Abstract Algebra, 3rd Edition

David S. Dummit and Richard M. Foote
newell.jensen@gmail.com

Chapter 2 - Subgroups

Exercises:

2.1 DEFINITION AND EXAMPLES

Let G be a group.

1. In each of (a)-(e) prove that the specified subset is a subgroup of the given group:

Let us denote the subset of the given form as H.

(a) the set of complex numbers of the form $a + ai, a \in \mathbb{R}$ (under addition)

Proof.

H is non-empty as we can let $a = 0 \implies 0 + 0i = 0$, the identity element.

Let $x, y \in H$ such that $x = a + ai, y = b + bi$. Then $x - y = (a + ai) - (b + bi) = (a - b) + (a - b)i$, which is also in H.

Therefore, H is a subgroup of the complex numbers. □

(b) the set of complex numbers of absolute value 1, i.e., the unit circle in the complex plane (under multiplication)

Proof.

H is non-empty as $1 + 0i = 1 \implies |1 + 0i| = 1$.

Let $x, y \in H$ so that $xy^{-1} \implies |xy^{-1}| = |x||y^{-1}| = |1||1| = 1$. Therefore, $xy^{-1} \in H$.

Therefore, H is a subgroup of the complex numbers. □

(c) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators divide n (under addition)

Proof.

H is non-empty as $1 \in \mathbb{Q}$ and $1 \mid n$.

Let $x, y \in H$ such that $x = a/b, y = c/d$ so that $b \mid n$ and $d \mid n$. Then we must have that $b = n/e, d = n/f$ for some $e, f \in \mathbb{Z}^+$.

Therefore, $xy^{-1} \implies x - y \implies \frac{a}{b} - \frac{c}{d} = \frac{ae}{n} - \frac{bf}{n} = \frac{ae-bf}{n}$ and since $n \mid n$ we see that this denominator obviously divides n so this rational number must be in H.

Therefore, H is a subgroup of the rational numbers. □

(d) for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators are relatively prime to n (under addition)

Proof.

H is non-empty as $1 \in \mathbb{Q}$ and 1 is relatively prime to any n.

Let $x, y \in H$ such that $x = a/b, y = c/d$ so that $\gcd(b, n) = \gcd(d, n) = 1 \implies \gcd(bd, n) = 1$.

Therefore, $\frac{a}{b} - \frac{c}{d} = \frac{ad-cb}{bd}$ and since $\gcd(bd, n) = 1$, we have that the denominator of this rational number is relatively prime with n so this rational number must be in H.

Therefore, H is a subgroup of the rational numbers. □

(e) the set of nonzero real numbers whose square is a rational number (under multiplication)

Proof.

H is non-empty as any nonzero squared integer is an integer and any integer is a rational number.

Let $x, y \in H$ such that $x^2 = a/b, y^2 = c/d$. Then, $xy^{-1} \implies (xy^{-1})^2 = x^2y^{-2} = x^2(y^2)^{-1} = \frac{a}{b} \cdot (\frac{c}{d})^{-1} = \frac{ad}{bc}$ which is a rational number so this nonzero real number is in H.

Therefore, H is a subgroup of the real numbers. □

2. In each of (a)-(e) prove that the specified subset is *not* a subgroup of the given group:

Let us denote the subset of the given form as H.

(a) the set of 2-cycles in S_n for $n \geq 3$

Proof.

Let $x, y \in H$ such that $x =$(1 2) and $y =$(1 3). Then $xy^{-1} \implies$ (1 2) $\cdot$ (3 1)=(1 3 2) $\notin H$.

Therefore, H is not a subgroup of S_n for $n \geq 3$. □

(b) the set of reflections in D_{2n} for $n \geq 3$

Proof.

A reflection in the dihedral group D_{2n} has the relation that $s^2 = 1$. That is, when we apply the *same* reflection twice, we get the identity element.

However, we can have different reflections for $n \geq 3$. A reflection will interchange a pair of points on the n-gon to create a 2-cycle within the reflection's cycle decomposition. And similar to (a) above, we see that the composition of 2-cycles that share an element, will result in a permutation that is not a 2-cycle and therefore does not belong to the group of reflections.

For an explicit example of this note that when $n = 3$ we have an equilateral triangle that has the reflections: (1 2),(1 3),(2 3)

These are the same 2-cycles we used in part (a) above and with the same reasoning we see that (1 3 2) $\notin H$.

Therefore, H is not a subgroup of 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

$$\{x \in G \mid |x| = n\} \cup \{1\}$$

Proof.

Let $x, y \in H$. Since n is composite we can write it as $n = ab$, where $a \leq b < n$.

Suppose $xy^{-1} \in H$

$$\begin{aligned}
(xy^{-1})^n = 1 &= x^n y^{-n} && \text{[property of the group]} \\
&= 1y^{-n} \\
&= y^{-n} \\
&= y^{-ab} \\
&= (y^{-a})^b \\
&= ((y^{-a})^b)^{-b} && [(1)^{-b} = 1] \\
&= y^{-a} \\
&= (y^{-1})^a
\end{aligned}$$

Thus, $(y^{-1})^a = 1$, which is contradiction as the group elements of G have order n. Therefore, $xy^{-1} \notin H$ and H is not a subgroup of G. □

(d) the set of (positive and negative) odd integers in $\mathbb{Z}$ together with 0

Proof.

Let $x, y \in H$ such that $x = 5, y = 3$ then $xy^{-1} \implies x - y \implies 5 - 3 = 2 \notin H$.

Therefore, this set is not a subgroup of $\mathbb{Z}$. □

(e) the set of real numbers whose square is a rational number (under addition)

Proof.

Let $x, y \in H$ such that $x^2 = a/b, y^2 = c/d$. Then, $xy^{-1} \implies x - y$ so that

$$(x-y)^2 = x^2 - 2xy + y^2 = \tfrac{a}{b} - 2xy + \tfrac{c}{d}$$
but
$$x = \sqrt{\tfrac{a}{b}} \text{ and } y = \sqrt{\tfrac{c}{d}}$$

which means the square of $x - y$ is not a rational number.

Therefore, H is a not a subgroup of the real numbers. □

3. Show that the following subsets of the dihedral group D_8 are actually subgroups:

For dihedral groups we have the relations $s^2 = 1, rs = sr^{-1}$.

Let us denote the subset of the given form as H.

(a) $\{1, r^2, s, sr^2\}$

Proof.

Obviously H is non-empty.

$n = 4$ for D_8 so $r^4 = 1$.

Each of the elements are their own inverses:

$$\begin{aligned}
1 \cdot 1 &= 1 \\
r^2 \cdot r^2 &= r^4 = 1 \\
s \cdot s &= s^2 = 1 && [s^2 = 1] \\
sr^2 \cdot sr^2 &= sr^2 sr^2 \\
&= sr(rs)rr \\
&= srsr^{-1}r && [rs = sr^{-1}] \\
&= s(rs)r \\
&= ssr^{-1}r && [rs = sr^{-1}] \\
&= s^2 = 1 && [s^2 = 1]
\end{aligned}$$

Thus, H is closed under inverses.

