Problem Set 10

Due Thursday, November 13

Instructions: You are encouraged to work together on these problems, but each student should hand in their own final draft, written in a way that indicates their individual understanding of the solutions. Never submit something for grading that you do not completely understand. You cannot use any resources besides me, your classmates, and our course notes.

I will post the .tex code for these problems for you to use if you wish to type your homework. If you prefer not to type, please *write neatly*. As a matter of good proof writing style, please use complete sentences and correct grammar. You may use any result stated or proven in class or in a homework problem, provided you reference it appropriately by either stating the result or stating its name (e.g. the definition of ring or Lagrange's Theorem). Please do not refer to theorems by their number in the course notes, as that can change.

Problem 1. Let p be a prime. Classify[1] all groups of order p^2 up to isomorphism.

Proof. Let p be a prime and G be a group of order p^2. We claim that G is abelian. Indeed, by a Theorem from class, $Z(G) \neq \{e\}$, so either $G = Z(G)$ in which case G is abelian, or else $|Z(G)| = p$. To obtain a contradiction, suppose that $|Z(G)| = p$. Then $|G/Z(G)| = p$, and hence is cyclic, by a problem from the midterm. But an earlier homework problem showed that if $G/Z(G)$ is cyclic, then G is abelian, contradicting that $Z(G) \subsetneq G$. Thus, G is abelian.

Then by the structure theorem for abelian groups (either form) either $G \cong \mathbb{Z}/p^2$ or $G \cong \mathbb{Z}/p \times \mathbb{Z}/p$. □

Problem 2. Consider a group G of order $75 = 5^2 \cdot 3$.

(a) Show that if G contains an element of order 25 then G is cyclic.

Proof. Let $n_5 = |\mathrm{Syl}_5(G)|$. 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 $n_5 = 3 \not\equiv 1 \pmod 5$. 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 $Q \cong \mathbb{Z}/25$.

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

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

[1] Hint: Consider the center.

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

$$G \cong \mathbb{Z}/3 \times \mathbb{Z}/25 \cong \mathbb{Z}/75,$$

and thus G is cyclic. □

(b) Show that there exists some group G_1 of order 75 that is abelian but not cyclic, and there exists some group G_2 of order 75 that is not abelian.

Proof. By the structure theorem of abelian groups, elementary divisor form, the abelian group $G_1 = \mathbb{Z}/5 \times \mathbb{Z}/15$ is not isomorphic to any other abelian group in elementary divisor form, and in particular not cyclic.

To obtain a nonabelian group of order 75, note that $\mathrm{Aut}(\mathbb{Z}/5 \times \mathbb{Z}/5) \cong \mathrm{GL}_2(\mathbb{Z}/5)$ is a group of order $(25-1)(25-5) = 2^5 \cdot 3 \cdot 5$, and hence has an element[2] x of order 3 by Cauchy's Theorem. Thus, by the UMP for cyclic groups there exists a nontrivial group homomorphism ρ from $\mathbb{Z}/3$ to $\mathrm{Aut}(\mathbb{Z}/5 \times \mathbb{Z}/5)$ mapping $[1] \in \mathbb{Z}/3$ to x. Then the group $(\mathbb{Z}/5 \times \mathbb{Z}/5) \rtimes_\rho \mathbb{Z}/3$ has order 75 and is not abelian, since any nontrival semidirect product is not abelian. □

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 $n_p = |\mathrm{Syl}_p(G)|$ 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

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

so $n_7 = 1$. Similarly,

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

but

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

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

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

[2] E.g., $\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/5)$ has order three.

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[3] that there are precisely two groups of order $105 = 3 \cdot 5 \cdot 7$ up to isomorphism.

Proof. Let $n_5 = |\mathrm{Syl}_5(G)|$ and $n_7 = |\mathrm{Syl}_7(G)|$. 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 $P \in \mathrm{Syl}_5(G)$ and $Q \in \mathrm{Syl}_7(G)$. 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 $K \in \mathrm{Syl}_3(G)$ 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

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

[3] Hint: You may want to show that (1) there is either a unique Sylow 5-subgroup or a unique Sylow 7-subgroup of G, and (2) G has a cyclic subgroup of order 35.
You can also without proof the Exercise from class giving a sufficient condition for two semidirect products to be isomorphic.

for some $\rho\colon K \to \mathrm{Aut}(H)$. 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 $\rho : C_3 \to \mathrm{Aut}(C_{35})$. By the UMP of cyclic groups such a ρ is uniquely determined by sending the generator of C_3 to some $z \in \mathrm{Aut}(C_{35})$ 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 $\rho\colon C_3 \to \mathrm{Aut}(C_{35})$. Such a nontrivial ρ exists exactly if there exists an element $z \in \mathrm{Aut}(C_{35})$ of order 3. We know that

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

By Cauchy's Theorem, $\mathrm{Aut}(C_{35})$ must have an element z of order 3, and thus there is indeed a nontrivial homomorphism $\rho : C_3 \to \mathrm{Aut}(C_{35})$. In that case, $\mathrm{im}(\rho) = \langle z \rangle$ has order 3. But $|\mathrm{Aut}(C_{35})| = 3 \cdot 2^3$, so the set of subgroups of $\mathrm{Aut}(C_{35})$ of order 3 is $\mathrm{Syl}_3(\mathrm{Aut}(C_{35}))$. By the Main Theorem of Sylow Theory, all the subgroups in $\mathrm{Syl}_3(\mathrm{Aut}(C_{35}))$ are conjugate. Thus by the lemma all the semidirect products $C_{35} \rtimes_\rho C_3$ corresponding to morphisms ρ whose image is in $\mathrm{Syl}_3(\mathrm{Aut}(C_{35}))$ 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 $\rho\colon C_3 \to \mathrm{Aut}(C_{35})$. □