ALGEBRA HW 1

CLAY SHONKWILER

1

Define the *center* of a group G to be $Z = \{g \in G | (\forall h \in G) gh = hg\}$.

(a) Is Z a subgroup? Is it normal?

Answer: Yes to both questions. To demonstrate that Z is a subgroup, we must demonstrate that it is closed under the group operation and that each element in the center has an inverse in the center (since associativity will be inherited and the identity is clearly in the center). To that end, let $a, b \in Z$ and let $h \in G$. Then

$$h(ab)h^{-1} = hah^{-1}hbh^{-1} = ab,$$

so Z is closed under the group operation. Now, let $a \in Z$. Then a has an inverse a^{-1} in G; we want to show that $a^{-1} \in Z$. Let $h \in G$. Then

$$(ha^{-1}h^{-1})^{-1} = hah^{-1} = a,$$

which implies that $ha^{-1}h^{-1} = a^{-1}$, so $a^{-1} \in Z$. Therefore, we conclude that Z is, in fact, a subgroup of G. Furthermore, the calculation we did above to demonstrate that Z is closed under the group operation is precisely the calculation necessary to demonstrate that Z is normal in G.

♣

(b) Find the center of C_n, D_n, S_n, A_n, Q, $\mathbb{Z}$, $GL_2(\mathbb{R})$.

Answer: Let $a \in C_n$. Then, for all $b \in C_n$, $ab = ba$, since C_n is abelian. Since our choice of a was arbitrary, we see that the center of C_n is C_n itself.

Consider D_n under the presentation $\langle x, y | x^n = y^2 = 1, yxy^{-1} = x^{-1} \rangle$. Then if $\sigma, \tau \in D_n$, there exist $i, j \in \{0, \ldots, n-1\}$, $a, b \in \{0, 1\}$ such that $\sigma = x^i y^a$, $\tau = x^j y^b$. Then if $a = b = 1$,

$$\sigma\tau = x^i y^a x^j y^b = x^i x^{-j} y^a y^b = x^{i-j} y^{a+b}$$

and

$$\tau\sigma = x^j y^b x^i y^a = x^j x^{-i} y^b y^a = x^{j-i} y^{a+b}.$$

If σ in the center of D_n, then it must be the case that $x^{i-j} = x^{j-i}$ for all choices of j; Clearly this is impossible. On the other hand, if $a = 0$, then

$$\sigma\tau = x^i x^j y^b = x^{i+j} y^b$$

and

$$\tau\sigma = x^j y^b x^i = \begin{cases} x^{j-i} y^b & \text{if } b = 1 \\ x^{j+i} & \text{if } b = 0. \end{cases}$$

If σ in the center of D_n, then it must be the case that

$$i + j \equiv j - i(\mod n)$$

for all choices of j. This, in turn, implies that $2i \equiv 0(modn)$, which is to say that $i = n/2$, which is only possible if n is even. Therefore, we conclude that the center of D_n is trivial when n is odd and is $\{1, x^{n/2}\}$ when n is even.

Since $S_2 = C_2$, the center of S_2 is itself. If $n \geq 3$, let $\sigma \in S_n$. We can write σ as the product of a unique decomposition of disjoint cycles, $\sigma = \zeta_1 \cdots \zeta_j$. If $j = 1$ and σ is just a transposition, then

$$\sigma = \zeta_1 = (ab)$$

for some $a, b \in \{1, \ldots, n\}$. Then

$$(bc)\sigma = (bc)(ab) = (acb) \neq (abc) = (ab)(bc) = \sigma(bc),$$

so σ is not in the center of S_n. If $j > 1$, then we know that $\zeta_1 = (a_1 a_2 \ldots a_m)$ for $m \leq n$, $a_i \in \{1, \ldots, n\}$. Then, since a_1 is fixed by ζ_i for $i > 1$ (because the cycle decomposition of σ is into disjoint cycles), the product

$$(a_1 a_2)\sigma = (a_1 a_2)\zeta_1 \cdots \zeta_j = (a_1 a_2)(a_1 a_2 \ldots a_m)\zeta_2 \cdots \zeta_j$$

fixes a_1. On the other hand,

$$\sigma(a_1 a_2) = (a_1 a_2 \ldots a_m)\zeta_2 \cdots \zeta_j(a_1 a_2) = (a_1 a_3 \ldots d)\xi_1 \cdots \xi_k,$$

where $d \in \{1, \ldots, n\}$ and the ξ_l are disjoint cycles. Specifically, a_1 is not fixed by $\sigma(a_1 a_2)$, so we see that σ is not in the center of S_n. Since our choice of σ was arbitrary, we see that the center of S_n is trivial.

