

# MATH 100A: Homework #9

Due on December 7, 2023 at 12:00pm

*Professor McKernan*

Section A02 5:00PM - 5:50PM

Section Leader: Castellano

Source Consulted: Textbook, Lecture, Discussion, [math.stackexchange.com](https://math.stackexchange.com)

**Ray Tsai**

A16848188

## Problem 1

In  $S_3$ , the symmetric group of degree 3, find all the conjugacy classes, and check the validity of the class equation by determining the orders of the centralizers of the elements of  $S_3$ .

*Proof.* The conjugacy classes of symmetric are defined by cycle types. In this case, the conjugacy classes of  $S_3$  are exactly

$$\{()\}, \{(1, 2), (1, 3), (2, 3)\}, \{(1, 2, 3), (1, 3, 2)\}.$$

Since the identity commutes with all elements, each two cycle only commutes with itself and the identity, and the three cycles commutes with each other and the identity, the orders of the centralizers of each size of the cycles are 6, 2, 3, respectively. Therefore, the class equation

$$|S_3| = \sum_a \frac{|S_3|}{|C(a)|} = 6 \left( \frac{1}{6} + \frac{1}{2} + \frac{1}{3} \right) = 6$$

is indeed valid. We can also observe that for each  $a \in S_3$ ,  $\frac{|S_3|}{|C(a)|} = |[a]|$ , which confirms the class equation in an alternative manner.  $\square$

## Problem 2

Do Problem 1 for  $G$  the dihedral group of order 8

*Proof.* We again first list out all conjugacy classes, namely

$$\{I\}, \{R, R^3\}, \{R^2\}, \{F_1, F_3\}, \{F_2, F_4\}.$$

For  $a \in G$ , the index of  $C(a)$  is equal to the size of the conjugacy class of  $a$ , and thus  $|C(a)| = \frac{|G|}{|[a]|}$ . Therefore, the class equation

$$|G| = \sum_a \frac{|S_3|}{|C(a)|} = \sum_a |[a]| = 8.$$

Thus, the class equation is indeed correct. □

### Problem 3

If  $a \in G$ , show that  $C(x^{-1}ax) = x^{-1}C(a)x$ .

*Proof.* Let  $g \in C(x^{-1}ax)$ , we know  $gx^{-1}ax = x^{-1}axg$ . Rearranged, we get  $(xgx^{-1})a = a(xgx^{-1})$ , which implies  $xgx^{-1} \in C(a)$ . Thus, we know  $g \in x^{-1}C(a)x$ , and so  $C(x^{-1}ax) \subseteq x^{-1}C(a)x$ .

We now prove the converse. Let  $h \in C(a)$ . We know  $h = aha^{-1}$ . Since

$$\begin{aligned} (x^{-1}hx)x^{-1}ax &= x^{-1}hax \\ &= x^{-1}ahx \\ &= x^{-1}a(xx^{-1})h(aa^{-1})x \\ &= x^{-1}ax(x^{-1}aha^{-1}x) \\ &= x^{-1}ax(x^{-1}hx), \end{aligned}$$

$x^{-1}hx$  commutes with  $x^{-1}ax$ , and so  $x^{-1}hx \in C(x^{-1}ax)$ . Therefore, we have  $C(x^{-1}ax) = x^{-1}C(a)x$ .  $\square$

## Problem 4

If  $\varphi$  is an automorphism of  $G$ , show that  $C(\varphi(a)) = \varphi(C(a))$  for  $a \in G$ .

*Proof.* Let  $g' \in C(\varphi(a))$ , and let  $g \in G$  such that  $\varphi(g) = g'$ . Since  $\varphi(ga) = \varphi(g)\varphi(a) = \varphi(g)\varphi(a) = \varphi(ag)$ , we know  $a$  and  $g$  commute. Thus,  $g \in C(a)$ , and so  $g' = \varphi(g) \in \varphi(C(a))$ .

We now prove the converse. Let  $h' \in \varphi(C(a))$ , and let  $h \in G$  such that  $\varphi(h) = h'$ . We know  $h \in C(a)$ . Thus,  $\varphi(a)\varphi(h) = \varphi(ah) = \varphi(ha) = \varphi(h)\varphi(a)$ , and so  $h' = \varphi(h) \in C(\varphi(a))$ .

Since  $C(\varphi(a)) \subseteq \varphi(C(a))$  and  $\varphi(C(a)) \subseteq C(\varphi(a))$ , we have  $C(\varphi(a)) = \varphi(C(a))$ . □

## Problem 5

If  $|G| = p^3$  and  $|Z(G)| \geq p^2$ , prove that  $G$  is abelian.

