MATH 210A

Name: Quin Darcy **Due Date:** 10/30/19
Instructor: Dr. Shannon **Assignment:** Homework 8

1. Find the conjugacy classes of the elements of A_4, and verify that the class equation holds for A_4. (recall that $c(a) = o(G)/o(N(a))$, and as part of this process, find $N((12)(34))$)

Solution. In S_4 we know that given any permutation $\sigma \in S_4$, the conjugacy class of σ will contain all other permutations with the same cycle structure as σ. Hence, in S_4, we have that

$$\begin{aligned} c((1)) &= \{(1)\} \\ c((12)) &= \{(12), (13), (14), (23), (24), (34)\} \\ c(((123)) &= \{(123), (132), (124), (142), (134), (143), (234), (243)\} \\ c((1234)) &= \{(1234), (1243), (1324), (1342), (1423), (1432)\} \\ c((12)(34)) &= \{(12)(34), (13)(24), (14)(23)\}. \end{aligned}$$

Since A_4 contains only even permutations, then it is only $c((1)), c((123))$, and $c((12)(34))$ that we are interested in. By simple calculations, we find that $c((123))$ in S_4 splits in A_4 whereas $c((1))$ and $c((12)(34))$ remain the same. Thus, the conjugacy classes in A_4 are

$$\begin{aligned} c((1)) &= \{(1)\} \\ c((123)) &= \{(123), (134), (142), (243)\} \\ c((132)) &= \{(132), (124), (143), (234)\} \\ c((12)(34)) &= \{(12)(34), (13)(24), (14)(23)\}. \end{aligned}$$

We can now use the fact that $c(a) = o(G)/o(N(a))$. Note that $o(A_4) = 12$. It follows that

$$o(N((1))) = \frac{12}{12} = 1 \qquad o(N((123))) = \frac{12}{4} = 3$$
$$o(N((132))) = \frac{12}{4} = 3 \qquad o(N((12)(34))) = \frac{12}{3} = 4.$$

Thus,

$$\begin{aligned} |A_4| &= \big|Z(A_4)\big| + \sum_{N(\sigma)\neq A_4} \frac{|A_4|}{\big|N(\sigma)\big|} \\ &= \big|\{(1)\}\big| + \frac{12}{3} + \frac{12}{3} + \frac{12}{4} \\ &= 1 + 4 + 4 + 3 \\ &= 12. \end{aligned}$$

Lastly, we have that $N((12)(34)) = \{(1), (12)(34), (13)(24), (14)(23)\}$.

3. Let $o(G) = 3 \times 5 \times 7$.

   (a) Prove that G is not simple.

   Proof. We want to show that G contains a proper normal subgroup. By Sylow I, G contains subgroups of orders $3, 5$, and 7, respectively. Since $3, 5$, and 7 are the highest powers of these primes that occur in the order of G, then it follows that those subgroups are Sylow subgroups. Thus, by Sylow III, we have that

$$n_3 \equiv 1 (\text{mod } 3) \wedge n_3 \mid 35, \quad n_5 \equiv 1 (\text{mod } 5) \wedge n_5 \mid 21, \quad n_7 \equiv 1 (\text{mod } 7) \wedge n_7 \mid 15.$$

   From these relations we conclude that $n_3 = 1$ or $n_3 = 7$; $n_5 = 1$; $n_7 = 1$. Thus, $P_5 \lhd G$ and $P_7 \lhd G$. Finally, since $|P_5| = 5 < 105 = o(G)$. Thus, $P_5 \subset G$. Thus, G contains a proper normal subgroup. Therefore, G is not simple. $\square$

   (b) Prove that G has a normal subgroup of order 35.

   Proof. From (a) we have that $P_5 \lhd G$ and $P_7 \lhd G$. Additionally, we have that $P_5 \cap P_7 = \{e\}$. Thus, $P_5P_7 \cong P_5 \times P_7 \cong \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{35}$. Since $P_5P_7 \subseteq_g G$, then it follows that G contains a subgroup of order 35. We now only need to show that $P_5P_7 \lhd G$. So let $g \in G$, $x \in P_5$, and $y \in P_7$. Then $g(xy)g^{-1} = (gxg^{-1})(gyg^{-1})$ and since $P_5 \lhd G$ and $P_7 \lhd G$, then $gxg^{-1} \in P_5$ and $gyg^{-1} \in P_7$. Thus, $(gxg^{-1})(gyg^{-1}) \in P_5P_7$. Thus, $g(xy)g^{-1} \in P_5P_7$. Thus, $P_5P_7 \lhd G$. Therefore, G contains a normal subgroup of order 35. $\square$

   (c) Prove that both $P_5 \lhd G$ and $P_7 \lhd G$.

