Abstract Algebra

Dummitt and Foote

Spring 2022

Contents

Chapter 1

Introduction to Groups

1.1 Basic Axioms and Examples

Definition 1.1.1 (Fundamental Terms)**.** .

1. A ***binary operation*** * on a set G is a function $*: G \times G \to G$. For any $a, b \in G$ we shall write $a * b$ for $*(a, b)$.

2. A binary operation $*$ on a set G is ***associative*** if for all $a, b, c \in G$ we have $a * (b * c) = (a * b) * c$.

3. if $*$ is a binary operation on a set G we say elements a and b of G ***commute*** if $a * b = b * a$. We say $*$ (or G) is ***commutative*** if for all $a, b \in G, a * b = b * a$.

Definition 1.1.2 (Group)**.** .

1. A ***group*** is an ordered pair $(G.*)$ where G is a set and $*$ is a binary operator on G satisfying the following axioms:

   (a) $(a * b * c = a * (b * c)$, for $a, b, \in inG$, .i.e., $*$ is ***associative***,

   (b) there exists an element e in G, called ***identity*** of G, such that for every $a \in G$ we have $a * e = e * a = a$,

   (c) for each $a \in G$ there is an element a^{-1} of G, called an ***inverse*** such that $a * a^{-1} = a^{-1} * a = e$.

2. The group $(G, *)$ is called ***abelian*** (or ***commutative***) if $a * b = b * a$ for all $a, b, \in G$.

Proposition 1.1.3. If G is a group under the operation $*$, then

1. The identity of G is unique.

   Let there exist two identity elements e_1, e_2 such that $e1 \neq e2$. Then for any $a \in G$, $a = e_1 a = e_2 a$. Let $a = e_1$ then $e_1 = e_1 * e_1 = e_1 * e_2 = e_2$

2. for each $a \in G, a^{-1}$ is uniquely determined.

   Proof by Contradiciton: Let $b = a^{-1}$ and $c = a^{-1}$ and $b \neq c$. Then $ba = e = ca$. Multiply both sides on the right by a^{-1}, that is $baa^{-1} = caa^{-1} \to be = ce \implies b = c$

3. $(a^{-1})^{-1} = a$ for all $a \in G$.

   Let $b = a^{-1}$. $e = ba$ and $b^{-1} = b^{-1}ba = ea = a$

4. $(a * b)^{-1} = (b^{-1}) * (a^{-1})$

$$\begin{aligned} c &= a * b \\ c * b^{-1} &= a * b * b^{-1} \\ a^{-1} * c * b^{-1} &= a^{-1} * a * b * b^{-1} = a * a^{-1} * b^{-1} * b = e \end{aligned}$$

5. for any $a_1, a_2, \ldots, a_n \in G$ the value of $a_1 * a_2 * \cdots * a_n$ is independent of how the expression is bracketed (this is called ***generalized associative law***).

   Inductive Proof:

Proposition 1.1.4. Let G be a group and let $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, the left and right cancellation laws hold in G, i.e.,

1. if $au = av$, then $u = v$, and

2. if $ub = vb$, then $u = v$.

Definition 1.1.5. For G a group and $x \in G$ define the ***order*** of x to be the smallest positive integer n such that $x^n = 1$, and denote this integer by $|x|$. In this case x is to be of order n. If no positive power of x is the identity, the order of x, is defined to be infinity and x is said to be of infinite order.

Definition 1.1.6. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group with $g_1 = 1$. The multiplication table or group table of G is the $n \times n$ matrix whose i, j entry is the group element $g_i g_j$.

Definition 1.1.7. An operator, $*$, is said to be ***well-defined*** if for all $a, b, c, d \in G$ if $a * b = c$ and $d * b = c$ then $a = d$.

1.1.1 Exercises

Let G be a group.

1. Determine which of the following binary operations are associative:

   (a) the operation $*$ on $\mathbb{Z}$ define by $a * b = a - b$.
   No, because $3 - 4 - 5 = (3 - 4) - 5 = -1 - 5 = -6$ or $3 - 4 - 5 = 3 - (4 - 5) = 3 - (-1) = 4$

   (b) the operation $*$ on $\mathbb{R}$ defined by $a * b = a + b + ab$.

$$a * (b * c) = a * (b + c + bc) = a + b + c + bc + a(b + c + bc) = a + b + c + bc + ab + ac + abc$$
$$(a * b) * c = (a * b) + c + (a * b)c = (a + b + ab)c + (a + b + ab)c = ac + bc + abc + ac + bc + 2abc$$

   (c) the operation $*$ on $\mathbb{Q}$ defined by $a * b = \frac{a+b}{5}$.

$$\begin{aligned} a * b * c = a * (b * c) = a * \left(\frac{b+c}{5}\right) &= \frac{a + \left(\frac{b+c}{5}\right)}{5} = \frac{5a + b + c}{25} \\ = (a * b) * c = \frac{(a * b) + c}{5} &= \frac{\frac{a+b}{5} + c}{5} = \frac{a + b + 5c}{25} \end{aligned}$$

   (d) the operation $*$ on $\mathbb{Z} \times \mathbb{Z}$ defined $(a, b) * (c, d) = (ad + bc, bd)$.

$$\begin{aligned} (a, b) * (c, d) * (e, f) &= ((a, b) * (c, d)) * (e, f) = (ad + bc, bd) * (e, f) = ((ad + bc)f + bde, bdf) \\ &= (a, b) * ((c, d) * (e, f)) = (a, b) * (cf + de, df) = (adf + b(df + de), bdf) \end{aligned}$$

   (e) the operation $*$ on $\mathbb{Q} - \{0\}$ defined by $a * b = \frac{a}{b}$.

$$\frac{ab}{c} \neq \frac{a}{bc}$$

2. Decide which of the binary operations in the preceding exercise are commutative.

   (a) the operation $*$ on $\mathbb{Z}$ define by $a * b = a - b$.

$$\begin{aligned} a - b &= b - a \\ &= a - b + a \\ &= b - a + a \\ &= b \\ a &= 2b \end{aligned}$$

   and not true for all a

   (b) the operation $*$ on $\mathbb{R}$ defined by $a * b = a + b + ab$.

$$a * b = a + b + ab = b + a + ba = b * a$$

   which is true for all $a, b \in \mathbb{R}$.

(c) the operation $*$ on $\mathbb{Q}$ defined by $a * b = \frac{a+b}{5}$.

$$a * b = \frac{a+b}{5} = a * b = \frac{b+a}{5} = b * a$$

(d) the operation $*$ on $\mathbb{Z} \times \mathbb{Z}$ defined $(a, b) * (c, d) = (ad + bc, bd)$.

$$(a, b) * (c, d) = (ad + bc, bd) = (cb + da, db) = (c, d) * (a, b)$$

(e) the operation $*$ on $\mathbb{Q} - \{0\}$ defined by $a * b = \frac{a}{b}$.

$$a * b - b * a = \frac{a}{b} - \frac{b}{a} = \frac{a^2 - b^2}{ab} = 0$$

which is only true when $a^2 = b^2$ or $a = \pm b$. Hence, NOT commutative.

3. Prove that addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).
Given $a, b, c \in [0, \ldots, n - 1]$. If $a + b + c \leq n - 1$ we know that this is associative because $a, b, c, a + b + c \in \mathbb{Z}$. We need only prove that this is true when $a + b + c > n - 1$

4. Prove that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative (you may assume it is well defined).c

5. Prove for all $n > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.
Let $n = 6$ (or any even number for that matter). There is no $a \in Z/nZ$ such that $a * 2 = 1$

6. Determine which of the following sets are groups under addition:

(a) The set of rational numbers (include$0 = 0/1$) in lowest terms whose denomination are odd.
Let $a, b, c, d \in \mathbb{Z}$ where b, d are odd. Then

$$\text{Let } x = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

we know bc is an even number therefore x is not a member of this set. Hence, it does not form a group.
We might have to go further than this and show that the numerator is not divisible by the denominator

(b) the set of rational numbers (including$0 = 0/1$) in lowest terms whose denomitators are even.
Sinilar to 6a we must show that the numerator is not divisible by the denominator and that, if so, it is still even.

(c) the set of rational numbers of absolute value < 1.
No because $0.9 + 0.9 = 1.8 > 1$

(d) the set of rational numbers of absolute value ≥ 1 together with 0.
no because 1 does not have an inverse

(e) the set of rational numbers with denominators equal to 1 or 2.
Is it associative?
Does it have an identity?
Is there an inverse for each element?

(f) the set of rational number denominators equal to 1,2, or 3. Same as 6a, verify that if the numerator is divisible by 1,2, or 3 that the denominator becomes 1,2, or 3.

