MATH 6320 - Modern Algebra
Homework 7

Joel Sleeba

November 4, 2024

1. **Solution:** Since p is a prime and P is a subgroup of S_p of order p, we notice that P is a cyclic subgroup with $p-1$ elements of P having order p. Now let $g \in S_p$ and $h \in P$ with $|h| = p$. Then we claim that $|ghg^{-1}| = p$.

   Since $(ghg^{-1})^p = e$, we see that $|ghg^{-1}| | p$. Since p is a prime the only possibilities are $|ghg^{-1}| = 1$ or p. If $|ghg^{-1}| = 1$, this would force $gh = g$ and $h = e$, contradicting our assumption. Hence we see that $|ghg^{-1}| = p$. Therefore, we see that conjugation with elements of S_p, preserves the order of elements of P.

   Moreover, we know that since P is a subgroup, every conjugate gPg^{-1} must also be a subgroup of S_p with p elements. (That gPg^{-1} has p elements may be seen by assuming $ghg^{-1} = gkg^{-1}$ and showing $h = k$, by left and right multiplication with g^{-1} and g respectively). Since we know that conjugation preserves the order of elements, we know that each conjugate of P has $p-1$ p-cycles.

   Also, each of the distinct conjugate groups gPg^{-1} intersect only at the identity, otherwise if $e \neq x \in gPg^{-1} \cap hPh^{-1}$, since gPg^{-1}, hPh^{-1} are cyclic groups of order p, we'll get $gPg^{-1} = \langle x \rangle = hPh^{-1}$.

   If $\tau \in S_p$, we know that

   $$\tau(1\ 2\ 3 \ldots p)\tau^{-1} = (\tau(1)\ \tau(2)\ \ldots \tau(p))$$

   Hence we see that any p cycle can be written as a conjugate of any other p-cycle if we carefully choose τ. Thus conjugates of P contain all the p-cycles of S_p. We know that the number of p-cycles of in S_p is $(p-1)!$. Moreover we know that the number of the conjugates of P is the index of $N_{S_p}(P)$. Hence

$$\begin{aligned}(p-1)! &= (p-1)|S_p : N_{S_p}(P)| \\ &= (p-1)\frac{|S_p|}{|N_{S_p|}(P)} \\ &= (p-1)\frac{p!}{|N_{S_p}(P)|}\end{aligned}$$

which on simplification gives $|N_{S_p}(P)| = p(p-1)$

2. **Solution:** Since $r \in D_8$, has order 4, if $\phi : D_8 \to D_8$ is any automorphism, then $\phi(r)$ must also have the same order. Hence the possible $\phi(r)$ are $r, r^{-1} \in D_8$. Similarly since $|s| = 2$, $\phi(s)$ also must have order 2, which gives $\phi(s) \in \{s, r^2, sr, sr^2, sr^3\}$. But since $\phi(r) \in \{r, r^3\}$, if $\phi(s) = r^2$, $\phi(D_8) = \langle r \rangle$, and ϕ will not be an automorphism. Hence $\phi(s) \in \{s, sr, sr^2, sr^3\}$. Since s, r generate D_8, and each of them have 4 and 2 possible options, by the counting argument, $\mathrm{Aut}(D_8)$ can have at most 8 elements.

3. **Solution:** Since $D_8 \trianglelefteq D_{16}$, we see that $\phi : D_{16} \to \mathrm{Aut}(D_8) : g \to \phi_g$, where $\phi_g : h \to ghg^{-1}$ is a well defined map. Since

$$\begin{aligned}\phi_g\phi_{g'}(h) &= \phi_g(g'h(g')^{-1}) \\ &= gg'h(g')^{-1}g^{-1} \\ &= (gg')h(gg')^{-1} \\ &= \phi_{gg'}(h)\end{aligned}$$

we see that ϕ is a group homomorphism. Moreover, we know that $\mathrm{Ker}(\phi) = C_{D_{16}}(D_8) = \langle r^4 \rangle = \{r^4, e\}$. Hence by the first isomorphism theorem, we see that $\phi(D_{16}) = \frac{D_{16}}{\langle r^4 \rangle} \cong D_8$. Hence D_8 is isomorphic to a subgroup of $\mathrm{Aut}(D_8)$. But from the previous exercise, we see that $\mathrm{Aut}(D_8)$ can have atmost 8 elements. Since D_8 has 8 elements, this forces $D_8 \cong \mathrm{Aut}(D_8)$.

4. **Solution:** From what we proved in the class, we know that if $H \leqslant G$, then $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. Hence in the question, we know that $N_{S_p}(P)/C_{S_p}(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$.

   Since P is a cyclic group of order p, $P \cong \mathbb{Z}/p\mathbb{Z}$ and hence the number of automorphisms of P are precisely $p-1$.

