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,

$$xy^{-1} \implies (xy^{-1})^2 = x^2y^{-2} = x^2(y^2)^{-1} = \frac{a}{b} \cdot \left(\frac{c}{d}\right)^{-1} = \frac{ad}{bc}$$

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 $xy^{-1} \implies (1\ 2)(3\ 1) = (1\ 3\ 2) \notin H$.

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 $xy^{-1} \in H$

$$(xy^{-1})^n = 1 = x^n y^{-n} \qquad \text{[property of the group]}$$

$$
\begin{aligned}
&= 1y^{-n} \\
&= y^{-n} \\
&= y^{-ab} \\
&= (y^{-a})^b \\
&= ((y^{-a})^b)^{-b} && [(1)^{-b} = 1] \\
&= y^{-a} \\
&= (y^{-1})^a
\end{aligned}
$$

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

$$(x - y)^2 = x^2 - 2xy + y^2 = \frac{a}{b} - 2xy + \frac{c}{d}$$

but

$$x = \sqrt{\frac{a}{b}} \text{ and } y = \sqrt{\frac{c}{d}}$$

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:

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

$$= s^2 = 1 \qquad [s^2 = 1]$$

Thus, H is closed under inverses.

For multiplication we can look at the combinations:

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

Thus, H is closed under multiplication.

Therefore, H is a subgroup of D_8. □

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

Proof. Obviously H is non-empty.

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

Each of the elements are their own inverses:

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

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

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 $n-1$ 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

$$xy^{-1} \implies (xy^{-1})^{\operatorname{lcm}(a,b)} = x^{\operatorname{lcm}(a,b)} y^{-\operatorname{lcm}(a,b)} = 1 \implies |xy^{-1}| = \operatorname{lcm}(a,b)$$

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

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

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 $a_1^n a_2^{-n} = (a_1 a_2^{-1})^n$,

$$a_1^n a_2^{-n} = a_{11} a_{12} \cdots a_{1n} a_{21}^{-1} a_{22}^{-1} \cdots a_{2n}^{-1}$$

$$= (a_1a_2^{-1})_1(a_1a_2^{-1})_2 \cdots (a_1a_2^{-1})_n = (a_1a_2^{-1})^n$$

Thus, $a_1a_2^{-1}$ 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 $(a_1a_2^{-1})^n = 1$,

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

Thus, $a_1a_2^{-1}$ 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. 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, note that 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: For $n = 2$ 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: For $n = k$ suppose that H_k is a subgroup of $GL_k(F)$.

induction step: For $n = k + 1$ an upper triangular matrix can be broken up as an upper block-diagonal matrix

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

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

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

The inverse of B is

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

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

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

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

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 $\{(a_{ij}) \in GL_n(F) \mid a_{ij} = 0 \text{ for all } i > j, \text{ and } a_{ii} = 1 \text{ for all } i\}$ 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?

$$\begin{aligned} S_3 &= \{1, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\} \\ C_{S_3}(1) &= S_3 \\ C_{S_3}((1\,2)) &= \{1, (1\,2)\} \\ C_{S_3}((1\,3)) &= \{1, (1\,3)\} \\ C_{S_3}((2\,3)) &= \{1, (2\,3)\} \\ C_{S_3}((1\,2\,3)) &= \{1, (1\,2\,3), (1\,3\,2)\} \\ C_{S_3}((1\,3\,2)) &= \{1, (1\,2\,3), (1\,3\,2)\} \\ Z(S_3) &= 1 \\ D_8 &= \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} \\ C_{D_8}(1) &= D_8 \\ C_{D_8}(r) &= \{1, r, r^2, r^3\} \\ C_{D_8}(r^2) &= \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} \\ C_{D_8}(r^3) &= \{1, r, r^2, r^3\} \\ C_{D_8}(s) &= \{1, r^2, s, sr^2\} \\ C_{D_8}(sr) &= \{1, r^2, sr, sr^3\} \\ C_{D_8}(sr^2) &= \{1, r^2, s, sr^2\} \\ C_{D_8}(sr^3) &= \{1, r^2, sr, sr^3\} \\ Z(D_8) &= \{1, r^2\} \end{aligned}$$

$$
\begin{aligned}
Q_8 &= \{1, -1, i, -i, j, -j, k, -k\} \\
\mathrm{C}_{Q_8}(1) &= Q_8 \\
\mathrm{C}_{Q_8}(-1) &= Q_8 \\
\mathrm{C}_{Q_8}(i) &= \{1, -1, i, -i\} \\
\mathrm{C}_{Q_8}(-i) &= \{1, -1, i, -i\} \\
\mathrm{C}_{Q_8}(j) &= \{1, -1, j, -j\} \\
\mathrm{C}_{Q_8}(-j) &= \{1, -1, j, -j\} \\
\mathrm{C}_{Q_8}(k) &= \{1, -1, k, -k\} \\
\mathrm{C}_{Q_8}(-k) &= \{1, -1, k, -k\} \\
\mathrm{Z}(Q_8) &= \{1, -1\}
\end{aligned}
$$

Yes, Lagrange's Theorem helps because we know that since $\mathrm{C}_G(A) \leq G$ then we must have that $|\mathrm{C}_G(A)|$ 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, $\mathrm{C}_G(A) = A$ and $\mathrm{N}_G(A) = G$.

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

Proof. We know that $\mathrm{C}_G(A) \leq G$ so by Lagrange's Theorem we know that $|\mathrm{C}_G(A)|$ divides $|G|$. Thus, $|\mathrm{C}_G(A)|$ 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 $|\mathrm{C}_G(A)|$ must be equal to 3, and more specifically to A.

We know that $\mathrm{C}_G(A) \leq \mathrm{N}_G(A) \leq G$ (as mentioned in the text) so by Lagrange's Theorem again we know that $|\mathrm{C}_G(A)|$ divides $|\mathrm{N}_G(A)|$, which divides $|G|$.

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

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

Proof. From Lagrange's Theorem we know that the order of $\mathrm{C}_G(A)$ 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 $|\mathrm{C}_G(A)| = 4$. Thus, $G_G(A) = A$.

We know that $\mathrm{C}_G(A) \leq \mathrm{N}_G(A) \leq G$ (as mentioned in the text) so by Lagrange's Theorem again we know that $|\mathrm{C}_G(A)|$ divides $|\mathrm{N}_G(A)|$, which divides $|G|$.

Therefore, since $|\mathrm{C}_G(A)| = 4$ we must have that $|\mathrm{N}_G(A)|$ 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 $r \in \mathrm{N}_G(A)$ so we must have that the order of $\mathrm{N}_G(A)$ is 8 since $\mathrm{C}_G(A) = A \leq \mathrm{N}_G(A)$. Therefore, $\mathrm{N}_G(A) = G$. □

(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 $\mathrm{C}_G(A)$ 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 $\mathrm{C}_G(A) = A$.

We know that $\mathrm{C}_G(A) \leq \mathrm{N}_G(A) \leq G$ (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, $sr^ks^{-1} = srr^{k-1}s^{-1} = r^{-1}sr^{k-1}s^{-1} = \cdots = r^{-k}ss^{-1} = r^{-k} = r^k$.

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

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

$$= \sigma^{-1}(i) \qquad [\text{since } \sigma \in G_i]$$

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

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

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 $\mathrm{N}_H(A)$ to be the set $\{h \in H \mid hAh^{-1} = A\}$. Show that $\mathrm{N}_H(A) = \mathrm{N}_G(A) \cap H$ and deduce that $\mathrm{N}_H(A)$ is a subgroup of H (note that A need not be a subset of H).

Proof. Let $h \in \mathrm{N}_H(A)$. Then

$$\begin{aligned}&h \in H \text{ and } hAh^{-1} = A\\ &h \in H \text{ and } h \in G \text{ and } hAh^{-1} = A && [A \subseteq G]\\ &h \in H \text{ and } h \in \mathrm{N}_G(A) && [\text{definition of normalizer of } A \text{ in } G]\\ &h \in H \cap N_g(A)\end{aligned}$$

Therefore, $\mathrm{N}_H(A) \subseteq \mathrm{N}_G(A) \cap H$.

Conversely, let $h \in \mathrm{N}_G(A) \cap H$.

$$\begin{aligned}&h \in G \text{ and } hAh^{-1} = A \text{ and } h \in H\\ &(h \in G \text{ and } h \in H) \text{ and } hAh^{-1} = A\\ &h \in H \text{ and } hAh^{-1} = A && [A \subseteq G]\\ &h \in \mathrm{N}_H(A)\end{aligned}$$

Thus, $\mathrm{N}_G(A) \cap H \subseteq \mathrm{N}_H(A)$.

Therefore, $\mathrm{N}_H(A) = \mathrm{N}_G(A) \cap H$. □

10. Let H be a subgroup of order 2 in G. Show that $\mathrm{N}_G(H) = \mathrm{C}_G(H)$. Deduce that if $\mathrm{N}_G(H) = G$ then $H \leq \mathrm{Z}(G)$.

Proof. Since we know that $\mathrm{N}_G(H)$ and $\mathrm{C}_G(H)$ are both subgroups of G we can show equality by showing that they are subsets of each other.