7. Let $G = \{x \in \mathbb{R} \,|\, 0 \leq x < 1\}$ and for $x, y \in G$ let $x * y$ be the fractional part of $x + y$ (i.e., $x * y = x + y - [x + y]$ where $[a]$ is the greatest integer less than or equal to a). Prove that $*$ is a well defined binary operation on G and that G is an abelian group under $*$ (called the *real numbers mod 1*).

- Well-defined

$$\begin{aligned}
\text{Let } a * b = c &\text{ and } a * d = c \\
a + b - [a + b] &= a + d - [a + d] \\
-a + a + b - [a + b] &= -a + a + d - [a + d] \\
b - [a - b] &= d - [a + d] \\
-d + b - [a - b] &= -d + d - [a + d] \\
-d + b &= [a + b] - [a + d] \\
&= [b - d]
\end{aligned}$$

which can only be true if $b = d$.

- Is it associative?

$$\begin{aligned}
a * (b * c) &= a * (b + c - [b + c]) \\
&= a + (b + c - [b + c]) - [a + (b + c - [b + c])] \\
&= a + b + c - [b + c] - [a + b + c - [b + c]] \\
&= a + b + c - [a + b + c] \\
&= (a + b) + c - [[a + b] - c] \\
&= (a * b) * c
\end{aligned}$$

- Does it have an identity?
  Assume that the identity exists and let e be the identity. Then,

$$\begin{aligned}
a &= e * a \\
&= e + a - [e + a] \\
-a + a &= -a + e + a - [e + a] \\
0 &= e - [e + a] \\
e &= [e + a] \\
e &= 0
\end{aligned}$$

- Is there an inverse for each element?
  Given any $a \in G$ then

$$\begin{aligned}
0 = a * b &= a + b - [a + b] \\
a + b &= [a + b]
\end{aligned}$$

- Does it commute?
  Since the integer part and the fraction parts both commute and they are linearly independent of each other, then the $*$ operator commutes. That is,

$$\begin{aligned}
a * b &= a + b - [a + b] \\
&= b + a - [b + a] \\
&= b * a
\end{aligned}$$

8. Let $G = \{z \in \mathbb{C} \,|\, z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

   (a) Prove that G is a group under multiplication (called the group of *roots of unity* in $\mathbb{C}$).
   First note the following examples:

$$\begin{aligned}
n = 2 &\implies G = \{1, -1\} = \{1, e^{i\frac{\pi}{2}}\} \\
n = 3 &\implies G = \{1, \frac{2}{\sqrt{3}} + i\frac{1}{\sqrt{3}}, -\frac{2}{\sqrt{3}} + i\frac{1}{\sqrt{3}}\} = \{1, e^{i\frac{2\pi}{3}}, e^{i\frac{-2\pi}{3}}\} \\
n = 4 &\implies G = \{1, -1, i, -i\} = \{1, -1, e^{i\frac{\pi}{2}}, e^{i\frac{-\pi}{2}}\} \\
&\text{in general } G = \{e^{i\frac{2\pi k}{n}}, k = 0, 1, 2, \ldots, n-1\}
\end{aligned}$$

   The elements of each set are on the unit circle and there are precisely n elements in each set.

   (b) Prove that G is not a group under addition.
   Simple. For $n = 2$ we have $1 + (-1) = 0 \notin G$

9. Let $G = \{a + b\sqrt{2} \in \mathbb{R} \,|\, a, n \in \mathbb{Q}\}$.

   (a) Prove that G is a group under addition.
   Associative?
   Let $a, b, c, d, f, g \in \mathbb{R}$ and $a + b\sqrt{2}, c + d\sqrt{2}$, and $f + g\sqrt{2} \in G$. Then

$$\begin{aligned}
[(a + b\sqrt{2}) + (c + d\sqrt{2})] + f + g\sqrt{2} &= (a + b\sqrt{2} + c + d\sqrt{2}) + f + g\sqrt{2} \quad (1.1) \\
&= a + b\sqrt{2} + c + d\sqrt{2} + f + g\sqrt{2} \quad (1.2) \\
&= a + b\sqrt{2} + (c + d\sqrt{2} + f + g\sqrt{2}) \quad (1.3)
\end{aligned}$$

   (1.1) because real numbers are associative, (1.2) & (1.3) for the same reason.

Identity exists?

Let $e = 0 + 0\sqrt{2}$. Then given any

$$\begin{aligned} 0 + 0\sqrt{2} &= a + b\sqrt{2} + c + d\sqrt{2} \\ &= a + c = 0 \text{ and } b + d = 0 \\ \therefore -(a + b\sqrt{2}) &= c + d\sqrt{2} \end{aligned}$$

Inverses exists and are unique?

(b) Prove that nonzero elements of G are a group under multiplication. ["Rationalize the denominators" to find multiplicative inverses.]

Associative?

$$\begin{aligned} [(a + b\sqrt{2})(c + d\sqrt{2})](f + g\sqrt{2}) &= (ac + ad\sqrt{2} + b\sqrt{2}c + 2bd)(f + g\sqrt{2}) \\ &= acf + acg\sqrt{2} + adf\sqrt{2} + adg\sqrt{2} + b\sqrt{2}cf + 2bcg + 2bdf + 2bdg\sqrt{2} \\ &= (a + b\sqrt{2})(cf + cg\sqrt{2} + df\sqrt{2} + 2dg) \\ &= (a + b\sqrt{2})[(c + d\sqrt{2})(f + g\sqrt{2})] \end{aligned}$$

Identity exists?

Let $e = 1 + 0\sqrt{2}$ then

$$(a + b\sqrt{2})(1 + 0\sqrt{2}) = a + b\sqrt{2}$$

Inverses exists and are unique?

$$\begin{aligned} 1 &= (a + b\sqrt{2})(c + d\sqrt{2}) \\ &= ac + 2bd + \sqrt{2}(bc + ad) \\ \therefore bc &= -ad \text{ and } 1 = ac + 2bd \\ \text{and } c &= \frac{-ad}{b} \text{ and } d = \frac{1}{2b - \frac{a^2}{b}} \end{aligned}$$

10. Prove that a finite group is abelian if and only if its group table is a symmetric matrix.

   (⇒) Assuming that G is abelian then given any two elements g_i, g_j then $g_i g_j = g_j g_i$. Given that the i^{th} column and j^{th} row will have value $g_i g_j$ respectively, then the j^{th} column and the i^{th} row will have $g_j g_i$ which is the same.

   (⇐) similar argument to above.

11. Find the order of each element of additive group $\mathbb{Z}/12\mathbb{Z}$.

   Order of 1 is 12, 2 is 6, 3 is 4, 4 is 3, 5 is 12, 6 is 2, 7 is 12, 8 is 3, 9 is 4, 10 is 5, 11 is 12

12. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/12\mathbb{Z})^\times : \overline{1}, \overline{-1}, \overline{5}, \overline{7}, \overline{-7}, \overline{13}$.

   $(\mathbb{Z}/12\mathbb{Z})^\times : |\overline{1}| = |\overline{13}| = 1, |\overline{-1}| = |\overline{5}| = |\overline{7}| = |\overline{-7}| = 2.$

13. Find the orders of the following element so fthe additive group $(\mathbb{Z}/36\mathbb{Z})^\times : \overline{1}, \overline{2}, \overline{6}, \overline{9}, \overline{10}.\overline{12}, \overline{-1}, \overline{-10}, \overline{-18}$.

   $(\mathbb{Z}/36\mathbb{Z})^\times : |\overline{1}| = 1, |\overline{2}| = \infty, |\overline{6}| = \infty, |\overline{9}| = \infty, |\overline{10}| = \infty.|\overline{12}| = \infty, |\overline{-1}| = 2, |\overline{-10}| = \infty, |\overline{-18}| = \infty.$

14. Find the orders of the following elements of the multiplicative group $(\mathbb{Z}/36\mathbb{Z})^\times : \overline{1}, \overline{-1}, \overline{5}, \overline{13}, \overline{-13}, \overline{17}$.

15. Prove that $(a_1 a_2 \dots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \dots a_1^{-1}$ for all $a_1, a_2, \dots, a_n \in G$.

   Notice that $(a_1 a_2 \dots a_n)^{-1} = (a_2 a_3 \dots a_n)^{-1} a_1^{-1} = (a_3 a_4 \dots a_n)^{-1} a_2^{-1} a_1^{-1}$ Continuing in this way until we get the desired result.