*Proof.* Since  $Z(G)$  is a subgroup,  $|Z(G)| \mid p^3$ , by Lagrange's Theorem. However,  $|Z(G)| \geq p^2$ , so  $|Z(G)|$  must be either  $p^2$  or  $p^3$ . Suppose for the sake of contradiction that  $|Z(G)| = p^2$ . Let  $x \in G \setminus Z(G)$ . Since,  $x \in C(x)$  and  $Z(G) \subset C(x)$ , we know  $|C(x)| > p^2$ , so  $|C(x)| = p^3$ , which forces  $C(x) = G$ . This implies that  $x$  commutes with all elements in  $G$ , so  $x \in Z(G)$ , contradiction. Therefore,  $|Z(G)| = p^3$ , and so  $G$  is abelian.  $\square$

## Problem 6

Prove that  $N(x^{-1}Hx) = x^{-1}N(H)x$ , where  $N(H) = \{x \in G \mid x^{-1}Hx = H\}$ .

*Proof.* Let  $g \in N(x^{-1}Hx)$ . We know  $gx^{-1}Hx = x^{-1}Hxg$ . Rearranged, we get  $xgx^{-1}H(xgx^{-1})^{-1} = H$ , which implies  $xgx^{-1} \in N(H)$ . Thus, we have  $g \in x^{-1}N(H)x$ .

We now prove for the converse. Let  $k \in x^{-1}N(H)x$ . We know  $xkx^{-1} \in N(H)$ , which implies  $(xkx^{-1})H(xkx^{-1})^{-1} = H$ . Rearranged, we get  $kx^{-1}Hxk = x^{-1}Hx$ , and thus  $k \in N(x^{-1}Hx)$ .

Therefore, we have shown that  $N(x^{-1}Hx) = x^{-1}N(H)x$ . □

## Problem 7

Show that a group of order 36 has a normal subgroup of order 3 or 9.

*Proof.* Let  $G$  be a group of order 36. By Sylow's Theorem,  $G$  has a subgroup  $P$  of order 9. Let  $L = \{kP \mid k \in G\}$ , the set of left cosets of  $P$ . Note that  $|L| = [G : P] = 4$ . Define an action of  $G$  on  $L$  as  $(g, kP) \rightarrow gkP$ . We then get an representation  $\phi : G \rightarrow \text{Aut}(L) \simeq S_4$ ,  $\phi(g) = \sigma_g$ , where  $\sigma_g(kP) = gkP$ . Thus,  $G$  contains a normal subgroup  $\text{Ker } \phi$ . Note that  $\text{Ker } \phi$  cannot be trivial, otherwise  $\frac{|G|}{|\text{Ker } \phi|} = 36 > 24 = |S_4|$ . Let  $g \in \text{Ker } \phi$ . Then,  $\sigma_g(kP) = gkP = kP$ , so  $k^{-1}gk \in P$ , for all  $k \in G$ . Consider  $k = 1$ .  $g \in P$ , and so  $\text{Ker } \phi \subset P$ . However,  $P$  is of order  $3^2$ , so the order of  $\text{Ker } \phi$  is either 3 or 9, and this completes the proof.  $\square$



## Problem 8

Show that a group of order 108 has a normal subgroup of order 9 or 27.

*Proof.* Let  $G$  be a group of order 108. By Sylow's Theorem,  $G$  has a subgroup  $P$  of order 27. Let  $L = \{kP \mid k \in G\}$ , the set of left cosets of  $P$ . Note that  $|L| = [G : P] = 4$ . Define an action of  $G$  on  $L$  as  $(g, kP) \rightarrow gkP$ . We then get an representation  $\phi : G \rightarrow \text{Aut}(L) \simeq S_4$ ,  $\phi(g) = \sigma_g$ , where  $\sigma_g(kP) = gkP$ . Thus,  $G$  contains a normal subgroup  $\text{Ker } \phi$ . Let  $g \in \text{Ker } \phi$ . Then,  $\sigma_g(kP) = gkP = kP$  for all  $k \in G$ , so  $k^{-1}gk \in P$ . Consider  $k = 1$ .  $g \in P$ , and so  $\text{Ker } \phi \subset P$ . However,  $P$  is a subgroup of order  $3^3$ , so the order of  $\text{Ker } \phi$  is either 1, 3, 9 or 27. Since the image of  $\phi$  is a subgroup in  $S_4$ ,  $\frac{|G|}{|\text{Ker } \phi|} \mid |S_4|$ . Therefore, we know that  $|\text{Ker } \phi|$  cannot be 1 or 3, so it must be 9 or 27, and we are done.  $\square$

## Problem 9

Let  $K \subset H \subset G$  be three groups. True or False? If true then give a proof and if false then give a counterexample.