Let $g \in \mathrm{C}_G(H)$. Then

$$\begin{aligned}&ghg^{-1} = h \text{ for all } h \in H \implies gHg^{-1} = H\\ &g \in \mathrm{N}_G(H)\end{aligned}$$

Thus, $\mathrm{C}_G(H) \subseteq \mathrm{N}_G(H)$.

Conversely, let $g \in \mathrm{N}_G(H)$. 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 $g \in \mathrm{C}_G(H)$.

Thus, $\mathrm{N}_G(H) \subseteq \mathrm{C}_G(H)$ and therefore, $\mathrm{N}_G(H) = \mathrm{C}_G(H)$. □

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,

$$12x_1^5x_2^7x_4 - 18x_2^3x_3 + 11x_1^6x_2x_3^3x_4^{23} \qquad (*)$$

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 $p \in R$, 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

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

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

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

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

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.

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

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.

Proof. From Exercise 11 of Section 1.4 we saw:

Let $H(F) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in F \right\}$ — 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

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

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

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

For example, $\langle \overline{3} \rangle = \langle \overline{6} \rangle$ because $(6, 45) \mid (3, 45)$.

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 the number of 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)
```

As we can see from the Python code (using sagemath), the number of generators is 16800.

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 $\mathbb{Z}/48\mathbb{Z}$.

First, let us look at the cyclic subgroups that are generators for $\mathbb{Z}/48\mathbb{Z}$.

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

Since these groups are generators they will all generate the integers mod 48, i.e., $\{0, 1, \dots, 47\}$. For example, $\langle \overline{1} \rangle = \{1 \cdot n \mid n \in \mathbb{Z}/48\mathbb{Z}\} = \{1 \cdot 0, 1 \cdot 1, \dots, 1 \cdot 47\} = \{0, 1, \dots, 47\}$.

Now let us take a look at all the other cyclic subgroups.

$\langle \overline{2} \rangle = \langle \overline{10} \rangle = \langle \overline{14} \rangle = \langle \overline{22} \rangle = \langle \overline{26} \rangle = \langle \overline{34} \rangle = \langle \overline{38} \rangle = \langle \overline{46} \rangle = \{0, 2, 4, 6, \dots, 46\}$

$\langle \overline{3} \rangle = \langle \overline{9} \rangle = \langle \overline{15} \rangle = \langle \overline{21} \rangle = \langle \overline{27} \rangle = \langle \overline{33} \rangle = \langle \overline{39} \rangle = \langle \overline{45} \rangle = \{0, 3, 6, 9, \dots, 45\}$

$\langle \overline{4} \rangle = \langle \overline{20} \rangle = \langle \overline{28} \rangle = \langle \overline{44} \rangle = \{0, 4, 8, 12, \dots, 44\}$

$\langle \overline{6} \rangle = \langle \overline{18} \rangle = \langle \overline{30} \rangle = \langle \overline{42} \rangle = \{0, 6, 12, 18, \dots, 42\}$

$\langle \overline{8} \rangle = \langle \overline{40} \rangle = \{0, 8, 16, 24, 32, 40\}$

$\langle \overline{12} \rangle = \langle \overline{36} \rangle = \{0, 12, 24, 36\}$

$\langle \overline{16} \rangle = \langle \overline{32} \rangle = \{0, 16, 32\}$

$\langle \overline{24} \rangle = \{0, 24\}$

$\langle \overline{0} \rangle = \{0\}$

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.

The map given by $\overline{1} \mapsto x$ means that we have $\overline{k} \mapsto x^k$, where x^k is the generator for the cyclic subgroup. Therefore, all subgroups of Z_{48} as computed in the preceding exercise are:

$$\langle 1 \rangle, \langle x \rangle, \langle x^2 \rangle, \langle x^3 \rangle, \langle x^4 \rangle, \langle x^6 \rangle, \langle x^8 \rangle, \langle x^{12} \rangle, \langle x^{16} \rangle, \langle x^{24} \rangle$$

Please note that $\langle 1 \rangle \neq \langle \overline{1} \rangle$ as the former is the identity element of Z_{48} while the later is Z_{48} itself.

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}.

These integers are just the integers for the generators of $\mathbb{Z}/48\mathbb{Z}$ which are:

$$1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47$$

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?

Proof. Let us see when this map is well-defined. That is, if $\overline{a} = \overline{b}$, then we must have that $\psi_a(\overline{a}) = \psi_a(\overline{b})$.

Suppose $\overline{m}, \overline{n} \in \mathbb{Z}/48\mathbb{Z}$ and $\overline{m} = \overline{n}$ so that $n = m + 48k$, for some $k \in \mathbb{Z}$. That is, the elements of these residue classes differ by a multiple of 48. For $\psi_a(\overline{m}) = \psi_a(\overline{n})$ we need that

$$\begin{aligned}
\psi_a(\overline{m}) &= \psi_a(m \cdot \overline{1}) \\
&= \psi_a(\overline{1}_1 + \overline{1}_2 + \cdots + \overline{1}_m) \\
&= \psi_a(\overline{1})_1 \psi_a(\overline{1})_2 \cdots \psi_a(\overline{1})_m \\
&= \psi_a(\overline{1})^m \\
&= (x^a)^m \\
&= x^{am}
\end{aligned}$$

The same argument applies to $\overline{n}$ and we see that $am = an$. However, we need them to be equal in the image of ψ_a for this to be well-defined so

$$\begin{aligned}
am &\equiv an \pmod{36} \\
am &\equiv a(m + 48k) \pmod{36} \\
am &\equiv am + 48ak \pmod{36} \\
am - am &\equiv 48ak \pmod{36} \\
0 &\equiv 48ak \pmod{36} \\
48ak &\equiv 0 \pmod{36}
\end{aligned}$$

which shows that $48ak$ must be a multiple of 36. Since k can be any integer, if we let $k = 1$ then we see that 36 divides $48a$ which implies that a must be divisible by 3. Therefore, the homomorphism is well-defined if $3 \mid a$.

For ψ_a to be surjective the order of x^a would need to be 36 but the order of x^a is $\dfrac{36}{(36, a)}$. Since a has a factor of 3 $(36, a)$ will be at least 3 or greater meaning $\dfrac{36}{(36, a)}$ will at most be 12. Therefore, ψ_a cannot be surjective. □

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

The order of $\overline{30}$ in $\mathbb{Z}/54\mathbb{Z}$ is $\dfrac{54}{(54, 30)} = 9$.

The elements of $\angle\overline{30}\rangle$ are:

$$\{0,6,12,18,24,30,36,42,48\}$$

The order of these elements are:

$$|0| = 1, |6| = 9, |12| = 9, |18| = 3, |24| = 9, |30| = 9, |36| = 3, |42| = 9, |48| = 9$$

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

The cyclic subgroups of D_8 are:

$$\{1, r, r^2, r^3\}, \{1, r^2\}, \{1, s\}, \{1, sr\}, \{1, sr^2\}, \{1, sr^3\}$$

A proper subgroup of D_8 that is not cyclic is $\{1, r^2, s, sr^2\}$ as each element either has order 1 or 2 while order of the group is 4.

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

(a) $Z_2 \times Z_2$

Proof. $Z_2 \times Z_2 = \{(1,1),(1,x),(x,1),(x,x)\}$ but all of these elements have either order 1 or 2 while order of the group is 4. □

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

Proof. $Z_2 \times \mathbb{Z} = \{(a,b) \mid a \in Z_2, b \in \mathbb{Z}\}$

The generators for Z_2 and $\mathbb{Z}$ are x and 1 or -1, respectively. The group operation for Z_2 is multiplication while the group operation for $\mathbb{Z}$ is addition.

Suppose $(x,1)$ is the generator for $Z_2 \times \mathbb{Z}$. Then $(1,1)$ is a possible element of $Z_2 \times \mathbb{Z}$ which implies that

$$(x,1)^n = (1,1)$$
$$(x^n, n \cdot 1) = (1,1)$$

which implies $x^n = 1$ and $n \cdot 1 = 1$. From $n \cdot 1 = 1$ we see that $n = 1$ which implies that $x^1 = 1$ which is a contradiction because x is the generator for Z_2 and not the identity element. Therefore, $Z_2 \times \mathbb{Z}$ is not cyclic. □