16. Let x be an element of G. Prove that $x^2 = 1$ if and only if $|\,x\,|$ is either 1 or 2.

17. Let x be an element of G. Prove that if $|\,x\,| = n$ for some positive integer n then $x^{-1} = x^{n-1}$.

$$\begin{aligned} x^{-1} &= x^{n-1} \\ xx^{-1} &= xx^{n-1} \\ 1 &= x^n \end{aligned}$$

18. Let x and y be elements of G. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.
    if $xy = yx$ then $y^{-1}xy = y^{-1}yx = x$ and if $y^{-1}xy = x$ then $y^{-1}xy = yy^{-1}xy = yx$

19. Let $x \in G$ and let $a, b \in \mathbb{Z}^+$.
    (a) Prove that $x^{a+b} = x^a x^b$ and $(x^a)^b = x^{ab}$.
    Notice that $xx^a = x^{a+1}$. Then assume that it is true for $b-1$, that is, $x^{b-1}x^a = x^{b-1+a}$ then $xx^{b-1}x^a = x^{1+b-1+a} = x^{a+b}$
    (b) Prove that $(x^a)^{-1} = x^{-a}$
    $1 = x^a x^{-a} = x^{a-a} = x^0 = 1$
    (c) Establish part (a) for arbitrary integers a and b (positive, negative or zero).

20. For x an element in G show that x and x^{-1} have the same order.
    Let $|x| = n$ then $x^n = 1$ and $x^n x^{-n} = 1x^{-n} = (x^{-1})^n = 1$

21. Let G be a finite group and let x be an element of G of order n. Prove that if n is odd, then $x = (x^2)^k$ for some k.
    $x^n = 1$ if n is odd then there exists k such that $n = 2k-1$. Therefore $x^n = x^{2k-1} = 1$ and $xx^{2k-1} = (x^2)^k = x$

22. If x and g are elements of the group G, prove that $|\,x\,| = |\,g^{-1}xg\,|$. Deduce that $|\,ab\,| = |\,ba\,|$ for all $a, b \in G$.

$$\begin{aligned} (g^{-1}xg)^n &= \underbrace{g^{-1}xgg^{-1}xg\dots}_{n \text{times}} \\ &= g^{-1}x^n g \\ &= g^{-1}g \\ &= 1 \\ \therefore |\,g^{-1}xg^x\,| &= n \end{aligned}$$

23. Suppose $x \in G$ and $|\,x\,| = n < \infty$. If $n = st$ for some positive integers s and t, prove that $|\,x^s\,| = t$.
    $x^n = (x^s)^t = 1$ which implies that $|\,x^s\,| = t$.

24. if a and b are *commuting* elements of G, prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{Z}$. [Do this by induction for positive n first.]

25. Prove that if $x^2 = 1$ for $x \in G$ then G is abelian.
    Given $a, b \in G$ then $a^2 = b^2 = 1$, also $(ab)^2 = 1$. Therefore $1 = abab = aa$ and $bab = a$ which implies that $bab^2 = ab$ and $ba = ab$.

26. Assume H is a nonempty subset of $(G, *)$ which is closed under the binary operation on G and is closed under inverses, i.e., for all $h, k \in H, h * k$ and $h^{-1} \in H$; Prove that H is a group under the operation * restricted to H (such a subset H is called a *subgroup* of G).
    The key point is that for every $h, k \in H \implies h^{-1} \in H$ and $h * k \in H$.

27. Prove that if x is an element of the group G then $\{x^n \mid n \in \mathbb{Z}\}$ is a subgroup (cf, the preceding exercise) of G (called the *cyclic subgroup* of G generated by x).
    Let $h, k \in G$ then there exists $i, k \in \mathbb{Z}$ such that $x^i = h, x^j = k$. Clearly $hk = x^i x^j = x^{i+j} \in G$. Further, $h^{-1} = (x^i)^{-1}$ hence $1 = hh^{-1} = x^i(x^i)^{-1}$ therefore $h^{-1} = x^{-i} \in G$.

28. Let $(A, *)$ and $(B, \circ)$ be groups and let $A \times B$ be their direct product (as defined in Example 6). Verify all the group axioms for $A \times B$:
    (a) prove that the associative law holds:
    for all $(a_i, b_i) \in A \times B, i = 1, 2, 3\, (a_1, b_1)[(a_2, b_2)(a_3, b_3)] = [(a_1, b_1,)(a_2, b_2)](a_3, b_3)$

   (b) prove that $(1,1)$ is the identity of $A \times B$, and

   (c) prove that the inverse of (a,b) is (a^{-1}, b^{-1}).

29. Prove that $A \times B$ is an abelian group if and only if both A and B are abelian.

30. Prove that the elements $(a,1)$ and $(1,b)$ of $A \times B$ commute and deduce that the order of (a,b) is the least common multiple of $\overline{a}$ and $\overline{b}$.

31. Prove that any finite group G of even order contains an element of order 2. [Let $t(G)$ be the set $\{g \in G \,|\, g \neq g^{-1}\}$. Show that $t(G)$ has an even number of elements and every nonidentity element of $G - t(G)$ has order 2.]

32. If x is an element of finite order n in G, Prove that the element $1, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|\, x \,| \leq |\, G \,|$.

33. Let x be an element of finite order n in G.

   (a) Prove that if n is odd then $x^i \neq x^{-i}$ for all $i = 1, 2, \ldots, n-1$.

   (b) Prove that if $n = 2k$ and $1 \leq i < n$ then $x^i = x^{-i}$ if and only if $i = k$.

34. If x is an element of infinite order in G, prove that the elements $x^n, n \in \mathbb{Z}$ are all distinct.

35. If x is an element of finite order n in G, use the Division Algorithm to show that any integral power of x equals one of the elements in the set $\{1, x, x^2, \ldots, x^{n-1}\}$ (so these are all distinct elements of the cyclic subgroup (cf, Exercise 27 above) of G generated by x).

36. Assume $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume also that G has no elements of order 4 (so by Exercise 32, every element has order ≤ 3). Use the cancellation laws to show that rhere is a unique group table for G. Deduce that G is abelian.

1.2 Dihedral Groups

Definition 1.2.1 (Dihedral Group D_{2n})**.** For each $n \in \mathbb{Z}^+, n \geq 3$ let D_{2n} be the set of symmetries of a regular n-gon, i.e., a rotation and/or flipping of the points of the n-gon onto itself. Note: n refers to the number of points and $2n$ refers to the number of ways that the shape can be imposed on those points, hence the order of the group.

Remark 1.2.2. Note that rotation, r, and flipping or switching, s, are operations that a can be performed on any dihedral element and equations from one element two the other will result in just these two operations. These are examples of *generators.*

Definition 1.2.3 (Generators)**.** A subset S of a group G with the property that every element in G can be written as a (finite) product of elements in S and their inverses is called a ***set of generators by*** S or S ***generates*** G.

Definition 1.2.4 (Relations)**.** Any equations in a general group G that the generators satisfy are called ***relations*** in G. Thus, in D_{2n} we have relations: $r^n = 1, s^2 = 1$, and $rs = sr^{-1}$. Moreover, in D_{2n} these three relations have the additional property that *any* other relation between elements of the group may be derived from these three.

Definition 1.2.5 (Presentation)**.** In general, if some group G is generated by a subset S and there is some collection of relations, say $R_1, R_2, \ldots, R_m$ (here each R_i is an equation of the elements from $S \cup \{1\}$) such that any relation among the elemnts of S can be deduced from these we shall call these generators and relations a ***presentation*** of G and write

$$G = \langle\, S \,|\, R_1, R_2, \ldots, R_m \,\rangle\,.$$

One presentation for the dihedral group D_{2n} (using the generators and relations above) is then

$$D_{2n} = \left\langle\, r, s \,|\, r^n = s^2 = 1, rs = sr^{-1} \,\right\rangle.$$

1.2.1 Exercises

In these exercises, D_{2n} has the usual presentation $D_{2n} = \left\langle\, r, s \,|\, r^n = s^2 = 1, rs = sr^{-1} \,\right\rangle$.

1. Compute the order of each of the elements in the following groups:

   (a) D_6.

   $|x_0| = |r^0| = 1, |x_1| = |r^1| = 3, |x_2| = |r^2| = 3, |x_3| = |sr^0| = 2, |x_4| = |sr^1| = 2, |x_5| = |sr^2| = 2$

   (b) D_8

   $|x_0| = |r^0| = 1, |x_1| = |r^r| = 4, |x_2| = |r^2| = 2, |x_3| = |r^3| = 4, |x_4| = |sr^0| = 2, |x_5| = |sr^1| = 2, |x_6| = |sr^2| = 2, |x_7| = |sr^3| = 2$

(c) D_{10}

$x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9$

2. Use the generators and relations above to show that if x is any element of D_{2n} which is not a power of r, then $rx = xr^{-1}$.

   Let $x \in G$ and there is $k \in \mathbb{Z}+$ such that $x = r^k s$.

   $$rx = rr^k s = r^k rs = r^k sr^{-1} = xr^{-1}$$

3. Use the generators and relations above to show that every element of D_{2n} which is not a power of r has order 2. Deduce that D_{2n} is generated by the two elements s and sr, both of which have order 2.

