MATH 210A

Name: Quin Darcy **Due Date:** 9/9/19
Instructor: Dr. Shannon **Assignment:** Homework 5

1. Assume that G is a group, and $a \in G$

   (a) Assume that $o(a) = r$, and that $m \mid r$, say $r = mt$. Prove that $o(a^t) = m$.

   Proof. Let $y = o(a^t)$. From the above assumption, it follows that $a^r = a^{mt} = (a^t)^m = e$. Thus, by 5 of hw 1, $y \mid m$. Thus, there exists $k_1 \in \mathbb{Z}$ such that $m = k_1 y$. By the division algorithm, there exists $\alpha, \beta \in \mathbb{Z}$ with $0 \leq \beta < m$ such that $y = \alpha m + \beta$. Thus,

   $$\begin{aligned}(a^t)^y &= (a^t)^{\alpha m+\beta} \\ &= (a^t)^{\alpha m}(a^t)^{\beta} \\ &= \big((a^t)^m\big)^{\alpha}(a^t)^{\beta} \\ &= e^{\alpha}(a^t)^{\beta} \\ &= (a^t)^{\beta} \\ &= e.\end{aligned}$$

   Hence, by 5 of hw 1, $y \mid \beta$. Thus, there exists $k_2 \in \mathbb{Z}$ such that $\beta = k_2 y$. Note that since $y > 0$ by definition, then since $y = \alpha m + \beta$ and $m > \beta$, then it follows that $\alpha m > 0$ and $\beta \geq 0$. Now substituting for m and β we get that

   $$y = \alpha(k_1 y) + (k_2 y).$$

   Since $\alpha k_1 \in \mathbb{Z}$, then for ease of notation we will let $n = \alpha k_1$ and $k = k_2$. Thus, $y = ny + ky$. Thus, $1 = n + k$. Since $n > 0$ and $k \geq 0$ and both n and k are integers, then it follows that $k = 0$ and $n = 1$. Thus, $\alpha k_1 = 1$. Thus, $\alpha = 1$ and $k_1 = 1$. Thus, $m = k_1 y = y$. Therefore, $o(a^t) = y = m$. □

   (b) Assume that $G/\langle a\rangle$ has an element $\langle a\rangle d$ of order m. Let $o(d) = k$. Prove that $m \mid k$, and if $k = ms$ then $o(d^s) = m$.

   Proof. It follows from our assumptions that $d^k = e$. Thus, $\big(\langle a\rangle d\big)^k = \langle a\rangle d^k = \langle a\rangle$. Thus, by 5 of hw 1, $m \mid k$. Since $o(d) = k$ and $m \mid k$, which implies $k = ms$ for $s \in \mathbb{Z}$, then by (a), $o(d^s) = m$. □

2. Recall (from p 10) that if $\sigma, \tau \in S_n$, and $\sigma = (a_1 a_2 \ldots a_k)$ is a cycle of length k, then $\tau \circ \sigma \circ \tau^{-1} = (\tau(a_1)\tau(a_2)\ldots\tau(a_k))$. Using this, prove that if $n > 2$, then $Z(S_n) = \{(1)\}$.

   Proof. Recall that $Z(S_n) = \{\sigma \in S_n \mid \forall \tau \in S_n \colon \tau \circ \sigma \circ \tau^{-1} = \sigma\}$. Let $n > 2$, $\sigma \in Z(S_n)$, and suppose $\sigma = (a_1 a_2 \ldots a_k)$. Then it follows that for all $\tau \in S_n$

   $$\tau \circ \sigma \circ \tau^{-1} = \sigma.$$

Thus,

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(a_1)\tau(a_2) \dots \tau(a_k)) = (a_1 a_2 \dots a_k).$$

It follows that $\tau(a_i) = a_i$ for all $1 \le i \le k$. Thus, $\tau = (1)$. Thus, for all $\sigma \in Z(S_n)$, the conjugate of σ is the identity. By pg. 10, two permutations are conjugates iff they have the same cycle structure. Thus, since τ is the conjugate of σ and τ has cycle structure 1, then σ has cycle structure 1. Thus, $\sigma = (1)$. Hence, if $\sigma \in Z(S_n)$, then $\sigma \in \{(1)\}$. Thus, $Z(S_n) \subseteq \{(1)\}$.

Now let $\sigma \in \{(1)\}$. Then $\sigma = (1)$. Then if $\tau \in S_n$, we have that $\tau \circ (1) \circ \tau^{-1} = (1)$. Hence, $(1) \in Z(S_n)$. Thus, $\{(1)\} \subseteq Z(S_n)$. Therefore, $Z(S_n) = \{(1)\}$. $\square$

4. Assume that $G = \langle a \rangle$, and $o(G) = n$. Prove that $\mathrm{Aut}(G) \cong (\mathbb{Z}_{(n)}, \odot)$.

Proof. Let $f\colon \mathrm{Aut}(G) \to \mathbb{Z}_{(n)}$ be defined as $f(\theta) = [k]$ where $\theta(a) = a^k$, where $k \in \mathbb{Z}$ such that $(n,k) = 1$. By definition, f is defined over $\mathrm{Aut}(G)$. Next, we will check if f is well defined. Let $\theta, \gamma \in \mathrm{Aut}(G)$ and assume $\theta = \gamma$. Then we want to show that $f(\theta) = f(\gamma)$. We have that $\theta(a) = a^i$ and $\gamma(a) = a^j$. Thus, $f(\theta) = [i]$ and $f(\gamma) = [j]$. Since $\theta = \gamma$, then $a^i = a^j$. Thus, $\theta(a) = a^j$. Hence, $f(\theta) = [j] = f(\gamma)$. So f is well defined.