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

Proof. $\mathbb{Z} \times \mathbb{Z} = \{(a,b) \mid a,b \in \mathbb{Z}\}$

The generators for $\mathbb{Z}$ are 1 or -1. Addition is the group operation for $\mathbb{Z}$.

Suppose $(1,1)$ is the generator for $\mathbb{Z} \times \mathbb{Z}$. Then $(1,0)$ is a possible element of $\mathbb{Z} \times \mathbb{Z}$ which implies that $(1,1)^n = (1,0)$.

$(1,1)^n = (1,0) = (n \cdot 1, n \cdot 0) \implies 1 = n \cdot 1$ and $1 = n \cdot 0$ which implies that $n = 1$ and that $1 = 1 \cdot 0 = 0$, which is a contradiction. Therefore $\mathbb{Z} \times \mathbb{Z}$ is not cyclic. □

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

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

Proof. $(0,x) \in \mathbb{Z} \times Z_2$ and $|(0,x)| = 2$, while no element of $\mathbb{Z}$ contains an element of order 2. Therefore, $\mathbb{Z} \times Z_2$ and $\mathbb{Z}$ are not isomorphic. □

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

Proof. $(0,x) \in \mathbb{Q} \times Z_2$ and $|(0,x)| = 2$, while no element of $\mathbb{Q}$ contains an element of order 2. Therefore, $\mathbb{Q} \times Z_2$ and $\mathbb{Q}$ are not isomorphic. □

14. Let $\sigma =$(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

σ is equivalent to a single permutation from a 12-gon, which is equivalent to $r \in D_2 4$. Therefore,

$$r^{13} = r^{12+1} = r$$
$$r^{65} = r^{12(5)+5} = r^5 = (1\ 5\ 10\ 3\ 8\ 1\ 6\ 11\ 4\ 9\ 2\ 7\ 12)$$
$$r^{626} = r^{12(52)+2} = r^2 = (1\ 3\ 5\ 7\ 9\ 11)(2\ 4\ 6\ 8\ 10\ 12)$$
$$r^{1195} = r^{12(99)+7} = r^7 = (1\ 8\ 3\ 10\ 5\ 12\ 7\ 2\ 9\ 4\ 11\ 6)$$
$$r^{-6} = r^6 = (1\ 7)(2\ 8)(3\ 9)(4\ 10)(5\ 7\ 10)(2\ 5\ 8\ 11)(3\ 6\ 9\ 12)$$

$$r^{-570} = r^{-12(47)-6} = r^{-6} = r^6$$
$$r^{-1211} = r^{-12(100)-11} = r^{-11} = r$$

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

Proof. Suppose that $\mathbb{Q} \times \mathbb{Q}$ is cyclic and that its generator is $(1,1)$. Then $(1,0)$ should be an element in this group such that

$$\begin{aligned} (1,1)^n &= (1,0) \\ n(1,1) &= (1,0) \\ (n \cdot 1, n \cdot 1) &= (1,0) \\ \implies n \cdot 1 = 1, n \cdot 1 &= 0 \end{aligned}$$

which implies $n = 1$ and $n = 0$, which is a contradiction. Therefore, $\mathbb{Q} \times \mathbb{Q}$ 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 $|y|$.

Proof. Since $|x| = n$ and $|y| = m$ we see that

$$\begin{aligned} (xy)^{\text{lcm}(n,m)} &= x^{\text{lcm}(n,m)} y^{\text{lcm}(n,m)} && [x \text{ and } y \text{ commute}] \\ &= 1 \cdot 1 = 1 \end{aligned}$$

which implies $|xy| = \text{lcm}(n,m)$ and obviously $|xy|$ divides $\text{lcm}(n,m)$ as they are equal.

If x and y do not commute this need *not* be true. For example, as we saw in Exercise 6 of Section 2.1, there are examples where non-commuting elements of a group with finite order, have a product with infinite order. □

17. Find a presentation for Z_n with one generator.

$\langle x \mid x^n = 1 \rangle$

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 $x \mapsto h$.

Proof. Let $\varphi : Z_n \to H$ such that $\varphi(x^k) = h^k$. Then

$$\varphi(x_1^k \cdot x_2^k) = h_1^k \cdot h_2^k = \varphi(x_1^k)\varphi(x_2^k)$$

showing φ is a homomorphism.

To show uniqueness, assume there is another homomorphism f with $f(x) = h$. Then

$$f(x^k) = f(x)^k = h^k = \varphi(x^k)$$

showing that $f = \varphi$. □

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 $1 \mapsto h$.

Proof. Let $\varphi : \mathbb{Z} \to H$ such that $\varphi(n) = h^n$. Then

$$\varphi(n+n) = h^n + h^n = \varphi(n) + \varphi(n)$$

showing φ is a homomorphism.

To show uniqueness, assume there is another homomorphism f with $f(1) = h$. Then

$$f(n) = f(1_1 + \cdots + 1_n) = f(1)^n = h^n = \varphi(n)$$

showing that $f = \varphi$. □

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 $x^{p^n} = 1$ then $|x| = p^m$ from some $m \leq n$.

Proof. We will show that this is valid for all $n > 0$ with proof by induction.

If $x^p = 1$, then $|x| = p \implies m = 1$ and $1 \leq n$ is true as $n > 0$.

Assume that $x^{p^{n-1}} = 1$ so that $|x| = p^{n-1} \implies m = n-1$ and $n-1 \leq n$ is obviously true.

If $x^{p^n} = 1$, then $|x| = p^n \implies m = n$ and thus $n \leq n$ is true.

Therefore, if x is an element of the group G such that $x^{p^n} = 1$ then $|x| = p^m$ from some $m \leq n$ for all $n > 0$.

We could have also proved this is by noting that $x^{p^n} = 1 \implies |x| = p^n$ which shows that the order of x divides p^n. Then, since p is prime, the only divisors of p^n are $p^0, p^1, p^2, \ldots, p^n$. Therefore, $|x| = p^m$ for 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 $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Proof. Let p be an odd prime number and $z \equiv 1 \pmod{p}$. Then

$$\operatorname{ord}_p(z^p - 1) = \operatorname{ord}_p(z-1) + 1$$

Here, for a nonzero integer N, $\operatorname{ord}_p(N)$ is the largest power of p which divides N (think of this as the amount of times that p divides N). We can write $z = 1+xp$ for some integer x, so $\operatorname{ord}_p(z-1) = \operatorname{ord}_p(xp) = 1+\operatorname{ord}_p(x)$. Then, using the Binomial Theorem

$$\begin{aligned} z^p - 1 &= (1+xp)^p - 1 \\ &= \binom{p}{1}(xp) + \binom{p}{2}(xp)^2 + \cdots + \binom{p}{p-1}(xp)^{p-1} + (xp)^p \end{aligned}$$

where the first term of the binomial expansion has

$$\operatorname{ord}_p\left(\binom{p}{1}xp\right) = 2 + \operatorname{ord}_p(x) = \operatorname{ord}_p(z-1) + 1$$

and the remaining terms have larger p-orders so we see that the overall p-order (i.e., the largest power of p that will divide all terms) is $\operatorname{ord}_p(z-1)+1$. Since, $z^{p^k} - 1 = (z^{p^{k-1}})^p - 1$, by induction we see that $\operatorname{ord}_p(z^{p^k} - 1) = \operatorname{ord}_p(z-1) + k$.

Now, if $z = 1 + p$ then

$$\begin{aligned}\operatorname{ord}_p\left(z^{p^{k-1}} - 1\right) &= \operatorname{ord}_p(z-1) + k - 1 \\ &= \operatorname{ord}_p(1+p-1) + k - 1 \\ &= \operatorname{ord}_p(p) + k - 1 \\ &= 1 + k - 1 \\ &= k\end{aligned}$$

for all $k \in \mathbb{Z}^+$. Therefore, $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ but $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$.

Since $((1+p), p^n) = 1$ and $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ we see 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-2} in the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$.

Proof. Using what was built upon in Exercise 21, if $z = 1 + 2x$, with $x = 2$ so that $z = 5$ then

$$\begin{aligned}\operatorname{ord}_2(z^2-1) &= \operatorname{ord}_2(z-1) + \operatorname{ord}_2(z+1) \\ &= \operatorname{ord}_2(z-1) + \operatorname{ord}_2(6) \\ &= \operatorname{ord}_2(z-1) + 1\end{aligned}$$

which is similar form as Exercise 21. Again, inductively, we have $\operatorname{ord}_2(z^{2^k} - 1) = \operatorname{ord}_2(z-1) + k$ so that

$$\begin{aligned}\operatorname{ord}_2(5^{2^k} - 1) &= \operatorname{ord}_2(5-1) + k \\ &= \operatorname{ord}_2(4) + k \\ &= 2 + k\end{aligned}$$

Therefore, we see that with exponent 2^{k-2} we would get integer k which would be congruent to $0 \pmod{2^n}$ so that $(1+2^2)^{2^{n-2}} \equiv 1 \pmod{2^n}$ and $(1+2^2)^{2^{n-3}} \not\equiv 1 \pmod{2^n}$.

Since $(5, 2^n) = 1$ and $5^{2^{n-2}} \equiv 1 \pmod{2^n}$ we see that 5 is an element of order 2^{n-2} 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.]

Proof. From Theorem 7 (3) we know that if the group H is cyclic and of finite order n, then there will be a *unique* subgroup of order a where a is a divisor of n.

For $(\mathbb{Z}/2^n\mathbb{Z})^\times$ the order is 2^n and obviously 2 is a divisor of this order. However, if there is more than one subgroup of this order then $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic.