   $x = r^k s$ then $xx^{-1} = 1, r^k sx^{-1} = 1, x^{-1} = sr^{-k}$

4. If $n = 2k$ is even and $n \geq 4$, show that $z = r^k$ is an element of order 2 which commutes with all elements of D_{2n}. Show also that z is the only nonidentity element of D_{2n} which commutes with all elements of D_{2n}. [cf. Exercise 33 of section 1.]

   $r^n = 1$ and $z = r^k$, $z^2 = (r^k)^2 = r^2 = 2k = r^n = 1$
   Let there be i such that $x \in D_{2n}, r^i = x$. Then $zx = r^k r^i = r^{k+i} = r^{i+k} = r^i r^k = xz$
   Let there be j such that $x \in D_{2n}, x = r^j s$. The $zx = r^k r^j s = r^{k+j} s = r^j r^k s = r^j sr^{-k} = r^j sr^k = xz$.
   k is the only element that can do this because $z = r^k = r^{-k}$.

5. If n is odd and $n \geq 3$, show that the identity is the only element of D_{2n} which commutes with all elements of D_{2n}.

   the whole thing depends on finding an element $x = r^k$ such that

   $$\begin{aligned} r^k &= r^{-k} \\ r^k r^k &= r^k r^{-k} \\ r^2 k &= r^{k-k} = r^0 = 1 \\ r^2 k &= r^n \end{aligned}$$

   but n is odd and there is no $k \in \mathbb{Z}$ such that $2k = n$.

6. Let x and y be elements of order 2 in any group G. Prove that if $t = xy$ then $tx = xt^{-1}$ (so that if $n = |\, xy \,| < \infty$ then x, t satisfy the same relations in G as s, r do in $D + 2n$).

   $1 = tt^{-1} = xyt^{-1} \to x = yt^{-1} \to yx = t^{-1} \to xyx = tx \to tx = xt^{-1}$

7. Show that $\langle\, a, b \,|\, a^s = b^s = (ab)^n = 1 \,\rangle$ gives a presentation for D_{2n} in terms of the two generators $a = s$ and $b = sr$ of order 2 computed in Exercise 3 above. [Show that the relations for r and s follow from the relations for a and b and, conversely, the relations for a and$b$ follow from those for r and s.]

8. Find the order of the cyclic subroup of D_{2n} generated by r (cf Exercise 27 of Section 1).

   $|D_{2n}| = 2n$ and $|s| = 2$ that is, given any $x = sr^k$ for some k, there can be at most n of these. That leaves n more that have the form $x = r^k$.

In each of Exercises 9 to 13 you can find the order of the group of rigid motions in $\mathbb{R}^3$ (also called the group of rotations) of the given Platonic solid by following the proof for the order of D_{2n}; find the number of positions to which an adjacent pair of vertices can be sent. Alternatively, you can find the number of places to which a given face may be sent and, once a face is fixed, the number of positions to which a vertex on that face may be sent.

9. Let G be the group of rigid motions in $\mathbb{R}^3$ of a tetrahedron. Show that $|G| = 12$.

10. Let G be the group of rigid motions in $\mathbb{R}^3$ of a cube. Show that $|G| = 24$.

11. Let G be the group of rigid motions in $\mathbb{R}^3$ of an octahedran. Show that $|G| = 24$.

12. Let G be the group of rigid motions in $\mathbb{R}^3$ of a dodecahedron. Show that $|G| = 60$.

13. Let G be the group of rigid motions in $\mathbb{R}^3$ of a icosahedron. Show that $|G| = 60$.

14. Find a set of generators for $\mathbb{Z}$.

15. Find a set of generators and relations for $\mathbb{Z}/n\mathbb{Z}$.

16. Show that the group $\langle\, x_1, y_1) \,|\, x_1^2 = y_1^2 = (x_1 y_1)^2 = 1 \,\rangle$ is the dihedral group D_4 (where x_1 may be replaced by the letter r and y_1 by s). [Show that the last relation is the same as: $x_1 y_1 = y_1 x_1^{-1}$.]

17. Let X_{2n} be the group whose representaion is displayed in (1.2).

(a) Show that if $n = 3$, then X_{2n} has order 6, and it has the same generators and relations as D_6 where x is replaced by r and y by s.

(b) Show that if $(3, n) = 1$, then x satisfies the additional relation: $x = 1$. In this case deduce that X_{2n} has order 2. [Use the facts that $x^n = 1$ and $x^3 = 1$.]

18. Let Y be the group whose presentation is displayed in (1.3).

(a) Show that $v^2 = v^{-1}$. [Use the relation: $v^3 = 1$.]

(b) Show that v commutes with u^3. [Show that $v^2u^3v = u^3$ by writing the left hand side as $(v^2u^2)(uv)$ and using the relation to reduce this to the right hand side. Then use part (a).]

(c) Show that v commutes with u. [Show that $u^9 = u$ and then use part (b).]

(d) Show that $uv = 1$. [Use part (c) and the last relation.]

(e) Show that $u = 1$, deduce that $v = 1$, and conclude that $y = 1$. [Use part(d) and the equation $u^4v^3 = 1$.]

1.3 Symmetric Groups

1.3.1 Exercises

1. Let σ be the permutation (1 3 5)(2 4) and let τ be the permutation (1 5)(2 3). Find the cycle decompositions of each of the following:

(a) σ^2

$\sigma^2 = (1\ 3\ 5)(2\ 4)(1\ 3\ 5)(2\ 4) = (1\ 5\ 3)$

(b) $\sigma\tau$

$\sigma\tau = (1\ 3\ 5)(2\ 4)(1\ 5)(2\ 3) = (2\ 5\ 3\ 4)$

(c) $\tau\sigma$

$\tau\sigma = (1\ 5)(2\ 3)(1\ 3\ 5)(2\ 4) = (1\ 2\ 4\ 3)$

2. Let $\sigma = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)$ and $\tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)$. Find the cycle decompositions of the following permutations:

(a) σ^2

$\sigma^2 = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)(1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9) = (1\ 5)(3\ 8\ 15)(4\ 11\ 12)(7\ 9\ 14)$

(b) $\sigma\tau$

$\sigma\tau = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)(1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11) = (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)$

(c) $\tau\sigma$

$\tau\sigma = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)(1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9) = (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14)$

(d) $\tau^2\sigma$

$\tau^2\sigma = [(1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)]\ [(1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)]\ [(1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)] = (1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10)$

3. For each of the permutations whose cycle decompositions were computed in the preceding two exercises compute its order. Note: since each of the sub-cycles are disjoint, we know that each will have an order of its own and the whole composite cycle will have the order of the least common multiple.

(a) $|\sigma^2|$

Since $\sigma^2 = (1\ 5)(3\ 8\ 15)(4\ 11\ 12)(7\ 9\ 14)$ we must find

- $|(1\ 5)| = 2$
- $|(3\ 8\ 15)| = 3$
- $|(4\ 11\ 12)| = 3$
- $|(7\ 9\ 14)| = 3$

Thus when $k = 6$ or $|\sigma^2| = 6$

(b) $|\sigma\tau|$

$\sigma\tau = (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)$ we must find

- $|(1\ 11\ 3)| = 3$
- $|(2\ 4)|= 2$
- $|(5\ 9\ 8\ 7\ 10\ 15)| = 6$

Thus when $k = 6$ or $|\sigma\tau| = 6$

(c) $|\tau\sigma|$

(d) $|\tau^2\sigma|$

4. Compute the order of each of the elements of the following groups (a) S_3 (b) S_4

    (a) S_3 (1) (1 2) (2 3) (1 3) (1 2 3) (1 3 2)

    (b) S_4 (1) (1 2) (1 3) (1 4) (2 3) (2 4) (3 4) (1 2 3) (1 3 2) (1 2 4) (1 4 2) (1 3 4) (1 4 3) (2 3 4) (2 4 3) (1 2 4 3) (1 3 2 4) (1 3 4 2) (1 4 2 3) (1 4 3 2) (1 2)(3 4) (1 3)(2 4) (1 4)(2 3)

5. find the order of (1 12 8 10 4)(2 13)(5 11 7)(6 9). 30

6. Write out the cycle decompsition of each element of order 4 in S_4.

    (1 2 4 3) (1 3 2 4) (1 3 4 2) (1 4 2 3) (1 4 3 2)

7. Write out the cycle decomposition of each element of order 2 in S_4.

    (1 2) (1 3) (1 4) (2 3) (2 4) (3 4) (1 2)(3 4) (1 3)(2 4) (1 4)(2 3)

8. Prove that if $\Omega = \{1, 2, 3, \dots\}$ then S_Ω is an infinite group (do not say $\infty! = \infty$).

    Proof by Contradiction: assume that S_Ω is finite then determine which n makes $S_\Omega = S_n$.

9. (a) Let σ be the 12-cycle. For which positive integers i is σ^i also a 12-cycle?