   Proof. This follows from part (a). $\square$

   (d) Prove that if $P_3 \lhd G$, then G is Abelian.

   Proof. Assume that $P_3 \lhd G$. Then since $P_3 \cap P_5 = \{e\}$, $P_3 \cap P_7 = \{e\}$, and $P_5 \cap P_7 = \{e\}$, then $G = P_3P_5P_7 \cong P_3 \times P_5 \times P_7 \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{105}$. Therefore, G is Abelian. $\square$

   (e) Prove that there are only two groups of order 105.

   Proof. Let $P_3 = \langle a \rangle$, $P_5 = \langle b \rangle$, and $P_7 = \langle c \rangle$. Then since $P_7 \lhd G$ and $P_3 \subseteq_g G$, then $\langle a \rangle \langle c \rangle \subseteq_g G$. Let $H = \langle a \rangle \langle c \rangle$. Now assume that $\theta \colon H \to \text{Aut}(\langle b \rangle)$ is a homomorphism, where $\theta(h) = \varphi_k$ and $\varphi_k(x) = x^k$. From class we know that each φ_k corresponds to $hbh^{-1} = b^k$, for $h \in H$. Additionally, we must also satisfy $o(\theta(h)) \mid o(h)$. Thus, since $\langle a \rangle \cap \langle c \rangle = \{e\}$, then $o(\langle a \rangle \langle c \rangle) = 21$ and so $o(\theta(h)) \mid 21$. Note that it must also hold that $o(\theta(h)) \mid o(\text{Aut}(\langle b \rangle)) = 4$. Thus, $o(\theta(h)) = 1$ and $hbh^{-1} = b$. Finally, since $G = H\langle b \rangle$ (since $H \cap \langle b \rangle = \{e\}$) and from hw 7, there are two possibilities for H ($\mathbb{Z}_{21}$ and the nonabelian group), then there are only two possible groups of order 105. $\square$

4. Determine if the following are always true. If the statement if always true, then prove it, and if it is not always, then give a counter example.

   (a) If G is a group, $N \lhd G$, G/N is Abelian, and N is Abelian, then G is Abelian.

   Proof. This is not always true. Suppose $o(G) = 6$, then G has a 3-Sylow subgroup which is normal in G. Additionally, we have that $\left|G/P_3\right| = 2$ and it is therefore Abelian. However, by the results on pg. 22, G is either isomorphic to $\mathbb{Z}_6$ or isomorphic to D_6. The latter case is an instance of a nonabelian group. Therefore, we have that $P_3 \lhd G$, G/P_3 is Abelian, P_3 is Abelian, but G is not Abelian. $\square$

   (b) If G is a group, $N \lhd G$, $G/N \cong M$, then $G \cong N \times M$.

   Proof. This is not always true. Let $G = S_3$ and let $N = A_3$. Since $|A_3| = 3$, then $[S_3 \colon A_3] = 2$ and thus by hw 2, $A_3 \lhd G$. Now define $\theta \colon S_3/A_3 \to \mathbb{Z}_2$, by

$$\theta(\sigma A_3) = \begin{cases} [0] & \text{if} \quad \sigma \in A_3 \\ [1] & \text{if} \quad \sigma \notin A_3, \end{cases}$$

By definition, $\theta(S_3/A_3) \subseteq \mathbb{Z}_2$. Now let $\sigma A_3, \gamma A_3 \in S_3/A_3$ and to show θ is well defined assume that $\sigma A_3 = \gamma A_3$. Then if $\sigma \in A_3$, then $\sigma A_3 = \gamma A_3$ implies that for $\delta, \lambda \in A_3$, $\sigma\delta = \gamma\lambda$. Thus, $\gamma = \sigma\delta\lambda^{-1} \in A_3$. Thus, if $\sigma \in A_3$ and $\sigma A_3 = \gamma A_3$, then $\gamma \in A_3$. Thus, $\theta(\sigma A_3) = [0] = \theta(\gamma A_3)$. If $\sigma \notin A_3$ and $\sigma A_3 = \gamma A_3$, then by the same reasoning, $\gamma = \sigma\delta\lambda^{-1} \notin A_3$. Thus, $\theta(\sigma A_3) = [1] = \theta(\gamma A_3)$. Hence, θ is well defined.