$(\mathbb{Z}/2^n\mathbb{Z})^\times$ are the elements of $\mathbb{Z}/2^n\mathbb{Z}$ that are relatively prime to 2^n. Therefore, $(\mathbb{Z}/2^n\mathbb{Z})^\times$ will contain all the positive odd integers less than 2^n. Thus, $2^k - 1$ and $2^{k-1} - 1$ will both be elements of $(\mathbb{Z}/2^n\mathbb{Z})^\times$. However

$$\begin{aligned}(2^k - 1)^2 &= 2^{k+1} - 2^k + 1 \equiv 1 \pmod{2^k} \\ (2^{k-1} - 1)^2 &= 2^{2k-2} - 2^k + 1 \equiv 1 \pmod{2^k}\end{aligned}$$

which shows that both elements generator a different subgroup of order 2. When $n < 3$, we see that this gives the same group.

Therefore, $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. □

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 $a \in \mathbb{Z}$.

Proof. By definition if $g \in N_G(\langle x \rangle)$ then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$ since x and x^a are both in $\langle x \rangle$. □

(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 $g\langle x \rangle g^{-1} = \langle x \rangle$.]

Proof. If $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$ then

$$\begin{aligned} gxg^{-1} &= x^a \\ (gxg^{-1})^k &= (x^a)^k \\ (gxg^{-1})_1 \cdots (gxg^{-1})_k &= x^{ak} \\ gx^kg^{-1} &= x^{ak} \qquad [gg^{-1} = 1] \end{aligned}$$

for any integer k so that $g\langle x \rangle g^{-1} \leq \langle x \rangle$. If x has order n, then suppose that $gx^ig^{-1} = x^d$ and $gx^jg^{-1} = x^d$ for $i, j \in \{0, 1, \ldots, n-1\}$ then

$$\begin{aligned} gx^ig^{-1} = x^{ai} = x^d &\implies ai = d \implies i = d/a \\ gx^jg^{-1} = x^{aj} = x^d &\implies aj = d \implies j = d/a \\ &\implies \\ i &= j \end{aligned}$$

therefore, gx^ig^{-1} are unique up to order n so that $g\langle x \rangle g^{-1}$ is a cyclic group with generator gxg^{-1}. We also see that $|g\langle x \rangle g^{-1}| = |\langle x \rangle| = n$ and since two finite cyclic groups of the same order are isomorphic, we have that $g\langle x \rangle g^{-1} = \langle x \rangle$.

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

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.)

Proof. Since G is cyclic and of order n we can use Theorem 7 (3) which tells us that for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$. Therefore, since $(n, k) = 1$ we have that

$$\begin{aligned} \langle x^k \rangle &= \langle x^{(n,k)} \rangle \\ &= \langle x^1 \rangle \\ &= \langle x \rangle \end{aligned}$$

which shows that the map $x \mapsto x^k$ for $(n, k) = 1$ is surjective as it generates G.

For any group G, Lagrange's Theorem tells us the that the orders of the subgroups of G divide the order of G. For any element x in G one can form the cyclic subgroup of x which will have order $|x|$. As this is a subgroup of G its order must divide the order of G. Therefore, the order of x in G divides the order of G. This also applies for elements of the subgroups, as they are groups.

Since $(n, k) = 1$, x^k doesn't belong to any subgroup of G (this is because if it did belong to a subgroup of G its order would need to be a divisor of the order of that subgroup, which would mean it was also a divisor of n) but its order must divide the order of G (by Lagrange's Theorem) so it must divide the order of G itself. Therefore, the map $x \mapsto x^k$ is 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).

Proof. If σ_a is an automorphism then it is surjective which means it is onto Z_n and from Exercise 25 we know that the map $x \mapsto x^a$ is only surjective when a and n are relatively prime.

Conversely, if a and n are relatively prime then from Exercise 25 we know that the map $x \mapsto x^a$ is surjective. Now we just need to show it is injective. If $\sigma_a(x_1) = \sigma_a(x_2)$ then

$$\begin{aligned} \sigma_a(x_1) &= \sigma_a(x_2) \\ x_1^a &= x_2^a \\ (x_1^a)^{1/a} &= (x_2^a)^{1/a} \\ x_1 &= x_2 \end{aligned}$$

Thus σ_a is an isomorphism and since it is onto itself, it is an automorphism.

Therefore, σ_a is an automorphism of Z_n if and only if a and n are relatively prime □

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

Proof. If $\sigma_a = \sigma_b$ and since $\sigma_a, \sigma_b \in Z_n$ we see that

$$\begin{aligned} x^a &\equiv x^b \pmod{n} \\ \log_x(x^a) &\equiv \log_x(x^b) \pmod{n} \\ a &\equiv b \pmod{n} \end{aligned}$$

Conversely, if $a \equiv b \pmod{n}$ then

$$\begin{aligned} a &\equiv b \pmod{n} \\ x^a &\equiv x^b \pmod{n} \\ \sigma_a &= \sigma_b \end{aligned}$$

Therefore, $\sigma_a = \sigma_b$ 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.

Proof. Since an automorphism of Z_n is a map from $Z_n \to Z_n$ that is also bijective, we see that σ_a is equal to any automorphism of Z_n when a is relatively prime to n, as seen in part (a), as it is bijective map from $Z_n \to Z_n$. □

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

Proof.

$$\begin{aligned} \sigma_a \circ \sigma_b &= \sigma_a(\sigma_b(x)) \\ &= \sigma_a(x^b) \\ &= (x^b)^a \\ &= x^{ab} \\ \sigma_{ab} &= x^{ab} \end{aligned}$$

so that

$$\sigma_a \circ \sigma_b = \sigma_{ab}$$

$(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to $\mathrm{Aut}(Z_n)$ because the map $\bar{a} \mapsto \sigma_a$, let's denote it φ, is a bijection.

injective:

$$\begin{aligned} \varphi(\overline{a_1}) &= \varphi(\overline{a_2}) \\ \sigma_{a_1} &= \sigma_{a_2} \\ a_1 &\equiv a_2 \pmod{n} && \text{[part (b)]} \\ \overline{a_1} &= \overline{a_2} \end{aligned}$$

showing that φ is injective.

surjective: Let σ_a be an element of the image of φ.

Then, from part (b) we know that $\sigma_a \implies a \equiv a \pmod{n}$, so that $a \in \bar{a}$. Therefore, $\varphi(\bar{a}) = \sigma_a$ and φ is surjective.

Therefore, the map $\bar{a} \mapsto \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of Z_n. □

2.4 SUBGROUPS GENERATED BY SUBSETS OF A GROUP

1. Prove that if H is a subgroup of G then $\langle H \rangle = H$.

Proof. If H is a subgroup of G then we know that the intersection of H with any other subgroups of G that contain *all* the elements of H must be equal to H itself. Therefore, by the definition of the subgroup of G generated by H, $\langle H \rangle = H$. □

2. Prove that if A is a subset of B then $\langle A \rangle \leq \langle B \rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A \rangle = \langle B \rangle$.

Proof. If $x \in A$ then $x \in \langle A \rangle$ by definition. Yet, if $x \in A$ then $x \in B$ since $A \subseteq B$. Then if $x \in B$, we also have that $x \in \langle B \rangle$ by definition. Therefore, $\langle A \rangle \leq \langle B \rangle$.

Let $A = \{1\}$ and $B = \{1, 2\}$ so that $A \subset B$. These finite sets both generate the infinite group of the integers under addition. Therefore, $\langle A \rangle = \langle B \rangle$. □

3. Prove that if H is an abelian subgroup of a group G then $\langle H, \mathrm{Z}(G) \rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, \mathrm{C}_G(H) \rangle$ is not abelian.

Proof. Since the elements of $\mathrm{Z}(G)$ commute with all elements of G and H is itself an abelian subgroup of G the *words* created by $\overline{H \cup \mathrm{Z}(G)}$ will also commute with one another which shows that $\langle H, \mathrm{Z}(G) \rangle$ is abelian.

Let $G = D_8$ and let $H = \{1, r^2\}$. We know that H is a subgroup because it is non-empty, r^2 is its own inverse, and $r^4 = 1$ (order 2). But we can also see that s and r are both in $\mathrm{C}_G(H)$ and these do not commute. Therefore, $\langle H, \mathrm{C}_G(H) \rangle$ is not abelian. □

4. Prove that if H is a subgroup of G then H is generated by the set $H - \{1\}$.

