Math 504 HW4

Rohan Mukherjee

December 4, 2023

1. (a) Let $\varphi : \mathbb{Z}/2 \to \text{Aut}(\mathbb{Z}/m)$ by $\varphi(0)(x) = x$ and $\varphi(1)(x) = -x$. Then φ is a homomorphism and $\mathbb{Z}/m \rtimes \mathbb{Z}/2 = \langle (1,0), (0,1) \rangle$, since this group contains $\langle (1,0) \rangle = \mathbb{Z}/m$ and $\langle (0,1) \rangle = \mathbb{Z}/2$, so it contains their product. Now, notice that $(0,1)(1,0)(0,1) = (-1,1)(0,1) = (-1,0) = -(1,0)$. Similarly, $2 \cdot (0,1) = (0,0)$, and lastly, $m(1,0) = (m,0) = (0,0)$. So, $\langle (1,0), (0,1) \mid m(1,0) = 2(0,1) = (0,0), (0,1)(1,0)(0,1) = -(1,0) \rangle = D_m$.

   (b) We see that D_m acts faithfully on the set of vertices of a regular m-gon by definition, since D_m is the group of symmetrices of the m-gon. If two elements of D_m induced the same permutation of the vertices, then they would be the same symmetry. So, letting π_{D_m} be the permutation representation of D_m on the vertices of the m-gon, π_{D_m} is an injective homomorphism from D_m to S_m, so D_m is isomorphic to a subgroup of S_m.

   (c) We recall from the above that $D_m = \left\langle r, s \mid r^m = s^2 = e, srs = r^{-1} \right\rangle$. We claim that D_m is an isomorphic copy of $\left\langle \begin{pmatrix} \cos\left(\frac{2\pi}{m}\right) & -\sin\left(\frac{2\pi}{m}\right) \\ \sin\left(\frac{2\pi}{m}\right) & \cos\left(\frac{2\pi}{m}\right) \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$. We need only verify the relations. Clearly $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^2 = I$. Geometrically, since $\begin{pmatrix} \cos\left(\frac{2\pi}{m}\right) & -\sin\left(\frac{2\pi}{m}\right) \\ \sin\left(\frac{2\pi}{m}\right) & \cos\left(\frac{2\pi}{m}\right) \end{pmatrix}$ is a rotation matrix, and rotates by $\frac{2\pi}{m}$ radians, its order is just m. Finally, an explicit calculations shows that

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \cos\left(\frac{2\pi}{m}\right) & -\sin\left(\frac{2\pi}{m}\right) \\ \sin\left(\frac{2\pi}{m}\right) & \cos\left(\frac{2\pi}{m}\right) \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos\left(\frac{2\pi}{m}\right) & -\sin\left(\frac{2\pi}{m}\right) \\ -\sin\left(\frac{2\pi}{m}\right) & -\cos\left(\frac{2\pi}{m}\right) \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$= \begin{pmatrix} \cos\left(\frac{2\pi}{m}\right) & \sin\left(\frac{2\pi}{m}\right) \\ -\sin\left(\frac{2\pi}{m}\right) & \cos\left(\frac{2\pi}{m}\right) \end{pmatrix} = \begin{pmatrix} \cos\left(-\frac{2\pi}{m}\right) & -\sin\left(-\frac{2\pi}{m}\right) \\ \sin\left(-\frac{2\pi}{m}\right) & \cos\left(-\frac{2\pi}{m}\right) \end{pmatrix}$$

   Which is indeed the inverse of r (just rotating clockwise $2\pi/m$ radians).

2. (a) Since $S_2 \cong \mathbb{Z}/2$, which is abelian, we have the chain $1 \trianglelefteq S_2$. Since $\langle(123)\rangle$ is a subgroup of index 2 in S_3, we have the chain $1 \trianglelefteq \langle(123)\rangle \trianglelefteq S_3$. Lastly, conjugating each generator of $\langle(12)(34),(13)(24)\rangle \leq A_4$ shows they are still in the group, so this subgroup is normal, and of order 4. Lastly, we claim that $\{ e, (12)(34), (13)(24), (14)(23) \} = \langle(12)(34),(13)(24)\rangle \leq A_4$ is normal. By Theorem 2.8 on the last homework, conjugating any element with 2 transpositions will also have 2 transpositions. The above group is precisely the group where each element has exactly 2 transpositions, so this subgroup is normal. We get the chain $1 \trianglelefteq V_4 \cong \langle(12)(34),(13)(24)\rangle \trianglelefteq A_4 \trianglelefteq S_4$, since $\langle(12)(34),(13)(24)\rangle$ is a group of order 4 isomorphic to the Klein 4-group V_4 (it has no element of order 4).

