Dummit & Foote Ch. 2.2: Centralizers and Normalizers, Stabilizers and Kernels

Scott Donaldson

Jun. 2023

1. (6/5/23)

Prove that $C_G(A) = \{g \in G \mid g^{-1}ag = a \text{ for all } a \in A\}$.

Proof. By definition, $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$ (that is, it is the set of elements of G that commute with all elements of A).

Let $g \in C_G(A), a \in A$. Then $gag^{-1} = a$, which implies that $ga = ag$, and so left-multiplying by g^{-1} we obtain $a = g^{-1}ag$. Therefore, equivalently, $C_G(A)$ is the set of elements $g \in G$ such that $g^{-1}ag = a$ for all $a \in A$. □

2. (6/5/23)

Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

Proof. Recall that $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$. Let $z \in Z(G)$, so z commutes with every element of G.

Also recall that $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. When $A = Z(G)$, then every element of g commutes with every element of A. Therefore for all $g \in G$, $g \in C_G(Z(G))$. Thus $C_G(Z(G)) = G$.

Note that, since $C_G(A) \leq N_G(A)$ for all subsets A, we must have $G = C_G(Z(G)) \leq N_G(Z(G))$. Since there is no greater set of elements, we also have $N_G(Z(G)) = G$. □

3. (6/8/23)

Prove that if A and B are subsets of G with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

Proof. Let $a \in A$ and $g \in C_G(B)$. Then g commutes with every element of b, that is, $gb = bg \Rightarrow gbg^{-1} = b$ for all $b \in B$. Since $A \subseteq B$, we also have $gag^{-1} = a$ for all $a \in A$. Therefore $g \in C_G(A)$, which implies that $C_G(B) \subseteq C_G(A)$.

From the introduction to this chapter, centralizers are subgroups, so both $C_G(B) \leq G$ and $C_G(A) \leq G$. Since $C_G(B)$ is contained within $C_G(A)$ and both are subgroups of G, $C_G(B)$ must be closed within $C_G(A)$ and closed under inverses within $C_G(A)$, so it is also a subgroup of $C_G(A)$. $\square$

4. (6/8/23)

For each of S_3, D_8, and Q_8 compute the centralizers of each element and find the center of each group.

S_3

- $C_{S_3}((1)) = S_3$
- $C_{S_3}((1,2)) = \{(1),(1,2)\}$
- $C_{S_3}((1,3)) = \{(1),(1,3)\}$
- $C_{S_3}((2,3)) = \{(1),(2,3)\}$
- $C_{S_3}((1,2,3)) = C_{S_3}((1,3,2)) = \{(1),(1,2,3),(1,3,2)\}$

The center $Z(S_3)$ consists only of the identity permutation.

D_8

- $C_{D_8}(1) = D_8$
- $C_{D_8}(r) = C_{D_8}(r^2) = C_{D_8}(r^3) = \{1, r, r^2, r^3\}$
- $C_{D_8}(s) = C_{D_8}(sr^2) = \{1, r^2, s, sr^2\}$
- $C_{D_8}(sr) = C_{D_8}(sr^3) = \{1, r^2, sr, sr^3\}$

The center $Z(D_8)$ is $\{1, r^2\}$.

Q_8

- $C_{D_8}(1) = C_{D_8}(-1) = Q_8$
- $C_{D_8}(i) = C_{D_8}(-i) = \{1, -1, i, -i\}$
- $C_{D_8}(j) = C_{D_8}(-j) = \{1, -1, j, -j\}$
- $C_{D_8}(k) = C_{D_8}(-k) = \{1, -1, k, -k\}$

The center $Z(Q_8)$ is $\{1, -1\}$.

5. (6/8/23)

In each of parts (a) through (c) show that for the specified group G and subgroup A of G, $C_G(A) = A$ and $N_G(A) = G$.

(a) $G = S_3$ and $A = \{(1), (1,2,3), (1,3,2)\}$.

