Takehome 4

Due Friday, May 15th

First of all, thank you everybody for your patience and perseverance this spring. It's been a difficult couple of months to say the least, and I must say I am impressed and grateful for all of you.

To finish off the course, we're going to do some classifications of groups of order p^2q for p, q prime. **Important note:** when classifying groups you must show your work and **justify your steps**. A lot of folks on HW 11 Problem 4 (classifying groups of order 20), just listed the groups with no justification. As in HW11, this will not recieve credit.

You are welcome to use all course notes, but make sure everything is cited! This includes the "table of stuff," we generated while studying Sylow's theorems, which I think you will find especially useful. This table is available in its entirety on the course website, as the second page of the April 29 lecture notes. **All work must be your own and outside resources are not allowed**. So break out this "table of stuff" and let's get started. You will need the following three facts, which you may use freely without proving yourself.

Fact (Automorphisms of abelian groups of order p and p^2)**.** *Let p a prime number. Then:*

- $\text{Aut } Z_p \cong Z_{p-1}$
- $\text{Aut } Z_{p^2} \cong Z_{p(p-1)}$.
- $\text{Aut } (Z_p \times Z_p) \cong GL_2(\mathbb{F}_p)$.

Good luck!

1. A lot of studying semidirect products comes down to enumerating and classifying homomorphisms. So let's begin by doing that. For the rest of this exercise we fix a group G.

   (a) Show that giving a homomorphism $Z_n \to G$ is the same as selecting an element $g \in G$ with $|g|$ dividing n. That is, give a bijection between the following sets:

   $$\left\{ \begin{array}{c} \text{Homomorphisms} \\ Z_n \to G \end{array} \right\} \iff \left\{ \begin{array}{c} \text{Elements } g \in G \\ \text{where } |g| \text{ divide } n \end{array} \right\}$$

   Proof. Fix once and for all a generator x of Z_n. Then given a map $\varphi : Z_n \to G$, we know that $g = \varphi(x) \in G$ has order dividing $|x| = n$ (HW3 Probelem 1(c)). Conversely, given $g \in G$ of order dividing n, the map $\psi : x^i \mapsto g^i$ is a homomorphism from $Z_n \to G$. One readily checks that these are inverse constructions. □

   (b) If p is prime show that giving a *nontrivial* map $Z_p \to G$ is the same as choosing an element of order p in G. (Note: the trivial map is the one that sends every element to the identity of G).

   Proof. In part (a) we saw tat a map $Z_p \to G$ is the same as an element of G whose order divides p. The trivial map corresponds to 1_G, so all other maps correspond to elements of order p. □

   (c) Show that giving a homomorphism $Z_{n_1} \times \cdots \times Z_{n_r} \to G$ is the same as chosing elements $g_1, \cdots, g_r \in G$ such that all the g_i commute with eachother and each $|g_i|$ divides n_i.

Proof. This is essentially identical to part (a). Fix generators x_i of Z_{n_1}. Given a homomorphism φ we let $g_i = \varphi(x_i)$ and remark that its order must divide $|x_i| = n_i$ (again HW3 1(c)). Furthermore, we notice that:

$$g_i g_j = \varphi(x_i)\varphi(x_j) = \varphi(x_i x_j) = \varphi(x_j x_i) = \varphi(x_j)\varphi(x_i) = g_j g_i,$$

so that they commute. Conversely, given such g_i, we define ψ on the generators of $Z_{n_1} \times \cdots \times Z_{n_r}$ via the rule

$$\psi(x_1^{j_1}, \cdots, x_r^{j_r}) = g_1^{j_1} \cdots g_r^{j_r},$$

noting that ψ is a homomorphism precisely because the g_i commute and have order dividing x_i. □

(d) Suppose G is abelian and p is prime. Describe the set of homomorphisms $Z_p \times Z_p \to G$ as a subset of $G \times G$.

Proof. By part (c) this should correspond to pairs $(a, b) \in G \times G$ such that $a^p = b^p = 1$. In particular, we remark that this is the p-torsion of $G \times G$, i.e., in the notation of Takehome 3 it is $G_p \times G_p$. □

2. With this in hand let's do some general work. Let $|G| = p^2 q$ for $p \neq q$ prime numbers. Let P be a Sylow p-subgroup and Q a Sylow q-subgroup.