3. (a) $[(ijk),(ijl)] = (kji)(lji)(ijk)(ijl) = (kji)(lik) = (kj)(il)$.
   (b) Next, $[(ik),(ij)] = (ik)(ij)(ik)(ij) = (ik)(jk) = (ijk)$.
   (c) Finally, $[(ikl),(ijm)] = (lki)(mji)(ikl)(ijm) = (lki)(mkl) = (l)(kim) = (kim)$.

4. (1) Recall that $\mathrm{Sgn}(\sigma) : S_n \to \mathbb{Z}/2$ is a homomorphism. Now, $\mathrm{Sgn}(\sigma^{-1}\tau^{-1}\sigma\tau) = \mathrm{Sgn}(\sigma^{-1})\mathrm{Sgn}(\tau^{-1})\mathrm{Sgn}(\sigma)\mathrm{Sgn}(\tau) = \mathrm{Sgn}(\sigma)^2\mathrm{Sgn}(\tau)^2$, since $\mathbb{Z}/2$ is commutative, and $(-1)^{-1} = -1$, and $1^{-1} = 1$. Since $(-1)^2 = 1$ and $1^2 = 1$, the above is simply equal to 1, so the commutator is even, and in A_n. First, $[S_2, S_2]$ contains the identity, and is contained in $\langle 1\rangle$, so it just equals 1 ($A_2 = \langle 1\rangle$). For $n \geq 3$, we have at least 3 distinct elements, so by problem 3, we can get any 3-cycle (ijk) by $[(ik),(ij)]$ which generates A_n.
   (2) The above proof showed that $[S_n, S_n] \leq A_n$, and by part (c) of question 3, given any 3-cycle (kim) in A_n, we can find two numbers l, j that are none of k, i, m (since $n \geq 5$), to see that $[(ikl),(ijm)] = (kim)$. Since A_n is generated by 3-cycles, we have all of A_n, and we are done.

5. (1) Clearly, each automorphism of $\mathbb{Z}/q$ is uniquely determined by where 1 is sent. That is, given $f \in \mathrm{Aut}(\mathbb{Z}/q)$, $f(x) = xf(1)$. Thus every automorphism is of the form $f(x) = rx$ for some $r \in \mathbb{Z}/q$. Clearly $f(x) = 0x$ is not an automorphism. We shall now show that $f_r(x) = rx$ is an automorphism for each $r \neq 0$. r admits a multiplicative inverse mod q, since by Bezout's lemma we can find $x, y \in \mathbb{Z}$ such that $xr + yq = 1$, i..e $xr \equiv 1 \mod q$. Now, $f_r(x)$ has inverse $f_{r^{-1}}(x)$, since $(f_r \circ f_{r^{-1}})(x) = r^{-1}rx = x$, with the left inverse holding similarly. Also, $f_r(x+y) = r(x+y) = rx+ry = f_r(x)+f_r(y)$, so each f_r is indeed an automorphism. Finally, let $\varphi : \mathrm{Aut}(\mathbb{Z}/q) \to \mathbb{Z}/(q-1)$ be defined by $f_r(x) \mapsto r$. φ is well-defined since if $f_r(x) = f_t(x)$, then $r \cdot 1 = t \cdot 1$. φ is clearly bijective,

so all we have left to check is that it is a homomorphism. We see that $(f_r \circ f_t)(x) = rtx$, so $f_r \circ f_t \mapsto rt = \varphi(f_r) \cdot \varphi(f_t)$. Thus, we have shown that $\mathrm{Aut}(\mathbb{Z}/q) \cong \mathbb{Z}/(q-1)$.

(2) let G be a group of order p^2 (assume $p = q$). We know by the class equation that $Z(G) \neq \langle 1 \rangle$, so $|Z(G)| = p$ or p^2. In the second case G is abelian, and in the first $G/Z(G)$ has prime order, hence is cyclic, hence G is abelian. Now, if G has an element of order p^2, then G is cyclic and isomorphic to $\mathbb{Z}/p^2$. Otherwise, every element has order dividing p by Langrange. Let x be an element of order p, and take $y \in G \setminus \langle x \rangle$. Now, $\langle x \rangle \trianglelefteq G$, so $\langle x \rangle \langle y \rangle$ is a subgroup of G, and we have the following tower:

$$\begin{aligned} \langle x \rangle &< \langle x \rangle \langle y \rangle \leq G \\ \implies p &< |\langle x \rangle \langle y \rangle| \leq p^2 \end{aligned}$$

Which shows that $\langle x \rangle \langle y \rangle = G$. Finally, $p^2 = |\langle x \rangle \langle y \rangle| = |\langle x \rangle||\langle y \rangle|/|\langle x \rangle \cap \langle y \rangle| = p^2/|\langle x \rangle \cap \langle y \rangle|$, so $\langle x \rangle \cap \langle y \rangle = \langle 1 \rangle$, and we have concluded that $G = \langle x \rangle \langle y \rangle \cong \langle x \rangle \times \langle y \rangle = \mathbb{Z}/p \times \mathbb{Z}/p$.