Proof. From Exercise 4, we have $C_G((1,2,3)) = C_G((1,3,2)) = A$. No other non-identity permutation is in any of the centralizers of any element of A, therefore $C_G(A) = A$.

Next, consider $\sigma^{-1}(1,2,3)\sigma$ for some other permutation in S_3, for example $(1,2)(1,2,3)(1,2)$. This is equal to $(1,3,2)$, which is an element of A, so $(1,2)$ is in the normalizer of A. Since $C_G(A) \leq N_G(A)$ for all A, $A \subseteq N_G(A)$, and it follows that $N_G(A)$ consists of at least A and the element $(1,2)$. Then, because $N_G(A)$ is a subgroup, it is closed under permutation composition, and therefore must contain all elements of S_3. $\square$

(b) $G = D_8$ and $A = \{1, s, r^2, sr^2\}$.

Proof. We know that $C_G(A)$ is a subgroup of G, and from Exercise 4, we have $A \leq C_G(A)$ (since A is commutative). Then $|C_G(A)| \geq 4$. By Lagrange's Theorem, the order of $C_G(A)$ divides the order of G, 8. Then we must have either $C_G(A) = A$ or $C_G(A) = G$. However, r is not in the centralizer of A, because $rsr^{-1} = rsr^3 = sr^{-1}r^3 = sr^2 \neq s$. Therefore $C_G(A) = A$.

When we consider the normalizer of A, note that $rsr^{-1} = sr^2 \in A$. Thus $N_G(A)$ is a subgroup of G that contains both A and the element r. By closing the subgroup, we obtain $N_G(A) = G$. $\square$

(c) $G = D_{10}$ and $A = \{1, r, r^2, r^3, r^4\}$.

Proof. Since A consists only of powers of r, A is commutative, and so (as above) $A \leq C_G(A)$. The centralizer of A does not contain the element s, because $s^{-1}rs = srs = ssr^4 = r^4 \neq r$. Then we must have $|A| = 5 \leq |C_G(A)| \leq 9 = |G - \{s\}|$. Again by Lagrange's Theorem, the order of $C_G(A)$ must divide 10, and since it at least 5 and at most 9, it must be 5. Therefore $C_G(A) = A$.

When we consider the normalizer of A, note that $s^{-1}r^4s = r \in A$. Thus $N_G(A)$ is a subgroup of G that contains both A and the element s. By closing the subgroup, we obtain $N_G(A) = G$. $\square$

6. (6/9/23)

Let H be a subgroup of the group G.

(a) Show that $H \leq N_G(H)$. Give an example to show that this is not necessarily true if H is not a subgroup.

Proof. Let $h_1, h_2 \in H$ (to show that $h_1 \in N_G(H)$). Because H is a subgroup of G, it is closed and closed under inverses, so $h_1 h_2 h_1^{-1} \in H$. So the conjugate of every element with every other element of H is in H, which implies that $H \leq N_G(H)$.

However, this does not follow if H is merely a subset of G. For example, let $G = D_6$ and $H = \{s, r\}$. Then $rsr^{-1} = sr^2r^2 = sr \notin H$, which implies that $r \notin H$. Therefore H is not contained within its normalizer. □

(b) Show that $H \leq C_G(H)$ if and only if H is abelian.

Proof. First, let H be abelian and let $h_1, h_2 \in H$. Because H is abelian, we have $h_1h_2 = h_2h_1 \Rightarrow h_2 = h_1h_2h_1^{-1}$, so the conjugate of h_2 by h_1 is h_2. Thus the arbitrary element h_1 is in the centralizer of H, and so $H \leq C_G(H)$.