For multiplication we can look at the combinations:

$$\begin{aligned}
r^2 \cdot s &= r(rs) \\
&= (rs)r^{-1} && [rs = sr^{-1}] \\
&= sr^{-1}r^{-1} && [rs = sr^{-1}] \\
&= sr^{-2} \\
&= sr^2 && [r^2 \text{ is its own inverse}] \\
r^2 \cdot sr^2 &= r(rs)rr \\
&= (rs)r^{-1}rr && [rs = sr^{-1}] \\
&= (rs)r \\
&= sr^{-1}r && [rs = sr^{-1}] \\
&= s \\
s \cdot r^2 &= sr^2 \\
s \cdot sr^2 &= s^2 r^2 \\
&= r^2 && [s^2 = 1] \\
sr^2 \cdot s &= sr(rs) \\
&= s(rs)r^{-1} && [rs = sr^{-1}] \\
&= ssr^{-1}r^{-1} && [rs = sr^{-1}] \\
&= s^2 r^{-2} && [s^2 = 1] \\
&= r^2 && [r^2 \text{ is its own inverse}] \\
sr^2 \cdot r^2 &= sr^4 \\
&= s && [r^4 = 1]
\end{aligned}$$

Thus, H is closed under multiplication.

Therefore, H is a subgroup of D_8. □

(b) $\{1, r^2, sr, sr^3\}$

Obviously H is non-empty.

$n = 4$ for D_8 so $r^4 = 1$.

Each of the elements are their own inverses:

$$
\begin{aligned}
1 \cdot 1 &= 1 \\
r^2 \cdot r^2 &= r^4 = 1 \\
sr \cdot sr &= s(rs)r \\
&= ssr^{-1}r && [rs = sr^{-1}] \\
&= s^2 = 1 && [s^2 = 1] \\
sr^3 \cdot sr^3 &= sr^3sr^3 \\
&= srr(rs)rrr \\
&= srrsr^{-1}rrr && [rs = sr^{-1}] \\
&= sr(rs)rr \\
&= srsr^{-1}rr && [rs = sr^{-1}] \\
&= s(rs)r \\
&= ssr^{-1}r && [rs = sr^{-1}] \\
&= s^2 = 1 && [s^2 = 1]
\end{aligned}
$$

Thus, H is closed under inverses.

For multiplication we can look at the combinations:

$$
\begin{aligned}
r^2 \cdot sr &= r(rs)r \\
&= (rs)r^{-1}r && [rs = sr^{-1}] \\
&= sr^{-1}r^{-1}r && [rs = sr^{-1}] \\
&= sr^{-2}r \\
&= sr^3 && [r^2 \text{ is its own inverse}] \\
r^2 \cdot sr^3 &= r(rs)rrr \\
&= (rs)r^{-1}rr && [rs = sr^{-1}] \\
&= sr^{-2}r^3 && [rs = sr^{-1}] \\
&= sr^5 && [r^2 \text{ is its own inverse}] \\
&= sr && [r^4 = 1] \\
sr \cdot r^2 &= sr^3 \\
sr \cdot sr^3 &= s(rs)r^3 \\
&= ssr^{-1}r^3 && [rs = sr^{-1}] \\
&= s^2r^2 \\
&= r^2 && [s^2 = 1] \\
sr^3 \cdot r^2 &= sr^5 \\
&= sr^4r \\
&= sr && [r^4 = 1] \\
sr^3 \cdot sr &= srr(rs)r \\
&= sr(rs)r^{-1}r && [rs = sr^{-1}] \\
&= s(rs)r^{-1}r^{-1}r && [rs = sr^{-1}] \\
&= s^2r^{-3}r && [rs = sr^{-1}] \\
&= r^{-2} \\
&= r^2 && [r^2 \text{ is its own inverse}]
\end{aligned}
$$

Thus, H is closed under multiplication.

Therefore, H is a subgroup of D_8. □

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

Proof. Let G be $\mathbb{Z}$ and let H be the infinite set $\mathbb{Z}^+$ under addition. H is closed under addition but it does not contain the identity nor additive inverses. Therefore, H is not a subgroup of G. □

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

Proof. From Exercise 19 of Section 1.7, we know that if G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Since $n = |G| > 2$ we know that G is finite. In order to have a subgroup H with order $n-1$ because this would mean that $n - 1 \mid n$ and this can only be true if $n = 2$. □

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.

Proof. Let us denote the subset of the above form as H.

H is non-empty as it contains the identity element.

If $x, y \in H$ then we know that the orders of x and y are finite. Let $|x| = a$ and $|y| = b$, for some positive integers a, b. Then, since $|y| = |y^{-1}| = b$ we see that $xy^{-1} \implies (xy^{-1})^{lcm(a,b)} = x^{lcm(a,b)}y^{-lcm(a,b)} = 1 \implies |xy^{-1}| = lcm(a, b)$.

Therefore, H is a subgroup of G. □

For an explicit example where this subset is not a subgroup when G is non-abelian let's have $H = GL_n(\mathbb{Q})$ and

$$x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$y = \begin{pmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{pmatrix}$$
$$y^{-1} = \frac{1}{-1}\begin{pmatrix} 0 & -2 \\ -\frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{pmatrix} = y$$
$$x^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$$
$$y^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$$

However , xy^{-1} has infinite order:

$$(xy^{-1})^2 = \begin{pmatrix} \frac{1}{4} & 0 \\ 0 & 4 \end{pmatrix}$$
$$(xy^{-1})^3 = \begin{pmatrix} \frac{1}{8} & 0 \\ 0 & 8 \end{pmatrix}$$
... etc.

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.

The torsion subgroup is the set of elements that have finite order. For $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$ this is the additive subgroup

$$\{(0, i) \mid i \in \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}\}$$

where the identity element is $(0, \overline{0})$.

The set of elements of infinite order together with the identity is not a subgroup because we can see that it is not closed under addition as $(19, \overline{1}) + (-19, \overline{0}) = (0, \overline{1})$, which is an element of finite order.

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 $K \subseteq H$.

Proof.

If $H \cup K \leq G$, then let $x \in H$ and $y \in K$.

$$
\begin{aligned}
x \in H &\implies x \in H \cup K \\
y \in K &\implies y \in H \cup K \\
&\implies xy \in H \cup K \\
&\implies xy \in H \text{ or } xy \in K \\
\text{If } xy \in H, \text{ then } y \in H &\implies K \subseteq H \\
\text{If } xy \in K, \text{ then } x \in K &\implies H \subseteq K
\end{aligned}
$$

Therefore, either $K \subseteq H$ or $H \subseteq K$.

Conversely, if either $K \subseteq H$ or $H \subseteq K$, then let $x \in H$ and $y \in K$.

$$
\begin{aligned}
\text{If } H \subseteq K \text{ then } xy \in K &\implies xy \in H \cup K \\
\text{If } K \subseteq H \text{ then } xy \in H &\implies xy \in H \cup K
\end{aligned}
$$

Thus, $H \cup K$ is closed under multiplication.

Since H and K are groups, the same arguments can be used for inverses and the identity. Thus, $H \cup K$ is a subgroup of G.

Therefore, $H \cup K$ 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 $SL_n(F) \leq GL_n(F)$.

Proof.

identity -

The identity element for GL_nF is the identity matrix for the field F and since this is an identity matrix, its determinant is equal to 1.

Therefore, $SL_n(F)$ contains the identity element.

closed under multiplication -

Let $X, Y \in SL_n(F)$. For square matrices we know that $\det(AB)=\det(A) \cdot \det(B)$.

