Suppose now that H is finite and closed under multiplication and let x be any element in H. Then there are only finitely many distinct elements among $x, x^2, x^3, \dots$ and so $x^a = x^b$ for some integers a, b with $b > a$. If $n = b - a$, then $x^n = 1$ so in particular every element $x \in H$ is of finite order. Then $x^{n-1} = x^{-1}$ is an element of H, so H is automatically also closed under inverses.

EXERCISES

Let G be a group.

1. In each of (a) – (e) prove that the specified subset is a subgroup of the given group:
 (a) the set of complex numbers of the form $a + ai$, $a \in \mathbb{R}$ (under addition)
 (b) the set of complex numbers of absolute value 1, i.e., the unit circle in the complex plane (under multiplication)
 (c) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators divide n (under addition)
 (d) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators are relatively prime to n (under addition)
 (e) the set of nonzero real numbers whose square is a rational number (under multiplication).

2. In each of (a) – (e) prove that the specified subset is *not* a subgroup of the given group:
 (a) the set of 2-cycles in S_n for $n \geq 3$
 (b) the set of reflections in D_{2n} for $n \geq 3$
 (c) for n a composite integer > 1 and G a group containing an element of order n, the set $\{x \in G \mid |x| = n\} \cup \{1\}$
 (d) the set of (positive and negative) odd integers in $\mathbb{Z}$ together with 0
 (e) the set of real numbers whose square is a rational number (under addition).

3. Show that the following subsets of the dihedral group D_8 are actually subgroups:
 (a) $\{1, r^2, s, sr^2\}$, **(b)** $\{1, r^2, sr, sr^3\}$.

4. Give an explicit example of a group G and an infinite subset H of G that is closed under the group operation but is not a subgroup of G.

5. Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

6. Let G be an abelian group. Prove that $\{g \in G \mid |g| < \infty\}$ is a subgroup of G (called the *torsion subgroup* of G). Give an explicit example where this set is not a subgroup when G is non-abelian.

7. Fix some $n \in \mathbb{Z}$ with $n > 1$. Find the torsion subgroup (cf. the previous exercise) of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$. Show that the set of elements of infinite order together with the identity is *not* a subgroup of this direct product.

8. Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

9. Let $G = GL_n(F)$, where F is any field. Define

$$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1\}$$

(called the *special linear group*). Prove that $SL_n(F) \leq GL_n(F)$.

10. **(a)** Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.
 (b) Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable).

11. Let A and B be groups. Prove that the following sets are subgroups of the direct product $A \times B$:

(a) $\{(a, 1) \mid a \in A\}$
(b) $\{(1, b) \mid b \in B\}$
(c) $\{(a, a) \mid a \in A\}$, where here we assume $B = A$ (called the *diagonal subgroup*).

12. Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A:
(a) $\{a^n \mid a \in A\}$
(b) $\{a \in A \mid a^n = 1\}$.

13. Let H be a subgroup of the additive group of rational numbers with the property that $1/x \in H$ for every nonzero element x of H. Prove that $H = 0$ or $\mathbb{Q}$.

14. Show that $\{x \in D_{2n} \mid x^2 = 1\}$ is not a subgroup of D_{2n} (here $n \geq 3$).

15. Let $H_1 \leq H_2 \leq \cdots$ be an ascending chain of subgroups of G. Prove that $\cup_{i=1}^{\infty} H_i$ is a subgroup of G.

16. Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in GL_n(F) \mid a_{ij} = 0 \text{ for all } i > j\}$ is a subgroup of $GL_n(F)$ (called the group of *upper triangular* matrices).

17. Let $n \in \mathbb{Z}^+$ and let F be a field. Prove that the set $\{(a_{ij}) \in GL_n(F) \mid a_{ij} = 0 \text{ for all } i > j,$ and $a_{ii} = 1 \text{ for all } i\}$ is a subgroup of $GL_n(F)$.

2.2 CENTRALIZERS AND NORMALIZERS, STABILIZERS AND KERNELS

We now introduce some important families of subgroups of an arbitrary group G which in particular provide many examples of subgroups. Let A be any nonempty subset of G.

Definition. Define $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the *centralizer* of A in G. Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements of G which commute with every element of A.