Also $C_{S_p}(P) = P$. Since P is cyclic, it is clear that $P \subset C_{S_p}(P)$. Conversely, without loss of genrality, assume that $(1\ 2\ 3..p) \in P$. If $\tau \in S_p$, then

$$\tau(1\ 2\ 3\ldots p)\tau^{-1} = (\tau(1)\ \tau(2)\ \ldots \tau(p)) = (1\ 2\ 3\ \ldots p)$$

if and only if $(\tau(1)\ \tau(2)\ \ldots \tau(p))$ is a rotation of the $1, 2, \ldots p$, preserving the order. This happens only when $\tau = (1\ 2\ 3\ldots p)^k$ for some k. Hence we see that $C_{S_p}(P) = P$.

Moreover, we know that $|N_{S_p}(P)| = p(p-1)$. Therefore, we see that

$$\left|\frac{N_{S_p}(P)}{C_{S_p}(P)}\right| = \frac{|N_{S_p}(P)|}{|C_{S_p}(P)|} = \frac{p(p-1)}{p} = p - 1$$

Therefore we see that $N_{S_p}(P)/C_{S_p}(P) \cong \mathrm{Aut}(P)$.

5. **Solution:** Let $(1, k) \in C_K(H)$. Then for any $(h, 1) \in G$,

$$(h, k) = (h\varphi(1)(1), k) = (h, 1)(1, k) = (1, k)(h, 1) = (1\varphi(k)(h), k)$$

forces $\varphi(k)(h) = h$. Since this is true for all $h \in H$, we see that $\phi(k)$ is the trivial automorphism of H. Hence $k \in \mathrm{Ker}(\phi)$.

Conversely, if $k \in \mathrm{Ker}(\phi)$, then $\phi(k)(h) = h$ for all $h \in H$. Then for any $(h, 1) \in H$(identified as a subgroup of G)

$$(h, 1)(1, k) = (h\varphi(1)(1), k) = (h, k) = (\phi(k)(h), k) = (1, k)(h, 1)$$

shows that $(1, k) \in C_K(H)$. Hence $C_K(H) = \mathrm{Ker}(\varphi)$.

6. **Solution:** We know that $\mathrm{Hol}(H) = H \rtimes_\varphi \mathrm{Aut}(H)$, where $\varphi : \mathrm{Aut}(H) \to \mathrm{Aut}(H)$ is the identity map.

   (a) We notice that $H = Z_2 \times Z_2 \cong V_4$, the Klein 4 group. Therefore, by a slight abuse of notation, let $H = V_4 = \{1, a, b, c\}$. Since we know that any two of a, b, c generate the group V_4 we see that any permutation of a, b, c will be a group automorphism. Hence we see that $\mathrm{Aut}(H) \cong S_3$. Hence we see that $\mathrm{Hol}(Z_2 \times Z_2) \cong H \rtimes K$, where $H = Z_2 \times Z_2$ and $K \cong S_3$. Also, $|H \rtimes K| = |H \times K| = |H| \times |K| = 4 \times 6 = 24$

   (b) Let $G = H \rtimes K$ act on the left cosets of K, $\tilde{K} = \{K, aK, bK, cK\}$ as

$$(h, k)(gK) = hk(g)K$$

Since every element in the coset gK is of the form (g, k) for some $k \in K$, well defineness of the map follows. Moreover,

$$\begin{aligned}
(h_1, k_1)((h_2, k_2)(gK)) &= (h_1, k_1)(h_2 k_2(g)K) \\
&= h_1 k_1(h_2 k_2(g))K \\
&= h_1 k_1(h_2) k_1(k_2(g))K \\
&= (h_1 k_1(h_2), k_1 k_2)(gK) \\
&= ((h_1, k_1)(h_2, k_2))(gK)
\end{aligned}$$

and

$$(e_H, e_K)(gK) = e_H e_K(g)K = K$$

shows that the above defined map is indeed an action.

Consider $\varphi : H \rtimes K \to S_{\tilde{K}}$, the associated permutation representation of the above action. Once we show that φ is bijective, since $|\tilde{K}| = 4$, this will show that $H \rtimes K \cong S_4$.

Let $(h, k) \in \text{Ker}(\varphi)$. Then $(h, k)gK = hk(g)K = gK$ for all $g \in H$. This implies $hk(g) = g$ for all $g \in H$ (This is because $hk = (h, 1)(1, k) = (h, k)$ as H, K are identified as subgroup of G). Now let $g = e_H$. Since $k \in K$ is an automorphism, this forces $k(e_H) = e_H$. Then we see that $h = e_H$. Substituting for h in (h, k), we see that $k(g) = g$ for all $g \in H$, which forces $k \in \text{Aut}(H)$ to be the trivial automorphism. Hence we see that $\text{Ker}(\varphi) = \{(e_H, e_K)\}$ and φ is injective, hence an isomorphism. Thus $H \rtimes K \cong S_4$.

7. **Solution:** We know that since $75 = 3 \times 5^2$, the fundamental theorem for Abelian groups immediately gives two groups $Z_3 \times Z_{5^2} \cong Z_{75}$ and $Z_3 \times Z_5 \times Z_5$.