Therefore, $\det(XY)=\det(X) \cdot \det(Y) = 1 \cdot 1=1$.

Thus, $SL_n(F)$ is closed under multiplication.

closed under inverses -

$SL_n(F)$ is also closed under inverses as the determinate for the inverse of square matrix A is

$$\tfrac{1}{det(A)} \implies \tfrac{1}{1} = 1.$$

Therefore, $SL_n(F) \leq GL_n(F)$. □

10.

(a) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.

Proof. Since H and K are both subgroups of G then properties (1) and (2) of the Subgroup Criterion hold. Additionally, since H and K both contain the identity element $H \cap K$ must as well.

If $x, y \in H \cap K$, then x, y are in both H and K. Therefore, their products and inverses must be as well since they are groups. Thus, $H \cap K$ is closed under multiplication and inverses.

Therefore, 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).

Proof. In part (a) we proved that the intersection of two subsets is itself a subset of G. Therefore, if we take the intersection of this subset with another subset of G, by the same argument of part (a) above, we will see that once again we will have a subset of G. □

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

(a) $\{(a, 1) \mid a \in A\}$

Proof. Since A and B are both groups, they both contain the identity element 1. Thus, this set contains the identity element of $A \times B$ which is the ordered pair $(1, 1)$.

Let a_1, a_2 be elements of this set. Then $a_1 a_2^{-1} \implies (a_1, 1) \cdot (a_2^{-1}, 1) = (a_1 a_2^{-1}, 1)$ which is in this set since $a_1 a_2^{-1} \in A$ as it is a group.

Therefore, this set is a subgroup of $A \times B$. □

(b) $\{(1, b) \mid b \in B\}$

Proof. Since A and B are both groups, they both contain the identity element 1. Thus, this set contains the identity element of $A \times B$ which is the ordered pair $(1, 1)$.

Let b_1, b_2 be elements of this set. Then $b_1 b_2^{-1} \implies (1, b_1) \cdot (1, b_2^{-1}) = (1, b_1 b_2^{-1})$ which is in this set since $b_1 b_2^{-1} \in B$ as it is a group.

Therefore, this set is a subgroup of $A \times B$. □

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

Proof. Since A and B are both groups, they both contain the identity element 1. Thus, this set contains the identity element of $A \times B$ which is the ordered pair $(1, 1)$.

Let a_1, a_2 be elements of this set. Then $a_1 a_2^{-1} \implies (a_1, a_1) \cdot (a_2^{-1}, a_2^{-1}) = (a_1 a_2^{-1}, a_1 a_2^{-1})$ which is in this set since $a_1 a_2^{-1} \in A$ as it is a group.

Therefore, this set is a subgroup of $A \times B$. □

12. Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A:

(a) $\{a^n \mid a \in A\}$

Proof. Since $1^n = 1$ this set contains the identity element.

Let a_1, a_2 be elements of this set. Then if $a_1 a_2^{-1}$ is in this set we must have that $a_1^n a_2^{-n} = (a_1 a_2^{-1})^n$,

$$\begin{aligned} a_1^n a_2^{-n} &= a_{11}a_{12}\cdots a_{1n}a_{21}^{-1}a_{22}^{-1}\cdots a_{2n}^{-1} \\ &= (a_1a_2^{-1})_1(a_1a_2^{-1})_2\cdots(a_1a_2^{-1})_n = (a_1a_2^{-1})^n \end{aligned}$$

Therefore, $a_1a_2^{-1}$ is in this set since $a_1a_2^{-1} \in A$.

Therefore, this set is a subgroup of A. □

(b) $\{a \in A \mid a^n = 1\}$

Proof. Since $1 \in A$ and $1^n = 1$ this set contains the identity element.

Let a_1, a_2 be elements of this set. Then if $a_1a_2^{-1}$ is in this set we must have that $(a_1a_2^{-1})^n = 1$,

$$\begin{aligned} (a_1a_2^{-1})^n &= (a_1a_2^{-1})_1(a_1a_2^{-1})_2\cdots(a_1a_2^{-1})_n \\ &= a_{11}a_{12}\cdots a_{1n}a_{21}^{-1}a_{22}^{-1}\cdots a_{2n}^{-1} \\ &= a_1^n a_2^{-n} = a_1^n(a_2^n)^{-1} \\ &= 1\cdot 1^{-1} = 1\cdot 1 = 1 \end{aligned}$$

Therefore, $a_1a_2^{-1}$ is in this set.

Therefore, this set is a subgroup of A. □

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 $\mathbb{Q}$.

Proof. Since H is a subgroup it must contain the additive identity element which is 0.

If $H \neq \{0\}$ then it contains an element other than the identity element. Let that element be x. Since x is a rational number we can denote it as $x = \frac{a}{b}$ for integers a, b. Since x is nonzero H also contains the element $\frac{1}{x} = \frac{b}{a}$. Additionally, since H is a group it also contains the additive inverses of these elements, $-\frac{a}{b}$ and $-\frac{b}{a}$.

Since H is closed under addition we know that there must be an element of the group for adding $\frac{a}{b}$ to itself b times to give us $b\frac{a}{b} = a$. Since a is an integer, and noting that the same argument is valid for $-\frac{a}{b}$, we see that H contains all of $\mathbb{Z}$ and their inverses (using the property of H).

Thus, since any rational number can be constructed from combinations of integers and their reciprocals we see that $\mathbb{Q} \subseteq H$. But $H \subseteq \mathbb{Q}$ so therefore we have $H = \mathbb{Q}$. □

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

Proof.

Let x, y be elements of the set. To have xy^{-1} in the set it must satisfy the condition that $(xy^{-1})^2 = 1$. But D_{2n} is non-abelian so,

$$(xy^{-1})^2 = xy^{-1}xy^{-1} \neq 1 \text{ if } x \neq y$$

Therefore, this is not a subgroup of D_{2n}. □

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

Proof. Let us denote $H_1 \leq H_2 \leq \cdots$ as H.

Since H_1 is a group, it must contain the identity element so therefore H contains the identity element as well.

Let $x, y \in H$ so that $x \in H_m$ and $y, y^{-1} \in H_n$ for some positive integers m, n. Then $xy^{-1} \in H_N$ where $N = \max(m, n)$, which implies that $xy^{-1} \in H$.

Therefore, H 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*).

Proof. [Induction] Let us denote $\{(a_{ij}) \in GL_n(F) \mid a_{ij} = 0$ as H_n

A matrix that is 1×1 is trivially an upper triangular matrix.

Additionally, so we don't have to prove this for each step, it is easy to see that the H_n contains the identity matrix I_n, for all n, as it is an upper triangular matrix.

base case ($n = 2$) -

Let $A, B \in H_2$ such that

$$A = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}$$
$$B = \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix}$$

The inverse of B is

$$B^{-1} = \frac{1}{b_{11}b_{22}} \begin{pmatrix} b_{22} & -b_{12} \\ 0 & b_{11} \end{pmatrix}$$

Thus, H_2 is closed under inverses.

H_2 is also closed under multiplication as

$$A \cdot B = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} + a_{12}b22 \\ 0 & a_{22}b_{22} \end{pmatrix}$$

is an upper triangular matrix.