We show $C_G(A)$ is a subgroup of G. First of all, $C_G(A) \neq \emptyset$ because $1 \in C_G(A)$: the definition of the identity specifies that $1a = a1$, for all $a \in G$ (in particular, for all $a \in A$) so 1 satisfies the defining condition for membership in $C_G(A)$. Secondly, assume $x, y \in C_G(A)$, that is, for all $a \in A$, $xax^{-1} = a$ and $yay^{-1} = a$ (note that this does *not* mean $xy = yx$). Observe first that since $yay^{-1} = a$, multiplying both sides of this first on the left by y^{-1}, then on the right by y and then simplifying gives $a = y^{-1}ay$, i.e., $y^{-1} \in C_G(A)$ so that $C_G(A)$ is closed under taking inverses. Now

$$\begin{aligned}
(xy)a(xy)^{-1} &= (xy)a(y^{-1}x^{-1}) && \text{(by Proposition 1.1(4) applied to } (xy)^{-1}\text{)}\\
&= x(yay^{-1})x^{-1} && \text{(by the associative law)}\\
&= xax^{-1} && \text{(since } y \in C_G(A)\text{)}\\
&= a && \text{(since } x \in C_G(A)\text{)}
\end{aligned}$$

so $xy \in C_G(A)$ and $C_G(A)$ is closed under products, hence $C_G(A) \leq G$.

In the special case when $A = \{a\}$ we shall write simply $C_G(a)$ instead of $C_G(\{a\})$. In this case $a^n \in C_G(a)$ for all $n \in \mathbb{Z}$.

For example, in an abelian group G, $C_G(A) = G$, for all subsets A. One can check by inspection that $C_{Q_8}(i) = \{\pm 1, \pm i\}$. Some other examples are specified in the exercises.

We shall shortly discuss how to minimize the calculation of commutativities between single group elements which appears to be inherent in the computation of centralizers (and other subgroups of a similar nature).

Definition. Define $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$, the set of elements commuting with all the elements of G. This subset of G is called the *center* of G.

Note that $Z(G) = C_G(G)$, so the argument above proves $Z(G) \leq G$ as a special case. As an exercise, the reader may wish to prove $Z(G)$ is a subgroup directly.

Definition. Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Define the *normalizer* of A in G to be the set $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$.

Notice that if $g \in C_G(A)$, then $gag^{-1} = a \in A$ for all $a \in A$ so $C_G(A) \leq N_G(A)$. The proof that $N_G(A)$ is a subgroup of G follows the same steps which demonstrated that $C_G(A) \leq G$ with appropriate modifications.

Examples

(1) If G is abelian then all the elements of G commute, so $Z(G) = G$. Similarly, $C_G(A) = N_G(A) = G$ for *any* subset A of G since $gag^{-1} = gg^{-1}a = a$ for every $g \in G$ and every $a \in A$.

(2) Let $G = D_8$ be the dihedral group of order 8 with the usual generators r and s and let $A = \{1, r, r^2, r^3\}$ be the subgroup of rotations in D_8. We show that $C_{D_8}(A) = A$. Since all powers of r commute with each other, $A \leq C_{D_8}(A)$. Since $sr = r^{-1}s \neq rs$ the element s does not commute with all members of A, i.e., $s \notin C_{D_8}(A)$. Finally, the elements of D_8 that are not in A are all of the form sr^i for some $i \in \{0, 1, 2, 3\}$. If the element sr^i were in $C_{D_8}(A)$ then since $C_{D_8}(A)$ is a *subgroup* which contains r we would also have the element $s = (sr^i)(r^{-i})$ in $C_{D_8}(A)$, a contradiction. This shows $C_{D_8}(A) = A$.

(3) As in the preceding example let $G = D_8$ and let $A = \{1, r, r^2, r^3\}$. We show that $N_{D_8}(A) = D_8$. Since, in general, the centralizer of a subset is contained in its normalizer, $A \leq N_{D_8}(A)$. Next compute that

$$sAs^{-1} = \{s1s^{-1},\ srs^{-1},\ sr^2s^{-1},\ sr^3s^{-1}\} = \{1,\ r^3,\ r^2,\ r\} = A,$$

so that $s \in N_{D_8}(A)$. (Note that the *set* sAs^{-1} equals the *set* A even though the elements in these two sets appear in different orders — this is because s is in the normalizer of A but not in the centralizer of A.) Now both r and s belong to the *subgroup* $N_{D_8}(A)$ and hence $s^i r^j \in N_{D_8}(A)$ for all integers i and j, that is, every element of D_8 is in $N_{D_8}(A)$ (recall that r and s *generate* D_8). Since $D_8 \leq N_{D_8}(A)$ we have $N_{D_8}(A) = D_8$ (the reverse containment being obvious from the definition of a normalizer).