When $n \leq 3$, A_n is cyclic and so its center is all of A_n. If $n \geq 4$, let $\sigma \in S_n$. Then we can write σ as the product of disjoint cycles $\sigma = \zeta_1 \cdots \zeta_j$. Suppose ζ_1 is at least a 3-cycle. Then

$$\sigma = \zeta_1 \cdots \zeta_j = (a_1 a_2 a_3 \ldots a_m)\zeta_2 \cdots \zeta_j$$

for $m \geq 3$. Then $(a_1 a_2 a_3) = (a_1 a_3)(a_1 a_2) \in A_n$ and

$$(a_1 a_2 a_3)\sigma = (a_1 a_2 a_3)(a_1 a_2 a_3 \ldots a_m)\zeta_1 \cdots \zeta_j = (a_1 a_3 \ldots d)\xi_1 \cdots \xi_k$$

for $d \in \{1, \ldots, n\}$ and disjoint cycles ξ_l. On the other hand,

$$\sigma(a_1 a_2 a_3) = (a_1 a_2 a_3 \ldots a_m)\zeta_1 \cdots \zeta_j(a_1 a_2 a_3)$$

fixes a_1, so $(a_1 a_2 a_3)\sigma \neq \sigma(a_1 a_2 a_3)$ and so σ is not in the center of A_n. Therefore, if σ is to be in the center of A_n, it must be the case that ζ_1 is a transposition; specifically,

$$\sigma = \zeta_1 \cdots \zeta_j = (b_1 b_2)(b_3 b_4 \cdots b_r)\zeta_3 \cdots \zeta_j$$

for $r \geq 2$. Now, again, $(b_1 b_2 b_3) = (b_1 b_3)(b_1 b_2) \in A_n$ and

$$(b_1 b_2 b_3)\sigma = (b_1 b_2 b_3)(b_1 b_2)(b_3 b_4 \ldots b_r)\zeta_3 \cdots \zeta_j = (b_1 b_3 \ldots c)\xi_1 \cdots \xi_k$$

for $c \in \{1, \ldots, n\}$ and disjoint cycles ξ_l. On the other hand,

$$\sigma(b_1 b_2 b_3) = (b_1 b_2)(b_3 b_4 \ldots b_r)\zeta_3 \cdots \zeta_j(b_1 b_2 b_3)$$

fixes b_1, meaning $(b_1b_2b_3)\sigma \neq \sigma(b_1b_2b_3)$ and so σ is not in the center of A_n. Since ζ_1 must either be a transposition or a cycles of length ≥ 3 and we've just demonstrated that in both cases $\sigma \notin Z$, we conclude that the center of A_n is trivial.

Suppose $a \in Q$. If $a = \pm 1$, the fact that $ag = ga$ for all $g \in Q$ follows directly from the definition of Q. Otherwise, since

$$\begin{aligned} ij &= k \\ ji &= -k \\ ik &= -j \\ ki &= j \end{aligned}$$

we see that a cannot be in the center of Q. Thus, the center of Q is simply $\{1, -1\}$.

Since $\mathbb{Z}$ is abelian, the same argument we gave to show that the center of C_n is the entire group suffices to show that the center of $\mathbb{Z}$ is $\mathbb{Z}$ itself.

To characterize the center of $GL_2(\mathbb{R})$, let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be in the center of $GL_2(\mathbb{R})$ and let $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in GL_2(\mathbb{R})$. Then it must be the case that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$$

is equal to

$$\begin{pmatrix} e & f \\ g & h \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ae + cf & be + df \\ ag + ch & bg + dh \end{pmatrix}.$$

Hence, it must be the case that

$$ae + bg = ae + cf,$$

or

$$bg = cf.$$

Since our choice of B was arbitrary, we see that this relationship must hold for *any* choice of g and f. The only values of b and c for which this is true are if $b = c = 0$. Using this fact, then the equation

$$af + bh = be + df$$

reduces to

$$af = df$$

or $a = d$. Hence, elements in the center of $GL_2(\mathbb{R})$ must be of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. Furthermore, if $a \neq 0$, then

$$C \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aC \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} C = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} C$$

so every matrix of this form is in the center. Hence, the center of $GL_2(\mathbb{R})$ is the set

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} | a \neq 0 \right\}.$$

♣

2

If H is a subgroup of G, define the *normalizer* of H by $N(H) = \{a \in G | aHa^{-1} = H\}$. Is $N(H)$ a subgroup of G? Is H a subgroup of $N(H)$? Is $H \lhd N(H)$? Is $N(H) \lhd G$?

Answer: To demonstrate that $N(H)$ is a subgroup of G, we need to demonstrate that it is closed under the group operation, that the identity is in $N(H)$ and that the inverse of each element in $N(H)$ is in $N(H)$. To that end, let $a, b \in N(H)$ and let $h \in H$. Then we know that $bhb^{-1} = h'$ for some $h' \in H$. Therefore,

$$(ab)h(ab)^{-1} = abhb^{-1}a^{-1} = ah'a^{-1} \in H.$$

Therefore, $ab \in N(H)$. The identity e is clearly in $N(H)$, since

$$ehe^{-1} = ehe = eh = h \in H.$$

Now, suppose $a \in N(H)$ and $h \in H$. Then a has an inverse a^{-1} in G. Furthermore, since $a \in N(H)$, $aHa^{-1} = H$, so there exists $h' \in H$ such that $ah'a^{-1} = h$. Multiplying both sides of this equation by a^{-1} on the left and a on the right, we see that

$$h' = a^{-1}ha = a^{-1}h(a^{-1})^{-1},$$

so $a^{-1} \in N(H)$. Therefore, we conclude that $N(H)$ is a subgroup of G.