Next, let $H \leq C_G(H)$. Then for all $h_1, h_2 \in H$, $h_2 = h_1h_2h_1^{-1} \Rightarrow h_2h_1 = h_1h_2$, and so H is an abelian subgroup of G. □

7. (6/13/23)

Let $n \in \mathbb{Z}$ with $n \geq 3$. Prove the following:

(a) $Z(D_{2n}) = \{1\}$ if n is odd

Proof. Recall that $Z(D_{2n}) = \{x \in D_{2n} \mid xy = yx \text{ for all } y \in D_{2n}\}$. Let $x \in Z(D_{2n}), y \in D_{2n}$. We will consider separately the cases where $x = r^k$ and $x = sr^k$.

Suppose $x = r^k$ for some $0 < k < n$ (clearly if $x = r^0 = 1$, then it is in the center of D_{2n}). If $y = s$, then $xy = r^ks = sr^{-k}$ and $yx = sr^k$. These are only equal when $k = -k \pmod{n}$; since n is odd there are no values of k that satisfy this equality, and so $x = r^k$ does not commute with every element of D_{2n} and is not in $Z(D_{2n})$.

Next, suppose $x = sr^k$. Then if $y = r$, we have $xy = sr^kr = sr^{k+1}$ and $yx = rsr^k = sr^{-1}r^k = sr^{k-1}$. No values of k satisfy this equality and so no x of the form sr^k is in $Z(D_{2n})$. Thus the center of D_{2n} consists of only the identity when n is odd. □

(b) $Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$

Proof. The case where $x = sr^k$ is identical to the above proof; if $y = r$ then they do not commute and so no x of the form sr^k is in $Z(D_{2n})$.

Consider $x = r^k$ for some $0 < k < n$. If $y = r^p, 0 \leq p < n$, then they commute because both elements are powers of r. So let $y = sr^p$. Then $xy = r^k sr^p = sr^{-k}r^p = sr^{p-k}$ and $yx = sr^p r^k = sr^{p+k}$. These are equal to each other when $p - k = p + k$, that is, when $-k = k \pmod{n}$, which implies that $2k = n$. Since n is even, there is a value of k for which this occurs, $n/2$.

Thus the center of D_{2n} when $n = 2k$ is $\{1, r^k\}$. □

8. (6/13/23)

Let $G = S_n$, fix an $i \in \{1, 2, ..., n\}$ and let $G_i = \{\sigma \in G \mid \sigma(i) = i\}$ (the stabilizer of i in G). Use group actions to prove that G_i is a subgroup of G. Find $|G_i|$.

Proof. There is a group action of G on $\{1, ..., n\}$ defined by $\sigma \cdot k = \sigma(k)$. The identity permutation applied to any k is always k, and closure is easily demonstrated by composition of permutations.

Now let $\sigma_1, \sigma_2 \in G_i$ (to show that $\sigma_1 \circ \sigma_2 \in G_i$). Then $\sigma_1(i) = i$ and $\sigma_2(i) = i$. It follows that $\sigma_1(\sigma_2(i)) = \sigma_1(i) = i$, and since this is equal to $(\sigma_1 \circ \sigma_2)(i)$, $\sigma_1 \circ \sigma_2$ is in G_i, so it is closed.

Next, note that $\sigma(i) = i$ for some $\sigma \in G_i$ implies that $i = \sigma^{-1}(i)$, so σ^{-1} is also in G_i and it is therefore closed under inverses. Thus G_i is a subgroup of G.

To find the order of G_i, recall from Ch. 1.3 that the order of S_n is $n!$. Further, G_i consists of those permutations of S_n whose cycle decompositions do not include i. We will show that G_i has the same cardinality as S_{n-1} and that its order is therefore $(n-1)!$.

Let $\varphi : G_i \to S_{n-1}$ be defined on elements of $\{1, ..., n\}$ by $\varphi(\sigma(m)) = \sigma(m)$ if $m < i$ and $= \sigma(m) - 1$ if $m > i$. For example, if $i = 10$, φ maps the permutation with cycle decomposition $(1, 5, 9, 13, 17)$ to $(1, 5, 9, 12, 16)$.