Therefore, H_2 is a subgroup of $GL_2(F)$.

induction hypothesis ($n = k$) -

Assume that H_k is a subgroup of $GL_k(F)$.

induction step ($n = k + 1$) -

An upper triangular matrix can be broken up as an upper block-diagonal matrix

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1(k+1)} \\ 0 & a_{22} & \cdots & a_{2(k+1)} \\ 0 & 0 & \ddots & \cdots \\ 0 & 0 & \cdots & a_{(k+1)(k+1)} \end{bmatrix} = \left[\begin{array}{ccc|c} & & & a_{1(k+1)} \\ & A_k & & a_{2(k+1)} \\ & & & \vdots \\ & & & a_{k(k+1)} \\ \hline 0 & 0 & \cdots & a_{(k+1)(k+1)} \end{array}\right]$$

Let $A, B \in H_{k+1}$ such that

$$A = \left[\begin{array}{ccc|c} & & & a_{1(k+1)} \\ & A_k & & a_{2(k+1)} \\ & & & \vdots \\ & & & a_{k(k+1)} \\ \hline 0 & 0 & \cdots & a_{(k+1)(k+1)} \end{array}\right]$$

$$B = \left[\begin{array}{ccc|c} & & & b_{1(k+1)} \\ & B_k & & b_{2(k+1)} \\ & & & \vdots \\ & & & b_{k(k+1)} \\ \hline 0 & 0 & \cdots & b_{(k+1)(k+1)} \end{array}\right]$$

The inverse of B is

$$B^{-1} = \frac{1}{B_k b_{(k+1)(k+1)}} \left[\begin{array}{ccc|c} & & & b_{1(k+1)} \\ & b_{(k+1)(k+1)} & & b_{2(k+1)} \\ & & & \vdots \\ & & & b_{k(k+1)} \\ \hline 0 & 0 & \cdots & B_k \end{array}\right]$$

Thus, H_{k+1} is closed under inverses (since the block-diagonal matrix can be converted back to an upper triangular matrix).

H_{k+1} is also closed under multiplication as

$$A \cdot B = \left[\begin{array}{ccc|c} & & & a_{1(k+1)} \\ & A_k & & a_{2(k+1)} \\ & & & \vdots \\ & & & a_{k(k+1)} \\ \hline 0 & 0 & \cdots & a_{(k+1)(k+1)} \end{array}\right] \left[\begin{array}{ccc|c} & & & b_{1(k+1)} \\ & B_k & & b_{2(k+1)} \\ & & & \vdots \\ & & & b_{k(k+1)} \\ \hline 0 & 0 & \cdots & b_{(k+1)(k+1)} \end{array}\right] =$$

$$\left[\begin{array}{c|c} A_k B_k & A_k \begin{bmatrix} b_{1(k+1)} \\ b_{2(k+1)} \\ \vdots \\ b_{k(k+1)} \end{bmatrix} + \begin{bmatrix} a_{1(k+1)} \\ a_{2(k+1)} \\ \vdots \\ a_{k(k+1)} \end{bmatrix} b_{(k+1)(k+1)} \\ \hline 0 \ 0 \ \cdots \ 0 & a_{(k+1)(k+1)} b_{(k+1)(k+1)} \end{array}\right]$$

is an upper triangular matrix (since the block-diagonal matrix can be converted back to an upper triangular matrix).

Therefore, H_{k+1} is a subgroup of $GL_{k+1}(F)$ and by induction H_n is a subgroup of $GL_n(F)$ for all n. □

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

Proof. Using the same proof as Exercise 16 but this time with the added condition that the diagonal elements must be equal to 1.

Obviously the identity matrix satisfies this and it is easy to see that for $n = 2$ it does as well by looking at the inverse and the multiplication portions of the proof.

For the induction hypothesis we assume it holds for $n = k$. Then in the induction step, we can see it holds for inverses and multiplication of matrices from the induction hypothesis, so that it indeed holds for $n = k + 1$ and therefore by induction, all of n. □

2.2 CENTRALIZERS AND NORMALIZERS, STABILIZERS AND KERNELS

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

Proof. The definition of $C_G(A)$ is $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$.

$$\begin{aligned} gag^{-1} &= a \\ gag^{-1}g &= ag \\ ga &= ag \\ g^{-1}ga &= g^{-1}ag \\ a &= g^{-1}ag \end{aligned}$$

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

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

Proof. The definition for $Z(G)$ is $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$.

Therefore, *all* the elements of $Z(G)$ commute with *all* the elements of G.

The definition of $C_G(A)$ is the elements of G that commute with *all* the elements of the subset A. If the subset is $Z(G)$, we already know that *all* the elements of $Z(G)$ commute with *all* the elements of G. Therefore, $C_g(Z(G)) = G$. □

The elements of $N_G(A)$ are the elements of G that commute either point wise or to another element of the set A. For $Z(G)$ we already know that all of the elements of G commute point wise with all the elements of $Z(G)$, therefore $N_G(Z(G)) = G$.

3. 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. Centralizers are groups, as proved in the text, so we must show that $C_G(B) \subseteq C_G(A)$.

Let $g \in C_G(B)$, then

$$\begin{aligned} &gbg^{-1} = b \text{ for all } b \in B \\ &gbg^{-1} = b \text{ for all } b \in A && [A \subseteq B] \\ &g \in C_G(A). \end{aligned}$$

Thus, $C_G(B) \subseteq C_G(A)$.

Therefore, $C_G(B) \leq C_G(A)$. □

4. For each of S_3, D_8, and Q_8 compute the centralizers of each element and find the center of each group. Does Lagrange's Theorem (Exercise 19 in Section 1.7) simplify your work?

$$
\begin{aligned}
S_3 &= \{1, (12), (13), (23), (123), (132)\} \\
C_{S_3}(1) &= S_3 \\
C_{S_3}((12)) &= \{1, (12)\} \\
C_{S_3}((13)) &= \{1, (13)\} \\
C_{S_3}((23)) &= \{1, (23)\} \\
C_{S_3}((123)) &= \{1, (123), (132)\} \\
C_{S_3}((132)) &= \{1, (123), (132)\} \\
Z(S_3) &= 1 \\
D_8 &= \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} \\
C_{D_8}(1) &= D_8 \\
C_{D_8}(r) &= \{1, r, r^2, r^3\} \\
C_{D_8}(r^2) &= \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} \\
C_{D_8}(r^3) &= \{1, r, r^2, r^3\} \\
C_{D_8}(s) &= \{1, r^2, s, sr^2\} \\
C_{D_8}(sr) &= \{1, r^2, sr, sr^3\} \\
C_{D_8}(sr^2) &= \{1, r^2, s, sr^2\} \\
C_{D_8}(sr^3) &= \{1, r^2, sr, sr^3\} \\
Z(D_8) &= \{1, r^2\} \\
Q_8 &= \{1, -1, i, -i, j, -j, k, -k\} \\
C_{Q_8}(1) &= Q_8 \\
C_{Q_8}(-1) &= Q_8 \\
C_{Q_8}(i) &= \{1, -1, i, -i\} \\
C_{Q_8}(-i) &= \{1, -1, i, -i\} \\
C_{Q_8}(j) &= \{1, -1, j, -j\} \\
C_{Q_8}(-j) &= \{1, -1, j, -j\} \\
C_{Q_8}(k) &= \{1, -1, k, -k\} \\
C_{Q_8}(-k) &= \{1, -1, k, -k\} \\
Z(Q_8) &= \{1, -1\}
\end{aligned}
$$

Yes, Lagrange's Theorem helps because we know that since $C_G(A) \leq G$ then we must have that $|C_G(A)|$ divides $|G|$. With this information we know that the orders of our centralizers must meet this criteria.