To see that H is a subgroup of $N(H)$, it suffices to show that H is contained in $N(H)$, since both H and $N(H)$ are subgroups of G. However, this is clear, since for any $a, b \in H$,

$$bab^{-1} \in H.$$

This implies that $b \in N(H)$. Since our choices of a and b were arbitrary, we see that every element of H is in $N(H)$, and so we conclude that H is a subgroup of $N(H)$.

The fact that $H \lhd N(H)$ follows directly from how we have defined $N(H)$. For any $a \in N(H)$, $aHa^{-1} = H$, which is precisely what it means to say that $H \lhd N(H)$.

To see that it is not necessarily the case that $N(H) \lhd G$, consider the case where $G = S_3$ and $H = \langle (12) \rangle = \{1, (12)\}$. Now,

$$\begin{aligned} (13)(12)(13) &= (23) \\ (23)(12)(23) &= (13) \\ (123)(12)(132) &= (23) \\ (132)(12)(123) &= (13), \end{aligned}$$

so we see that $N(H) = H$. However, the above calculations demonstrate that H is not normal in G, so it's clear that $N(H)$ is not normal in G.

♣

3

(a) If H is a subgroup of G and $H \neq G$, we say that H is a *maximal* subgroup if the only subgroups containing H are itself and G. Show that if H is maximal then so is aHa^{-1}, for any $a \in G$.

Proof. Suppose H is a maximal subgroup of G. Let $a \in G$ and let K be a maximal subgroup containing aHa^{-1}. Let $g \in H$. Then $aga^{-1} \in aHa^{-1} \subseteq K$, which implies that

$$a^{-1}aga^{-1}a = g \in a^{-1}Ka.$$

Since our choice of g was arbitrary, this in turn means that $H \subseteq a^{-1}Ka$. Since $a^{-1}Ka$ is a subgroup of G and H is maximal, either $a^{-1}Ka = G$ or $a^{-1}Ka = H$. In the first case, $K = G$, which is impossible, since K is a maximal subgroup, and in the second case, $K = aHa^{-1}$, which implies that aHa^{-1} is a maximal subgroup. Since our choice of a was arbitrary, we see that aHa^{-1} is maximal for all $a \in G$. □

(b) Define the *Frattini* subgroup Φ of G to be the intersection of the maximal subroups of G. Show that $\Phi \lhd G$.

Proof. Let $g \in \Phi$ and let $a \in G$. Let H be a maximal subgroup of G. Then $g \in H$. Furthermore, by part (a) above, $a^{-1}Ha$ is also a maximal subgroup of G, meaning that $g \in a^{-1}Ha$. Now, since

$$a(a^{-1}Ha)a^{-1} = H,$$

$aga^{-1} \in H$. Since our choice of H was arbitrary, we see that aga^{-1} is an element of every maximal subgroup of G, which means that $aga^{-1} \in \Phi$. Since our choices of a and g were arbitrary, this in turn implies that $a\Phi a^{-1} \subseteq \Phi$ for all $a \in G$, so $\Phi \lhd G$. □

(c) Find the Frattini subgroup Φ of D_4, C_4, and Q. In each case, find G/Φ. Conjecture?

Answer: On the attached sheet are reproduced complete subgroup diagrams for each of these groups. From these, we can conclude that the Frattini subgroup of D_4 is $\{1, x^2\}$, of C_4 is $\{1, a^2\}$ and of Q is $\{\pm 1\}$. It's immediately clear, simply on the basis of order considerations, that $C_4/\Phi \simeq C_2$, since this is the only group of order 2. As for D_4/Φ, we can derive a group presentation for D_4/Φ by adding the relation $x^2 = 1$ to the presentation for D_4, yielding

$$\langle x, y | x^2 = y^2 = 1, yxy = x \rangle = \langle x, y | x^2 = y^2 = 1, yx = xy \rangle \simeq C_2 \times C_2.$$

As for Q, taking the quotient by $\Phi = \{\pm 1\}$ means that, viewed as elements of Q/Φ, $i^2 = j^2 = k^2 = 1$. Since Q/Φ has order 4 and contains three elements of order 2, it must be the case that $Q/\Phi \simeq C_2 \times C_2$ as well.