Now assume that $f(\theta) = f(\gamma)$. Then $[i] = [j]$. Thus, $i \in [j]$ and so there exists some $m \in \mathbb{Z}$ such that $i = mn + j$. Thus, $a^i = a^{mn+j} = a^{mn}a^j = a^j$. It follows that $\theta(a) = \gamma(a)$, and since a generates G, then $\theta = \gamma$. Hence, f is 1-1.

Now let $[k] \in \mathbb{Z}_{(n)}$. Now consider some φ whose domain is G, where $\varphi(a) = a^k$. Then we want to show that $\varphi \in \mathrm{Aut}(G)$. By definition, $\mathrm{ran}(\varphi) \subseteq G$ and so $\varphi\colon G \to G$. Now assume that $x, y \in G$ and that $x = y$. Then since $G = \langle a \rangle$, then $x = a^s$ and $y = a^t$, for some $s, t \in \mathbb{Z}$. Thus, $\varphi(x) = \varphi(a^s) = (a^s)^k$, and $\varphi(y) = \varphi(a^t) = (a^t)^k$. But since $a^s = a^t$, then $(a^s)^k = (a^t)^k$. Thus, $\varphi(x) = \varphi(y)$. Thus, φ is well defined. Now let $a^i, a^j \in G$. Then $\varphi(a^i a^j) = \varphi(a^{i+j}) = (a^{i+j})^k = a^{ik}a^{jk} = \varphi(a^i)\varphi(a^j)$. Thus, φ is a homomorphism. Now assume $\varphi(x) = \varphi(y)$. Thus, $(a^s)^k = (a^t)^k$, for some $s, t \in \mathbb{Z}$. Thus, $a^{k(s-t)} = e$. Then $n \mid k(s-t)$, Since $(n,k) = 1$, then $n \mid (s-t)$. Thus, $s = qn + t$, for some $q \in \mathbb{Z}$. Thus, $a^s = a^{qn+t} = a^{qn}a^t = a^t$. Hence, $x = y$ and φ is 1-1. Since $(n,k) = 1$, then $\langle a \rangle = \langle a^k \rangle$. Thus, φ is onto. Therefore, $\varphi \in \mathrm{Aut}(G)$ and $f(\varphi) = [k]$. Thus, f is onto.

Now we want to show that f is a homomorphism. Let $\theta, \gamma \in \mathrm{Aut}(G)$ and suppose $\theta(a) = a^i$ and $\gamma(a) = a^j$. Then we have that $(\theta \circ \gamma)(a) = \theta(\gamma(a)) = \theta(a^j) = (a^j)^i = a^{ji}$. Then $f(\theta \circ \gamma) = [ji] = [j] \odot [i] = f(\gamma) \odot f(\theta) = f(\theta) \odot f(\gamma)$. Thus, f is a homomorphism. Therefore, f is an isomorphism. Hence, $\mathrm{Aut}(G) \cong (\mathbb{Z}_{(n)}, \odot)$. $\square$

6. Assume that G is a group, $k \in \mathbb{Z}^+$, and that $p^k \mid o(G)$. Let $S = \{H \subseteq_g G\colon o(H) = p^k\}$. On exam 1 we proved that $: G \times S \to S$ by $\varphi(g, H) = gHg^{-1}$ is an action of G on S. Let R be one of the orbits under this action (so $R \subseteq S$), and let $P \in S$. Define θ with domain $P \times R$ by $\theta(d, H) = dHd^{-1}$. Explain why θ is an action of P on R.

Proof. In order for θ to be an action of P on R, we first need that $\theta\colon P \times R \to R$. We can see that this holds since $R = \{gMg^{-1}\colon g \in G\}$, for some $M \in S$, and for any $(d, H) \in P \times R$, it follows that $\theta(d, H) = \theta(d, gMg^{-1}) = d(gMg^{-1})d^{-1}$. Thus, because $dg \in G$, then $d(gMg^{-1})d = (dg)M(dg)^{-1} \in R$. Thus, $\theta(d, H) \in R$ for all $(d, H) \in P \times R$. Thus, $\theta \colon P \times R \to R$. Now let $c, d \in P$ and $H \in R$, then

$$\theta(cd, H) = (cd)H(cd)^{-1} = c(dHd^{-1})c^{-1} = \theta(c, dHd^{-1}) = \theta(c, \theta(d, H)).$$

Lastly, consider

$$\theta(e, H) = eHe^{-1} = H.$$

Thus, θ is an action of P on R. $\square$