Proof. The only difference between the subgroup H and the set $H - \{1\}$ is obviously $\{1\}$, i.e., the identity element. When generating a subgroup of G with a subset of G, the finite products of the subset's elements and their *inverses* close the set under the group operation. In this case $H - \{1\}$ will generate all the elements of the subgroup H including the identity element since $x, x^{-1} \in \overline{H - \{1\}} \implies xx^{-1} = 1 \in \overline{H - \{1\}}$ so that $\overline{H - \{1\}} = \langle H \rangle$ and by Exercise 1, $\langle H \rangle = H$.

Therefore, if H is a subgroup of G then H is generated by the set $H - \{1\}$. □

5. Prove that the subgroup generated by any two distinct elements of order 2 in S_3 is all of S_3.

Proof. The elements of S_3 are: $\{1,(1\,2),(1\,3),(2\,3),(1\,2\,3),(1\,3\,2)\}$.

For $(1\,2)$ and $(2\,3)$:

$$\begin{aligned}(1\,2)(1\,2) &= 1\\ (1\,2)(2\,3) &= (1\,2\,3)\\ (2\,3)(1\,2) &= (1\,3\,2)\\ (2\,3)(1\,2\,3) &= (1\,3)\end{aligned}$$

For $(1\,2)$ and $(1\,3)$:

$$\begin{aligned}(1\,2)(1\,2) &= 1\\ (1\,2)(1\,3) &= (1\,3\,2)\\ (1\,3)(1\,2) &= (1\,2\,3)\\ (1\,3)(1\,3\,2) &= (2\,3)\end{aligned}$$

For $(1\,3)$ and $(2\,3)$:

$$\begin{aligned}(1\,3)(1\,3) &= 1\\ (1\,3)(2\,3) &= (1\,3\,2)\\ (2\,3)(1\,3) &= (1\,2\,3)\\ (2\,3)(1\,3\,2) &= (1\,2)\end{aligned}$$

Therefore, the subgroup generated by any two distinct elements of order 2 in S_3 is all of S_3. □

6. Prove that the subgroup of S_4 generated by $(1\,2)$ and $(1\,2)(3\,4)$ is a noncyclic group of order 4.

Proof. For $(1\,2)$ and $(1\,2)(3\,4)$:

$$\begin{aligned}(1\,2)(1\,2) &= 1\\ (1\,2)(3\,4)((1\,2)(3\,4)) &= 1\\ (1\,2)((1\,2)(3\,4)) &= (3\,4)\\ ((1\,2)(3\,4))(1\,2) &= (3\,4)\\ (3\,4)(3\,4) &= 1\\ (3\,4)((1\,2)(3\,4)) &= (1\,2)\end{aligned}$$

Thus, the subgroup of S_4 is $\{1,(1\,2),(3\,4),(1\,2)(3\,4)\}$, which has order 4. The reason it is a non-cyclic group is because no element has order 4.

Therefore, the subgroup of S_4 generated by $(1\,2)$ and $(1\,2)(3\,4)$ is a noncyclic group of order 4. □

7. Prove that the subgroup of S_4 generated by $(1\,2)$ and $(1\,3)(2\,4)$ is isomorphic to the dihedral group of order 8.

Proof. We will show that there are elements in the subgroup of S_4 generated by $(1\,2)$ and $(1\,3)(2\,4)$ that are equivalent to the generators r and s of the dihedral group D_8. Let $\varphi : D_8 \to S_4$ be the map where $r \mapsto R, s \mapsto S$ and let $A = (1\,2)$ and $B = (1\,3)(2\,4)$ so that $S = (1\,2)$ and $R = AB = (1\,3\,2\,4)$. The order of R is 4 and the order of S is 2. Additionally, R and S also obey the relationship $rs = sr^{-1}$ as $RS = SR^{-1} = B$. Thus, φ is an isomorphism.

Therefore, the subgroup of S_4 generated by $(1\,2)$ and $(1\,3)(2\,4)$ is isomorphic to the dihedral group of order 8. □

8. Prove that $S_4 = \langle (1\,2\,3\,4), (1\,2\,4\,3) \rangle$.

Proof.

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

Thus we have all 24 elements of S_4 so that $S_4 = \langle (1\,2\,3\,4), (1\,2\,4\,3) \rangle$. □

9. Prove that $SL_2(\mathbb{F}_3)$ is the subgroup of $GL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. [Recall from Exercise 9 of Section 1 that $SL_2(\mathbb{F}_3)$ is the subgroup of matrices of determinant 1. You may assume this subgroup has order 24 — this will be an exercise in Section 3.2.]

Proof. Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Then,

$$A^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

$$B^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

$$A \cdot B = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

$$B \cdot A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

$$(A \cdot B)^2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

$$(A \cdot B)^3 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$$

$$(B \cdot A)^3 = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$$

$$(A \cdot B) \cdot A = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}$$

$$A \cdot (A \cdot B) = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}$$

$$(A \cdot B) \cdot B = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}$$

$$B \cdot (A \cdot B) = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

$$B \cdot (B \cdot A) = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}$$

$$(B \cdot A) \cdot A = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}$$

$$A \cdot B^2 \cdot A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$$

$$B \cdot A^2 \cdot B = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

$$A \cdot (A \cdot B)^2 = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}$$

$$B \cdot (A \cdot B)^2 = \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}$$

$$A \cdot (A \cdot B)^3 = \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}$$

$$(A \cdot B)^3 \cdot B = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}$$

$$(B \cdot A)^3 \cdot A = \begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix}$$

$$B \cdot (B \cdot A)^3 = \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix}$$

which shows that its order is 24 and that all of the determinants are equal to $1 \pmod 3$.

Therefore $SL_2(\mathbb{F}_3)$ is the subgroup of $GL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. □

10. Prove that the subgroup of $SL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is isomorphic to the quaternion group of order 8. [Use a presentation for Q_8.]

Proof. A presentation for Q_8 is $\langle \bar{e}, i, j, k \mid \bar{e}^2 = e, i^2 = j^2 = k^2 = ijk = \bar{e} \rangle$. Noting that $-1 \equiv 2 \pmod 3$ and that

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

which is equivalent to $(B \cdot A)(A \cdot B)$ and $(B \cdot A)$ from Exercise 9, respectively. Therefore, looking at Exercise 9 we can see all of the combinations where these elements are used and that they map to the matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

which map to the elements $\{e, i, j, k, \bar{e}, \bar{i}, \bar{j}, \bar{k}\}$ and where the relations of the presentation for Q_8 all hold.

Therefore, the subgroup of $SL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is isomorphic to the quaternion group of order 8. □

11. Show that $SL_2(\mathbb{F}_3)$ and S_4 are two nonisomorphic groups of order 24.

Proof. It is necessary that the order of the elements of these groups match for there to be an isomorphism. The highest order of S_4 is 4 (cf. Exercise 9, Section 1.6) while the order of $(B \cdot A) \cdot A$ is 6. Therefore, $SL_2(\mathbb{F}_3)$ and S_4 are two nonisomorphic groups of order 24. □

12. Prove that the subgroup of upper triangular matrices in $GL_3(\mathbb{F}_2)$ is isomorphic to the dihedral group of order 8. (cf. Exercise 16, Section 1). [First find the order of this subgroup.]

Proof. The order of this subgroup must be 8 if it is to be isomorphic to D_8. The upper triangular matrices in $GL_3(\mathbb{F}_2)$ are:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where these matrices correspond to the Heisenberg group modulo 2, which is known to be isomorphic to D_8.

Therefore, the subgroup of upper triangular matrices in $GL_3(\mathbb{F}_2)$ is isomorphic to the dihedral group of order 8. □

13. Prove that the multiplicative group of positive rational numbers is generated by the set $\{\frac{1}{p} \mid p \text{ is a prime}\}$.

Proof. Let $\overline{\frac{1}{p}}$ be the set of finite products from the set $\{\frac{1}{p} \mid p \text{ is a prime}\}$. Since the exponents of the members are ± 1, we see that from the Fundamental Theorem of Arithmetic that we can form any positive numerator or positive denominator and therefore any positive rational number. The multiplicative identity is also part of the group.