♣

4

(a) If $x \in G$, define its *centralizer* $C(x) = \{g \in G | xg = gx\}$. Show that $C(x)$ is a subgroup of G, and that its index $(G : C(x))$ equals the number of elements in the conjugacy class $\{gxg^{-1} | g \in G\}$ of x.

Proof. To show that $C(x)$ is a subgroup, we need to demonstrate that it is closed under the group operation, contains the identity and, for each element in $C(x)$, there is an inverse of that element in $C(x)$. Let $x \in G$ and let $g, h \in C(x)$. Then

$$x(gh) = (xg)h = (gx)h = g(xh) = g(hx) = (gh)x$$

which implies that $gh \in C(x)$. Since our choice of g and h was arbitrary, we see $C(x)$ is closed under the group operation.

Now, obviously $1c = c1 = c$, so $1 \in C(x)$.

Finally, let $g \in C(x)$. Then g has an inverse, g^{-1}, in G. Then, since $g \in C(x)$, $xg = gx$, which in turn implies that $x = gxg^{-1}$. Multiplying on the left by g^{-1}, we see that

$$g^{-1}x = xg^{-1},$$

which is to say that $g^{-1} \in C(x)$.

Having shown that $C(x)$ is a subgroup of G, we move on to showing that $(G : C(x))$ equals the number of elements in the conjugacy class of x. To that end, let's define a map

$$f : \{\text{left cosets of } C(x)\} \to \{gxg^{-1} | g \in G\}$$

where, if $aC(x)$ is a left coset of $C(x)$, then we choose a representative $h \in aC(x)$ and let

$$f(aC(x)) = hxh^{-1}.$$

First, we need to check that this map is well-defined. To that end, let $h, h' \in aC(x)$, where $aC(x)$ is a coset of $C(x)$. Then $h = ag$ for some $g \in C(x)$ and $h' = ag'$ for some $g' \in C(x)$. Then

$$hxh^{-1} = (ag)x(ag)^{-1} = agxg^{-1}a^{-1} = axa^{-1}$$

and

$$h'xh'^{-1} = (ag')x(ag')^{-1} = ag'xg'^{-1}a^{-1} = axa^{-1}.$$

Hence, we see that no matter what representative element h we choose from $aC(x)$,

$$f(aC(x)) = hxh^{-1} = axa^{-1},$$

so f is well-defined. On the other hand, we define

$$\overline{f} : \{gxg^{-1} | g \in G\} \to \{\text{left cosets of } C(x)\}$$

given by $\overline{f}(gxg^{-1}) = gC(x)$. Again, we need to check that $\overline{f}$ is well-defined. To that end, suppose $g, h \in G$ such that $gxg^{-1} = hxh^{-1}$. Let $a \in C(x)$. Then

$$\begin{aligned}(ga)x(ga)^{-1} &= g(axa^{-1})g^{-1} \\ &= gxg^{-1} \\ &= hxh^{-1} \\ &= haxa^{-1}h^{-1}.\end{aligned}$$

This implies that $ga = haxa^{-1}h^{-1}gax$; if we can show that $axa^{-1}h^{-1}gax \in C(x)$, then this suffices to show that $gC(x) = hC(x)$. To see this, note that

$$\begin{aligned}(axa^{-1}h^{-1}gax)x(axa^{-1}h^{-1}gax)^{-1} &= (xh^{-1}gax)x(xh^{-1}gax)^{-1} \\ &= xh^{-1}gax(xx^{-1})a^{-1}g^{-1}hx^{-1} \\ &= xh^{-1}g(axa^{-1})g^{-1}hx^{-1} \\ &= xh^{-1}(gxg^{-1})hx^{-1} \\ &= xh^{-1}(hxh^{-1})hx^{-1} \\ &= xxx^{-1} \\ &= x,\end{aligned}$$

so, indeed, $axa^{-1}h^{-1}gax \in C(x)$ and thus $\overline{f}$ is well-defined. Finally, we see that

$$f \circ \overline{f}(gxg^{-1}) = f(gC(x)) = gxg^{-1}$$

and

$$\overline{f} \circ f(gC(x)) = \overline{f}(gxg^{-1}) = gC(x),$$

which means $f \circ \overline{f} = id$ and $\overline{f} \circ f = id$. Therefore, the cardinalities of the set of cosets of $C(x)$ and the conjugacy class of x are equal or, stated another way,

$$(G : C(x)) = \#\{gxg^{-1} | g \in G\}.$$

□

(b) Consider the conjugacy classes in G that have more than one element. Chose one element from each such class, and gather them together as a set S. Show that $\#G = \#Z + \sum_{x \in X}(G : C(x))$, where Z is the center of G.

Proof. First, suppose the $x \in G$ such that the conjugacy class of x is a single element. It's clear that, if e is the identity in G, $exe = x$, so x is in it's own conjugacy class. Therefore, the conjugacy class of x is simply $\{x\}$. This implies that $gxg^{-1} = x$ for all $g \in G$. Multiplying both sides of this equation on the right by g, we see that $gx = xg$, which is to say $x \in Z$, the center of G.

