M403 - Fall 2013 - HW 12 - Enrique Areyan (1)

65/70

~~(1)~~ Determine generators and relations for the group D_n, using two generators and three relations.

7

Solution: Let x and y be the generators for D_n, then the claim is that $D_n \cong G = \langle x, y \mid x^n = y^2 = (xy)^2 = 1 \rangle$. One way to argue that this must be the case is that x represents the rotation by an angle of $\frac{2\pi}{n}$ and y the reflection about the x-axis if we were to place the n-gon appropiately in the xy-plane. So the induced homomorphism from the free group G to D_n; $f: G \to D_n$ given by $f(x^n) = \rho_{\frac{2\pi}{n}}$ and $f(y) = r$, maps the set of generators $\{x, y\}$ in G to the set of generators $\{\rho_{\frac{2\pi}{n}}, r\}$ in D_n, so that $D_n \cong G$.
Moreover, the third relation $(xy)^2 = e$ tell us that $xy = y^{-1}x^{-1}$, but $y^{-1} = y$ (since $y^2 = e$) so: $xy = yx^{-1}$, Also $xy = yx^{n-1}$, (since $x^{-1} = x^{n-1}$)
So every word in the quotient free group G must satisfy $xy = yx^{n-1}$ further constraining G to be isomorphic to D_n.

~~(2)~~ (a) Determine generators and relations for the quaternion group Q_8
(b) Compute $|Aut(Q_8)|$.

Solution:

(a) Claim $Q_8 \cong G = \langle x, y \mid x^2 = y^2, x^{-1}yx = y^{-1} \rangle$.

$x^4 = y^4$

Pf: We want to show that a generating set of Q_8 satisfies these relations and that any group G presented in this way has at most 8 elements.

Consider the set of generators of Q_8 $\{i, j\}$. then letting $i = x$ and $j = y$, we have that $i^2 = -1 = j^2$, so the first relation is satisfied, $i^{-1}ji = (-i)(-k) = ik = -j = j^{-1}$, so the second relation is satisfied.

Now, reasoning on the length of reduced words: let w be a word in G, then,

$|w| = 0 \Rightarrow$ we have the reduced word 1 (identity).

$|w| = 1 \Rightarrow$ we have the reduced words x, y.

$|w| = 2 \Rightarrow$ we have: xx, xy, yx, yy, but $x^2 = xx = y^2 = yy$, so we only have 3 reduced words

$|w| = 3$, $\Rightarrow$ Note that for xyx we have:

$$(xyx)y = (xy)^2 = y^2 \Rightarrow xyx = y \text{ , Right cancellation}$$

So this word is already accounted for. A similar argument for all other words of length 3 shows that the only reduced words of lenght 3 are: x^3, x^2y. (for example $y^3 = y^2y = x^2y$, and so on)

$|w| = 4 \Rightarrow$ provides no new reduced words. For example,

$x^4 = 1 = y^4$, $x^2y^2 = y^2x^2 = 1$, $x^3y = xy^3 = x^2xy = y^2xy = xy$, $\rightarrow$ right cancellation

and so on.

therefore, there are at most 8 elements, that is:

$1, x, y, xy, yx, y^2, x^3, x^2y$ (choosing a representative for each one e.g. $y^2 = x^2$).

this shows that $Q_8 \cong G$, so that a representation for Q_8 is

$$\langle x, y \mid x^2 = y^2, x^{-1}yx = y^{-1} \rangle.$$

+8

(b) we want to compute $|Aut(Q_8)|$

Claim: $|Aut(Q_8)| = 24$.

Pf: An automorphism must send a set of generators to a set of generators. In particular, an element $\varphi \in Aut(Q_8)$ must send x to a generator, say $\varphi(x)$ and y to a generator $\varphi(y)$ s.t $\varphi(x) \neq \varphi(y)$. Now, there are only 6 elements of order 4 in Q_8 (1 and -1 are elements of order 2, all others are of order 4). therefore, we inmediately set an upper bound for the number of possible automorphisms namely 6! However, not all of these will work. One way to see this is that we have to have $y \notin \langle \varphi(x) \rangle$. otherwise φ would not preserve the subgroup generated by y ($\langle \varphi(y) \rangle = \langle \varphi(x) \rangle$ in case $y \in \langle \varphi(x) \rangle$), and hence φ would not an automorphism. therefore, having chosen $\varphi(x)$, we only have $8 - \langle \varphi(x) \rangle$ possibilities. But $\langle \varphi(x) \rangle = \{e, \varphi(x), \varphi(x)^2, \varphi(x)^3\}$, since $\varphi(x)$ has order 4. So there are $8 - \langle \varphi(x) \rangle = 8 - 4 = 4$. choices where to send y. So far we have $6 \cdot 4 = 24$ choices, But then $|\{\varphi(x), \varphi(x)^2, \varphi(x)^3, \varphi(y), \varphi(y)^2, \varphi(y)^3\}| = 7$

Since we know that an automorphism must send the identity to itself and -1 to -1 (since these are the only elements of order 2) we now have the following elements to chose from:

$$\left| Q_8 \setminus \{1, -1, \varphi(x), \varphi(x)^2, \varphi(x)^3, \varphi(y), \varphi(y)^2, \varphi(y)^3\} \right| = 0,$$

So we have no more choices left, which means that

$$\boxed{|Aut(Q_8)| = 24.}$$

---

(3) Identify the following group:

$$G = \langle x, y, z \mid x^2 = y^2 = z^2 = e,\ xz = zx,\ xyx = yxy,\ yzy = zyz \rangle.$$

Solution: Claim $S_4 \simeq G$.