φ is one-to-one: If $\varphi(\sigma_1(m)) = \varphi(\sigma_2(m))$, then they are by definition equal if $\sigma_1(m)$ and $\sigma_2(m)$ are either both less than or both greater than i. Without loss of generality, suppose that $\sigma_1(m) < i$ and $\sigma_2(m) > i$. Then $\varphi(\sigma_1(m)) < i$ and $\varphi(\sigma_2(i)) \geq i$, so they cannot be equal.

φ is onto: Let $\sigma \in S_{n-1}$. There is a unique permutation G_i that maps to σ whose cycle decomposition contains the same values in the same positions as σ when those values are less than i, and the successor of those values in the same positions as σ when those values are greater than i. Formally, the inverse $\varphi^{-1} : S_{n-1} \to G_i$ is well-defined by $\varphi(\sigma(m)) = \sigma(m)$ if $m < i$ and $= \sigma(m) + 1$ if $m > i$.

This proves that φ is a bijection (note that the additional requirement that it is an isomorphism is unnecessary because we are only concerned with the size of these groups). Therefore $|G_i| = |S_{n-1}| = (n-1)!$. □

9. (6/13/23)

For any subgroup H of G and any nonempty subset A of G define $N_H(A)$ to be the set $\{h \in H \mid hAh^{-1} = A\}$. Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of H (note that A need not be a subset of H).

Proof. To show that $N_H(A) = N_G(A) \cap H$, we will show that membership in one implies membership in the other, and vice-versa.

First, let $h \in N_H(A)$ (to show that $h \in N_G(A) \cap H$). Then $hAh^{-1} = A$. Also, by definition, $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$, so $h \in N_G(A)$. Further, since $N_H(A)$ consists of only those $h \in N_G(A)$ that are also in H, it follows that $h \in N_G(A) \cap H$.

Next, let $h \in N_G(A) \cap H$, that is, $h \in N_G(A)$ and $h \in H$. Since $h \in N_G(A)$, $hAh^{-1} = A$. It follows immediately that $h \in N_H(A)$. Therefore $N_H(A) = N_G(A) \cap H$.

Now from Ch. 2.1, exercise 10., the intersection of two subgroups (of G) is again a subgroup (of G). Since $N_H(A)$ is also restricted to H and containment of subgroups is transitive, we deduce that $N_H(A)$ is a subgroup of H. $\square$

10. (6/13/23)

Let H be a subgroup of order 2 in G. Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$ then $H \leq Z(G)$.

Proof. Let $H = \{1, h\} \leq G$. In order to prove that $N_G(H) = C_G(H)$, we will show that membership in one implies membership in the other, and vice-versa.

For some $g \in G$, let $g \in N_G(H)$. Then $gHg^{-1} = H$. Since $g \cdot 1 \cdot g^{-1} = 1$, we must have $ghg^{-1} = h$, which implies that $gh = hg$. Then g commutes with both 1 and h, that is, with every element of H, and so $g \in C_G(H)$. Since we know that $C_G(H) \leq N_G(H)$, this proves that $N_G(H) = C_G(H)$.

Next suppose that $N_G(H) = G$. Then for every $g \in G$, $gh = hg$. So an arbitrary element g commutes with every element of H. Put differently, every element of H commutes with every element of G. It follows that H is contained in the center of G, that is, $H \leq Z(G)$. $\square$

11. (6/14/23)

Prove that $Z(G) \leq N_G(A)$ for any subset A of G.