Now, suppose $x \in G$ has a conjugacy class with more than one element in it. Let y, z be in the conjugacy class of x. Then there exist $g, h \in G$ such that $y = gxg^{-1}$, $z = hxh^{-1}$. Then $x = h^{-1}zh$, so

$$y = gxg^{-1} = g(h^{-1}zh)g^{-1} = (gh^{-1})z(gh^{-1})^{-1};$$

in other words, y and z are in eachother's conjugacy classes. Since our choices of y and z were arbitrary, we see that the conjugacy classes of elements in G form a partition of G. Thus, we can compute the cardinality of

G by summing the cardinalities of these partitions; since Z contains all and only those elements in singleton partitions we could compute this by adding the cardinality of Z to the sum of the cardinalities of the partitions containing more than one element. By part (a) above, we know that the cardinality of each of these partitions can be determined by choosing a representative element x and computing $(G : C(x))$, yielding the equation:

$$\#G = \#Z + \sum_{x \in X} (G : C(x)).$$

□

5

Let H and K be subgroups of G. If $k \in K$, call the subgroup kHk^{-1}a *K-conjugate* of H. Show that the number of K-conjugates of H is $(K : K \cap N(H))$, where $N(H)$ is the normalizer of H.

Proof. Much as we did in 4(a) above, we will construct and invertible set map between C, the set of K-conjugates of H, and L, the set of left cosets of $K \cap N(H)$. Let

$$f : C \to L$$

be given by $f(kHk^{-1}) = k(K \cap N(H)) = \overline{k}$. To see that this is well-defined, suppose $k_1, k_2 \in K$ such that $k_1 H k_1^{-1} = k_2 H k_2^{-1}$. Then we need to demonstrate that $\overline{k_1} = \overline{k_2}$. To this end, let $a \in K \cap N(H)$ and let $h \in H$. Then there exist $h_1, \ldots, h_6 \in H$ such that

$$\begin{aligned} k_1 h k_1^{-1} &= k_2 h_1 k_2^{-1} \\ a h_2 a^{-1} &= h \\ a h_3 a^{-1} &= h_1 \\ h_4 &= a h_2^{-1} a^{-1} \end{aligned}$$

Therefore,

$$\begin{aligned} k_1 a h_2 a^{-1} k_1^{-1} &= k_1 h k_1^{-1} \\ &= k_2 h_1 k_2^{-1} \\ &= k_2 a h_3 a^{-1} k_2^{-1}, \end{aligned}$$

or

$$\begin{aligned} k_1 a &= k_2 a h_3 a^{-1} k_2^{-1} k_1 a h_2^{-1} a^{-1} \\ &= k_2 h_1 k_2^{-1} k_1 h_4. \end{aligned}$$

To show that $\overline{k_1} = \overline{k_2}$, it suffices to show that $b = h_1 k_2^{-1} k_1 h_4 \in K \cap N(H)$. Since $a \in K$, and $k_1 a = k_2 b$, $b = k_2^{-1} k_1 a \in K$. To see that $b \in N(H)$, we need to conjugate some element of H by b. To that end, let $g \in H$ and note that there exist $h_5, h_6 \in H$ such that

$$\begin{aligned} h_5 &= h_4 g h_4^{-1} \\ k_2 h_6 k_2^{-1} &= k_1 h_5 k_1^{-1}. \end{aligned}$$

Therefore,

$$\begin{aligned} bgb^{-1} &= (h_1k_2^{-1}k_1h_4)g(h_1k_2^{-1}k_1h_4)^{-1} \\ &= h_1k_2^{-1}k_1(h_4gh_4^{-1})k_1^{-1}k_2h_1^{-1} \\ &= h_1k_2^{-1}(k_1h_5k_1^{-1})k_2h_1^{-1} \\ &= h_1k_2^{-1}(k_2h_6k_2^{-1})k_2h_1^{-1} \\ &= h_1h_6h_1^{-1} \in H. \end{aligned}$$

Therefore, we conclude that $b \in K \cap N(H)$ and so $\overline{k_1} = \overline{k_2}$.

On the other hand, define

$$\overline{f} : L \to C$$

given by

$$\overline{f}(\overline{k}) = kHk^{-1}.$$

Suppose $\overline{k_1} = \overline{k_2}$. Then there exist $a_1, a_2 \in K \cap N(H)$ such that $k_1a_1 = k_2a_2$. Therefore,

$$\begin{aligned} \overline{f}(\overline{k_1}) = k_1Hk_1^{-1} = k_1(a_1Ha_1^{-1})k_1^{-1} &= (k_1a_1)H(k_1a_1)^{-1} \\ &= (k_2a_2)H(k_2a_2)^{-1} \\ &= k_2(a_2Ha_2^{-1})k_2^{-1} \\ &= k_2Hk_2^{-1} \\ &= \overline{f}(\overline{k_2}), \end{aligned}$$

so $\overline{f}$ is well-defined.