(4) We show that the center of D_8 is the subgroup $\{1, r^2\}$. First observe that the center of any group G is contained in $C_G(A)$ for any subset A of G. Thus by Example 2 above $Z(D_8) \leq C_{D_8}(A) = A$, where $A = \{1, r, r^2, r^3\}$. The calculation in Example 2 shows that r and similarly r^3 are not in $Z(D_8)$, so $Z(D_8) \leq \{1, r^2\}$. To show the

reverse inclusion note that r commutes with r^2 and calculate that s also commutes with r^2. Since r and s generate D_8, every element of D_8 commutes with r^2 (and 1), hence $\{1, r^2\} \leq Z(D_8)$ and so equality holds.

(5) Let $G = S_3$ and let A be the subgroup $\{1, (1\,2)\}$. We explain why $C_{S_3}(A) = N_{S_3}(A) = A$. One can compute directly that $C_{S_3}(A) = A$, using the ideas in Example 2 above to minimize the calculations. Alternatively, since an element commutes with its powers, $A \leq C_{S_3}(A)$. By Lagrange's Theorem (Exercise 19 in Section 1.7) the order of the subgroup $C_{S_3}(A)$ of S_3 divides $|S_3| = 6$. Also by Lagrange's Theorem applied to the subgroup A of the group $C_{S_3}(A)$ we have that $2 \mid |C_{S_3}(A)|$. The only possibilities are: $|C_{S_3}(A)| = 2$ or 6. If the latter occurs, $C_{S_3}(A) = S_3$, i.e., $A \leq Z(S_3)$; this is a contradiction because $(1\,2)$ does not commute with $(1\,2\,3)$. Thus $|C_{S_3}(A)| = 2$ and so $A = C_{S_3}(A)$.

Next note that $N_{S_3}(A) = A$ because $\sigma \in N_{S_3}(A)$ if and only if

$$\{\sigma 1 \sigma^{-1}, \sigma(1\,2)\sigma^{-1}\} = \{1, (1\,2)\}.$$

Since $\sigma 1 \sigma^{-1} = 1$, this equality of sets occurs if and only if $\sigma(1\,2)\sigma^{-1} = (1\,2)$ as well, i.e., if and only if $\sigma \in C_{S_3}(A)$.

The center of S_3 is the identity because $Z(S_3) \leq C_{S_3}(A) = A$ and $(1\,2) \notin Z(S_3)$.

Stabilizers and Kernels of Group Actions

The fact that the normalizer of A in G, the centralizer of A in G, and the center of G are all subgroups can be deduced as special cases of results on group actions, indicating that the structure of G is reflected by the sets on which it acts, as follows: if G is a group acting on a set S and s is some fixed element of S, the *stabilizer* of s in G is the set

$$G_s = \{g \in G \mid g \cdot s = s\}$$

(see Exercise 4 in Section 1.7). We show briefly that $G_s \leq G$: first $1 \in G_s$ by axiom (2) of an action. Also, if $y \in G_s$,

$$\begin{aligned} s = 1 \cdot s &= (y^{-1}y) \cdot s \\ &= y^{-1} \cdot (y \cdot s) && \text{(by axiom (1) of an action)} \\ &= y^{-1} \cdot s && \text{(since } y \in G_s) \end{aligned}$$

so $y^{-1} \in G_s$ as well. Finally, if $x, y \in G_s$, then

$$\begin{aligned} (xy) \cdot s &= x \cdot (y \cdot s) && \text{(by axiom (1) of an action)} \\ &= x \cdot s && \text{(since } y \in G_s) \\ &= s && \text{(since } x \in G_s). \end{aligned}$$

This proves G_s is a subgroup[1] of G. A similar (but easier) argument proves that the *kernel* of an action is a subgroup, where the kernel of the action of G on S is defined as

$$\{g \in G \mid g \cdot s = s, \text{ for all } s \in S\}$$

(see Exercise 1 in Section 1.7).

[1]Notice how the steps to prove G_s is a subgroup are the same as those to prove $C_G(A) \leq G$ with axiom (1) of an action taking the place of the associative law.