5. In each of parts (a) to (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. We know that $C_G(A) \leq G$ so by Lagrange's Theorem we know that $|C_G(A)|$ divides $|G|$. Thus,

$|C_G(A)|$ is equal to 2, 3 or 6. Since (1 2) doesn't commute with (1 2 3) it must be either 2 or 3. Noting that (1 2 3) and (1 3 2) commute with one another we see that $|C_G(A)|$ must be equal to 3, and more specifically to A.

We know that $C_G(A) \leq N_G(A) \leq G$ (as mentioned in the text) so by Lagrange's Theorem again we know that $|C_G(A)|$ divides $|N_G(A)|$, which divides $|G|$.

Therefore, $3 \mid |N_G(A)| \leq 6$. This shows that $|N_G(A)|$ is equal to 3 or 6. If the former, then $N_G(A) = A$ but since (1 2) $\circ$ (1 2 3)=(1 3 2) $\in A$, then (1 2) $\in N_G(A)$. Therefore, $|N_G(A)| = 6$ and thus $N_G(A) = G$. □

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

Proof. From Lagrange's Theorem we know that the order of $C_G(A)$ is either 1, 2, 4, or 8. It can't be the later since we know that s and r don't commute, i.e. $rs = sr^{-1}$. Additionally, we know that since G is generated from r and s and that both commute with r^2 (along with 1), so all elements will commute with r^2. For A, we also see that s will commute with all the elements so we must have that $|C_G(A)| = 4$. Thus, $G_G(A) = A$.

We know that $C_G(A) \leq N_G(A) \leq G$ (as mentioned in the text) so by Lagrange's Theorem again we know that $|C_G(A)|$ divides $|N_G(A)|$, which divides $|G|$.

Therefore, since $|C_G(A)| = 4$ we must have that $|N_G(A)|$ is either 4 or 8. However, since $rsr^{-1} = sr^{-1}r^{-1} = sr^{-2} = sr^2$ which is an element of A, we see that $r \in N_G(A)$ so we must have that the order of $N_G(A)$ is 8 since $C_G(A) = A \leq N_G(A)$. Therefore, $N_G(A) = G$. □

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

Proof. From Lagrange's Theorem we know that the order of $C_G(A)$ is either 1, 2, 5, or 10. Since s and r don't commute it can't be 10 nor can it be 2 as r commutes with all of the other powers of r. Therefore, it must have order 5 and is therefore $C_G(A) = A$.

We know that $C_G(A) \leq N_G(A) \leq G$ (as mentioned in the text) so by Lagrange's Theorem again we know that $|C_G(A)|$ divides $|N_G(A)|$, which divides $|G|$.

Therefore, since $|C_G(A)| = 5$ we must have that $|N_G(A)|$ is either 5 or 10. However, since $sr^2s^{-1} = srrs^{-1} = r^{-1}srs^{-1} = r^{-1}r^{-1}ss^{-1} = r^{-2} = r^2$ which is an element of A, we see that $s \in N_G(A)$ so we must have that the order of $N_G(A)$ is 10 since $C_G(A) = A \leq N_G(A)$. Therefore, $N_G(A) = G$. □

6. 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 $x \in H$. Then since $x \in G$ we have that $xx = xx$ so that $x \in N_G(H)$. Therefore, $H \leq N_G(HG)$.

If H is not a subgroup it could be a subset of G that does not contain the identity element and the identity element belongs to $N_G(H)$. □

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

Proof. Suppose $H \leq C_G(H)$, then for $x \in C_G(H) \implies x \in H$ so that $xx = xx$, for all $x \in H$. Therefore, H is abelian.

If H is abelian, then for $x \in H \implies x \in G$ we have that $xx = xx$ for all $x \in H$. Therefore, $x \in C_G(H)$ so that $H \leq C_H(G)$. □

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

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

Proof. For D_{2n} the generators are r and s, which don't commute. However, we have seen that powers of r do commute for with s in some of the previous exercises. For example, for D_8 we saw that r^2 commuted with s. The reason this power of r commuted with s is because n was a number where $r^{-2} = r^2$. That is the inverse rotations matched up with forward rotations, which can only happen in the middle of the n-gon. If $n = 2k$ is an even number then $r^k = r^{-k}$.

If n is an odd number then $n = 2k+1$ and we see that we will not have an even number of forward rotations that match up with the same amount of inverse rotations.

Therefore, $Z(D_{2n}) = 1$ if n is odd. □

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

Proof. Most of the leg work for this proof is done in part (a) above, as we have already seen that if $n = 2k$ is an even number then $r^k = r^{-k}$.

Thus, $sr^k s^{-1} = srr^{k-1}s^{-1} = r^{-1}sr^{k-1}s^{-1} = \cdots = r^{-k}ss^{-1} = r^{-k} = r^k$.

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

8. Let $G = S_n$, fix an $i \in \{1, 2, \ldots, n\}$ 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. $1 \in G_i$ by axiom (2) of an action.

If $\sigma \in G_i$, then

$$\begin{aligned} i = 1(i) &= (\sigma^{-1}\sigma)(i) \\ &= \sigma^{-1}(\sigma(i)) && \text{[by axiom (1) of an action]} \\ &= \sigma^{-1}(i) && \text{[since } \sigma \in G_i\text{]} \end{aligned}$$

Therefore, $\sigma^{-1} \in G_i$. If $\sigma_1, \sigma_2 \in G_i$, then

$$\begin{aligned} (\sigma_1\sigma_2)(i) &= \sigma_1(\sigma_2(i)) && \text{[by axiom (1) of an action]} \\ &= \sigma_1(i) && \text{[since } \sigma_2 \in G_i\text{]} \\ &= i && \text{[since } \sigma_1 \in G_i\text{]} \end{aligned}$$

Therefore, G_i is a subgroup of G.

The order of $|G_i|$ is the number of permutations that fix i. If we fix one element then we can permute the other $n-1$ numbers. Therefore, the order is $n-1$. □

9. 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.

Let $h \in N_H(A)$. Then

$h \in H$ and $hAh^{-1} = A$

$h \in H$ and $h \in G$ and $hAh^{-1} = A$ $[A \subseteq G]$

$h \in H$ and $h \in N_G(A)$ [definition of normalizer of A in G]

$h \in H \cap N_g(A)$

Therefore, $N_H(A) \subseteq N_G(A) \cap H$.

Conversely, let $h \in N_G(A) \cap H$.

$h \in G$ and $hAh^{-1} = A$ and $h \in H$

$(h \in G$ and $h \in H)$ and $hAh^{-1} = A$

$h \in H$ and $hAh^{-1} = A$ $[A \subseteq G]$

$h \in N_H(A)$

Thus, $N_G(A) \cap H \subseteq N_H(A)$.

Therefore, $N_H(A) = N_G(A) \cap H$. □

10. 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. Since we know that $N_G(H)$ and $C_G(H)$ are both subgroups of G we can show equality by showing that they are subsets of each other.