Now, if $k \in K$, then

$$f \circ \overline{f}(\overline{k}) = f(kHk^{-1}) = \overline{k}$$

and

$$\overline{f} \circ f(kHk^{-1}) = \overline{f}(\overline{k}) = kHk^{-1}.$$

Therefore, since we've created an invertible set map between L and C, their cardinalities must be equal, which is to say that the number of K-conjugates of H is $(K : K \cap N(H))$. □

6

Define the *commutator* subgroup G' of G to be the subgroup of G generated by the set $C := \{aba^{-1}b^{-1} | a, b \in G\}$.

(a) Show $G' \lhd G$.

Proof. Since C generates G', if we can show that $cCc^{-1} \subset G'$ for all $c \in G$, that will suffice to show that $G' \lhd G$. To that end, let $g \in G$ and $c \in C$. Then there exist $a, b \in G$ such that $aba^{-1}b^{-1} = c$. Now, we consider what conjugation of c by g looks like:

$$gcg^{-1} = gaba^{-1}b^{-1}g^{-1}.$$

Now, $gag^{-1}a^{-1} \in C$, as is

$$agba^{-1}(gb)^{-1} = agba^{-1}b^{-1}g^{-1}.$$

Now, if we multiply these two elements of C, we see that

$$(gag^{-1}a^{-1})(agba^{-1}b^{-1}g^{-1}) = gaba^{-1}b^{-1}g^{-1} = gcg^{-1}.$$

Thus, gcg^{-1} is the product of two elements of C, meaning that $gcg^{-1} \in G$. Since our choices of g and c were arbitrary, we see that $gCg^{-1} \subset G'$ for all g, which means that $G' \lhd G$. □

(b) Show that G/G' is abelian.

Proof. Let $\overline{a}, \overline{b} \in G/G'$. If we let $a \in \overline{a}, b \in \overline{b}$ be representative elements, then $aba^{-1}b^{-1} \in H$, so

$$\overline{a}\overline{b}\overline{a}^{-1}\overline{b}^{-1} = H,$$

which is the identity in G/G'. This in turn implies that

$$\overline{a}\overline{b} = \overline{b}\overline{a}.$$

Since our choice of $\overline{a}$ and $\overline{b}$ was arbitrary, this implies that G/G' is abelian. □

(c) Find G' and G/G' if $G = \mathbb{Z}, D_4, S_3, C_2 \times C_3$.

Answer: Let $a, b \in \mathbb{Z}$. Since $\mathbb{Z}$ is abelian,

$$a + b + (-a) + (-b) = a + (-a) + b + (-b) = 0.$$

Our choices of a and b were arbitrary, so we see that the commutator subgroup of $\mathbb{Z}$ is trivial, which in turn implies that G/G' is isomorphic to $G = \mathbb{Z}$ in this case.

When $G = D_4$, let $\sigma, \tau \in G$. Then there exist $i, j \in \{0, 1, 2, 3\}$ and $a, b \in \{0, 1\}$ such that $\sigma = x^i y^a$ and $\tau = x^j y^b$. If $a = b = 0$, then

$$\sigma\tau\sigma^{-1}\tau^{-1} = x^i x^j x^{-i} x^{-j} = x^{i+j-i-j} = x^0 = 1.$$

If $a = b = 1$, then

$$\sigma\tau\sigma^{-1}\tau^{-1} = x^i y x^j y x^{-i} y x^{-j} y = x^i x^{-j} y y x^{-i} x^j y y = x^{i-j} x^{j-i} = x^{i-j+j-i} = x^0 = 1.$$

If $a = 1, b = 0$, then

$$\sigma\tau\sigma^{-1}\tau^{-1} = x^i y x^j x^{-i} y x^{-j} = x^{i-j} y x^{j-i} y = x^{i-j} x^{i-j} y^2 = x^{2(i-j)}.$$

Since $2k(\mod 4)$ is either 0 or 2, this implies that either $\sigma\tau\sigma^{-1}\tau^{-1}$ is equal to 1 or x^2. Finally, if $a = 0, b = 1$,

$$\sigma\tau\sigma^{-1}\tau^{-1} = x^i x^j y x^{-i} x^{-j} y = x^{i+j} y x^{-i-j} y = x^{2(i+j)},$$

which is again either 1 or x^2. Having exhausted all possibilities, we see that $C = \{1, x^2\}$; since this is a group, $G' = \{1, x^2\}$. As we saw in 3(c) above, the quotient $G/G' \simeq C_2 \times C_2$.