Therefore, the multiplicative group of positive rational numbers is generated by the set $\{\frac{1}{p} \mid p \text{ is a prime}\}$. □

14. A group H is called *finitely generated* if there is a finite set A such that $H = \langle A \rangle$.

(a) Prove that every finite group is finitely generated.

Proof. If the set A is finite, then there will only be a finite amount of combinations, i.e., words, that will be members of $\langle A \rangle$. Therefore, H will be finite and thus every finite group is finitely generated. □

(b) Prove that $\mathbb{Z}$ is finitely generated.

Proof. The additive group of $\mathbb{Z}$ can be generated from the set {-1,1}. □

(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. [If H is a finitely generated subgroup of $\mathbb{Q}$, show that $H \leq \langle \frac{1}{k} \rangle$, where k is the product of all the denominators which appear in a set of generators for H.]

Proof. Since $H = \langle A \rangle$ and A is finite, let k be the product of all the denominators for the elements in A. Then, since the group operation is addition, we see that all elements of $\langle A \rangle$, and therefore H, can be constructed from $\frac{1}{k}$. That is, $\frac{1}{k}$ is a generator and thus $\langle \frac{1}{k} \rangle$ is cyclic. Therefore, $H \leq \langle \frac{1}{k} \rangle$ and since $\langle \frac{1}{k} \rangle$ is cyclic, we know that H is cyclic as well since every subgroup of a cyclic group is also cyclic [cf. Theorem 7 (1)]. □

15. Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic.

The p-adic rationals are a proper subgroup of $\mathbb{Q}$:

$$\left\{ \frac{a}{p^2} \mid a \in \mathbb{Z}, p \text{ a prime number} \right\}$$

but this group is not cyclic because it doesn't have a single generating element.

16. A subgroup M of a group G is called a *maximal subgroup* if $M \neq G$ and the only subgroups of G which contain M are M and G.

(a) Prove that if H is a proper subgroup of the finite group G then there is a maximal subgroup of G containing H.

Proof. If H is the largest proper subgroup of the finite group G then H contains H and it is the maximal subgroup.

If H is not the largest proper subgroup of the finite group G then there is a larger proper subgroup of G which is the maximal subgroup that contains H.

Therefore, if H is a proper subgroup of the finite group G then there is a maximal subgroup of G containing H. □

(b) Show that the subgroup of all rotations in a dihedral group is a maximal subgroup.

Proof. The subgroup of all rotations in a dihedral group of order $2n$ is $\{1, r, r^2, \dots, r^{n-1}\}$, which has order n. Since the largest divisor of an even number is the remainder after division by 2, which in this case is n, we see that the subgroup of all rotations in a dihedral group is a maximal subgroup. □

(c) Show that if $G = \langle x \rangle$ is a cyclic group of order $n \geq 1$ then a subgroup H is maximal if and only if $H = \langle x^p \rangle$ for some prime p dividing n.

Proof. $G = \langle x \rangle$ is a cyclic group of order n.

Let $H = \langle x^d \rangle$, where d is composite such that $d = a_1 a_2$, where a_1, a_2 are both positive integers greater than 1. Then

$$H = \langle x^d \rangle = \langle x^{a_1 a_2} \rangle < \langle x^{a_1} \rangle$$

since $a_1 \mid a_1 a_2$. Therefore, if d is composite then H cannot be a maximal subgroup.

On the other hand, let $H = \langle x^p \rangle$ for some prime number p and assume that $H < K$ for some subgroup K of G. Since all subgroups of a cyclic group then $K = \langle x^k \rangle$. But then k must divide p. Thus

$$k = 1 \implies K = Gk = p \implies K = H$$

In either case we see that K does not contain H properly, which is a contradiction with our assumption. Therefore, H is maximal. □

17. This is an exercise involving Zorn's Lemma (see Appendix I) to prove that every nontrivial finitely generated group possesses maximal subgroups. Let G be a finitely generated group, say $G = \langle g_1, g_2, \cdots, g_n \rangle$, and let $\mathcal{S}$ be the set of all proper subgroups of G. Then $\mathcal{S}$ is partially ordered by inclusion. Let $\mathcal{C}$ be a chain in $\mathcal{S}$.

(a) Prove that the union, H, of all subgroups in $\mathcal{C}$ is a subgroup of G.

Proof. $\mathcal{C}$ is a chain of proper subgroups in $\mathcal{S}$

$$S_1 \leq S_2 \cdots < G \text{ where } S_i \in \mathcal{C}$$

The union of all of these proper subgroups H is

$$H = \bigcup_i S_i \text{ where } S_i \in \mathcal{C}$$

Since each of these subgroups are already groups *The Subgroup Criterion*, i.e. that H is both nonempty and for all $x, y \in H \implies xy^{-1} \in H$, holds.

Therefore, H is a subgroup of G. □

(b) Prove that H is a *proper* subgroup. [If not, each g_i must lie in H and so must lie in some element of the chain $\mathcal{C}$. Use the definition of a chain to arrive at a contradiction.]

Proof. Suppose that H is not a proper subgroup of G. Then each g_i must be in H and since a chain is a totally ordered subset of G, whether the chain is infinite or not, some proper subgroup in $\mathcal{C}$ will contain each g_i which is a contradiction as that means some subgroup of $\mathcal{S}$ is not a proper subgroup. Therefore, H must be a proper subgroup of G. □

(c) Use Zorn's Lemma to show that $\mathcal{S}$ has a maximal element (which is, by definition, a maximal subgroup).

Zorn's Lemma - If A is a nonempty partially ordered set in which every chain has an upper bound then A has a maximal element.

Proof. $\mathcal{S}$ is a partially ordered set by inclusion. The proof of part (b) was with a general chain $\mathcal{C}$ which showed that H, and therefore the chain $\mathcal{C}$, had an upper bound as it was a proper subgroup.

Therefore, by Zorn's Lemma, S has a maximal subgroup. □

18. Let p be a prime and let $Z = \{z \in \mathbb{C} \mid z^{p^n} = 1 \text{ for some } n \in \mathbb{Z}^+\}$ (so Z is the multiplicative group of all p-power roots of unity in $\mathbb{C}$). For each $k \in \mathbb{Z}^+$ let $H_k = \{z \in Z \mid z^{p^k} = 1\}$ (the group of p^kth roots of unity). Prove the following:

(a) $H_k \leq H_m$ if and only if $k \leq m$

Proof. If $k \leq m$ then

$$z^{p^k} = 1 \implies z^{p^m} = (z^{p^k})^{p^{m-k}} = 1$$

Thus, $H_k \subseteq H_m$ and since H_k is a group, $H_k \leq H_m$

An n^{th} root of unity, is a number z satisfying the equation $z^n = 1$, which for the complex numbers are

$$\exp \frac{2\pi i t}{n} = \cos \frac{2\pi t}{n} + i \sin \frac{2\pi t}{n},\ t = 0, 1, \dots, n-1$$

showing that there are n roots, i.e., that the order is n.

Without loss of generality, H_k and H_m can be written in the above form, showing that they are finite groups. Then by Lagrange's Theorem, the order of the subgroup H_k must divide the order of H_m, since $H_k \leq H_m$. Thus,

$$|H_k| = p^k \mid p^m = |H_m|$$
$$\implies k \leq m$$

Therefore, $H_k \leq H_m$ if and only if $k \leq m$. □

(b) H_k is cyclic for all k (assume that for any $n \in \mathbb{Z}^+$, $\{e^{2\pi i t/n} \mid t = 0, 1, \dots, n-1\}$ is the set of all n^{th} roots of 1 in $\mathbb{C}$)

Proof. Let $H_k = \{e^{2\pi i t/p^k} \mid t = 0, 1, \dots, p, \dots, 2p, \dots, p^{k-1}\}$. We see that H_k can be generated by the single element $e^{2\pi i/p^k}$. Therefore, H_k is cyclic for all k. □

(c) every proper subgroup of Z equals H_k for some $k \in \mathbb{Z}^+$ (in particular, every proper subgroup of Z is finite and cyclic)

Proof. Let H be a proper subgroup of Z. Then $H = \{z_1, z_2, \dots, z_i\}$ for $z_i \in Z$. H is generated by these z_i such That

$$H = \langle z_1, z_2, \dots, z_i \rangle$$

$$= \left\langle e^{2\pi i/p^{k_1}}, e^{2\pi i p^{k_2}}, \dots, e^{2\pi i p^{k_i}} \right\rangle$$