Let $g \in C_G(H)$. Then

$ghg^{-1} = h$ for all $h \in H \implies gHg^{-1} = H$

$g \in N_G(H)$

Thus, $C_G(H) \subseteq N_G(H)$.

Conversely, let $g \in N_G(H)$. Then

$$\{g1g^{-1}, ghg^{-1}\} = \{1, h\}$$

Since $g1g^{-1} = 1$, this equality of sets occurs if and only if $ghg^{-1} = h$ as well, i.e., if and only if $g \in C_G(H)$.

Thus, $N_G(H) \subseteq C_G(H)$.

Therefore, $N_G(H) = C_G(H)$. □

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

Proof. Since we know that $Z(G)$ and $N_G(A)$ are both subgroups of G we only need to show that $Z(G) \subseteq N_G(A)$.

If $g \in Z(G)$, then

$$
\begin{aligned}
&gx = xg \text{ for all } x \in G \\
&gx = xg \text{ for all } x \in A && [A \subseteq G] \\
&gx = xg \text{ for some } x \in A \\
&gxg^{-1} = xgg^{-1} \text{ for some } x \in A \\
&gxg^{-1} = x \text{ for some } x \in A \\
&gAg^{-1} = A && [\text{definition of } gAg^{-1}] \\
&g \in N_G(A)
\end{aligned}
$$

Therefore, $Z(G) \subseteq N_G(A)$. □

12. 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 elements 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 $r_1, \ldots, r_4$ are non-negative 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 $\{x_1, \ldots, x_4\}$ 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).

For example, if $\sigma =$(1 2)(3 4) and $p(x_1, \ldots, x_4)$ is the polynomial in $(*)$ above, then

$$
\begin{aligned}
\sigma \cdot p(x_1, x_2, x_3, x_4) &= 12x_2^5x_1^7x_3 - 18x_1^3x_4 + 11x_2^6x_1x_4^3x_3^{23} \\
&= 12x_1^7x_2^5x_3 - 18x_1^3x_4 + 11x_1x_2^6x_3^3x_3^{23}x_4^3
\end{aligned}
$$

(a) Let $p = p(x_1, \ldots, x_4)$ be the polynomial in $(*)$ above, let $\sigma =$(1 2 3 4) and let $\tau =$(1 2 3). Compute $\sigma \cdot p, \tau \cdot (\sigma \cdot p), (\tau \circ \sigma) \cdot p$, and $(\sigma \circ \tau) \cdot p$.

$$
\begin{aligned}
\sigma \cdot p = (1\ 2\ 3\ 4) \cdot p &= 12x_2^5x_3^7x_1 - 18x_3^3x_4 + 11x_2^6x_3x_4^3x_1^{23} \\
&= 12x_1x_2^5x_3^7 - 18x_3^3x_4 + 11x_1^{23}x_2^6x_3x_4^3 \\
\tau \cdot (\sigma \cdot p) = (1\ 2\ 3) \cdot ((1\ 2\ 3\ 4) \cdot p) &= 12x_2x_3^5x_1^7 - 18x_1^3x_4 + 11x_2^{23}x_3^6x_1x_4^3 \\
&= 12x_1^7x_2x_3^5 - 18x_1^3x_4 + 11x_1x_2^{23}x_3^6x_4^3 \\
(\tau \circ \sigma) \cdot p = (1\ 3\ 4\ 2) \cdot p &= 12x_3^5x_1^7x_2 - 18x_1^3x_4 + 11x_3^6x_1x_4^3x_2^{23} \\
&= 12x_1^7x_2x_3^5 - 18x_1^3x_4 + 11x_1x_2^{23}x_3^6x_4^3 \\
(\sigma \circ \tau) \cdot p = (1\ 3\ 2\ 4) \cdot p &= 12x_3^5x_4^7x_1 - 18x_4^3x_2 + 11x_3^6x_4x_2^3x_1^{23} \\
&= 12x_1x_3^5x_4^6 - 18x_2x_4^3 + 11x_1^{23}x_2^3x_3^6x_4
\end{aligned}
$$

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

Proof.

Let $p \in R$. Then $1 \in S_4$ is the identity permutation that fixes all independent variables of p and we have that

$$1 \cdot p = p \text{ for all } p \in R.$$

Let $\sigma_1, \sigma_2 \in S_4$ and $pinR$, then

$$\begin{aligned}
\sigma_1 \cdot (\sigma_2 \cdot p) &= \sigma_1 \cdot p(x_{\sigma_2(1)}, x_{\sigma_2(2)}, x_{\sigma_2(3)}, x_{\sigma_2(4)}) && \text{[definition of } \sigma \cdot p\text{]} \\
&= p(x_{\sigma_1(\sigma_2(1))}, x_{\sigma_1(\sigma_2(2))}, x_{\sigma_1(\sigma_2(3))}, x_{\sigma_1(\sigma_2(4))}) && \text{[definition of } \sigma \cdot p\text{]} \\
&= p(x_{(\sigma_1 \circ \sigma_2)(1)}, x_{(\sigma_1 \circ \sigma_2)(2)}, x_{(\sigma_1 \circ \sigma_2)(3)}, x_{(\sigma_1 \circ \sigma_2)(4)}) && \text{[definition of composition]} \\
&= (\sigma_1 \circ \sigma_2) \cdot p && \text{[definition of } \sigma \cdot p\text{]}
\end{aligned}$$

Therefore, these definitions give a left 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.

The elements of S_4 that stabilize the 4th element are: {1, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)}

The elements of S_3 have the cycle decompositions: {1, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)} [Exercise 4 Section 1.3]

Since these sets are equivalent, we see that all permutations in S_4 that stabilize x_4 is a group and is isomorphic to S_3. □

(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.

The elements of S_4 that stabilize the element $x_1 + x_2$ are: {1, (1 2), (3 4), (1 2)(3 4)}

1 is an element of the set and

$$\begin{gathered}
(1\ 2) \circ (3\ 4) = (1\ 2)(3\ 4) \\
(3\ 4) \circ (1\ 2) = (1\ 2)(3\ 4) \\
(1\ 2) \circ (1\ 2)(3\ 4) = (1)(2)(3\ 4) = (3\ 4) \\
(1\ 2)(3\ 4) \circ (1\ 2) = (1)(2)(3\ 4) = (3\ 4) \\
(3\ 4) \circ (1\ 2)(3\ 4) = (1\ 2)(3)(4) = (1\ 2) \\
(1\ 2)(3\ 4) \circ (3\ 4) = (1\ 2)(3)(4) = (1\ 2)
\end{gathered}$$

Therefore, this is an abelian subgroup of order 4. □

(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.

The elements of S_4 that stabilize the element $x_1x_2 + x_3x_4$ are:

$$\{1, (1\ 2), (3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3)\}$$

This set has order 8, so let's see if we can find if the elements match to the elements of D_8. We know that D_8 is generated by r and s with $s^2 = 1, r^4 = 1, rs = sr^{-1}$.