Proof. Let A be a subset of G and let $g \in Z(G)$. Then g commutes with every other element of G, so in particular $ga = ag$ for all $a \in A$. It follows that $gag^{-1} = a$ for all $a \in A$, and therefore that $gAg^{-1} = A$. Thus $g \in N_G(A)$, and so $Z(G)$ is contained in $N_G(A)$. By the transitivity of subgroups, we must also have $Z(G) \leq N_G(A)$. $\square$

12. (6/17/23)

Let R be the set of all polynomials with integer coefficients in the independent variables x_1, x_2, x_3, x_4 i.e., the members of R are finite sums of the form $ax_1^{r_1}x_2^{r_2}x_3^{r_3}x_4^{r_4}$, where a is any integer and $r_1, ..., r_4$ are nonnegative integers. For example,

$$12x_1^5x_2^7x_4 - 18x_2^3x_3 + 11x_1^6x_2x_3^3x_4^{23}$$

is a typical element of R. Each $\sigma \in S_4$ gives a permutation of $\{x_1, ..., x_4\}$ by defining $\sigma \cdot x_i = x_{\sigma(i)}$. This may be extended to a map from R to R by defining

$$\sigma \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$$

for all $p(x_1, x_2, x_3, x_4) \in R$ (i.e., σ simply permutes the indices of the variables).

(a) Let $p = p(x_1, x_2, x_3, x_4)$ be the polynomial above, let $\sigma = (1, 2, 3, 4)$ and $\tau = (1, 2, 3)$. Compute:

- $\sigma \cdot p = 12x_1x_2^5x_3^7 - 18x_3^3x_4 + 11x_1^{23}x_2^6x_3x_4^3$
- $\tau \cdot (\sigma \cdot p) = \tau \cdot 12x_1x_2^5x_3^7 - 18x_3^3x_4 + 11x_1^{23}x_2^6x_3x_4^3 =$
  $12x_1^7x_2x_3^5 - 18x_1^3x_4 + 11x_1x_2^{23}x_3^6x_4^3$
- $(\tau \circ \sigma) \cdot p = (1, 3, 4, 2) \cdot p = 12x_1^7x_2x_3^5 - 18x_1^3x_4 + 11x_1x_2^{23}x_3^6x_4^3$
- $(\sigma \circ \tau) \cdot p = (1, 3, 2, 4) \cdot p = 12x_1x_3^5x_4^7 - 18x_2x_4^3 + 11x_1^{23}x_2^3x_3^6x_4$

(b) Prove that these definitions give a (left) group action of S_4 on R.

Proof. To show that these definitions give a group action, we have to show that $(1) \cdot p = p$, and $\sigma_1 \cdot (\sigma_2 \cdot p) = (\sigma_1 \circ \sigma_2) \cdot p$ for all $p \in R, \sigma_1, \sigma_2 \in S_4$.

First, $(1) \cdot p(x_1, x_2, x_3, x_4) = p(x_1, x_2, x_3, x_4)$ satisfies the identity condition.

Next, let $\sigma_1, \sigma_2 \in S_4$. Then:

$$\begin{aligned}\sigma_1 \cdot (\sigma_2 \cdot p(x_1, x_2, x_3, x_4)) = \sigma_1 \cdot p(x_{\sigma_2(1)}, x_{\sigma_2(2)}, x_{\sigma_2(3)}, x_{\sigma_2(4)}) &= \\ p(x_{\sigma_1(\sigma_2(1))}, x_{\sigma_1(\sigma_2(2))}, x_{\sigma_1(\sigma_2(3))}, x_{\sigma_1(\sigma_2(4))}) &= \\ (\sigma_1 \circ \sigma_2) \cdot p(x_1, x_2, x_3, x_4)&,\end{aligned}$$

as desired. Thus the definitions give a group action of S_4 on R. □

(c) Exhibit all permutations in S_4 that stabilize x_4 and prove that they form a subgroup isomorphic to S_3.

Proof. Given the above group action of S_4 on R, a permutation stabilizes x_4 if its cycle decomposition does not include 4. For example, $(1, 3)$ stabilizes x_4 because it maps x_4 to x_4, but $(1, 4)$ does not stabilize x_4 because it maps x_4 to x_1. The permutations in S_4 whose cycle decompositions do not include 4 are: $(1),(1,2),(1,3),(2,3),(1,2,3)$, and $(1,3,2)$. In fact these are exactly those permutations that make up the group S_3 (which is closed and closed under inverses). Thus the permutations in S_4 that stabilize x_4 form a subgroup isomorphic to S_3. $\square$

(d) Exhibit all permutations in S_4 that stabilize the element x_1+x_2 and prove that they form an abelian subgroup of order 4.