(a) First suppose that $q > p$.

i. Show if $|G| \neq 12$ then $G \cong Q \rtimes P$

Proof. We know that if $q > p$ then either $Q \trianglelefteq G$ or $G \cong A_4$. Since $|G| \neq 12$ it can't be A_4 so that Q is normal. By Lagrange's theorem $Q \cap P = 1$, and so $|PQ| = |P||Q| = |G|$ implying that $PQ = G$. The result follows by the recognition theorem for semidirect products. □

ii. Show that if $p \not| q - 1$ then G is abelian. List all possible values of G.

Proof. By part (i), the semidirect product must be induced by a map $P \to \operatorname{Aut} Q$. We also know that P is either Z_{p^2} or $Z_p \times Z_p$, and that $Q \cong Z_q$ so that $\operatorname{Aut}(Q) \cong Z_{q-1}$. Let's first considerthe case wehre $P \cong Z_{p^2}$ so that we are studying maps

$$Z_{p^2} \to Z_{q-1}.$$

By 1(a) this corresponds to an element $g \in Z_{q-1}$ whose order divides p^2. $|g|$ is one of $1, p, p^2$. By Lagrange's theorem we also know $|g|$ divides $q - 1$. Since we assumes $p \not| q - 1$, then also $p^2 \not| q - 1$, so that $|g| = 1$ and $g = 1$. Therefore the only map $Z_{p^2} to Z_{q-1}$ is the trivial one, and so the semidirect product is the direct product, implying that

$$G \cong Z_q \times Z_{p^2} \cong Z_{p^2 q}.$$

On the ohter hand, we could have $P \cong Z_p \times Z_p$. So we are studying maps

$$Z_p \times Z_p \to Z_{q-1}.$$

By 1(d) we see that this corresponds to (ordered) pairs of elements a, b whose orders are either p or 1, and also divide $q-1$. Again by assumption, this implies $a = b = 1$ and so the only maps are trivial. Therefore the semidirect product is direct so that

$$G \cong Z_q \times Z_p \times Z_p \cong Z_{pq} \times Z_p.$$

□

We remark that you could also solve this problem using Sylow's theorems. We outline how.

Proof. We know $n_p \equiv 1 \mod p$ and $n_p | q$ by Sylow's theorems. If $n_p = 1 + kp | q$ implying that either $p | kp | q - 1$ or $k = 0$. By assumption it must be the latter so $n_p = 1$ and $P \trianglelefteq G$. Therefore $G \cong Q \rtimes P \cong Q \times P$. Since P, Q are both abelian, their product is. The list then can be computed using the fundemental theorem. □

iii. $p | q - 1$. Show that G can be nonabelian. (You may have to deal with the case wehre $|G| = 12$ separately).

Proof. If $G = A_4$ then certainly G can be nonabelian. Otherwise $G \cong Q \rtimes P$ for some map $P \to \operatorname{Aut} Q$ (as in part i). In order for G to be nonabelian, we must find a nontrivial one of these. We remark that there are several ways to do this. We will let $P = Z_{p^2}$. Since $p | q - 1$, then by Cauchy's theorem there is an element $g \in Z_{q-1}$ of order p. We let $\phi : Z_{p^2} \to Z_{q-1}$ be the map sending a generator to this g. Then $G = Z_q \rtimes_\varphi Z_{p^2}$ is not abelian and of order $p^2 q$. □

(b) Now suppose $p > q$

i. Show that $G \cong P \rtimes Q$.

Proof. We already showed that $G = PQ$ and that $P \cap Q = 1$. It suffices to show that $P \trianglelefteq G$ but we showed this in class. □

ii. Suppose $q | p - 1$ Show that G can be nonabelian.