Now assume $\theta(\sigma A_3) = (\gamma A_3)$. Then either $\sigma, \gamma \in A_3$ or $\sigma, \gamma \notin A_3$. In the former case, we have that $\sigma, \gamma \in A_3$ and thus $\sigma A_3 = A_3 = \gamma A_3$. In the latter case where $\sigma, \gamma \notin A_3$, then since $[S_3 \colon A_3] = 2$ it follows that $\sigma A_3 = \gamma A_3 \neq A_3$. Thus, θ is 1-1.

We can see that $\theta(A_3) = [0]$ and $\theta((12)A_3) = [1]$ and thus θ is onto.

Finally, we see that for $\sigma A_3, \gamma A_3 \in S_3/A_3$ we have three cases:

(i) $\sigma, \gamma \in A_3$. In this case we have that

$$\theta(\sigma A_3 \gamma A_3) = \theta((\sigma\gamma)A_3) = [0] = [0] + [0] = \theta(\sigma A_3) + \theta(\gamma A_3).$$

(ii) $\sigma \in A_3$, $\gamma \notin A_3$. In this case we have that

$$\theta(\sigma A_3 \gamma A_3) = \theta((\sigma\gamma)A_3) = [1] = [0] + [1] = \theta(\sigma A_3) + \theta(\gamma A_3).$$

(iii) $\sigma, \gamma \notin A_3$. In this case we have that

$$\theta(\sigma A_3 \gamma A_3) = \theta((\sigma\gamma)A_3) = [0] = [1] + [1] = \theta(\sigma A_3) + \theta(\gamma A_3).$$

Therefore, θ is an isomorphism and $S_3/A_3 \cong \mathbb{Z}_2$. Now note that since $o(A_3) = 3$, then by hw 1, A_3 is Abelian. Also, since $\mathbb{Z}_2$ is Abelien, then $A_3 \times \mathbb{Z}_2$ is Abelian. However, S_3 is not Abelian. Thus, $S_3 \ncong A_3 \times \mathbb{Z}_2$. $\square$

(c) If G is cyclic then $\text{Aut}(G)$ is cyclic.

Proof. This is not always the case. Let G be a cyclic group of order 21. Then from hw 5, $\text{Aut}(G) \cong \mathbb{Z}_{(21)}$. We have that $o(\mathbb{Z}_{(21)}) = 12$. In order for $\text{Aut}(G)$ to be cyclic, it must be the case that $\mathbb{Z}_{(21)}$ is cyclic. However, we have that

$$
\begin{aligned}
\langle[1]\rangle &= \{[1]\} & \langle[11]\rangle &= \{[1],[2],[4],[8],[11],[16]\} \\
\langle[2]\rangle &= \{[1],[2],[4],[8],[11],[16]\} & \langle[13]\rangle &= \{[1],[13]\} \\
\langle[4]\rangle &= \{[1],[4],[16]\} & \langle[16]\rangle &= \{[1],[4],[16]\} \\
\langle[5]\rangle &= \{[1],[4],[5],[16],[17],[20]\} & \langle[17]\rangle &= \{[1],[4],[5],[16],[17],[20]\} \\
\langle[8]\rangle &= \{[1],[8]\} & \langle[19]\rangle &= \{[1],[4],[10],[13],[16],[19]\} \\
\langle[10]\rangle &= \{[1],[4],[10],[13],[16],[19]\} & \langle[20]\rangle &= \{[1],[20]\}.
\end{aligned}
$$

From this we can see that $\mathbb{Z}_{(21)}$ has no generator and is therefore not cyclic. Thus, $\text{Aut}(G)$ is not cyclic. □

(d) If $G/Z(G)$ is cyclic, then G is Abelian.

Proof. Since $G/Z(G)$ is cyclic, then for some $g \in G$, $\langle gZ(G)\rangle = G/Z(G)$. Now let $x, y \in G$, then for some $k, m \in \mathbb{Z}^+$, and $h, h' \in Z(G)$, we have $x = g^k h$ and $y = g^m h'$. Thus,

$$xy = g^k h g^m h' = g^k g^m h h' = g^{k+m} h' h = g^{m+k} h' h = g^m g^k h' h = g^m h' g^k h = yx.$$

Therefore, G is Abelian. □

(e) If $o(G) = n$, $m > 0$ and $m \mid n$, then G has a subgroup H, with $o(H) = m$.

Proof. This is not always the case. As we saw in part (c), $o(\mathbb{Z}_{(21)}) = 12$ and we have that $4 \mid 12$. However, $\mathbb{Z}_{(21)}$ does not have a subgroup of order 4. □

(f) If $k > 0$ and $k \mid n$, then $\mathbb{Z}_n$ has a unique subgroup of order k.

