Problem Set 9

Due Thursday, November 6

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. Prove that there is no simple group of order 48.

Proof. Let G be a group of order 48. By Sylow's Theorem, the number of Sylow 2-subgroups divides 3, so is either equal to 1 or 3. If there is only one Sylow 2-subgroup, it is normal, so G is not simple. Suppose that G has 3 Sylow 2-subgroups. Then G acts on the set X of Sylow 2-subgroups by conjugation, and this action is transitive by Sylow's Theorem; in particular, the action is nontrivial. This induces a permutation representation $\rho : G \to S_3$. Since $|G| = 48 > 6 = |S_3|$, this map cannot be injective, so the kernel of ρ is a nontrivial normal subgroup of G; it is proper since ρ is nontrivial. Thus, in either case G is not simple. □

Problem 2. Let C_n denote the cyclic group of order $n \geqslant 2$, and consider the group

$$(\mathbb{Z}/n)^\times = \{[j]_n \mid \gcd(j, n) = 1\}$$

with the binary operation given by the usual multiplication. Prove that

$$\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n)^\times.$$

Proof. Let $C_n = \langle x \mid x^n = e \rangle$. By the Universal Mapping Property for cyclic groups, each group homomorphism $C_n \to C_n$ is uniquely determined by the image of x. The possible images for x are the n elements in C_n, which are $x^i \in C_n$ for $0 \leqslant i < n$. Let $\rho_i : C_n \to C_n$ be the unique homomorphism determined by $\rho_i(x) = x^i$. We have for now shown that

$$\mathrm{Aut}(C_n) = \{\rho_i \mid 0 \leqslant i < n\}.$$

Note that $\mathrm{im}(\rho_i) = \langle x^i \rangle$, and we proved in class that $\langle x^i \rangle = C_n$ if and only if $\gcd(i, n) = 1$. Note moreover that if ρ_i is surjective, then it must also be injective, given that it is a function between two finite sets of the same order. Thus

$$\rho_i \in \mathrm{Aut}\,(C_n) \quad \text{if and only if} \quad [i]_n \in (\mathbb{Z}/n)^\times.$$

Now consider $\varphi \colon \mathrm{Aut}\,(C_n) \to (\mathbb{Z}/n)^\times$ given by

$$\varphi(\rho_i) = [i]_n.$$

Note that

$$(\rho_i \circ \rho_j)(x) = x^{ij} = \rho_{ij \pmod m}(x).$$

The uniqueness part of the UMP for cyclic groups implies that

$$\rho_i \circ \rho_j = \rho_{ij \pmod m}.$$

Hence,

$$\varphi(\rho_i \circ \rho_j) = \varphi\left(\rho_{ij \pmod m}\right) = [ij]_n = [i]_n[j]_n = \varphi(\rho_i)\varphi(\rho_j).$$

Thus φ is a group homomorphism.

Given $[j]_n \in (\mathbb{Z}/n)^\times$, by the UMP for cyclic groups there exists a unique homomorphism

$$\psi([j]_n) \colon C_n \to C_n$$

that takes $x \mapsto x^j$. This gives us a map $\psi : (\mathbb{Z}/n)^\times \to \mathrm{Aut}(C_n)$. We need to show that ψ is well-defined both in terms of independence of representative in $(\mathbb{Z}/n)^\times$ but also in terms of the the image landing in the automorphism group of C_n.[1] Indeed,

$$i \equiv i' \pmod n \implies x^i = x^{i'} \in C_n \implies \psi([i]_n) = \psi([i']_n).$$

Thus the definition of ψ does not depend on the choice of representative i for the class $[i]_n$. Moreover, the image of $\psi([i]_n)$ is the subgroup $\langle x^i \rangle$ of C_n, and since $\gcd(i, n) = 1$, we know that $\langle x^i \rangle = C_n$. This shows that $\psi([i]_n)$ is surjective, and hence bijective because its domain and codomain have the same number of elements. This shows that ψ is a well-defined function whose codomain is indeed $\mathrm{Aut}(C_n)$.

Finally,

$$\psi(\varphi(\rho_i)) = \psi([i]_n) = \psi_i \quad \varphi(\psi([i]_n) = \varphi(\rho_i) = [i]_n.$$

Therefore, φ is a group isomorphism, as desired. □

Problem 3. Prove that[2] the quaternion group Q_8 is not isomorphic to a semidirect product of nontrivial groups H, K.

Proof. It follows from results proven in class that Q_8 is isomorphic to $H \rtimes_\rho K$ if and only if there exist H' and K' such that $H' \trianglelefteq Q_8$, $K' \leq Q_8$, $H'K' = Q_8$, $H' \cap K' = \{e\}$, $H' \cong H$ and $K' \cong K$. However, any nontrivial subgroup contains the element -1, since the square of any element besides ± 1 is -1. Thus, no such subgroups H', K' exist. □

Problem 4.

(a) 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 $\rho : \mathbb{Z}/9 \to \mathrm{Aut}(\mathbb{Z}/7)$ 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 $f(i) = ai$.

[1] Note that in principle $\psi([j]_n)$ could simply be a homomorphism $C_n \to C_n$, rather than an isomorphism.

[2] Hint: You can use without proof that every subgroup of Q_8 is normal.

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 $f \neq \mathrm{id}$ then ρ is a nontrivial homomorphism, and we conclude that

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

is a nonabelian group. □

(b) Give 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 element can[3] be written as $u^a v^b$ for some integers a and b by replacing $v^2 u$ by uv. so that 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 $\mathbb{Z}/7 \rtimes_\rho \mathbb{Z}/9$. □

[3]Indeed, any element can be written in the form $g = u^{i_1} v^{j_1} \cdots u^{i_m} v^{j_m}$ for some integers i_t, j_t by definition of free group, and using the relations $u^7 = e$ and $v^9 = e$ in G we can take $i_t, j_t \geq 0$. We show the claim holds for any g with an expression of this form by induction on $n = \sum i_t + \sum j_t$. We can take $n = 0$ as the base case, in which $g = e$ and the claim is clear. Then for an arbitrary element g as above with $n \geq 1$, we can either write $g = g'u$, $g = g'v$ and rewrite $g' = u^i v^j$ by induction hypothesis. Then $g'v = u^i v^{j+1}$ and $g'u = u^i v^j u = u^{i+1} v^{2j}$ (using the relation $vu = u^2 v$ repeatedly) completing the induction and justifying the claim.