Proof. As in (a)(iii), it suffices to construct a nontrivial map $Q \to \operatorname{Aut} P$. We remark that there may be several ways to do this. We assume $P \cong Z_{p^2}$ so that $\operatorname{Aut} P \cong Z_{p(p-1)}$. Since $q | p - 1$ then by Cauchy's theorem there is an element g of order q in $Z_{p(p-1)}$, so we define $\varphi : Z_q \to Z_{p(p-1)}$ by sending a generator to g. Then $G = Z_{p^2} \rtimes_\varphi Z_q$ is a nonabelian group of order $p^2 q$. □

iii. Suppse $q \not| p - 1$. Show that there is a nonabelian group of order $p^2 q$ if and only if $q | p + 1$.

Proof. We remark that since $q \not| p - 1$ (and certainly $q \not| p$), then $q \not| p(p-1)$ so that (by 1(b)) there is no nontrivial map $Z_q \to Z_{p(p-1)}$, and so $Z_{p^2} \rtimes Z_q$ will always be abelian. Therefore the only possibility for a nonabelian group is where $P \cong Z_p \times Z_p$. We have now noticed there is a nonabelian group of our desired order if and only if there is a nontrivial map:

$$Z_q \longrightarrow \operatorname{Aut}(Z_p \times Z_p) \cong GL_2(\mathbb{F}_p).$$

Such a map corresponds (by 1(b)) to a nontrivial element of order q in $GL_2(\mathbb{F}_p)$, which exists if (Cauchy) and only if (Langrange) q divides $|GL_2(\mathbb{F}_p)|$. In HW7 Problem 4(d) we computed this value to be

$$|GL_2(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p = p(p-1)^2(p+1).$$

Since $q \not| p$ and $q \not| p-1$ by assumption, such an element exists if and only if $q|p+1$, completing the proof. □

Now we have a general framework. Let's do a couple of concrete examples.

3. You may find HW11 Problem 4 useful for this problem (note: you are welcome to refer to the HW11 Solutions on the course website).

   (a) Last week we studied the case where $|G| = 20$. Which of the cases (from Problem 2) does this fall into? (You can answer this like (a)(ii) or (b)(iii)). Fully justify your answer.

   Proof. Since $20 = 2^2 * 5 = p^2q$ with $p = 2$ and $q = 5$. Then $p < q$ and $2|4$ so that $p|q-1$. This is the case studied in problem (a)(iii), which jives with the homework problem since there are indeed nonabelian groups of order 20. □

   (b) The case where $|G| = 28$ should be similar. Classify all such groups being sure to fully justify your answer. There are fewer than the case for $|G| = 20$. Explain exactly why this happens (where is/are the missing group(s)?).

   Proof. $|G| = 2^2 * 7 = p^2q$ with $p = 2$ and $q = 7$, so that $p < q$ and $p|q-1$ as above. Since $|G| \neq 12$, by 2(a)(i) $G \cong Q \rtimes P$ where P is a Sylow 2-subgroup and Q is a Sylow 7-subgroup. In particular, $Q \cong Z_7$ and P is either Z_4 or $Z_2 \times Z_2$.

   ## Case 1: $P \cong Z_4$

   Since $\mathrm{Aut}(Q) = Z_6$ we are classifying maps $Z_4 \to Z_6$. By 1(a), this amounts to choosing an element of Z_6 whose order divides 4. The only choices are 1 or x^3 where x is the generator of Z_6. The map associated to 1 gives $Z_7 \times Z_4 = Z_{28}$.
   In the other case we get a (unique) nontrivial semidirect product $Z_7 \rtimes Z_4$. We remark now that for the order 20 case we were choosing maps to $\mathrm{Aut}(Z_5)$, which had 3 elements whose order divided 4, wheras $\mathrm{Aut}(Z_7)$ only has 1. This is why there are more nonabelian groups of order 20.

   ## Case 2: $P \cong Z_2 \times Z_2$

   This should look essentially identical to the order 20 case. We are now classifying maps $\psi : Z_2 \times Z_2 \to Z_6$ letting $Z_4 = \langle x \rangle$, and

   $$Z_2 \times Z_2 = \langle a \rangle \times \langle b \rangle = \langle a, b \rangle,$$

where a, b have order 2. Then ψ is determined by where it sends a and b. Since $|\psi(g)|$ must divide $|g|$ (HW3 Problem 1(c)), we see that both $\psi(a), \psi(b) \in \{1, x^3\}$. As before, there are four options, which we will denote by $\psi_{j,k}$ for $j, k \in \{0, 1\}$.