Suppose instead that $p < q$. Then take $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. Since Q has index the smallest prime dividing $|G|$, we have that $Q \trianglelefteq G$. Next, $|P \cap Q| \mid |Q| = q$ and $|p \cap Q| \mid |P| = p$, so $|p \cap Q| = 1$, since p, q are prime. Thus, PQ is a subgroup of order pq, so $PQ = G$, and we have concluded that $G \cong Q \rtimes P$ for some automorphism $\psi : P \to \mathrm{Aut}(Q) \cong \mathbb{Z}/(q-1)$. Letting $P = \langle x \rangle$, if $p \nmid q-1$, then $|\psi(x)| \mid p$ and $|\psi(x)| \mid q-1$, so $|\psi(x)| = 1$ and we only get the trivial automorphism, which yields the direct product $\mathbb{Z}/p \times \mathbb{Z}/q = \mathbb{Z}/pq$. Else, $\mathrm{Aut}(Q)$ has precisely one group subgroup of order p, $\langle \varphi(x) \rangle$. Since the image of $\mathbb{Z}/p$ is a subgroup of order dividing p, it either equals 1 or p, and in the second case the image is just $\langle \varphi(x) \rangle$. In particular, we can specify each homomorphism $\psi : P \to \mathrm{Aut}(Q)$ by specifying where 1 maps to in $\langle \varphi(x) \rangle$. Thus define $\psi_i : P \to \mathrm{Aut}(Q)$ by $1 \mapsto \varphi^i(x)$. Notice that this yields p different automorphisms. We now claim that $Q \rtimes_{\psi_i} P \cong Q \rtimes_{\psi_1} P$ for all $i \neq 0$. Notice that since $\langle \psi_1 \rangle = \mathrm{Aut}(Q)$, we can find an integer k such that $\psi_1 = \psi_i^k$, since $\psi_i \neq \mathrm{id}_Q$. Define the following map from $Q \rtimes_{\psi_1} P$ to $Q \rtimes_{\psi_i} P$:

$$\varphi : (a, x) \mapsto (a, x^k)$$

We see that $(a, x)(b, x) = (a\psi_1(b), x^2)$, and that $(a, x^k)(b, x^k) = (a\psi_{x^k}(b), x^{2k}) = (a\psi_x^k(b), x^{2k}) = (a\psi_i^k(b), x^{2k}) = (a\psi_1(b), x^{2k})$, so we can indeed extend the above map to a homomorphism. Finally, the above map is surjective since $x \mapsto x^k$ is an isomorphism since $p \nmid k$. Thus there is only one nonabelian group of order pq, $\mathbb{Z}/q \rtimes \mathbb{Z}/p$.

6. We claim that there exists a non-trivial semi-direct product $\mathbb{Z}/m \rtimes \mathbb{Z}/n$ iff $\gcd(\phi(m), n) \neq 1$, where $\phi(m)$ is the Euler totient function. This question is fully equivalent to asking when there is a non-trivial homomorphism $\psi : \mathbb{Z}/n \to \mathrm{Aut}(\mathbb{Z}/m)$. We recall from the book that $\mathrm{Aut}(\mathbb{Z}/m) \cong \mathbb{Z}/\varphi(m)$. We need only specify where the generator 1 of $\mathbb{Z}/n$ goes to determine a unique homomorphism. Suppose that $1 \mapsto f(x)$. Then $|\langle f(x)\rangle| \,|\, |\mathbb{Z}/n| = n$ and $|\langle f(x)\rangle| \mid |\mathbb{Z}/\varphi(m)| = \varphi(m)$. Thus, $|\langle f(x)\rangle| \mid \gcd(\varphi(m), n)$. If the right hand side equals 1 then 1 can only map to the identity element or it would break this condition. Suppose instead that it is d. Find a prime p dividing d, and find an element $g(x) \in \mathrm{Aut}(\mathbb{Z}/m)$ so that $|g(x)| = p$. Now the map $\psi : \mathbb{Z}/n \to \mathrm{Aut}(\mathbb{Z}/m)$ sending $1 \mapsto g(x)$ is a non-identity homomorphism, and hence induces a non-trivial semi-direct product, completing the proof.