Now we consider when $G = S_3$. Let $a, b \in S_3$. Now, for any $g \in S_3$, the parity of g^{-1} is the same as the parity of g. Hence,

$$aba^{-1}b^{-1}$$

must be an even permutation. Hence, $G' \subset A_3$. Now,

$$(12)(13)(12)^{-1}(13)^{-1} = (12)(13)(12)(13) = (123)$$

and

$$(12)(23)(12)^{-1}(23)^{-1} = (12)(23)(12)(23) = (132),$$

so it's clear that $G' \supset A_3$. Hence, we conclude that $G' = A_3$. Furthermore, we know that $G/G' = S_3/A_3$, which is just the cyclic group of order 2.

Finally, if $G = C_2 \times C_3$, since G is cyclic, its commutator is trivial by the same argument given for $\mathbb{Z}$ above.

♣

(d) Is it always the case that $G' = C$ for an arbitrary group? for a finite group?

7

(a) Show that Inn $G \lhd$ Aut G.

Proof. The elements of Inn G are of the form ϕ_a where $a \in G$ and $\phi_a(g) = aga^{-1}$ for all $g \in G$. Now, let $\phi_a \in$ Inn G and let $\sigma \in$ Aut G. In order to demonstrate that Inn $G \lhd$ Aut G, we must show that $\sigma \circ \phi_a \circ \sigma^{-1} \in$ Inn G. To that end, let $g \in G$. Then,

$$\begin{aligned}(\sigma \circ \phi_a \circ \sigma^{-1})(g) = \sigma(\phi_a(\sigma^{-1}(g))) = \sigma(a\sigma^{-1}(g)a^{-1}) \quad &= \sigma(a)\sigma(\sigma^{-1}(g))\sigma(a^{-1}) \\ &= \sigma(a)g\sigma(a)^{-1} \\ &= \phi_{\sigma(a)}(g).\end{aligned}$$

Since our choice of g was arbitrary, we see that, in fact,

$$\sigma \circ \phi_a \circ \sigma^{-1} = \phi_{\sigma(a)} \in \text{Inn } G.$$

Furthermore, since our choices of ϕ_a and σ were arbitrary, we see that

$$\sigma(\text{Inn } G)\sigma^{-1} \subset \text{Inn } G$$

for all $\sigma \in$ Aut G, so Inn $G \lhd$ Aut G. □

(b) Find Inn G and Aut G for $G = S_n$, $n \leq 4$. Conjecture?

Answer: When $G = S_1$, everything is trivial. When $G = S_2$, Aut G is again trivial, as any automorphism of S_2 must map the identity to itself and, therefore, the other element of S_2 to itself. The identity automorphism is clearly inner, so when $G = S_2$, Inn $G =$ Aut $G = \{1\}$.

When $G = S_3$, note that there can be at most 6 automorphisms of S_3. This is because an automorphism must preserve the order of elements; as such, if $\sigma \in$ Aut G, then there are three possible choices for $\sigma((12))$, $(12), (13)$ and (23), and there are two possible choices for $\sigma((123))$, (123) and (132). Since

$$(12)(123) = (23), (123)(12) = (13), \text{ and } (123)(123) = (132),$$

these choices completely determine σ. Since there are at most 6 automorphisms of G, if we can show that there are 6 distinct inner automorphisms, then this will suffice to demonstrate that Inn $G =$ Aut G. Let us examine

what each of the six possible inner automorphisms (one for each of the six elements of S_3) does to the element (12):

$$\begin{aligned} 1(12)1 &= (12) \\ (12)(12)(12) &= (12) \\ (13)(12)(13) &= (23) \\ (123)(12)(132) &= (23) \\ (23)(12)(23) &= (13) \\ (132)(12)(123) &= (13). \end{aligned}$$

Thus, there are three pairs of possible inner automorphisms that have the same effect on the element (12). However, as we will see, all define distinct automorphisms, as elements of the same pair from above map elements other than (12) to different places:

$$\begin{aligned} 1. \quad 1(13)1 &= (13) \\ (12)(13)(12) &= (23) \\ 2. \quad (13)(13)(13) &= (13) \\ (123)(13)(132) &= (12) \\ 3. \quad (23)(23)(23) &= (23) \\ (123)(23)(132) &= (13). \end{aligned}$$

Therefore, each of the six possible inner automorphisms is distinct from the others, so we see that $\text{Inn } G = \text{Aut } G$. Furthermore, if $a, b, c \in G$ and ϕ_a, ϕ_b are the inner automorphisms associated with a and b, respectively, then

$$(\phi_a \circ \phi_b)(c) = \phi_a(\phi_b(c)) = \phi_a(bcb^{-1}) = abcb^{-1}a^{-1} = (ab)c(ab)^{-1} = \phi_{ab}(c).$$

Since our choice of c was arbitrary, this implies that $\phi_a \circ \phi_b = \phi_{ab}$. In other words, $\text{Inn } G$ has the same group structure as G, so we can, finally, conclude that $\text{Inn } G = \text{Aut } G = G$.