    Squaring σ will generate two 6-cyclces. Cubing σ will generate three 4-cycles and σ^4 generates four 3-cycles. It is clear that, since it is a permuation, all elements must be accounted for. Thus, if the power, k, divides 12 it will separate into k different $k/12$-cycles.
    Five, however, does not divide into 12 thus it will consume all of the elements into a single 12-cycle.

    (b) Let τ by the 8-cycle. For which positive integers i is τ^i an 8-cycle?

    $\tau = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$
    $\tau^2 = (1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$
    $\tau^3 = (1\ 4\ 7\ 2\ 5\ 8\ 3\ 6)$

    (c) Let ω be the 14-cycle. For which positive integers i is ω^i also a 14-cycle?

    $\omega = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14)$
    $\omega^2 = (1\ 3\ 5\ 7\ 9\ 11\ 13)(2\ 4\ 6\ 8\ 10\ 12\ 14)$
    $\omega^3 = (1\ 4\ 7\ 10\ 13\ 2\ 5\ 8\ 11\ 14\ 3\ 6\ 9\ 12)$

    Once again it is the first power that does not divide 14.

10. Prove that if σ is the m-cycle $(a_1, a_2, \dots, a_m)$, then for all $i \in \{1, 2, \dots, m\}, \sigma^i(a_k) = a_{k+i}$, where $k+i$ is replaced by its least residue mod m when $k + i > m$. Deduce that $|\sigma| = m$.

    Note that $\sigma(a_m) = a_1, \sigma^2(a_m) = \sigma(\sigma(a_m)) = \sigma(a_1) = a_2$
    Now, in general, $\sigma(a_k) = a_{k+1}, \sigma^2(a_k) = \sigma(\sigma(a_k)) = \sigma(a_{k+1}) = a_{k+2} \dots \sigma^i(a_k) = \underbrace{\sigma(\sigma(\dots))}_{\text{i times}} = a_{k+i}$

11. Let σ be the m-cycle $(1\ 2\ \dots\ m)$. Show that σ^i is also an m-cycle if and only if i is relative prime to m

    If $i|m \to \exists d \in \mathbb{Z}, id = m$. Then, σ^i will be i d-cycles. After all, all m elements must be represented. When i is relative prime to m then $d = 1$ and σ^i must be an m-cycle.

12. (a) if $\tau = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)$ determine whether there is an n-cycle $\sigma(n \geq 10)$ with $\tau = \sigma^k$ for some integer k.

    Suppose that τ is some power of σ that is $\tau = \sigma^i$ where σ is a 10-cycle. Clearly, 5 divides 10 so, from the last problem, there must be a σ such that $\sigma^5 = \tau$.
    Let's try (1 3 5 7 9 2 4 6 8 10)

    (b) if $\tau = (1\ 2)(3\ 4\ 5)$ determine whether there is an n-cycle $\sigma(n \geq 5)$ with $\tau = \sigma^k$ for some integer k.

σ		(1 3 5 2 4)
σ^2	(1 3 5 2 4)	(1 5 4 3 2)
σ^3	(1 5 4 3 2)	(1 2 3 4 5)

    It seems that every 5-cycle generates a 5-cycle and cannot generate a 2-cycle followed by a 3-cycle. I suspect that this because it is prime. Could a 6-cycle do this?

13. Show that an element has order 2 in S_n if and only if its cycle decomposition is a product of commuting 2-cycles.

14. Let p be a prime. Show that an element has order p in S_n if and only if its cycle decomposition is a product of commuting p-cycles. Show by an explicit example that this need not be the case if p is not prime.

15. Prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition. [Use Exercise 10 and Exercise 24 of Section 1.]

16. Show that if $n \geq m$ then the number of m-cycles in S_n is given by

$$\frac{n(n-1)(n-1)\cdots(n-m+1)}{m}$$

    [Count the number of ways of forming an m-cycle and divide by the numberof representations of a particular m-cycle.]

17. Show that if $n \geq 4$ then the number of permutations in S_n which are the product of two disjount 2-cycles is $n(n-1)(n-2)(n-3)/8$.

18. Find all numbers n such that S_5 contains an element of order n.

    2:
    3:
    4:
    5: $(\,1\ 2\ 3\ 4\ 5\,)(\,1\ 2\ 3\ 5\ 4\,)(\,1\ 2\ 4\ 3\ 5\,)(\,1\ 2\ 4\ 5\ 3\,)(\,1\ 2\ 3\ 5\ 4\,)(\,1\ 2\ 5\ 3\ 4\,)$
    $(\,1\ 2\ 5\ 4\ 3\,)(\,1\ 3\ 3\ 4\ 5\,)(\,1\ 3\ 2\ 5\ 4\,)(\,1\ 3\ 2\ 4\ 5\,)(\,1\ 3\ 4\ 2\ 5\,)(\,1\ 3\ 4\ 5\ 2\,)\ldots$

19. Find all numbers n such that S_7 contains an element of order n.

20. Find a set of generators and relations for S_3.

1.4 Matrix Groups

Definition 1.4.1 (Field)**.** .

1. a ***field*** is a set F together with two binary operations $+$ and $\cdot$ on F such that $(F,+)$ is an abelian group (call its identity 0) and $(F-\{0\},\cdot)$ is also an abelian group, and the following *distributive* law holds:

$$a \cdot (b+c) = (a\cdot b) + (a \cdot c), \text{ for all } a,b,c \in F$$

2. for any field F let $F^{\times} = F - \{0\}$.

Definition 1.4.2 (General Linear Matrices $GL_n(F)$)**.** For each $n \in \mathbb{Z}^+$ let $GL_n(F)$ be the set of all $n \times n$ matrices whose entries come from $\mathbb{F}$ and whose determinant is nonzero, i.e.,

$$GL_n(F) = \{A \mid A \text{ is an } n \times n \text{ matrix with entries from } F \text{ and } \det(A) \neq 0\}$$

1.4.1 Exercises

Let F be a field and let $n \in \mathbb{Z}^+$.[1]

1. Prove that $|GL_2(\mathbb{F}_2)| = 6$.

   Let $X \in GL_2(F_2)$ and $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a,b,c,d \in \mathbb{Z}/2\mathbb{Z}$. It must also be that $ad - bc \neq 0$ and therefore $ad \neq bc$.

2. Write out all the elements $GL_2(\mathbb{F}_2)$ and compute the order of each element.

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

[1] For the sake of argument, $\mathbb{F} = \mathbb{R}$

3. Show that $GL_2(\mathbb{F}_2)$ is non-abelian.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

4. Show that if n is not prime than $\mathbb{Z}/n\mathbb{Z}$ is not a field.

   Let n be any non-prime integer. Then, there exists a d such that $d|n$ and x such that $dx = n$. Thus, $dx = 0 \notin F-\{0\}$.

5. Show that $GL_n(F)$ is a finite group if and only if F has a finite number of elements.

6. If $|F| = q$ is finite prove that $|GL_n(F)| < q^{n^2}$.

7. Let P be a prime. Prove that the order of $GL_2(\mathbb{F}_p)$ is $p^4 - p^3 - p^2 + p$ (do not just quote the order formula in this section. [Subtract the number of 2×2 matrices which is *not* invertible from the total number of 2×2 matrices over $\mathbb{F}_p$. You may use the fact that a 2×2 matrix is not invertible if and ony if one row is multiple of th eother.]

8. Show that $GL_n(F)$ is non-abelian for any $n \geq 2$ and any F.

9. Prove that the binary operation of matrix multiplication of 2×2 with real number entries is associative.

10. Let $G = \left[\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}, a \neq 0, c \neq 0\right]$.

    (a) Compute the product of $\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$ and $\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$ to show that G is closed under matrix multiplication.

    $$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}$$

    (b) Find the matrix $N = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ and deduce that G is closed under inverses.

    First, since it is closed under multiplication and $I_2 \in G$ then there must exist another matrix $M \in G$ such that $I = MX$.

    $$\begin{aligned} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} w & x \\ y & z \end{pmatrix} \\ &= \begin{pmatrix} aw + by & ax + bz \\ cy & cz \end{pmatrix} \\ \therefore y = 0 & \end{aligned}$$

    (c) Deduce that G is a subgroup of $GL_2(\mathbb{R})$ (cf Exercise 26, Section 1).

    Clearly, any $X \in G \implies X \in GL_X(\mathbb{R})$ and, given any two elements $X, Y \in G \implies XY \in G$ and $x^{-1} \in G$. Therefore, $G \underset{\text{group}}{\subseteq} GL_2(\mathbb{R})$

    (d) Prove that the set of elements of G whose two diagonal entries are equal (i.e., $a = c$) is also a subgroup of $G_2(\mathbb{R})$.

    First, $I_2 \in G$ hence it contains an identity.
    Next, is it associative?
    Then, does it contain inverses?