Proof. This is not always the case. Let $G = \mathbb{Z}_{12}$. Then we have that $3 \mid o(\mathbb{Z}_{12})$, however, $o(\langle 4\rangle) = 3 = o(\langle 8\rangle)$. □

5. Assume that G is a finite group, p is prime, $p \mid o(G)$, and for all $a, b \in G$, $(ab)^p = a^p b^p$.

(a) Prove, by induction, that for all $a, b \in G$, and for all $k \in \mathbb{Z}^+$, $(ab)^{p^k} = a^{p^k} b^{p^k}$.

Proof. Let $P(n) := (ab)^{p^k} = a^{p^k} b^{p^k}$. The case where $k = 1$ is given by our assumption.

<u>Base Case:</u> Let $k = 2$. Then $(ab)^{p^2} = \big((ab)^p\big)^p = \big(a^p b^p\big)^p$. Since $a^p, b^p \in G$, then by our assumption we have that $\big(a^p b^p\big)^p = (a^p)^p (b^p)^p = a^{p^2} b^{p^2}$. Therefore, $P(2)$ holds.

<u>Inductive Step:</u> Let $k > 2$ and assume that $P(k)$ holds. Then we have that $(ab)^{p^k} = a^{p^k} b^{p^k}$. We can then consider when we have $k+1$ and see that

$$(ab)^{p^{k+1}} = (ab)^{p^k p} = \left((ab)^{p^k}\right)^p = (a^{p^k} b^{p^k})^p = a^{p^k p} b^{p^k p} = a^{p^{k+1}} b^{p^{k+1}}.$$

Thus, if $P(k)$ holds then $P(k+1)$ holds. Therefore, $P(n)$ holds for all $a, b \in G$ and for all $n \in \mathbb{Z}^+$, $P(n)$ holds. $\square$

(b) Let $o(G) = p^m t$, where $(p,t) = 1$. Define $\theta \colon G \to G$ by $\theta(g) = g^{p^m}$. Prove that θ is a homomorphism.

Proof. Since G is closed, then for each $g \in G$, we have that $g^{p^m} \in G$. Thus, $\theta(G) \subseteq G$. Now let $h, g \in G$, then $\theta(gh) = (gh)^{p^m}$. Since $p \mid o(G)$ and $g, h \in G$, then by (a) it follows that $(gh)^{p^m} = g^{p^m} h^{p^m} = \theta(g)\theta(h)$. Therefore, θ is a homomorphsim. $\square$

(c) Prove that $o(\ker\theta) = p^m$.

Proof. Let $g \in \ker\theta$. Then $\theta(g) = g^{p^m} = e$. Thus, $o(g) \mid p^m$. Now let $g \in G$ such that $o(g) \mid p^m$. Then $g^{p^m} = e$ and thus $\theta(g) = e$, and so $g \in \ker\theta$. Therefore, $g \in \ker\theta$ iff $o(g) \mid p^m$.

Let P be a p-Sylow subgroup of G. Then $o(P) = p^m$ and for every $x \in P$, we have that $o(x) \mid p^m$. Thus, for any $x \in P$, it follows that $\theta(x) = x^{p^m} = e$. Hence, $x \in \ker\theta$. Therefore, $P \subseteq \ker\theta$.

If we let $a, b \in \ker\theta$ such that $a, b \in P$, then since P is a group, we have that $ab^{-1} \in P$. Thus, $P \subseteq_g \ker\theta$. By Lagrange's Theorem, $o(P) \mid o(\ker\theta)$. Thus, $o(\ker\theta) = kp^m$. Since $o(G) = p^m t$ and $(p,t) = 1$, then it cannot be the case that $p \mid k$. Otherwise, $o(\ker\theta)$ would contain a power of p greater than that which occurs in the order of G and this is not possible since $o(\ker\theta) \mid p^m t$.

If q is a prime distinct from p and $q \mid k$, then by Cauchy's Theorem, there exists some $y \in \ker\theta$ such that $o(y) = q$. However, since $(q,p) = 1$, then $q \nmid p^m$. Thus, $o(y) \nmid p^m$ and so by the above equivalence, $y \notin \ker\theta$ and k contains no powers of p, nor does it contain any prime factors distinct from p. Hence, $k = 1$. Therefore, $\ker\theta = p^m$. $\square$

(d) Prove that if P is a p-Sylow subgroup of G, then $P \triangleleft G$.

Proof. In (c) we showed that if P is any p-Sylow subgroup of G, then $P \subseteq_g \ker\theta$ and $o(P) = o(\ker\theta)$. Thus, $P = \ker\theta$. Additionally, we know that if $f \colon G \to H$ is a group homomorphism, then $\ker f \triangleleft G$. Thus, since θ is a group homomorphism, then $\ker\theta \triangleleft G$ and so $P \triangleleft G$. $\square$

(e) Let $N = \theta(G)$. Prove that if $N \triangleleft G$ and that G is the direct product of P and N.