$$= \left\langle e^{2\pi i/\operatorname{lcm}(p^{k_1}, p^{k_2}, \dots, p^{k_i})} \right\rangle$$

Therefore, H is finite and cyclic and equals H_k for some $k = \operatorname{lcm}(p^{k_1}, p^{k_2}, \dots, p^{k_i})$. □

(d) Z is not finitely generated.

Proof. Suppose Z is finitely generated. Then $Z = \langle z_1, z_2, \dots, z_m \rangle$ where the z_i are p^{k_i} roots of unity. Let

$$k = \max\{k_1, \dots, k_m\}$$

Then each of the z_i is also a $p^k th$ root of unity so that

$$Z \leq H_k$$

which is a contradiction as H_k is finite but Z is infinite.

Therefore, Z is not finitely generated. □

19. A nontrivial abelian group A (written multiplicatively) is called *divisible* if for each element $a \in A$ and each nonzero integer k there is an element $x \in A$ such that $x^k = a$, i.e., each element has a k^{th} root in A (in additive notation, each element is the k^{th} multiple of some element of A).

(a) Prove that the additive group of rational numbers, $\mathbb{Q}$, is divisible.

Proof. Let $a \in \mathbb{Q}$ and k a nonzero integer. We are seeking $x \in \mathbb{Q}$ such that

$$kx = a$$
$$x = \frac{a}{k} \in \mathbb{Q} \qquad [k \text{ is nonzero integer}]$$

Therefore, the additive group of the rational numbers, $\mathbb{Q}$, is divisible. □

(b) Prove that no finite abelian group is divisible.

Proof. Let G be a finite abelian group with order n.

If $n = 1$ then it is not divisible as it is not a nontrivial abelian group so let us assume that G is also a nontrivial abelian group.

Then, let $a \in G$ be a nonidentity element and let $k = n$ so that $x^n = a$. Yet, by Lagrange's Theorem we know that $x^n = 1$ for some $x \in G$. This implies that $a = 1$, which is a contradiction as we proposed that it was a nonidentity element.

Therefore, no finite abelian group is divisible. □

20. Prove that if A and B are nontrivial abelian groups, then $A \times B$ is divisible if and only if both A and B are divisible groups.

Proof. If $A \times B$ is divisible then for $(a, b) \in A \times B$ there exists $(x_1, x_2) \in A \times B$ such that

$$(a, b) = (x_1, x_2)^k$$
$$(a, b) = (x_1^k, x_2^k) \qquad [\text{operation is component wise}]$$
$$\implies a = x_1^k \text{ and } b = x_2^k$$

which implies that A and B are both divisible groups.

If A and B are both divisible groups then for $a \in A$ and $b \in B$ there exists $x_1 \in A$ and $x_2 \in B$ such that

$$\begin{aligned} a &= x_1^k \text{ and } b = x_2^k \\ (a,b) &= (x_1^k, x_2^k) \\ (a,b) &= (x_1, x_2)^k \qquad\qquad [\text{operation is component wise}] \end{aligned}$$

which implies that $A \times B$ is divisible.

Therefore, if A and B are nontrivial abelian groups, then $A \times B$ is divisible if and only if both A and B are divisible groups. □

2.5 THE LATTICE OF SUBGROUPS OF A GROUP

1. Let H and K be subgroups of G. Exhibit all possible sublattices which show only $G, 1, H, K$ and their joins and intersections. What distinguishes the different drawings?

The distinguisng factor is whether or not H or K are subgroups of one another.

2. In each of (a) to (d) list all subgroups of D_{16} that satisfy the given condition.

(a) Subgroups that are contained in $\langle sr^2, r^4 \rangle$

$$1, \langle r^4 \rangle, \langle sr^2 \rangle, \langle sr^6 \rangle, \langle sr^2, r^4 \rangle$$

(b) Subgroups that are contained in $\langle sr^7, r^4 \rangle$

$$1, \langle r^4 \rangle, \langle sr^3 \rangle, \langle sr^7 \rangle, \langle sr^7, r^4 \rangle$$

(c) Subgroups that contain $\langle r^4 \rangle$

$$\langle sr^2, r^4 \rangle, \langle s, r^4 \rangle, \langle r^2 \rangle, \langle sr^3, r^4 \rangle, \langle sr^5, r^4 \rangle, \langle s, r^2 \rangle, \langle r \rangle, \langle sr, r^2 \rangle, \langle r^4 \rangle$$

(d) Subgroups that contain $\langle s \rangle$

$$\langle s, r^4 \rangle, \langle s, r^2 \rangle, \langle s \rangle$$

3. Show that the subgroup $\langle s, r^2 \rangle$ of D_8 is isomorphic to V_4.

Proof. It is easy to see that the lattice for $\langle s, r^2 \rangle$ of D_8 and V_4 are equal but this doesn't prove that they are isomorphic as nonisomorphic groups can have the same lattice. However, had the lattices been different then we would have known for sure that they are not isomorphisc.

Looking at the multplication table for V_4 we can see that each element of V_4 is self-inverse. Looking at the elements of $\langle s, r^2 \rangle$

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

we see that they are self-inverse as well.

Therefore, the subgroup $\langle s, r^2 \rangle$ of D_8 is isomorphic to V_4. □

4. Use the given lattice to find all pairs of elements that generate D_8 (there are 12 pairs).

$$(s, r), (s, r^3), (r^2s, r), (r^2s, r^3), (r, rs), (r, r^3s), (r^3, rs), (r^3, r^3s), (s, rs), (s, r^3s), (r^2s, rs), (r^2s, r^3s)$$

5. Use the given lattice to find all elements $x \in D_{16}$ such that $D_{16} = \langle x, s \rangle$ (there are 16 such elements x).

$$(s, r), (s, r^3), (s, r^5), (s, r^7), (s, sr), (s, sr^3)(s, sr^5), (s, sr^7)(s, rs), (s, r^3s), (s, r^5s), (s, r^7s), (s, srs), (s, sr^3s)(s, sr^5s), (s, sr^7s)$$

6. Use the given lattices to help find the centralizers of every element in the following groups:

(a) D_8

$$\begin{aligned}
C_{D_8}(1) &= D_8 \\
C_{D_8}(r) &= \langle r \rangle \\
C_{D_8}(r^2) &= D_8 \\
C_{D_8}(r^3) &= \langle r \rangle \\
C_{D_8}(s) &= \langle s, r^2 \rangle \\
C_{D_8}(rs) &= \langle rs, r^2 \rangle \\
C_{D_8}(r^2s) &= \langle s, r^2 \rangle \\
C_{D_8}(r^3s) &= \langle rs, r^2 \rangle
\end{aligned}$$

(b) Q_8

$$\begin{aligned}
C_{Q_8}(1) &= Q_8 \\
C_{Q_8}(-1) &= Q_8 \\
C_{Q_8}(i) &= \langle i \rangle \\
C_{Q_8}(-i) &= \langle i \rangle \\
C_{Q_8}(j) &= \langle j \rangle \\
C_{Q_8}(-j) &= \langle j \rangle \\
C_{Q_8}(k) &= \langle k \rangle \\
C_{Q_8}(-k) &= \langle k \rangle
\end{aligned}$$

(c) S_3

$$\begin{aligned}
C_{S_3}(1) &= S_3 \\
C_{S_3}((1\,2)) &= \langle (1\,2) \rangle \\
C_{S_3}((1\,3)) &= \langle (1\,3) \rangle \\
C_{S_3}((2\,3)) &= \langle (2\,3) \rangle \\
C_{S_3}((1\,2\,3)) &= \langle (1\,2\,3) \rangle \\
C_{S_3}((1\,3\,2)) &= \langle (1\,2\,3) \rangle
\end{aligned}$$

(d) D_{16}

$$\begin{aligned}
\mathrm{C}_{D_{16}}(1) &= D_{16} \\
\mathrm{C}_{D_{16}}(r) &= \langle r \rangle \\
\mathrm{C}_{D_{16}}(r^2) &= \langle r \rangle \\
\mathrm{C}_{D_{16}}(r^3) &= \langle r \rangle \\
\mathrm{C}_{D_{16}}(r^4) &= D_{16} \\
\mathrm{C}_{D_{16}}(r^5) &= \langle r \rangle \\
\mathrm{C}_{D_{16}}(r^6) &= \langle r \rangle \\
\mathrm{C}_{D_{16}}(r^7) &= \langle r \rangle \\
\mathrm{C}_{D_{16}}(s) &= \langle s, r^4 \rangle \\
\mathrm{C}_{D_{16}}(sr) &= \langle sr^5, r^4 \rangle \\
\mathrm{C}_{D_{16}}(sr^2) &= \langle sr^2, r^4 \rangle \\
\mathrm{C}_{D_{16}}(sr^3) &= \langle sr^3, r^4 \rangle \\
\mathrm{C}_{D_{16}}(sr^4) &= \langle s, r^4 \rangle \\
\mathrm{C}_{D_{16}}(sr^5) &= \langle sr^5, r^4 \rangle \\
\mathrm{C}_{D_{16}}(sr^6) &= \langle sr^2, r^4 \rangle \\
\mathrm{C}_{D_{16}}(sr^7) &= \langle sr^3, r^4 \rangle
\end{aligned}$$

7. Find the center of D_{16}

$$\langle 1, r^4 \rangle$$

8. In each of the following groups find the normalizer of each subgroup:

(a) S_3

$$\begin{aligned}
\mathrm{N}_{S_3}(\langle 1 \rangle) &= S_3 \\
\mathrm{N}_{S_3}(\langle (1\,2) \rangle) &= \langle 1, (1\,2) \rangle \\
\mathrm{N}_{S_3}(\langle (1\,3) \rangle) &= \langle 1, (1\,3) \rangle \\
\mathrm{N}_{S_3}(\langle (2\,3) \rangle) &= \langle 1, (2\,3) \rangle \\
\mathrm{N}_{S_3}(\langle (1\,2\,3) \rangle) &= S_3
\end{aligned}$$

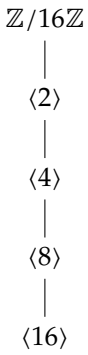
Note: the trick with the last subgroup is realizing that in the lattice, the subgroup $\langle (1\,2\,3) \rangle$ also generates its inverse which is $(1\,3\,2)$.