Let $r =$(1 3 2 4) and $s =$(1 3)(2 4) so that

$$\begin{aligned}
r^4 &= (1\ 3\ 2\ 4) \circ ((1\ 3\ 2\ 4) \circ ((1\ 3\ 2\ 4) \circ (1\ 3\ 2\ 4))) \\
&= (1\ 3\ 2\ 4) \circ ((1\ 3\ 2\ 4) \circ (1\ 2)(3\ 4)) \\
&= (1\ 3\ 2\ 4) \circ (1\ 4\ 2\ 3) \\
&= (1)(2)(3)(4) = 1 \\
s^2 &= (1\ 3)(2\ 4) \circ (1\ 3)(2\ 4) \\
&= (1)(2)(3)(4) = 1 \\
rs &= (1\ 3\ 2\ 4) \circ (1\ 3)(2\ 4) = (1\ 2) \\
sr^{-1} &= (1\ 3)(2\ 4) \circ (4\ 2\ 3\ 1) = (1\ 2)
\end{aligned}$$

This shows us that the relations match. Now, let's see if we can generate the rest of D_8 with r and s, which would show that this set is isomorphic to D_8:

$$\begin{aligned}
r^2 &= (1\ 3\ 2\ 4) \circ (1\ 3\ 2\ 4) = (1\ 2)(3\ 4) \\
r^3 &= (1\ 3\ 2\ 4) \circ (1\ 2)(3\ 4) = (1\ 4\ 2\ 3) \\
sr &= (1\ 3)(2\ 4) \circ (1\ 3\ 2\ 4) = (3\ 4) \\
sr^2 &= (1\ 3)(2\ 4) \circ (1\ 2)(3\ 4) = (1\ 4)(2\ 3) \\
sr^3 &= (1\ 3)(2\ 4) \circ (1\ 4\ 2\ 3) = (1\ 2)
\end{aligned}$$

Therefore, this set is isomorphic to D_8. □

(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). (The two polynomials appearing in parts (e) and (f) and the subgroup that stabilizes them will play an important role in the study of roots of quartic equations in Section 14.6.)

Proof. The permutations are {1, (1 2), (3 4), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3), (1 3 2 4), (1 4 2 3)}.

Obviously the identity element stabilizes the element $(x_1 + x_2)(x_3 + x_4)$.

$(x_1 + x_2)(x_3 + x_4) = x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4$

$$\begin{aligned}
(1\ 2) : x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 &\implies x_2x_3 + x_2x_4 + x_1x_3 + x_1x_4 \\
(3\ 4) : x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 &\implies x_1x_4 + x_1x_3 + x_2x_4 + x_2x_3 \\
(1\ 2)(3\ 4) : x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 &\implies x_2x_4 + x_2x_3 + x_1x_4 + x_1x_3 \\
(1\ 3)(2\ 4) : x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 &\implies x_3x_1 + x_3x_2 + x_4x_1 + x_4x_2 \\
(1\ 4)(2\ 3) : x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 &\implies x_4x_2 + x_4x_1 + x_3x_2 + x_3x_1 \\
(1\ 3\ 2\ 4) : x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 &\implies x_3x_2 + x_3x_1 + x_4x_2 + x_4x_1 \\
(1\ 4\ 2\ 3) : x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 &\implies x_4x_1 + x_4x_2 + x_3x_1 + x_3x_2
\end{aligned}$$

As we can see, the element $(x_1+x_2)(x_3+x_4) = x_1x_3+x_1x_4+x_2x_3+x_2x_4$ is stabilized after the permutations.

Therefore, 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). □

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

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

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

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

Proof. This is similar to part (b) of Exercise 12 and it is easy to see that instead of 4 independent variables for S_4, it will be true for n independent variables for S_n as the proof only depends on the function composition of each independent variable.

$$\begin{aligned}
\sigma_1 \cdot (\sigma_2 \cdot p) &= \sigma_1 \cdot p(x_{\sigma_2(1)}, x_{\sigma_2(2)}, \ldots, x_{\sigma_2(n)}) && \text{[definition of } \sigma \cdot p\text{]} \\
&= p(x_{\sigma_1(\sigma_2(1))}, x_{\sigma_1(\sigma_2(2))}, \ldots, x_{\sigma_1(\sigma_2(n))}) && \text{[definition of } \sigma \cdot p\text{]} \\
&= p(x_{(\sigma_1\circ\sigma_2)(1)}, x_{(\sigma_1\circ\sigma_2)(2)}, \ldots, x_{(\sigma_1\circ\sigma_2)(n)}) && \text{[definition of composition]} \\
&= (\sigma_1 \circ \sigma_2) \cdot p && \text{[definition of } \sigma \cdot p\text{]}
\end{aligned}$$

Therefore, these definitions give a left group action of S_n on R. □

14. 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.

From Exercise 11 of Section 1.4 we saw:

Let $H(F) = \{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F\}$ — called the *Heisenberg group* over F. Let $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}$ be elements of $H(F)$.

$$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix}$$

and that any matrix with $af \neq dc$ will not commute. Thus, they will commute if a and c are both zero.

Therefore, the center of the Heisenberg group is

$$Z(H(F)) = \{\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid b \in F\}$$

We now will prove that this is isomorphic to the additive group F. Let

$$\varphi(b) = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

It is obviously injective and surjective, so it is a bijection. It is also a homomorphism as

$$\varphi(a+b) = \begin{pmatrix} 1 & 0 & a+b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \varphi(a)\varphi(b)$$

Therefore, $Z(H(F)) \cong F$. □

2.3 CYCLIC GROUPS AND CYCLIC SUBGROUPS

1. Find all subgroups of $Z_{45} = \langle x \rangle$, giving a generator for each. Describe the containments between these subgroups.

$Z_{45} = \langle \overline{1} \rangle = \langle \overline{2} \rangle = \langle \overline{4} \rangle = \langle \overline{7} \rangle = \langle \overline{8} \rangle = \langle \overline{11} \rangle = \langle \overline{13} \rangle = \langle \overline{14} \rangle = \langle \overline{16} \rangle = \langle \overline{17} \rangle = \langle \overline{19} \rangle = \langle \overline{22} \rangle = \langle \overline{23} \rangle = \langle \overline{26} \rangle = \langle \overline{28} \rangle = \langle \overline{29} \rangle = \langle \overline{31} \rangle = \langle \overline{32} \rangle = \langle \overline{34} \rangle = \langle \overline{37} \rangle = \langle \overline{38} \rangle = \langle \overline{41} \rangle = \langle \overline{43} \rangle = \langle \overline{44} \rangle$ (order 45)

$\langle \overline{3} \rangle = \langle \overline{6} \rangle = \langle \overline{12} \rangle = \langle \overline{21} \rangle = \langle \overline{24} \rangle = \langle \overline{33} \rangle = \langle \overline{39} \rangle = \langle \overline{42} \rangle$ (order 15)

$\langle \overline{5} \rangle = \langle \overline{10} \rangle = \langle \overline{20} \rangle = \langle \overline{25} \rangle = \langle \overline{35} \rangle = \langle \overline{40} \rangle$ (order 9)

$\langle \overline{9} \rangle = \langle \overline{18} \rangle = \langle \overline{27} \rangle = \langle \overline{36} \rangle$ (order 5)

$\langle \overline{15} \rangle = \langle \overline{30} \rangle$ (order 3)

$\langle \overline{45} \rangle$ (order 1)

The containments between them are given by

$$\langle \overline{a} \rangle \leq \langle \overline{b} \rangle \text{ if and only if } (b, 45) \mid (a, 45),\ 1 \leq a, b \leq 45.$$

2. If x is an element of the finite group G and $|x| = |G|$, prove that $G = \langle x \rangle$. Give an explicit example to show that this result need not be true if G is an infinite group.