$$\psi_{0,0}: \begin{array}{l} a \mapsto 1 \\ b \mapsto 1 \end{array} \qquad \psi_{1,0}: \begin{array}{l} a \mapsto x^3 \\ b \mapsto 1 \end{array}$$

$$\psi_{0,1}: \begin{array}{l} a \mapsto 1 \\ b \mapsto x^3 \end{array} \qquad \psi_{1,1}: \begin{array}{l} a \mapsto x^3 \\ b \mapsto x^3 \end{array}$$

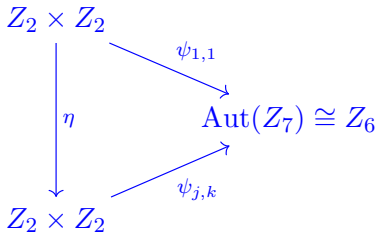
We let $G_{j,k} = Z_7 \rtimes_{\psi_{j,k}} (Z_2 \times Z_2)$. Since $G_{0,0}$ corresponds to the trivial map, we immediately see that it is isomorphic to $Z_7 \times (Z_2 \times Z_2) \cong Z_{14} \times Z_2$. Otherwise:

Case 2a: j, k not both 0

We claim that in this case all the $G_{j,k}$ are isomorphic. We remark that

$$Z_2 \times Z_2 \cong \langle a \rangle \times \langle b \rangle \cong \langle a \rangle \times \langle ab \rangle \cong \langle ab \rangle \times \langle b \rangle,$$

and each nontrivial $\psi_{j,k}$ takes 2 generators to x^3 and the third to 1. But $\mathrm{Aut}(Z_2 \times Z_2) = GL_2(\mathbb{F}_2)$ includes all the *change of basis* matrices which takes a pair of generators to any other pair of generators. In particular, if we fix any nontrivial $\psi_{j,k}$ and view $Z_2 = \langle g \rangle \times \langle h \rangle$ as generated by g and h for the two generators sent to x^3 (i.e., where $\psi_{j,k}(g) = \psi_{j,k}(h) = x^3$ and $\psi_{j,k}(gh) = 1$) then there exists some $\eta \in \mathrm{Aut}(Z_2 \times Z_2)$ where $\eta(a) = g$ and $\eta(b) = h$. That is, we have the following:



By HW11 Problem 2(b) this shows $G_{1,1} \cong G_{i,j}$, so that all three nontrivial $G_{i,j}$'s must be isomorphic.

So there are 4 groups of order 28. Since the nontrivial semidirect products are unique we may list them as follows:

$$Z_{28}, \qquad Z_{14} \times Z_2, \qquad Z_7 \rtimes Z_4, \qquad Z_7 \rtimes (Z_2 \times Z_2).$$

□

(c) Give presentations (i.e., generators and relations) for each group of order 28. As usual, fully justify your answer (just listing the presentations without explanation will not recieve credit).

Proof. The abelian cases are straightforward.

$$Z_{28} \cong \langle x \mid x^{28} = 1 \rangle$$

$$Z_{14} \times Z_2 \cong \langle x, y \quad | \quad x^{14} = y^2 = 1, \quad xy = yx \rangle .$$

Next let's consider $Z_7 \rtimes Z_4$. This is generated by the map $\varphi : Z_4 \to \mathrm{Aut}(Z_7)$ which takes a generator y of Z_4 to an automorphism of Z_7 of order 2. This can only be in inversion automorphism $\iota : g \mapsto g^{-1}$. Therefore. If we let x be the generator of Z_7, we get:

$$Z_7 \rtimes Z_4 \cong \langle x, y \quad | \quad x^7 = y^4 = 1, \quad yxy^{-1} = x^{-1} \rangle .$$

Similarly, $Z_7 \rtimes (Z_2 \times Z_2)$ can be identified with $G_{1,1}$ from the previous section. This was associated to the map $Z_2 \times Z_2 \to \mathrm{Aut}(Z_7)$ which sent both a and b to ι. Therefore we get:

$$Z_7 \rtimes (Z_2 \times Z_2) \cong \langle x, a, b \quad | \quad x^7 = a^2 = b^2 = 1, \quad ab = ba, \quad otaxa^{-1} = bxb^{-1} = x^{=1} \rangle .$$

□

4. Now let's classify all groups of order 75.

   (a) Which of the cases (from Problem 2) does this fall under?