The next exercise introduces the *Heisenberg group* over the field F and develops some of its basic properties. When $F = \mathbb{R}$ this group plays an important role in quantum mechanics and signal theory by giving a group theoretic interpretation (due to H. Weyl) of Heisenberg's Uncertainty Principle. Note also that the Heisenberg group may be defined more generally – for example with entries in $\mathbb{Z}$.

11. 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 in $H(F)$.

(a) Computer the matrix product XY and deduce that $H(F)$ is closed under matrix multiplication. Exhibit explicit matrices such that $XY \neq YX$ (so that $H(F)$ is always non-abelian).

(b) Find an explicit formula for the matrix inverse X^{-1} and deduce that $H(F)$ is closed under inverses.

(c) Prove the associative law for $H(F)$ and deduce tha $H(F)$ is a group of order $|F|^3$.

(d) Find the order of each element of the finite group $H(\mathbb{Z}/2\mathbb{Z})$.

(e) Prove that every nonidentity element of the group $H(\mathbb{R})$ has infinite order.

1.5 The Quaternion Group

Definition 1.5.1 (Quaternion Group, Q_8)**.** The ***quaternion group***, Q_8 is defined by

$$Q_8 = \{1, -1, i, -i, j, -jk, -k\}$$

with produce $\cdot$ computer as follows

$$\begin{aligned} 1 \cdot a = 1 \cdot = a, &\text{ for all } a \in Q_8 \\ (-1) \cdot (-1) = 1, (-1) \cdot a = a \cdot (-1) = -a, &\text{ for all } a \in Q_8 \\ i \cdot i = j \cdot j = k \cdot k = -1 \\ i \cdot j = k, j \cdot i = -k \\ j \cdot k = i, k \cdot j = -i \\ k \cdot i = j, i \cdot k = -j \end{aligned}$$

1.5.1 Exercises

1. Compute the order of each of the elements in Q_8.

   $|1| = 1,\ |-1| = 2,\ |i| = |j| = |k| = 4, |-i| = |-j| = |-k| = 4$

2. Write out the group tables for S_3, D_8 and Q_8.

S_3	(1)	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$
(1)	(1)	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	(1)	$(1\ 3)$	$(2\ 3)$	$(1\ 2)$
$(1\ 3\ 2)$	$(1\ 3\ 2)$	(1)	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$
$(1\ 2)$	$(1\ 2)$	$(2\ 3)$	$(1\ 3)$	(1)	$(1\ 3\ 2)$	$(1\ 2\ 3)$
$(1\ 3)$	$(1\ 3)$	$(1\ 2)$	$(2\ 3)$	$(1\ 2\ 3)$	(1)	$(1\ 3\ 2)$
$(2\ 3)$	$(2\ 3)$	$(1\ 3)$	$(1\ 2)$	$(1\ 3\ 2)$	$(1\ 2\ 3)$	(1)

D_8	1	r	r^2	r^3	s	sr	sr^2	sr^3
1	1	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	1	sr	sr^2	sr^3	s
r^2	r^2	r^3	1	r	sr^2	sr^3	s	sr
r^3	r^3	1	r	r^2	sr^3	s	sr	sr^2
s	s	sr	sr^2	sr^3	1	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r	r^2	r^2	1
sr^2	sr^2	sr^3	s	sr	r^2	r^3	1	r
sr^3	sr^3	s	sr	sr^2	r^3	1	r	r^2

Q_8	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-i$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	i	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$= i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	$= 1$

3. Find a set of generators and relations for Q_8.

1.6 Homomorphisms, Isomorphisms and Automorphisms

Definition 1.6.1 (Homomorphisms)**.** Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\varphi : G \underset{\text{homo}}{\longrightarrow} H$ such that

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y), \text{ for all } x, y \in G$$

is called a ***homomorphism***. If φ is bijective then it is called a ***isomorphism*** and G and H are said to be ***isomorphic***, written as $G \cong H$ ($G \cong_g H$ reads as "G is isomorphic by group to H".)

Remark 1.6.2. If $\varphi : G \to H$ is an isomorphism (i.e., $\varphi : G \underset{\text{iso}}{\longrightarrow} H$) then

1. $|G| = |H|$
2. G is abelian if and only if H is abelian.
3. for all $x \in G, |x| = |\varphi(x)|$.

Definition 1.6.3 (Kernel)**.** Define the ***kernel*** of φ to be $\{g \in G : \varphi(g) = 1_H\}$ (so the kernel is the set of elements in G which map to the identity of H, i.e., is the fiber over the identity of H).

Definition 1.6.4 (Automophism)**.** Let G be a group and let $\text{Aut}(G)$ be the set of all isomorphism from G to G. $\text{Aut}(G)$ is called the ***automorphism group*** of G and the elements of $\text{Aut}(G)$ are called ***automorphisms*** of G.).

1.6.1 Exercises

Let G and H be groups

1. Let $\varphi : G \underset{\text{homo}}{\longrightarrow} H$.

   (a) Prove that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}^+$
   First, $\varphi(x^2) = \varphi(x)\varphi(x) = \varphi(x)^2$.
   Assume that it is true for n, that is, $\varphi(x^n) = \varphi(x)^n$. Now let's take $\varphi(x^{n+1}) = \varphi(x^n \cdot x) = \varphi(x)^n\varphi(x) = \varphi(x)^{n+1}$

   (b) Do part (a) for $n = -1$ and deduce that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$
   $1 = xx^{-1}$ then $\varphi(1) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) = 1 \implies \varphi(x^{-1}) = \varphi(x)^{-1}$.

2. If $\varphi : G \underset{\text{iso}}{\longrightarrow} H$, prove that $|\varphi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if φ is only assumed to be a homomorphism?
   Let $|x| = n$ then $1 = \varphi(1) = \varphi(x^n) = \varphi(x)^n$. This is only true because φ is injective. So, if it is an injective homormorphism then it would also be true.

3. If $\varphi : G \underset{\text{iso}}{\longrightarrow} H$, prove that G is abelian if and only if H is abelian. If $\varphi : G \underset{\text{homo}}{\longrightarrow} H$, what additional conditions on φ (if any) are sufficeint to ensure that if G is abelian, then so is H?
   Let $x, y \in G$ then $xy = yx$ and

$$\varphi(xy) = \varphi(yx)$$
$$\iff$$
$$\varphi(x)\varphi(y) = \varphi(y)\varphi(x)$$

   therefore H is abelian.

4. Prove that the multiplicative groups $\mathbb{R} - \{0\}$ and $\mathbb{C} - \{0\}$ are not isomorphic.
   An isomorphism is bijective. There is no mapping from $\mathbb{R} - \{0\} \to \mathbb{C} - \{0\}$ that is bijective. For example, there is no $x \in \mathbb{R} - \{0\}$ such that $\varphi(x^2) = -1$.

5. Prove that the additive groups $\mathbb{R}$ and $\mathbb{Q}$ are not isomorphic.
   There is no $x \in \mathbb{Q}$ such that $x + x = \sqrt{2}$.

6. Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

7. Prove that D_8 and Q_8 are not isomorphic.
   There is no element x in D_8 such that $x^2 = s$.

8. Prove that if $n \neq m$, S_n and S_m are not isomorphic.
   $|S_n| \neq |S_m|$

9. Prove that D_{24} and S_4 are not isomorphic.

   D_{24} is abelian, S_4 is not

10. Fill in the details of the proof that the symmetric groups S_Δ and S_Ω are isomorphic if $|\Delta| = |\Omega|$ as follows: let $\theta : \Delta \leftrightarrow \Omega$. Define

$$\varphi : S_\Delta \to S_\Omega \text{ by } \varphi(\sigma) = \theta \circ \sigma \circ \theta^{-1} \text{ for all } \sigma \in S_\Delta$$

   and prove the following:

   (a) φ is well defined, that is, if σ is a permutation of Δ then $\theta \circ \sigma \circ \theta^{-1}$ is a permutation of Ω.

   (b) φ is an injection from S_Δ onto S_Ω. [Find a 2-sided inverse for φ]

   (c) φ is a homomorphism, that is, $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.
   Note the similrity to the *change of basis* or *similarity* transformations of matrices (we shall see the connectionb between these later in the text).

11. Let A and B be groups. Prove that $A \times A \cong B \times A$.

    Let $\varphi((a, b)) = (b, a)$

12. Let A, B, and C be groups and let $G = A \times B$ and $H = B \times C$. Prove that $G \times C \cong A \times H$.

13. Let G and H be groups and let $\varphi : G \underset{\text{homo}}{\longrightarrow} H$. Prove that the image of $\varphi, \varphi(G)$, is a subgroup of H (cf. Exercise 26 of Section 1). Prove that if φ is injective then $G \cong \varphi(G)$.