   Now, to find a non-Ableian group of order 75, consider the map $\varphi : Z_5 \to \text{Aut}(Z_{15})$ defined as
   $$\varphi(r) = (1\ 2\ 3\ 4\ 5)^r$$

   Clearly φ is an injective homomorphism. Then define $G = Z_{15} \rtimes_{\varphi} Z_5$. We note that G is not Abelian since

   $$(1, 1)(1, 2) = (\varphi(1)(1), 2) = (2, 2) \neq (3, 2) = (\varphi(2)(1), 2) = (1, 2)(1, 1)$$

   Since $75 = 15 \times 5$, we see that $|G| = 75$.

8. **Solution:** Let A be the given matrix. Then

$$A^5 = \begin{pmatrix} 0 & -1 \\ 1 & 4 \end{pmatrix}^5 = \begin{pmatrix} -1 & -4 \\ 4 & 15 \end{pmatrix}^2 \begin{pmatrix} 0 & -1 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

shows that $|A| = 5$. Now define a map $\varphi : Z_5 \to \mathrm{Aut}(Z_{19} \times Z_{19})$ as

$$\varphi(r)(x, y) = A^r \begin{bmatrix} x \\ y \end{bmatrix}$$

Since $A \in GL_2(\mathbb{F}_2)$, $A^r \in GL_2(\mathbb{F}_2)$ for each $r \in Z_5$ and hence is a bijection. Moreover matrix multiplication preserves additivity, we see that it is an isomorphism of $Z_{19} \times Z_{19}$. Hence $\varphi(r) \in \mathrm{Aut}(Z_{19} \times Z_{19})$.

Now consider the group $G = (Z_{19} \times Z_{19}) \rtimes_\varphi Z_5$. Then

$$((1, 1), 1) \rtimes ((1, 2), 2) = ((1, 1)A(1, 2), 2) = ((1, 1)(-2, 9), 2) = ((-1, 10), 2)$$

but

$$((1, 2), 2) \rtimes ((1, 1), 1) = ((1, 2)A^2(1, 1), 2) = ((1, 2)(-5, 19), 2) = ((-4, 2), 2)$$

shows that G is not Abelian. And it is evident that $|G| = 19 \times 19 \times 5 = 1805$.

Moreover, the fundamental theorem of Abelian groups gives us two other groups, $Z_{1805} \cong Z_5 \times Z_{361}$ and $Z_5 \times Z_{19} \times Z_{19} \cong Z_{95} \times Z_{19}$ of order 1805.

9. **Solution:** If $\phi : Z_2 \to \mathrm{Aut}(Z_{2^n})$ is a homomorphism, then it is completely determined by $\phi(1)$, since 1 generate Z_2. Moreover, since 1 has order 2 in Z_2, $\phi(1)$ has to divide 2. Then the only possibilities for $\phi(1)$ are either the trivial automorphism or $\phi(1)$ must have order 2.

We also see that the automorphisms of Z_{2^n} are also completely characterized by the image of 1 for the same reason. Hence if $\sigma \in \mathrm{Aut}(Z_{2^n})$ is an automorphism with $\sigma(1) = k$, we see that

$$\begin{aligned} \sigma^2(r) &= \sigma(\sigma(r)) \\ &= \sigma(r\sigma(1)) \\ &= \sigma(rk) \\ &= rk\sigma(1) \\ &= rk^2 \end{aligned}$$

If $\sigma^2 = e$, then $\sigma^2(r) = r$ for all $r \in Z_{2^n}$. This forces $k^2 \equiv 1 \mod 2^n$. We can show that the only choices for such $k \in Z_{2^n}$ are $\{1, 2^{n-1} - 1, 2^{n-1} + 1, 2^n - 1\}$.

That $1, 2^n - 1$ satisfies the above equation is evident. To see if there are any other, Let $k = 2^{n-1} + r$, then

$$\begin{aligned}(2^{n-1} + r)^2 &= 2^{2(n-1)} + r2^n + r^2 \\ &\equiv 2^n 2^n - 2 + r^2 \\ &\equiv r^2\end{aligned}$$

Thus we see that $r = \pm 1$ gives another solution for k.

Hence there are exactly 4 homomorphisms from $Z_2 \to \mathrm{Aut}(Z_{2^n})$. We'll denote each of these 4 homomorphisms by $\phi_1, \phi_2, \phi_3, \phi_4$, and the their corresponding images $\phi_i(1) \in \mathrm{Aut}(Z_{2^n})$ by $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ where each σ_i send 1 to $1, 2^{n-1} - 1, 2^{n-1} + 1, 2^n - 1$ respectively.

Clearly, we see that each $Z_{2^n} \rtimes_{\phi_i} Z_2$ contains 2^{n+1} elements. Since ϕ_1 is the trivial morphism, we see that $Z_{2^n} \rtimes_{\phi_1} Z_2 \cong Z_{2^n} \times Z_2$ by the representation theorem and hence Abelian. By the same reasoning none of the other direct products are Abelian.