(b) Q_8

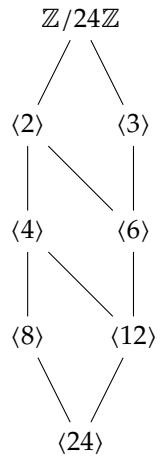
$$\begin{aligned}
\mathrm{N}_{Q_8}(1) &= Q_8 \\
\mathrm{N}_{Q_8}(\langle -1 \rangle) &= Q_8 \\
\mathrm{N}_{Q_8}(\langle i \rangle) &= Q_8 \\
\mathrm{N}_{Q_8}(\langle j \rangle) &= Q_8 \\
\mathrm{N}_{Q_8}(\langle k \rangle) &= Q_8
\end{aligned}$$

9. Draw the lattices of the subgroups of the following groups:

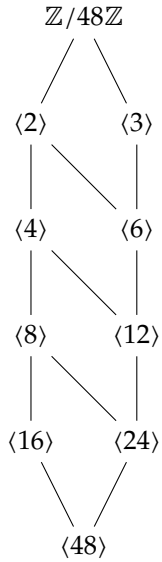
(a) $\mathbb{Z}/16\mathbb{Z}$



(b) $\mathbb{Z}/24\mathbb{Z}$



(c) $\mathbb{Z}/48\mathbb{Z}$ [See Exercise 6 of Section 3.]



10. Classify groups of order 4 by proving that if $|G| = 4$ then $G \cong Z_4$ or $G \cong V_4$. [See Exercise 36, Section 1.1.]

Proof. Since G is finite we know from Lagrange's Theorem that the order of elements of G must divide the order of G. The divisors of 4 are 4, 2, and 1. If there is an element of order 4 then we know that G is cyclic and therefore $G \cong Z_4$.

If G doesn't have any elements that have order 4 then we know that the nonidentity elements must have order 2. From Exercise 36, Section 1.1 we see that for $G = \{1, a, b, c\}$ we have that $a^2 = b^2 = (ab)^2 = 1$, which is the presentation for V_4 and therefore $G \cong V_4$.

Therefore, if $|G| = 4$ then $G \cong Z_4$ or $G \cong V_4$. □

11. Consider the group of order 16 with the following presentation:

$$QD_{16} = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$$

(called the *quasidihedral* or *semidihedral* group of order 16). This group has three subgroups of order 8: $\langle \tau, \sigma^2 \rangle \cong D_8, \langle \sigma \rangle \cong Z_8$ and $\langle \sigma^2, \sigma\tau \rangle \cong Q_8$ and every proper subgroup is contained in one of these three subgroups. Fill in the missing subgroups in the lattice of all subgroups of the quasidihedral group on the following page (please see original text for the diagram), exhibiting each subgroup with at most two generators. (This is another example of a nonplanar lattice.)

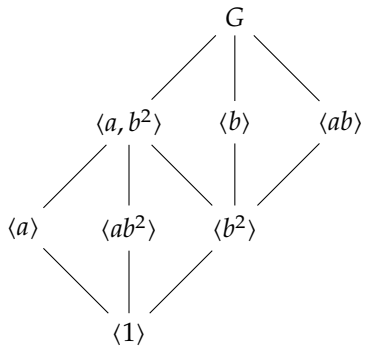
There are two rows that have entries to be filled in and going from left to right:

First row - $\langle \sigma^4, \tau\sigma^2 \rangle, \langle \sigma^2 \rangle, \langle \tau\sigma \rangle, \langle \tau\sigma^3 \rangle$

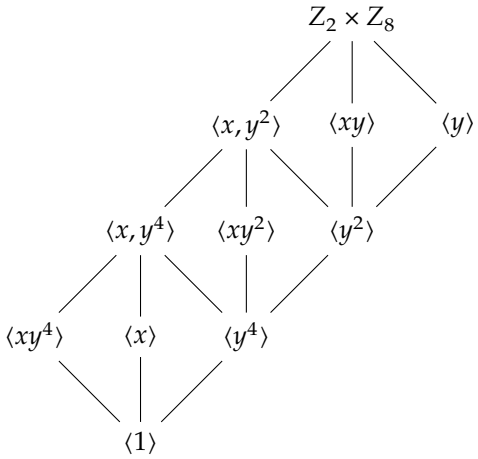
Second row - $\langle \tau\sigma^6 \rangle, \langle \tau\sigma^4 \rangle$

The next three examples lead to two nonisomorphic groups that have the same lattice of subgroups.

12. The group $A = Z_2 \times Z_4 = \langle a, b \mid a^2 = b^4 = 1, ab = ba \rangle$ has order 8 and has three subgroups of order 4: $\langle a, b^2 \rangle \cong V_4, \langle b \rangle \cong Z_4$ and $\langle ab \rangle \cong Z_4$ and every proper subgroup is contained in one of these three. Draw the lattice of all subgroups of A, giving each subgroup in terms of at most two generators.



13. The group $G = Z_2 \times Z_8 = \langle x, y \mid x^2 = y^8 = 1, xy = yx \rangle$ has order 16 and has three subgroups of order 8: $\langle x, y^2 \rangle \cong Z_2 \times Z_4, \langle y \rangle \cong Z_8$ and $\langle xy \rangle \cong Z_8$ and every proper subgroup is contained in one of these three. Draw the lattice of all subgroups of G, giving each subgroup in terms of at most two generators (cf. Exercise 12).



14. Let M be the group of order 16 with the following presentation:

$$\langle u, v \mid u^2 = v^8 = 1, vu = uv^5 \rangle$$

(sometimes called the *modular* group of order 16). It has three subgroups of order 8: $\langle u, v^2 \rangle, \langle v \rangle$ and $\langle uv \rangle$ and every proper subgroup is contained in one of these three. Prove that $\langle u, v^2 \rangle \cong Z_2 \times Z_4, \langle v \rangle \cong Z_8$ and $\langle uv \rangle \cong Z_8$. Show that the lattice of subgroups of M is the same as the lattice of subgroups of $Z_2 \times Z_8$ (cf. Exercise 13) but that these two groups are not isomorphic.

Proof. From Exercise 13 were were given that $\langle x, y^2 \rangle \cong Z_2 \times Z_4, \langle y \rangle \cong Z_8$ and $\langle xy \rangle \cong Z_8$.

$\langle u, v^2 \rangle = \{1, u, v^2, uv^2, v^4, uv^4, v^6, uv^6\}$ which is the same as $\langle x, y^2 \rangle$ if we replace x with u and y with v. Therefore, $\langle u, v^2 \rangle \cong \langle x, y^2 \rangle \cong Z_2 \times Z_4$.

$\langle v \rangle \cong Z_8$ since v has order 8.

$\langle uv \rangle = \{1, uv, v^2, uv^3, v^4, uv^5, v^6, uv^7\} \cong Z_8$.

The lattice will be the same but the reason these two groups are not isomorphic is that they do not have matching presentations. That is, $xy = yx$ but $uv \neq vu$ since $vu = uv^5$. □

15. Describe the isomorphism type of each of the three subgroups of D_{16} of order 8.

The three subgroups of D_{16} of order 8 are: $\langle s, r^2 \rangle, \langle r \rangle, \langle sr, r^2 \rangle$

$\langle s, r^2 \rangle \cong Z_2 \times Z_4$ since s has order 2 and r^2 has order 4.

$\langle r \rangle \cong Z_8$ since r has order 8.

$\langle sr, r^2 \rangle \cong Z_2 \times Z_4$ since sr has order 2 and r^2 has order 4.

16. Use the lattice of subgroups of the quasidihedral group of order 16 to show that every element of order 2 is contained in the proper subgroup $\langle \tau, \sigma^2 \rangle$ (cf. Exercise 11).

In the lattice, since $\langle \tau, \sigma^2 \rangle$ is in the row of groups with order 8 and the row below this are groups of order 4, we see that in the row below this the only groups of order 2 are contained in $\langle \tau, \sigma^2 \rangle$.

17. Use the lattice of subgroups of the modular group M of order 16 to show that the set $\{x \in M \mid x^2 = 1\}$ is a subgroup of M isomorphic to the Klein 4-group (cf. Exercise 14).

The elements of M that have order 2 are: the set $\{1, u, v^4, uv^4\}$

Thus $\langle u, v^4 \rangle$ generates this set and since u has order 2 and v^4 also has order two then this subgroup is isomorphic to $Z_2 \times Z_2$ which is isomorphic to V_4. We also proved in Exercise 10 that a group of order 4 where all nonidentity elements that have order 2 is isomorphic to V_4. Therefore, $\langle u, v^4 \rangle \cong V_4$.

18. Use the lattice to help find the centralizer of every element of QD_{16} (cf. Exercise 11).

$$\begin{aligned}
\mathrm{C}_{QD_{16}}(1) &= QD_{16} \\
\mathrm{C}_{QD_{16}}(\sigma) &= \langle \sigma \rangle \\
\mathrm{C}_{QD_{16}}(\sigma^2) &= \langle \sigma \rangle \\
\mathrm{C}_{QD_{16}}(\sigma^3) &= \langle \sigma \rangle \\
\mathrm{C}_{QD_{16}}(\sigma^4) &= QD_{16} \\
\mathrm{C}_{QD_{16}}(\sigma^5) &= \langle \sigma \rangle \\
\mathrm{C}_{QD_{16}}(\sigma^6) &= \langle \sigma \rangle \\
\mathrm{C}_{QD_{16}}(\sigma^7) &= \langle \sigma \rangle \\
\mathrm{C}_{QD_{16}}(\tau) &= \langle \tau, \sigma^4 \rangle \\
\mathrm{C}_{QD_{16}}(\tau\sigma) &= \langle \tau\sigma \rangle \\
\mathrm{C}_{QD_{16}}(\tau\sigma^2) &= \langle \tau\sigma^2, \sigma^4 \rangle \\
\mathrm{C}_{QD_{16}}(\tau\sigma^3) &= \langle \tau\sigma^3, \sigma^4 \rangle \\
\mathrm{C}_{QD_{16}}(\tau\sigma^4) &= \langle \tau, \sigma^4 \rangle \\
\mathrm{C}_{QD_{16}}(\tau\sigma^5) &= \langle \tau\sigma^5, \sigma^4 \rangle \\
\mathrm{C}_{QD_{16}}(\tau\sigma^6) &= \langle \tau\sigma^6, \sigma^4 \rangle \\
\mathrm{C}_{QD_{16}}(\tau\sigma^7) &= \langle \tau\sigma^7, \sigma^4 \rangle
\end{aligned}$$

19. Use the lattice to help find $\mathrm{N}_{D_{16}}(\langle s, r^4 \rangle)$.

$$\mathrm{N}_{D_{16}}(\langle s, r^4 \rangle) = \langle s, r^2 \rangle$$

20. Use the lattice of subgroups of QD_{16} (cf. Exercise 11) to help find the normalizers:

(a) $\mathrm{N}_{QD_{16}}(\langle \tau\sigma \rangle)$

$$\langle \tau\sigma, \sigma^2 \rangle$$

(b) $\mathrm{N}_{QD_{16}}(\langle \tau, \sigma^4 \rangle)$

$$QD_{16}$$