- (i) If  $K$  is characteristically normal in  $H$  and  $H$  is characteristically normal in  $G$  then  $K$  is characteristically normal in  $G$ .

*Proof.* True. Let  $\phi$  be an automorphism of  $G$ . Since  $H$  is characteristically normal in  $G$ ,  $\phi(H) = H$ . Thus, the function  $\psi : H \rightarrow H$ ,  $\psi(h) = \phi(h)$  is an automorphism. Since  $K$  is characteristically normal in  $H$ ,  $\phi(K) = \psi(K) = K$ , and thus  $K$  is characteristically normal in  $G$ .  $\square$

- (ii) If  $K$  is normal in  $H$  and  $H$  is characteristically normal in  $G$  then  $K$  is normal in  $G$ .

*Proof.* False. Consider  $G = A_3 \times S_3$ , and put  $H = A_3 \times A_3$ . Note that  $[G : H] = 2$ . By Sylow's Theorem, since  $H$  is the only Sylow 3-subgroup in  $G$ ,  $H$  is characteristically normal. Let  $K = \langle ((1, 2, 3), (1, 2, 3)) \rangle$ . Since both 3-cycles and the identity are abelian,  $H$  is abelian, so  $K$  is normal in  $H$ . However, notice that  $((1, 2), ())((1, 2, 3), (1, 2, 3))((1, 2), ())^{-1} = ((1, 2)(1, 2, 3), (1, 2, 3)) = ((1, 3, 2), (1, 2, 3)) \notin K$ , so  $K$  is not normal in  $G$ .  $\square$

- (iii) If  $K$  is characteristically normal in  $H$  and  $H$  is normal in  $G$  then  $K$  is normal in  $G$ .

*Proof.* True. Let  $\phi \in \text{Inn}(G)$ . We know  $\phi(H) = H$ . Thus, we may define an automorphism  $\psi : H \rightarrow H$  as  $\psi(h) = \phi(h)$ . Since  $K$  is characteristically normal in  $H$ ,  $\phi(K) = \psi(K) = K$ , and thus  $K$  is normal in  $G$ .  $\square$

- (iv) If  $K$  is normal in  $H$  and  $H$  is normal in  $G$  then  $K$  is normal in  $G$ .

*Proof.* False. Consider  $G = D_8$ ,  $H = \{I, F_1, F_2, R^2\}$ ,  $K = \{I, F_1\}$ , where  $F_1, F_2$  are horizontal and vertical flips, respectively. Since  $[G : H] = [H : K] = 2$ , we know  $H$  is normal in  $G$ , and  $K$  is normal in  $H$ . However, notice that  $RF_1R^{-1}$  is a diagonal flip, so  $K$  is not normal in  $G$ .  $\square$

## Problem 10

Show that the automorphism group of a cyclic group of order  $n$  is isomorphic to

$$\begin{cases} U_n & \text{if } n \text{ is finite} \\ \mathbb{Z}_2 & \text{otherwise.} \end{cases}$$