Pf: Let $x = (12)$, $y = (23)$, $z = (34)$. then the relations are satisfied

$x^2 = (12)^2 = e$. $y^2 = (23)^2 = e$. $z^2 = (34)^2 = e$.

$xz = (12)(34) = (34)(12) = zx$ (disjoint transpositions conmute).

$xyx = (12)(23)(12) = (2)(13) = (23)(12)(23) = yxy$.

$yzy = (23)(34)(23) = (3)(24) = (34)(23)(34) = zyz$

Moreover, $G = \langle (12), (23), (34) \rangle$; but then

$(12)(23)(12) = (13) \Rightarrow (13) \in G$

$(23)(34)(23) = (24) \Rightarrow (24) \in G$

$(12)(23)(34) = (41) \Rightarrow (41) \in G$

+10

therefore, G contains all transpositions in S_4.

By a theorem proved in a previous homework we know that every permutation can be written as a product of transposition.

So, $G \cong S_4$.

M403 - Fall 2013 - HW 12 - Enrique Areyan (4)

(4) Determine the automorphism group of D_4.

Solution: We can easily compute $|Aut(D_4)|$ as follow:

Consider $D_4 = \{R_1, R_2, R_3, H, V, D_1, D_2, e\}$. We know that the subgroups of D_4 are: $\{R_1, R_2, R_3, e\}$, $\{H, V, R_2, e\}$ and $\{D_1, D_2, R_2, e\}$. (these are the subgroups of order 4).

Now, any element $\alpha \in Aut(D_4)$ must preserve these groups. the only possibility for R_2 is to be mapped to R_2, otherwise it won't be able to be in all of the above subgroups.

Now consider $\{R_1, R_2, R_3\}$. we already know where R_2 has to be mapped therefore, R_1 could be mapped to itself or to R_3. So we have two ch for R_1. Having chosen the element R_1 is to be mapped, there is no further choice for R_3, it has to be mapped to R_1 if R_1 was mapped to R_3 or to itself. Note that e has to be mapped to itself.

Next, consider $\{H, V, R_2, e\}$. we already know where R_2, e has to go - to themselves -. Hence, there are 2 choices for H and 1 for V.

Finally, using a similar argument as before, D_1 could go to itself or D_2 and D_2 has to go to the other choice.

In sum, the choices are:

$$\underset{2}{R_1} \times \underset{1}{R_2} \times \underset{1}{R_3} \times \underset{2}{H} \times \underset{1}{V} \times \underset{2}{D_1} \times \underset{1}{D_2} \times \underset{1}{e} = 2^3 = \boxed{8}$$

Therefore, $\boxed{|Aut(D_4)| = 8}$

+20

Moreover, $Aut(D_4) \cong D_4$.

To see why this is the case, note that there are only two non-abelian groups of order 8: D_4 and Q_8.

the group $Aut(D_4)$ is not isomorphic to Q_8 because.

(first note $Aut(D_4)$ is not abelian, consider $\alpha_1, \alpha_2 \in Aut(D_4)$ like $\alpha_1(H) = V, \alpha_1(V) = D_1, \alpha_1(D_1) = D_2, \alpha_1(D_2) = H$, α_1 fixes all others & $\alpha_2(H) = D_2, \alpha_2(V) = D_1, \alpha_2(D_1) = H, \alpha_2(D_2) = V)$, α_2 fixes all others, then $\alpha_1\alpha_2(H) = \alpha_1(D_2) = H \neq D_1 = \alpha_2(V) = \alpha_2\alpha_1(H)$.).

Q_8 has only one element of order 2, whereas $Aut(D_4)$ has more than one element of order 2. therefore $Aut(D_4) \ncong Q_8 \Rightarrow \boxed{Aut(D_4) \cong D_4}$

(5) Let G be a group and H a subgroup. We have seen that G acts on G/H, the set of left cosets of H in G, by left multiplication, and that we obtain a homomorphism $\alpha : G \to A(G/H)$.