    Let $x, y \in G$ then $\varphi(x), \varphi(y) \in \varphi(G) \subseteq H$. Further, $\varphi(xy) = \varphi(x)\varphi(y) \in \varphi(G)$ and $\varphi(1) = \varphi(xx^{-1} = \varphi(x)\varphi(x^{-1}) = \varphi(x)\varphi(x)^{-1} = 1$. Therefore, $\varphi(G) \underset{\text{group}}{\subseteq} H$.

14. Let G and H be groups and let $\varphi : G \underset{\text{homo}}{\longrightarrow} H$. Define the *kernel* of φ to be $\{g \in G : \varphi(g) = 1_H\}$ (so the kernel is the set of element sin G which map to the identity of H, i.e., is the fiber over the identity of H). Prove that the kernel of φ is a subgroup (cf. Exercise 26 of Section 1) of G. Prove that φ is injective if and only if the kernel of φ is the identity of subgroup of G.

    Let $x, y \in \ker(\varphi)$. Then $\varphi(xy) = \varphi(x)\varphi(y) = 1 \cdot 1 = 1 \in \ker(\varphi)$. Also, $\varphi(1 \cdot x) = \varphi(1)\varphi(x) = varphi(1) \cdot 1 \implies \varphi(1) \in \ker(\varphi)$. Lastly, $1 = \varphi(xx^{-1}) = \varphi(x)\varphi(x)^{-1} \implies \varphi(x)^{-1} \in \ker(\varphi)$

15. Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π (cf Exercise 14).

    Let $a, b \in \mathbb{R}^2$ such that $a = (x, y), b = (u, v)$. Then $\pi(ab) = \pi(a)\pi(b) = xu \to ab = (xu, yv), \pi(ab) = xu$. And $\ker(\pi) = \{a = (x, y) \,|\, \pi((x, y)) = 1\}$ or when $a = (1, y), \forall y \in \mathbb{R}$.

16. Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels (cf. Exercise 14).

17. Let B be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

    Let $g, h \in G$ and $\varphi(g) = g^{-1}, \forall g \in G$. Then, $\varphi(gh) = \varphi(g)\varphi(h) = g^{-1}h^{-1} = (gh)^{-1} = h^{-1}g^{-1}$. Hence, abelian.

18. Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

    Let $\varphi(g) = g^2$.

$$\begin{aligned} \varphi(gh) &= \varphi(g)\varphi(h) \\ (gh)^2 &= g^2h^2 \\ ghgh &= gghh \\ g^{-1}ghghh^{-1} &= g^{-1}gghhh^{-1} \\ gh &= hg \end{aligned}$$

    hence abelian.

19. Let $G = \{z \in \mathbb{C} \,|\, z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \mapsto z^k$ is a surjective homomorphism but is not an isomorphism.

    Let $k > 1$ and $\varphi(z) = z^k$ where $z \in G$. Then given any $w \in G$ we can find the k^{th} root of w, namely y. $y^k = w = z^k$ for some $z \in G$. Hence, $y = z$. However, it is not isomorphic, as there are $k - 1$ elements that whose value raied to the power of k equals 1.

20. Let G be a group and let $\text{Aut}\,(G)$ be the set of all isomorphism from G to G. Prove that $\text{Aut}\,(G)$ is a group under function composition (called the *automorphism group* of G and the elements of $\text{Aut}\,(G)$ are called *automorphisms* of G.).

    Let $\varphi, \phi, \pi \in \text{Aut}\,(G)$.
    Associative? Does $(\varphi \circ \phi) \circ \pi = \varphi \circ (\phi \circ \pi)$?
    Identity exist? $I : G \to G$ such that $I(g) = g$, $\forall g \in G$. Then, $(\phi \circ I)(g) = \phi(I(g)) = \phi(g) \implies \phi \circ I = \phi$
    Inverses? each element is an isomorphism, which means that it is bijective and hence has an inverse.

21. Prove that for each fixed nonzero $k \in \mathbb{Q}$ the map from $\mathbb{Q}$ to itself defined by $q \mapsto kq$ is an automorphism of $\mathbb{Q}$ (cf.Exercise 20).

    Let $\varphi(q) = kq$ for some $k \in \mathbb{Q}$. Need to show that φ is a bijection.

22. Let A be an abelian group and fix some $k \in \mathbb{Z}$. Prove that the map $a \mapsto a^k$ is a homomorphism from A to itself. If $k = -1$ prove that this homomorphism is an isomorphism (i.e., is an automorphism of A).

    Let $a, b \in A$ and let $\varphi(a) = a^k$ for some k. Then, $\varphi(ab) = (ab)^k = \underbrace{ab \ldots ab}_{k\text{-times}}$. Since A is commutative we have $\underbrace{ab \ldots ab}_{k\text{-times}} = a^k b^k = \varphi(a)\varphi(b)$ and hence a homomorphism. If $k = -1$ then φ is injective because each inverse is unique, and surjective because every $a \in A$ has an inverse, hence an isomorphism.

23. Let G be a finite group which possesses an automorphism σ (cf.Exercise 20) such that $\sigma(g) = g$ if and only if $g = 1$. If σ^2 is the identity map from G to G, prove that G is abelian (such an automorphism σ is called *fixed point free* of order 2). [Show that every element of G can be written in the from $x^{-1}\sigma(x)$ and apply σ to such an expression.]

24. Let G be a finite group and let x nd y be distinct elements of order 2 in G that generate G. Prove that $G \cong D_{2n}$, where $n = |xy|$. [See Exercise 6 in Section 2.]

25. Let $n \in \mathbb{Z}^+$, let r and s be the usual generators of D_{2n} and let $\theta = 2\pi/n$.

    (a) Prove that the marix $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is the matrix of the linear transformation which rotates the x, y plane about the origin in a counterclockwise direction by θ radians.

    (b) Prove that the map $\varphi : D_{2n} \to GL_2\mathbb{R}$ defined on the gener/ators by

    $$\varphi(r) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ and } \phi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

    extends to a homomorphism of D_{2n} into $GL_2(\mathbb{R})$.

    (c) Prove that the homomorphism φ in part (b) is injective.

26. Let i and j be the generators of Q_8 described in Section 5. Prove that the map φ from Q_8 to $GL_2(\mathbb{C})$ defined on generators by

    $$\varphi(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \text{ and } \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

    extend to a homomorphism. Prove that φ is injective.

1.7 Group Actions

Definition 1.7.1 (Group Action)**.** A ***group action*** of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$, for all $g \in G$ and $a \in A$) satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, for all $g_1, g_2 \in G, a \in A$, and
2. $1 \cdot a = a$ for all $a \in A$.

Remark 1.7.2. Let the group G act on the set A. For each fixed $g \in G$ we get a map σ_g defined by

$$\sigma_g : A \to A$$
$$\sigma_g(a) = g \cdot a$$

with two important facts:

1. For each fixed $g \in G, \sigma_g$ is a *permutation* of A, and
2. for each map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism.

Definition 1.7.3 (Permutation Representation)**.** The homomorphism from G to S_A given above is called the ***permutation representation*** associated to the given action. It is easy to see that the process is reverisble in the sense that if $\varphi : G \to S_A$ is any homomorphism from a group G to the symmetric group on a set A, then the map from $G \times A$ to A defined by

$$g \cdot a = \varphi(g)(a), \text{ for all } g \in G, \text{ and } a \in A$$

satisfies the properties of a group action of G on A. Thus actions of a group G on a set A and the homoomorphisms from G into the symmetric group S_A are in bijective correspondence (i.e., are essentially the same notion, phrased in different terminology).

Definition 1.7.4. If G acts on a set B and distinct elements of G induce distinct permutations of B, the action is said to be ***faithful*** A faithful action is therefore one in which the associated permutation representation is injective.

Definition 1.7.5 (Conjugation)**.** Let G be a any group and let $A = G$. Show that he maps defined by $g \cdot a = gag^{-1}$ for all $g, a \in G$ *do* satisfy the axioms of a (left) group action (this action of G of itself is called ***conjugation***).

Definition 1.7.6 (Orbits)**.** Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined by

$$a \sim b \iff a = hb \text{ for some } h \in H$$

is an equivalence relation. (for each $x \in A$, the equivalence class of x under $\sim$ is called the ***orbit*** of x under the action of H. The orbits under the action of H partition the set A.)

Theorem 1.7.7 (Lagrange's Theorem)**.** *If G is a finite group and H is a subgoup of G then $|H|$ divides $|G|$.*

1.7.1 Exercises

1. Let F be a field. Show that the multiplicative group of nonzero elements of G (denoted by $F^{\times}$) acts on the set F by $g \cdot a = ga$, where $g \in F^{\times}, a \in F$ and ga is the usual product in F of the two field elements (state clearly which axioms in the definiton of a filed are used).

2. Show that the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$

3. Show that the additive group $\mathbb{R}$ acts on the x, y plane $\mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.

