63$. We conclude that

$$|G| = 63 = |\mathbb{Z}/7 \rtimes_\rho \mathbb{Z}/9|,$$

so that the surjective map φ must in fact be an isomorphism, proving that

$$\langle x, y \mid x^7 = e, y^9 = e, yx = x^2 y \rangle$$

is a presentation for $\mathbb{Z}/7 \rtimes_\rho \mathbb{Z}/9$. □

Problem 2. Let G be a group of order $75 = 5^2 \cdot 3$ which contains an element of order 25. Prove that G is cyclic.

Proof. Let $n_5 = |\operatorname{Syl}_5(G)|$. By the Main Theorem of Sylow Theory, n_5 divides 3, so $n_5 \in \{1, 3\}$. But the Main Theorem of Sylow Theory also gives us

$$n_5 \equiv 1 \pmod 5,$$

and $n_5 = 3 \not\equiv 1 (\mathrm{mod}\ 5)$. We conclude that $n_5 = 1$, and thus the unique Sylow 5-subgroup Q of G must be normal. Note moreover that G has an element of order 25, which must then generated a subgroup of order 25; that subgroup must then be Q. We conclude that $Q \cong \mathrm{Z}/25$.

Let P be a Sylow 3-subgroup. Since the order of $P \cap Q$ must divide both $|P| = 3$ and $|Q| = 25$, then $P \cap Q = \{e\}$. Therefore,

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = \frac{3 \cdot 25}{1} = 75,$$

so we conclude that $G = PQ$. So we have $G = PQ$, P normal in G, and $P \cap Q = \{e\}$.

By the Recognition Theorem for Semidirect Products, we have that $G = Q \rtimes_\phi P$ where ϕ is a homomorphism

$$\phi \colon P \longrightarrow \operatorname{Aut}(Q).$$

Note that $\operatorname{Aut}(Q) \cong \operatorname{Aut}(\mathrm{Z}/25) \cong \mathbb{Z}_{25}^\times$, which has order $\varphi(25) = 5(5-1) = 20$. In particular, the order of every element in $\operatorname{Aut}(Q)$ must divide 20.

Since $|P| = 3$, every nontrivial element in P has order 3, and thus for all $x \in P$ we have

$$\phi(x)^3 = \phi(x^3) = \phi(e) = e.$$

But $\gcd(3, 20) = 1$, so there are no elements in $\operatorname{Aut}(Q)$ of order 3. We conclude that ϕ must be the trivial map. Hence $G = P \times Q$, which is a direct product of cyclic groups of orders 3 and 5. Therefore, using the CRT we get

$$G \cong \mathbb{Z}/3 \times \mathbb{Z}/5 \cong \mathbb{Z}/15,$$

and thus G is cyclic. $\square$

Problem 3. Let G be a group of order $231 = 3 \cdot 7 \cdot 11$. Prove that there is a unique Sylow 11-subgroup of G, and that it is contained in $\mathrm{Z}(G)$.

Proof. Let $n_p = |\operatorname{Syl}_p(G)|$ for $p \in \{3, 7, 11\}$. By the Sylow Theorems,

$$\text{and } n_7 \text{ divides } 3 \cdot 11 \implies n_7 \in \{1, 3, 11, 33\},$$

But

$$n_7 \equiv 1 \pmod 7 \quad \text{and} \quad 3 \not\equiv 1 \ (\mathrm{mod}\ 7),\ 11 \not\equiv 1 \ (\mathrm{mod}\ 7),\ 33 \not\equiv 1 \ (\mathrm{mod}\ 7),$$

so $n_7 = 1$. Similarly,

$$n_{11} \text{ divides } 3 \cdot 7 \implies n_{11} \in \{1, 3, 7, 21\},$$

but

$$n_{11} \equiv 1 \pmod{11} \text{ and } 3 \not\equiv 1 \ (\mathrm{mod}\ 11),\ 7 \not\equiv 1 \ (\mathrm{mod}\ 11),\ 21 \not\equiv 1 \ (\mathrm{mod}\ 11).$$

Thus $n_{11} = 1$.

Let Q be the unique Sylow 7 subgroup and R be the unique Sylow 11-subgroup, which must then be normal. Let P be a Sylow subgroup of order 3. Since Q is normal, PQ is a subgroup of G of order 21, and since R is also normal, PQR is a subgroup of G of order 231, so $PQR = G$. By the Recognition Theorem for Semidirect Products, $G = R \rtimes_\phi PQ$ where

$$\phi \colon PQ \to \operatorname{Aut}(R).$$

Since 11 is prime and R is a group of order 11, we conclude that $R \cong \mathbb{Z}/11$ and $|\operatorname{Aut}(R)| = 10$. Moreover, $|\operatorname{im}(\phi)|$ must divide both $|PQ| = 21$ and $|\operatorname{Aut}(R)| = 10$, but since $\gcd(10, 21) = 1$, we conclude that ϕ must be the trivial map.

Hence $G \cong R \times PQ$, and every element of R commutes with every element of PQ. Since R is cyclic and thus abelian, we see that every element of R commutes with every element of $PQR = G$: indeed, the isomorphism $G \cong R \times PQ$, sends R to the subgroup of elements of the form (r, e), and for all $(a, b) \in R \times PQ$ we have

$$(r, e)(a, b) = (ra, b) = (ar, b) = (a, b)(r, e).$$

We conclude that $R \subseteq \mathrm{Z}(G)$. □

Problem 4. Prove that there are precisely two groups of order $105 = 3 \cdot 5 \cdot 7$ up to isomorphism. You can use the following lemma without proof:

Lemma 1. Let K be a finite cyclic group and let H be an arbitrary group. Suppose $\phi \colon K \to \operatorname{Aut}(H)$ and $\theta \colon K \to \operatorname{Aut}(H)$ are homomorphisms whose images are conjugate subgroups of $\operatorname{Aut}(H)$; that is, suppose there is $\sigma \in \operatorname{Aut}(H)$ such that $\sigma\phi(K)\sigma^{-1} = \theta(K)$. Then $H \rtimes_\phi K \cong H \rtimes_\theta K$.