   Proof. $75 = 5^2 * 3 = p^2 * q$ where $p = 5$ and $q = 3$. This falls into the case where $p > q$. We also have that $q \not| p-1$ ($3 \not| 4$) but $q | p+1$ so that there can still be nonabelian groups. We point out that if $|G| = 75$ then we showed (2(b)(i)) that $G \cong P \rtimes Q$ where P is a Sylow 5-subgroup and Q is a Sylow 3-subgroup. □

   (b) List all the abelian groups of order 75.

   Proof. These are Z_{75} and $Z_{15} \times Z_5$ □

   (c) Show that if a group of order 75 has a cyclic Sylow 5-subgroup then it is abelian.

   Proof. We argued this in 2(b)(iii), but we will repeat it here with numbers filled in. We know $Q \cong Z_3$ If $P \cong Z_{25}$, then since $G \cong P \rtimes Q$ we know it comes from a map from $Z_3 \to \mathrm{Aut}\, Z_{25} \cong Z_{20}$. Since $3 \not| 20$ there is no nontrivial map, so the semidirect product must be direct. □

   (d) Show that there is a unique nonabelian group of order 75. (Hint: show that 3 is the maximal 3-divisor of $|GL_2(\mathbb{F}_5)|$. Then use Sylow's theorems and HW11 Problem 2(c)).

   Proof. Notice (again with 2(b)(iii), or with 4(c) above) that to be nonabelian we must have $P \cong Z_5 \times Z_5$. Therefore we must study nontivial maps

   $$\psi : Z_3 \longrightarrow \mathrm{Aut}(Z_5 \times Z_5) \cong GL_2(\mathbb{F}_5).$$

   In HW 7 Problem 4(d) we computed:

   $$|GL_2(\mathbb{F}_5)| = 5^4 - 5^3 - 5^2 + 5 = 480 = 3 * 160.$$

   Since $3|480$ then by Cauchy's theorem there exists an element $M \in GL_2(\mathbb{F}_3)$ of order 3. If y is a generator of Z_3, then we let $\varphi(y) = M$ and get a nonabelian group

   $$G_\varphi = (Z_5 \times Z_5) \rtimes_\varphi Z_3$$

of order 75. In fact, any such group comes from choosing some N of order 3 in $|GL_2(\mathbb{F}_5)|$ and letting $\psi : y \mapsto N$ and building G_ψ as above. We finish the proof by showing $G_\psi \cong G_\varphi$.

Since $3 \nmid 160$, we know $\langle M \rangle$ and $\langle N \rangle$ are both Sylow 3-subgroups of $GL_2(\mathbb{F}_5)$. Therefore they are conjugate. That is, there is some $\alpha \in GL_2(\mathbb{F}_5)$ such that

$$\alpha \langle M \rangle \alpha^{-1} = \langle N \rangle.$$

Denote by $\sigma_\alpha \in \mathrm{Inn}(GL_2(\mathbb{F}_5))$ the associated inner automorphism. In particular, we see that $\sigma(M)$ is either N or N^2. Define $\gamma : Z_3 \to Z_3$ by the following rule. If $\sigma(M) = N$ then γ is the identity, and if $\sigma(M) = N^2$ then $\gamma : y \mapsto y^2$. In either case, $\gamma \in \mathrm{Aut}(Z_3)$. In particular, we have the following commutative diagram:

$$\begin{array}{ccc} Z_3 & \xrightarrow{\varphi} & GL_2(\mathbb{F}_5) \\ {\scriptstyle\gamma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ Z_3 & \xrightarrow[\psi]{} & GL_2(\mathbb{F}_5). \end{array}$$

Applying HW11 Problem 2(c) immediately implies:

$$G_\varphi = (Z_2 \times Z_2) \rtimes_\varphi Z_3 \cong (Z_2 \times Z_2) \rtimes_\psi Z_3 = G_\psi,$$

and so we are done. □