Proof. By the FHT, $G/\ker\theta \cong \theta(G)$ and thus $o(G/\ker\theta) = o(\theta(G)) = t$. Now let $x \in G$ and take $g^{p^m} \in \theta(G)$. Then $(xgx^{-1})^{p^m} = (xgx^{-1})(xgx^{-1}) \cdots (xgx^{-1})$. Cancelling out the x's, we find that $(xgx^{-1})^{p^m} = xg^{p^m}x^{-1}$. Thus, since $(xgx^{-1})^{p^m} \in N$, then $xg^{p^m}x^{-1} \in N$. Hence, $N \triangleleft G$. Now note that for any $g \in P$ such that $g \neq e$, we have that $o(g) \mid p^m$ and for any $h \in N$ such that $h \neq e$, we have that $o(h) \mid t$. Now suppose there exists $x \in N \cap P$ such that $x \neq e$. Then $o(x) \mid p^m$. Thus, there exists $k \in \mathbb{Z}$ such that $0 < k \leq m$ and $o(x) = p^k$. We also have that $o(x) \mid t$. Thus, $p^k \mid t$. Hence, for some $r \in \mathbb{Z}$, $t = p^k r = p(p^{k-1}r)$. Thus, $p \mid t$. This is not possible since $(p,t) = 1$. Thus, $N \cap P = \{e\}$. Therefore, $G = NP$. $\square$

2. Assume that G is an Abelian group, $o(G) = 3^8$, and that if $g \in G$, then $o(g) \leq 3^4$.

(a) Find all the possibilities for G.

Proof. By the restriction that for all $g \in G$, $o(g) \leq 3^4$, we have precluded the possibility of $G \cong \mathbb{Z}_{3^8}$. We now appeal to the Fundamental Theorem of Finite Abelian Groups we proved on pages 26-28. From this theorem the possibilities of G can be first written as

$$
\begin{array}{llll}
(3^4, 3^4) & (3^4, 3^3, 3) & (3^4, 3^2, 3^2) & (3^4, 3^2, 3, 3) \\
(3^4, 3, 3, 3, 3) & (3^3, 3^3, 3^2) & (3^3, 3^3, 3, 3) & (3^3, 3^2, 3^2, 3) \\
(3^3, 3^2, 3, 3, 3) & (3^3, 3, 3, 3, 3, 3) & (3^2, 3^2, 3^2, 3^2) & (3^2, 3^2, 3^2, 3, 3) \\
(3^2, 3^2, 3, 3, 3, 3) & (3^2, 3, 3, 3, 3, 3, 3) & (3, 3, 3, 3, 3, 3, 3, 3) & .
\end{array}
$$

Thus, the possibilities for G are

$$
\begin{array}{l}
\mathbb{Z}_{81} \times \mathbb{Z}_{81} \\
\mathbb{Z}_{81} \times \mathbb{Z}_{27} \times \mathbb{Z}_3 \\
\mathbb{Z}_{81} \times \mathbb{Z}_9 \times \mathbb{Z}_9 \\
\mathbb{Z}_{81} \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\
\mathbb{Z}_{81} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\
\mathbb{Z}_{27} \times \mathbb{Z}_{27} \times \mathbb{Z}_9 \\
\mathbb{Z}_{27} \times \mathbb{Z}_{27} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\
\mathbb{Z}_{27} \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \\
\mathbb{Z}_{27} \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\
\mathbb{Z}_{27} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\
\mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \\
\mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\
\mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\
\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \\
\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \quad .
\end{array}
$$

□

(b) Determine the number and the types of all Abelian groups of order $2^6 5^2 7^3$.

Proof. To determine this number, we count the number of ways we can partition 6, 2, and 3 and the answer will be the product of these 3 numbers. Thus, for 6 we have $6 : (6), (5, 1), (4, 2), (4, 1, 1), (3, 3), (3, 2, 1), (3, 1, 1, 1), (2, 2, 2),$ $(2, 2, 1, 1), (2, 1, 1, 1, 1, 1, 1), (1, 1, 1, 1, 1, 1)$. So there are 11 partitions for 6. For 2, we have $(2), (1, 1)$ so there are 2 partitions of 2. Lastly, for 3, we have $(3), (2, 1), (1, 1, 1)$ and so there are 3. Hence, the number of Abelian groups of order $2^6 5^2 7^3$ is $11 \times 2 \times 3 = 66$. □