Proof. A permutation σ stabilizes x_1+x_2 if it stabilizes x_1 and x_2, or if it assigns x_1 to x_2 and vice-versa (since $x_1+x_2 = x_2+x_1$). The permutations in S_4 of this form comprise the set $\{(1),(1,2),(3,4),(1,2)(3,4)\}$. In fact, this is a commutative subgroup of S_4 where each non-identity permutation has order 2 (thus isomorphic to the Klein four-group V_4). $\square$

(e) Exhibit all permutations in S_4 that stabilize the element $x_1x_2+x_3x_4$ and prove that they form a subgroup isomorphic to the dihedral group of order 8.

Proof. Consider all the presentations of $x_1x_2+x_3x_4$ that might be formed by permuting the subscripts but leaving the value unchanged. Including the above presentation, these are on the left, with the corresponding permutation in S_4 on the right in the table below:

$x_1x_2+x_3x_4$	(1)
$x_1x_2+x_4x_3$	$(3,4)$
$x_2x_1+x_3x_4$	$(1,2)$
$x_2x_1+x_4x_3$	$(1,2)(3,4)$
$x_3x_4+x_1x_2$	$(1,3)(2,4)$
$x_3x_4+x_2x_1$	$(1,3,2,4)$
$x_4x_3+x_1x_2$	$(1,4,2,3)$
$x_4x_3+x_2x_1$	$(1,4)(2,3)$

Now let φ be a map from D_8 to the set of permutations above defined on generators by $\varphi(s)=(1,2)$ and $\varphi(r)=(1,3,2,4)$. We will prove that φ is an isomorphism. The order of $(1,2)$ is 2 and the order of $(1,3,2,4)$ is 4, so this satisfies the requirements that $\varphi(s^2)=\varphi(s)^2=(1)$ and $\varphi(r^4)=\varphi(r)^4=(1)$.

Consider the additional relation that $sr=r^{-1}s$. To show that this holds under φ, we must show that $\varphi(s)\varphi(r)=\varphi(r)^{-1}\varphi(s)$ remains true. On the left we have $(1,2)(1,3,2,4)=(1,3)(2,4)$ and on the right we have $(1,3,2,4)^{-1}(1,2)=(1,4,2,3)(1,2)=(1,3)(2,4)$. Since the generators and relations of D_8 hold under φ in the stabilizer shown above, φ is a homomorphism. Finally it can be shown exhaustively that φ is a bijection, and is thus an isomorphism; thus the stabilizer is isomorphic to the dihedral group D_8. $\square$

(f) Show that the permutations in S_4 that stabilize the element $(x_1+x_2)(x_3+x_4)$ are exactly the same as those found in part (e).

Proof. By similar method to the above table, we expand $(x_1+x_2)(x_3+x_4) = x_1x_3+x_1x_4+x_2x_3+x_2x_4$ and create a table of the possible alternate presentations with their corresponding permutations:

$x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4$	(1)
$x_1x_4 + x_1x_3 + x_2x_4 + x_2x_3$	$(3, 4)$
$x_2x_3 + x_2x_4 + x_1x_3 + x_1x_4$	$(1, 2)$
$x_2x_4 + x_2x_3 + x_1x_4 + x_1x_3$	$(1, 2)(3, 4)$
$x_3x_1 + x_3x_2 + x_4x_1 + x_4x_2$	$(1, 3)(2, 4)$
$x_3x_2 + x_3x_1 + x_4x_2 + x_4x_1$	$(1, 3, 2, 4)$
$x_4x_1 + x_4x_2 + x_3x_1 + x_3x_2$	$(1, 4, 2, 3)$
$x_4x_2 + x_4x_1 + x_3x_2 + x_3x_1$	$(1, 4)(2, 3)$