*Proof.* Let  $G$  be a cyclic group of order  $n$ , and let  $a \in G$  be its generator. We first consider the finite case. Let  $\phi$  be an automorphism of  $G$ . Suppose that  $\phi(a) = \phi_i(a) = a^i$  for some  $i < n$ . Then,  $\phi(a^k) = \phi(a)^k = a^{ik}$  for all  $a^k \in G$ , and so all automorphisms of  $G$  must be of such form. Since  $\phi$  is surjective, for all  $a^m \in G$ , there exists  $a^k \in G$ , such that  $\phi(a^k) = a^{ik} = a^m$ . This implies that  $a^{ik} - a^m = e$ , and so  $ik - m = nl$ , for some  $l \in \mathbb{Z}$ . Thus, we know that for all  $m \in \mathbb{Z}$ , there exists integers  $k, l$ , such that  $ik - nl = m$ . Since this holds true for the case  $m = 1$ , by the Euclidean Algorithm,  $\text{Aut}(G)$  only contains  $\phi_i$  where  $i$  is relatively prime with  $n$ . We now suppose that  $i$  is coprime to  $n$ . Define  $\psi : G \rightarrow G$  as  $\psi(a^k) = a^{ik}$ .  $\psi$  is obviously well-defined. Since  $\psi(a^k)\phi(a^m) = a^{i(k+m)} = \psi(a^{k+m})$ ,  $\psi$  is an homomorphism. Suppose that  $a^k \in \text{Ker } \psi$ . Then,  $\psi(a^k) = a^{ik} = e$ . Since  $i$  is relatively prime with  $n$ ,  $n \mid k$ , which means that  $a^k = e$ . Since  $\text{Ker } \psi$  is trivial and  $G$  is a finite group,  $\psi$  is an automorphism. Therefore, we know that  $\text{Aut}(G) = \{\phi_i \mid \gcd(i, n) = 1\}$ . Define  $\theta : \text{Aut}(G) \rightarrow U_n$  as  $\theta(\phi_i) = i$  and  $\pi : U_n \rightarrow \text{Aut}(G)$  as  $\pi(i) = \phi_i$ . Note that  $\phi_i \circ \phi_j(a^k) = \phi_i(a^{jk}) = a^{ijk} = \phi_{ij}(a^k)$ . Since  $\theta(\phi_i)\theta(\phi_j) = ij = \theta(\phi_{ij})$  and  $\pi(i)\pi(j) = \phi_i\phi_j = \phi_{ij} = \pi(ij)$ ,  $\theta$  and  $\pi$  are both homomorphisms. Since both  $\theta$  and  $\pi$  are obviously well-defined functions and are each other's inverse,  $\theta$  is an isomorphism. Therefore,  $\text{Aut}(G) \simeq U_n$  when  $n$  is finite.

We now consider the infinite case. Let  $\phi$  be an automorphism of  $G$ . Suppose that  $\phi(a) = \phi_i(a) = a^i$ , for some  $i \in \mathbb{Z}$ . Since  $\phi$  is surjective, for all  $a^m \in G$ , there exists  $a^k$ , such that  $\phi(a^k) = a^{ik} = a^m$ . Notice that  $i \in \{1, -1\}$ , otherwise there does not exist  $a^k \in G$  such that  $\phi(a^k) = a^{ik} = a^m$ . Since  $\phi$  is simply the identity mapping when  $i = 1$ , and  $\phi$  is the inverse of itself when  $i = -1$ , we have confirmed that  $\phi$  is indeed an automorphism when  $i \in \{1, -1\}$ . Therefore,  $\text{Aut}(G)$  is of order 2, so  $\text{Aut}(G)$  must be isomorphic to  $\mathbb{Z}_2$ .  $\square$

## Problem 11

Classify all groups of order  $n$ , where  $n \in \{11, 13, 14\}$ .

*Proof.* Since 11, 13 are prime, all groups of those orders are cyclic groups. Suppose that a group  $G$  is of order 14. Since  $\mathbb{Z}_{14} \simeq \mathbb{Z}_2 \times \mathbb{Z}_7$ ,  $G$  is cyclic if it is abelian. Otherwise, all subgroups of  $G$  are of order 2 or 7, and we know not all elements are of order 2 by Lemma 20.2. Let  $a \in G$  be a element of order 7, and let  $H = \langle a \rangle$ . Since the index of  $H$  is 2,  $H$  is normal in  $G$ . Let  $b \in G \setminus H$ . Since  $|G/H| = 2$ ,  $b^2 \in H$ . Suppose that  $b^2 \neq e$ . Then,  $b^2 = a^i$ . However, this means  $b^2$  has order 7, which implies that  $b$  has order 14, contradiction. Thus, we know  $b^2 = e$ , and so  $G = \langle a, b \rangle$ . We now consider the conjugate  $bab^{-1}$ . Since  $H$  is normal,  $bab^{-1} \in H$ . We may suppose that  $bab^{-1} = a^i$ , where  $i \neq 0$ . Since  $G$  is not abelian, we also know  $i \neq 1$ . Suppose that  $i = 6$ . Then,  $bab^{-1} = a^{-1}$ , and  $G$  is isomorphic to  $D_7$ . Suppose that  $i \neq 6$ . Then,

$$\begin{aligned} a &= b^2 ab^{-2} \\ &= b(bab^{-1})b^{-1} \\ &= ba^i b^{-1} \\ &= (bab^{-1})^i \\ &= a^{i^2}. \end{aligned}$$

This means that  $a^{i^2-1} = e$ , and so  $i^2 - 1$  must divide 7. However, none of 2, 3, 4, 5 meets the requirement, and thus  $G$  is either cyclic or isomorphic to  $D_7$ .  $\square$