Proof. If $|G| = |x| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are distinct because if $x^a = x^b$, with say, $0 \leq a < b < n$, then $x^{b-a} = x^0 = 1$, contrary to n being the smallest positive power of x giving the identity. Therefore, G has at least n elements and it remains to show that these are all of them. If x^t is any power of x, use the Division Algorithm to write $t = nq + k$, where $0 \leq k < n$, so

$$x^t = x^{nq+k} = (x^n)^q x^k = 1^q x^k = x^k \in \{1, x, x^2, \ldots, x^{n-1}\}$$

There are all of the elements of G. Thus, $|G| = n$ and we also see that G is generated from x so that $G = \langle x \rangle$. □

3. Find all the generators for $\mathbb{Z}/48\mathbb{Z}$.

Any n such that $gcd(n, 48) = 1$ (i.e., the numbers less than 48 that have no factors of 2 or 3).

4. Find all the generators for $\mathbb{Z}/202\mathbb{Z}$.

Any n such that $gcd(n, 202) = 1$ (i.e., the numbers less than 202 that have no factors of 2 or 101).

5. Find all the generators for $\mathbb{Z}/49000\mathbb{Z}$.

```
sage: g = 0
sage: for i in range(1,49000):
....:     if gcd(i,49000) == 1:
....:         g += 1
....:
sage: g
16800
sage: euler_phi(49000)
16800
```

Any n such that $gcd(n, 49000) = 1$ (i.e., the numbers less than 49000 that have no factors of 2, 5 or 7).

6. In $\mathbb{Z}/48\mathbb{Z}$ write out all elements of $\langle\overline{a}\rangle$ for every $\overline{a}$. Find all inclusions between subgroups in $\mathbb{Z}/48\mathbb{Z}$.

$\mathbb{Z}/48\mathbb{Z} = \langle\overline{1}\rangle = \langle\overline{5}\rangle = \langle\overline{7}\rangle = \langle\overline{11}\rangle = \langle\overline{13}\rangle = \langle\overline{17}\rangle = \langle\overline{19}\rangle = \langle\overline{23}\rangle = \langle\overline{25}\rangle = \langle\overline{29}\rangle = \langle\overline{31}\rangle = \langle\overline{35}\rangle = \langle\overline{37}\rangle = \langle\overline{41}\rangle = \langle\overline{43}\rangle = \langle\overline{47}\rangle$

7. Let $Z_{48} = \langle x\rangle$ and use the isomorphism $\mathbb{Z}/48\mathbb{Z} \cong Z_{48}$ given by $\overline{1} \mapsto x$ to list all subgroups of Z_{48} as computed in the preceding exercise.

8. Let $Z_{48} = \langle x\rangle$. For which integers a does the map φ_a defined by $\varphi_a : \overline{1} \mapsto x^a$ extend to an *isomorphism* from $\mathbb{Z}/48\mathbb{Z}$ onto Z_{48}.

9. Let $Z_{36} = \langle x\rangle$. For which integers a does the map ψ_a defined by $\psi_a : \overline{1} \mapsto x^a$ extend to a *well defined homomorphism* from $\mathbb{Z}/48\mathbb{Z}$ into Z_{36}. Can ψ_a ever be a surjective homomorphism?

10. What is the order of $\overline{30}$ in $\mathbb{Z}/54\mathbb{Z}$? Write out all the elements and their orders in $\langle\overline{30}\rangle$.

11. Find all cyclic subgroups of D_8. Find a proper subgroup of D_8 which is not cyclic.

12. Prove that the following groups are *not* cyclic:

(a) $Z_2 \times Z_2$

(b) $Z_2 \times \mathbb{Z}$

(c) $\mathbb{Z} \times \mathbb{Z}$

13. Prove that the following pairs of groups are *not* isomorphic:

(a) $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$

(b) $\mathbb{Q} \times Z_2$ and $\mathbb{Q}$

14. Let σ =(1 2 3 4 5 6 7 8 9 10 11 12). For each of the following integers a compute σ^a:

a=13,65,626,1195,-6,-81,-570 and -1211

15. Prove that $\mathbb{Q} \times \mathbb{Q}$ is not cyclic.

16. Assume $|x| = n$ and $|y| = m$. Suppose that x and y *commute*: $xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n. Need this be true if x and y do *not* commute? Give an example of commuting elements x, y such that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$.

17. Find a presentation for Z_n with one generator.

18. Show that if H is any group and h is an element of H with $h^n = 1$, then there is a unique homomorphism from $Z_n = \langle x \rangle$ to H such that $x \mapsto h$.

19. Show that if H is any group and h is an element of H, then there is a unique homomorphism from $\mathbb{Z}$ to H such that $1 \mapsto h$.

20. Let p be a prime and let n be a positive integer. Show that if x is an element of the group G such that $x^p = 1$ then $|x| = p^m$ from some $m \leq n$.

21. Let p be an odd prime and let n be a positive integer. Use the Binomial Theorem to show that $(1+p)^{p^{n-1}} \equiv 1 \pmod{p}^n$ but $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p}^n$. Deduce that $1+p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

22. Let n be an integer ≥ 3. Use the Binomial Theorem to show that $(1+2^2)^{2^{n-2}} \equiv 1 \pmod{2}^n$ but $(1+2^2)^{2^{n-3}} \not\equiv 1 \pmod{2}^n$. Deduce that 5 is an element of order 2^{n-1} in the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

23. Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. [Find two distinct subgroups of order 2.] **24.** Let G be a finite group and let $x \in G$.

(a) Prove that if $g \in N_G(\langle x \rangle)$ then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) Prove conversely that if $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$ then $g \in N_G(\langle x \rangle)$. [Show first that $gx^kg^{-1} = (gxg^{-1})^k = x^{ak}$ for any integer k, so that $g\langle x \rangle g^{-1} \leq \langle x \rangle$. IF x has order n, show the elements $gx^ig^{-1}, i = 0, 1, \ldots, n-1$ are distinct, so that $|g\langle x \rangle g^{-1}| = |\langle x \rangle| = n$ and conclude that $g\langle x \rangle g^{-1} = \langle x \rangle$.]

25. Let G be a cyclic group of order n and let k be an integer relatively prime to n. Prove that the map $x \mapsto x^k$ is surjective. Use Lagrange's Theorem (Exercise 19, Section 1.7) to prove the same is true for any finite group of order n. (For such k each element has a k^{th} root in G. It follows from Cauchy's Theorem in Section 3.2 that if k is not relatively prime to the order of G then the map $x \mapsto x^k$ is not surjective.)

26. Let Z_n be a cyclic group of order n and for each integer a let

$$\sigma_a : Z_n \to Z_n \text{ by } \sigma_a(x) = x^a \text{ for all } x \in Z_n.$$

(a) Prove that σ_a is an automorphism of Z_n if and only if a and n are relatively prime (automorphisms were introduced in Exercise 20, Section 1.6).

(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod{n}$.

(c) Prove that *every* automorphism of Z_n is equal to σ_a for some integer a.

(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\overline{a} \mapsto \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of Z_n (so $Aut(Z_n)$ is an abelian group of order $\varphi(n)$).