When $G = S_4$, there are 9 elements of order 2, 8 of order 3 and 6 of order 4, so there are a maximum of $9 \cdot 8 \cdot 6 = 432$ possible automorphisms, assuming that we can generate the entire group with one element of each order. In fact, we can generate all of S_4 with only two elements, namely (12) and (243). To see this, note that we can generate at the very least the following 11 elements:

$$\begin{aligned} (12)(12) &= 1 \\ (243)(243) &= (234) \\ (12)(243) &= (1243) \\ (1243)(1243) &= (14)(23) \\ (1243)(14)(23) &= (1342) \\ (14)(23)(12) &= (1324) \\ (12)(14)(23) &= (1423) \\ (1423)(1423) &= (12)(34) \\ (12)(12)(34) &= (34) \\ (243)(34) &= (24) \\ (34)(243) &= (23). \end{aligned}$$

Along with (12) and (243), this is 13 elements in the subgroup generated by $\{(12), (243)\}$; since the order of this subgroup must divide the order of S_4, which is 24, we see that, in fact, $\langle (12), (243) \rangle = S_4$. Therefore, if $\phi \in \text{Aut } S_4$, ϕ is completely determined by its action on (12) and (243). Since (12) must be mapped to another element of order 2 and (243) to an element of order 3, our upper bound on the order of Aut S_4 is now $9 \cdot 8 = 72$. However, since (12) is not the product of transpositions, it cannot be mapped to an element that is; namely, $\phi((12))$ cannot be $(12)(34), (13)(24)$ or $(14)(23)$. Our upper bound, then is now $6 \cdot 8 = 48$. Suppose that

$$\phi((243)) = (abc).$$

Then $(ac)(abc) = (ab)$, $(ab)(abc) = (bc)$ and $(bc)(abc) = (ac)$; since, as we've already seen, $(12)(243) = (1243)$, it's clear that $\phi((12)) \notin \{(ab), (ac), (bc)\}$. Therefore, the order of Aut S_4 is at most $3 \cdot 8 = 24$.

On the other hand, suppose $\sigma \in S_4$. Then there corresponds to σ an inner automorphism ϕ_σ such that $\phi_\sigma(\tau) = \sigma\tau\sigma^{-1}$. Thus, we can construct the surjection

$$f : S_4 \to \text{Inn } S_4$$

given by

$$f : \sigma \mapsto \phi_\sigma.$$

To see that this is a homomorphism, let $\sigma, \gamma, \tau \in S_4$ and note that

$$\phi_\sigma \circ \phi_\gamma(\tau) = \phi_\sigma(\gamma\tau\gamma^{-1}) = \sigma\gamma\tau\gamma^{-1}\sigma^{-1} = \phi_{\sigma\gamma}(\tau).$$

The kernel of f is simply the center of S_4; since we determined in 1(b) that the center of S_4 is trivial, this implies that f is injective as well. Therefore, Inn $S_4 \simeq S_4$. Since the order of S_4 is 24 and we know there are a maximum of 24 automorphisms of S_4, we conclude that

$$\text{Aut } S_4 = \text{Inn } S_4 \simeq S_4.$$

Based on this information, we conjecture that Aut $S_n = \text{Inn } S_n \simeq S_n$ for all n.

8

Prove or disprove: A group is abelian if and only if every subgroup is normal.

Counter-Example: Consider the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. We want to demonstrate that every subgroup of Q is normal, even though it's clear that Q is not abelian, since $ij = k \neq -k = ji$. To that end, let $a, b \in Q$. We want to demonstrate that $bab^{-1} \in \langle a \rangle$. Since $\langle a \rangle$ must be contained in any subgroup containing a and our choices of a and b are arbitrary, this will demonstrate that every subgroup of Q is normal.

Now, if either a or b is ± 1, then it's clear that $bab^{-1} = a$, since ± 1 commute with all elements of Q. Hence, suppose $a, b \in \{\pm i, \pm j, \pm k\}$. Note that $a^{-1} = -a$ and $b^{-1} = -b$, so

$$bab^{-1} = ba(-b) = -bab.$$

Since $\langle a \rangle = \{\pm 1, \pm a\}$, we need to show that $-bab = \pm 1$ or $\pm a$. The following list of calculations demonstrates that, in fact, $-bab = -a$ for all possible choices of a and b:

$$\begin{aligned}
-iji &= -ki &&= -j \\
-i(-j)i &= ki &&= j \\
-iki &= -(-j)i &&= -k \\
-i(-k)i &= -ji &&= k \\
-jij &= -(-k)i &&= -i \\
-j(-i)j &= -kj &&= i \\
-jkj &= -ij &&= -k \\
-j(-k)j &= ij &&= k \\
-kik &= -jk &&= -i \\
-k(-i)k &= jk &&= i \\
-kjk &= -(-i)k &&= -j \\
-k(-j)k &= -ik &&= j.
\end{aligned}$$

Hence, every subgroup of Q is normal, even though Q is not abelian.

♣

DRL 3E3A, University of Pennsylvania
E-mail address: shonkwil@math.upenn.edu