(a) Prove that if $N \subseteq H$ is a normal subgroup of G, then $N \subseteq Ker(\alpha)$ (the kernel of α is the "largest" normal subgroup of G contained in H)

Pf: Let $x \in N$. WANT TO SHOW: $\alpha(x) = id$, where $id \in A(G/H)$ i.e., that is $id: A(G/H) \mapsto A(G/H)$. So, equivalently, we can write

$$\alpha(x)(\tilde{g}H) = \tilde{g}H. \quad \forall \tilde{g} \in G.$$

Now, since $x \in N \Rightarrow x = gng^{-1} \in N$, for some $g \in G$. and $n \in N$.
$(N \trianglelefteq G)$.

But then,
$$\begin{aligned} \alpha(x)(\tilde{g}H) &= \alpha(gng^{-1})(\tilde{g}H) \\ &= [\alpha(g)(\tilde{g}H)][\alpha(n)(\tilde{g}H)][\alpha(g^{-1})(\tilde{g}H)] && \text{since } \alpha \text{ is a homomorph} \\ &= [g(\tilde{g}H)][n(\tilde{g}H)][g^{-1}(\tilde{g}H)] && \text{By def of } \alpha. \\ &= [\tilde{g}H][\tilde{g}H][\tilde{g}H] \\ &= \tilde{g}H. \end{aligned}$$
; so $\alpha(x) \in Ker(\alpha)$. □

t.w

(b) Now assume G is finite and let $n = [G:H]$, so we may think of α as a homomorphism from G to S_n. Prove that $\alpha(H) \subset S_{n-1}$.

Pf: By hypothesis we have that $|G/H| = n$. Then

$$\alpha : G \to Aut(G/H) \hookrightarrow S_n$$

Let $f \in Aut(G/H)$. Note that $f(H) = H$. Since $[G:H] = n$, there are n distinct cosets of H. But then we will only have $n-1$ choices for $f(g_i H)$. and so $\alpha(H) \subset S_{n-1}$.

(c) Now assume G is finite and assume G has a subgroup H whose index in G is the smallest prime that divides the order of G.

Prove that $H \trianglelefteq G$.

Pf. We want to show: $\forall g \in G : \forall h \in H : ghg^{-1} \in H$. Equivalently, a homomo... we can show: $Ker(\alpha) = H$, for $\alpha : G \to Aut(G/H)$, and $O(\alpha(h)) \mid \frac{n}{p}$

Let $h \in H$: $O(h) \mid |H| = \frac{n}{p}$ and $O(\alpha(h)) \mid (p-1)!$

$\Rightarrow O(\alpha(h)) = 1 \Rightarrow h \in Ker(\alpha)$, since h was arbitrary $\Rightarrow H \subset Ker(\alpha)$.

clearly $Ker(\alpha) \subset H \Rightarrow H = Ker(\alpha)$ and so $H \trianglelefteq G$.

M403 - Fall 2013 - Enrique Areyan - HW 12

(6) Find a Sylow-p subgroup in $Gl_3(\mathbb{F}_p)$.

Solution: By previous homework we know that:

$$|Gl_3(\mathbb{F}_p)| = (p^3-1)(p^3-p)(p^3-p^2) = p^3(p^3-1)(p^2-1)(p-1)$$

Hence, $p^3 \| |G|$. By definition, since $Gl_3(\mathbb{F}_p)$ is a finite group we need to find a subgroup of order p^3.

Now consider the set $\mathcal{U} = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a,b,c \in \mathbb{F}_p \right\}$

Note that $\mathcal{U} \leq Gl_3(\mathbb{F}_p)$. b/c:

(i) $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b'+ac'+b \\ 0 & 1 & c'+c \\ 0 & 0 & 1 \end{pmatrix}$

So $\mathcal{U}$ is closed under inverses. +10

(ii) (i) also shows that $\mathcal{U}$ is closed under multiplication.

Now clearly $|\mathcal{U}| = p \cdot p \cdot p = p^3$ (p choices for a, p choices for b, p choices for c).

So $\mathcal{U}$ is a sylow-p subgroup in $Gl_3(\mathbb{F}_p)$.

---

(7) Prove there is no simple group of order 637.

Pf: First, note that the prime factors of 637 are 7 and 13

By Sylow theorem there exists subgroups P_1, P_2 of G s.t. $|P_1| = 7^2$ and $|P_2| = 13$ (this is because $7^2 \nmid 637$ & $13 \nmid 637$

Hence, there exists homomorphisms: (by previous exercise).

$$\alpha_1 : G \longrightarrow Aut(G/P_1) \subset S_{13}$$

(this is because $[G:P_1] = 13$). +10

Now, $|P_2| = 13 \Rightarrow \exists\, g \in P_2$ s.t. $o(g) = 13 \Rightarrow P_2 = \langle g \rangle$.

Since $\alpha(g^n) = [\alpha(g)]^n = id$ for $n \leq 12$.

therefore, since the order of the image has to divide the order of the element b/c α is a homomorphism.

Hence, note $13 \nmid 12! \Rightarrow g \in Ker(\alpha)$, so α has a nontrivial kernel, so G cannot be simple.