Hint: here are a few facts you likely want to prove:

- There is either a unique Sylow 5-subgroup or a unique Sylow 7-subgroup of G.
- G has a cyclic subgroup of order 35.

Proof. Let $n_5 = |\operatorname{Syl}_5(G)|$ and $n_7 = |\operatorname{Syl}_7(G)|$. By Sylow Theory,

$$n_5 \equiv 1 \pmod 5 \text{ and } n_5 \text{ divides } 21 \implies n_5 \in \{1, 21\}.$$
$$n_7 \equiv 1 \pmod 7 \text{ and } n_7 \text{ divides } 15 \implies n_5 \in \{1, 15\}.$$

Suppose $n_5 = 21$ and $n_7 = 15$. For a prime p, any two distinct subgroups of order p intersect trivially, as the order of the intersection divides p by Lagrange's Theorem but must be smaller than p. Thus any two Sylow 5-subgroups and any two Sylow 7-subgroups intersect trivially. Moreover, we showed in a previous problem set that the intersection of two subgroups whose orders are coprime is trivial, so any pair consisting of one Sylow 5-subgroup and one Sylow 7-subgroup intersect trivially. Thus we could count all the distinct elements among the Sylow 5-subgroups and the Sylow 7-subgroups, and get

$$n_5(5-1) + n_7(7-1) = 21 \cdot 4 + 15 \cdot 6 = 84 + 90 > 105.$$

This is absurd, so $n_5 = 1$ or $n_7 = 1$. This shows there is either a unique Sylow 5-subgroup or a unique Sylow 7-subgroup of G. Note that that unique subgroup must be normal.

Let $P \in \operatorname{Syl}_5(G)$ and $Q \in \operatorname{Syl}_7(G)$. Since at least one of P or Q is normal, then $PQ \leq G$. We know that $P \cap Q = \{e\}$, so the order of PQ is

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = 35.$$

By the Classification Theorem for groups of order pq with $p < q$ primes, where $p = 3 \nmid q - 1 = 4$, we know that there is a unique group of order 35 up to isomorphism, namely C_{35}. Thus $PQ \cong C_{35}$.

Let $K \in \operatorname{Syl}_3(G)$ and $H = PQ$ as above. Since $[G : H] = 3$ and 3 is the smallest prime dividing $|G|$, we must have $H \trianglelefteq G$. Since $|H$ and $|K$ are coprime, we must have $H \cap K = \{e\}$, and thus

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K} = 105 \implies HK = G.$$

By the Recognition Theorem for Semidirect Products, we conclude that

$$G \cong H \rtimes_\rho K$$

for some $\rho \colon K \to \operatorname{Aut}(H)$. Since $|K| = 3$ we deduce that $K \cong C_3$ and we showed above that $H \cong C_{35}$. Thus $G \cong C_{35} \rtimes_\rho C_3$ for some $\rho : C_3 \to \operatorname{Aut}(C_{35})$. By the UMP of cyclic groups such a ρ is uniquely determined by sending the generator of C_3 to some $z \in \operatorname{Aut}(C_{35})$ with $z^3 = \mathrm{id}$.

If ρ is trivial, the semidirect product is the direct product, and by the CRT we can rewrite it as

$$G \cong C_{35} \times C_3 \cong C_{105}.$$

We claim that there exist nontrivial homomorphisms $\rho \colon C_3 \to \operatorname{Aut}(C_{35})$. Such a nontrivial ρ exists exactly if there exists an element $z \in \operatorname{Aut}(C_{35})$ of order 3. We know that

$$|\operatorname{Aut}(C_{35})| = \varphi(35) = (7-1)(5-1) = 24 = 3 \cdot 2^3.$$

By Cauchy's Theorem, $\operatorname{Aut}(C_{35})$ must have an element z of order 3, and thus there is indeed a nontrivial homomorphism $\rho \colon C_3 \to \operatorname{Aut}(C_{35})$. In that case, $\operatorname{im}(\rho) = \langle z \rangle$ has order 3. But $|\operatorname{Aut}(C_{35})| = 3 \cdot 2^3$, so the set of subgroups of $\operatorname{Aut}(C_{35})$ of order 3 is $\operatorname{Syl}_3(\operatorname{Aut}(C_{35}))$. By the Main Theorem of Sylow Theory, all the subgroups in $\operatorname{Syl}_3(\operatorname{Aut}(C_{35}))$ are conjugate. Thus by the lemma all the semidirect products $C_{35} \rtimes_\rho C_3$ corresponding to morphisms ρ whose image is in $\operatorname{Syl}_3(\operatorname{Aut}(C_{35}))$ are isomorphic. Thus in this case we obtain a unique isomorphism class. Moreover, this group is nonabelian and hence not isomorphic to C_{105}.

Finally, we showed that there are exactly two distinct isomorphism classes of groups of order 105: C_{105} and the nonabelian group

$$G \cong C_{35} \rtimes_\rho C_3$$

given by any nontrivial homomorphism $\rho \colon C_3 \to \operatorname{Aut}(C_{35})$. $\square$