Thus the above permutations (isomorphic to the dihedral group D_8) are the same as those that stabilize $x_1x_2 + x_3x_4$. □

13. (6/17/23)

Let n be a positive integer and let R be the set of all polynomials with integer coefficients in the independent variables $x_1, x_2, ..., x_n$ i.e., the members of R are finite sums of the form $ax_1^{r_1}x_2^{r_2}...x_n^{r_n}$, where a is any integer and $r_1, ..., r_n$ are nonnegative integers.

For each $\sigma \in S_n$ define a map

$$\sigma : R \to R \text{ by } \sigma \cdot p(x_1, x_2, ..., x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}).$$

Prove that this defines a (left) group action of S_n on R.

Proof. To show that this is a group action, we must show that $(1) \cdot p = p$ for all $p \in R$, and that $\sigma_1 \cdot (\sigma_2 \cdot p) = (\sigma_1 \circ \sigma_2) \cdot p$ for all $p \in R, \sigma_1, \sigma_2 \in S_n$.

First, $(1) \cdot p(x_1, x_2, ..., x_n) = p(x_1, x_2, ..., x_n)$ satisfies the identity condition.

Next, let $\sigma_1, \sigma_2 \in S_n$. Then:

$$\begin{aligned} \sigma_1 \cdot (\sigma_2 \cdot p(x_1, x_2, ..., x_n)) = \sigma_1 \cdot p(x_{\sigma_2(1)}, x_{\sigma_2(2)}, ..., x_{\sigma_2(n)}) = \\ p(x_{\sigma_1(\sigma_2(1))}, x_{\sigma_1(\sigma_2(2))}, ..., x_{\sigma_1(\sigma_2(n))}) = \\ (\sigma_1 \circ \sigma_2) \cdot p(x_1, x_2, ..., x_n), \end{aligned}$$

as desired. □

14. (6/18/23)

Let $H(F)$ be the Heisenberg group over the field F introduced in Exercise 11 of Section 1.4. Determine which matrices lie in the center of $H(F)$ and prove that $Z(H(F))$ is isomorphic to the additive group F.

Proof. Let $H(F)$ be the Heisenberg group over the field F, that is, the group of 3×3 matrices of the form $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$, with $a, b, c \in F$, under the operation of matrix multiplication. From 1.4., it can be shown through matrix multiplication that the two matrices $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$ commute if and only if the upper-right entries of the products XY and YX are equal, namely $e + af + b = b + cd + e \Rightarrow af = cd$. In this case, if $a \neq 0$ and $c \neq 0$, then one can always choose $d = 0, f \neq 0$ so that $cd = 0$ but $af \neq 0$, which implies that the two matrices do not commute. Therefore, we must have $a = c = 0$ for the given matrix X to be guaranteed to commute with Y (regardless of the values of the entries d and f in Y). Thus the center of $H(F)$ is comprised of matrices of the form $\begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, x \in F$.

Next, let φ be a map from $Z(H(F))$ to F^+, the additive group F, defined by $\varphi(\begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}) = x$. For $A, B \in Z(H(F))$, let a and b be the upper-right entries, respectively. Then $\varphi(A)\varphi(B) = a+b$ and $\varphi(AB) = \varphi(\begin{pmatrix} 1 & 0 & a+b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}) = a + b$, so φ is a homomorphism.

In fact, φ is an isomorphism. It is one-to-one: Let $\varphi(A) = \varphi(B)$. Then $a = b$, so $A = B$. It is also onto: Let $x \in F^+$. Then $\varphi(X) = x$. Since φ is a bijective homomorphism, it is an isomorphism, and so $Z(H(F)) \cong F^+$. $\square$