4. Let G be a group acting on a set of A and fix some $a \in A$. Show that he following sets are subgroups of G (cf. Exercise 26 of Section 1):
   (a) the kernel of the action,
   (b) $\{g \in G \mid ga = a\}-$ this subgroup is called the *stabilizer* of a in G.

5. Prove that the kernel of an action of the group G on the set A is the same as the kernel of the corresponding permutation representation $G \to S_A$ (cf. Exercise 14 in Section 6).

6. Prove that a group G acts faithfuly on as set A if and only if the kernel of the action is the set consisting only of the identity.

7. Prove that in Example 2 in this section the action is faithful.

8. Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts on the set B consisting of all subsets of A of cardinality k by $\sigma \cdot \{a_1, \cdot, a_k\} = \{\sigma(a_1), \ldots, \sigma(a_k)\}$.
   (a) Prove that this is a group action.
   (b) Describe explicitly how the elements $(\ 1 \quad 2\ )$ and $(\ 1 \quad 2 \quad 3\ )$ act on the six 2-element subsets of {1,2,3,4}.

9. Do both parts of the preceding exercise wth "ordered k-tuples" in place of k-element subsets," where the action on k-tuples is defined as above but with set braces replaced by parentheses (not that, for example, the 2-tuple (1,2) and (2,1) are different even though the sets $\{1, 2\}$ and $\{2, 1\}$ are the same, so the sets being acted upon are different).

10. With reference to the preceding two exercises determine:
    (a) for which value sof k the action of S_n on k-element subsets is faithful, and
    (b) for which values of k th eaction of S_n on orderd k-tuples is faithful.

11. Write out the cycle decompowition o fthe eight permutations in S_4 corresponding to the elements of D_8 given by the action of D_8 on the vertices of a square (where the vertices of the square are labelled as in section 2).

12. Assume n is an even positive integer and show that D_{2n} acts on the set consisting of pairs of opposite vertice of a regular n-gon. Find the kernel fo this action (label vertices as usual).

13. Find the kernel of th eleft regular action.

14. Let G be a group and $A = G$. Show that if G is non-abelian then the maps defined by $g \cdot a = ag$ for all $g, a \in G$ do *not* satisfy the axioms of a (left) group action of G on itself.

15. Let G be any group and let $A = G$. Show that the maps defined by $g \cdot ag^{-1}$ for all $g, a \in G$ *do* satisfy the axioms of a left group action of G on itself.

16. Let G be a any group and let $A = G$. Show that the maps defined by $g \cdot a = gag^{-1}$ for all $g, a \in G$ o satisfy the axioms of a (left) group action (this action of G of itself is called *conjugation*).

17. Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by
$$x \mapsto gxg^{-1}$$
For fixed $G \in G$, prove that conjugation by g is an isomorphism from G onto itself (i.e., is an automorphism of G - cf. Exercise 20, section 6). Decuce that x and gxg^{-1} have the same order for all x in G and that for any subset A of $G, |A| = |gAg^{-1}|$ (here $gag^{-1} = \{gag^{-1} \mid a \in A\}$).

18. Let H be a group acting on aset A. Prove that the relation $\sim$ on A defined by
$$a \sim b \iff a = hb \text{ for some } h \in H$$
is an equivalence relation. (for each $x \in A$, the equivalence class of x under $\sim$ is called the *orbit* of x under the action of H. The orbits under the action of H partition the set A.)

19. Let H be a subgroup of (cf. Exercsie 26 of Section 10 of the finite group G and let H act on G (here $A = G$) by left multiplication. Let $x \in G$ and let $\mathcal{O}$ be the orbit of x under the action of H. Prove that the map
$$H \to \mathcal{O} \text{ defined by } h \mapsto hx$$
is a bijection (hence all orbits have cardinality $|H|$). From this and the preceding exerecise deduce *Lagrange's Theorem*:

    if G is a finite group and H is a subgoup of G then $|H|$ divides $|G|$.

20. Show that the group of rigid motions of a tetrahedron is isomorphic to a subgroup (cf. Exercise 26 of Section 1) of S_4.

21. Show that the group of rigid motions of a cube is isomorphic to S_4. [This group acts on the set of four pairs of opposite vertices.]

22. Show that the group of rigid motions of an octahedron is isomorphic to a subgroup (cf. Exerci e 26 of Section 1) of S_4. [This group acts on the set of four paris of opposite faces.] Deduce that the groups of rigid motions of a cube and octahedron are isomorphic. (These groups are isomorphic because these solids are 'dual" – *introduction to Geometry* by H. Coxeter, Wiley, 1961. We shall see later that the groups of rigid motions of the dodecahedron and icosahedron are isomorphic as well - these solids are also dual.)

23. Explain why the action of the group of rigid motions of a cube on the set of three pairs of opposite faces is not faithful. Find the kernel of this action.

Chapter 2

Subgroups

2.1 Definitions and Examples

Definition 2.1.1 (Subgroup)**.** Let G be a group. The subset H of G is a ***subgroup*** of G if H is nonempty and H is closed under products and inverses (i.e., $x, y \in H \implies x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$.

Proposition 2.1.2 (The Subgroup Criterion)**.** A subset H of a group G is a subgroup if and only if

1. $H \neq \emptyset$, and
2. for all $x, y \in H, xy^{-1} \in H$.

Definition 2.1.3 (Special Linear Group, $SL_n(F)$)**.** Define the ***special linear group*** on a field F, $SL_n(F)$ as:

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

Note $SL_n(F) \leq GL_n(F)$.

2.1.1 Exercises

Let G be a group.

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

   (a) the set of complex numbers of the from $a + ai, a \in \mathbb{R}$ (under addition).
   Let $a + ai, b + bi \in H$. $(b + bi)^{-1} = -b - bi$. Is $(a + ai) + (-b - bi) \in H$?

   $$(a + ai) + (-b - bi) = (a - b) + (a - b)i \in H$$

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

   $$\begin{aligned} \text{Let } x, y \in H \text{ and } x = e^{i\theta}, y = e^{i\phi} \\ y^{-1} &= y^{-i\phi} \\ xy^{-1} &= e^{i\theta}e^{-i\phi} \\ &= e^{i(\theta-\phi)} \\ \text{and } \left|e^{i(\theta-\phi)}\right| &= 1 \implies xy^{-1} \in H \end{aligned}$$

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

   $$\begin{aligned} \text{Let } x, y \in H \text{ and } x = \frac{a}{b}, y = \frac{c}{d} \text{ where } b|n, d|n \\ x \cdot y^{-1} &= \frac{a}{b} - \frac{c}{d} \\ &= \frac{ad - bc}{bd} \\ \text{clearly } bd|n \therefore x \cdot y^{-1} \in H \end{aligned}$$

   When $bd > n$ we can multiple top and bottom by the corresponding elements (i.e., where $bb' = n$ and $dd' = n$ and factor out an n reducing the fraction to one where the denominator divdes n.

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

(e) the set of nonzero real numbers whose square is a rational number (under mutiplication).
Let $p, q \in \mathbb{R} \to p^2, q^2 \in \mathbb{Q}$. Then $(q^{-1})^2 = q^{-2} = \frac{1}{q^2} \in \mathbb{Q}$. Therefore, $q^{-1} \in H$.
$pq^{-1} = \frac{p}{q}$ and $\left(pq^{-1}\right)^2 = \frac{p^2}{q^2} \in \mathbb{Q}$

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

(a) the set of 2-cycles in S_n for $n \geq 3$.
the identity is not a 2-cycle.

(b) the set of reflections in D_{2n} for $n \geq 3$.
the identity is not a reflection

(c) for n as a composite integer > 1 and G a group containing an element of order n, the set $\{x \in G \,|\, |x| = n\} \cup \{1\}$.
h

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

(e) the set of real numbers whose square is a rational number (under addition).
Let $p, q \in H$ then $(p+q)^2 = p^2 + q^2 + 2pq \notin H$.

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

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

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

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

5. Prove that G cannot have a subgoup H with $|H| = n - 1$, where $n = |G| > 2$.
$H = \{z \,|\, z = 1/d, d \in \mathbb{Z}\}$ over addition

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

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

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

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

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

(called the *special linear group*). Prove that $SL_n(F) \leq GL_n(F)$.
Let $x, y \in SL_n(F)$ then $\det(y^{-1}) = 1 \implies y^{-1} \in SL_n(F)$.
Then, $\det(xy^{-1}) = \det(x)\det(y^{-1}) = 1 \cdot 1 \implies xy^{-1} \in SL_n(F)$.

10. (a) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.
First 1 is in $H \cap K$, hence not empty. Next, if $y \in H \cap K$ then $y^{-1} \in H$ and $y^{-1} \in K$ therefore $y^{-1} \in H \cap K$.
A similar argument holds for $x, y \in H \cap K \implies xy \in H \cap K$

(b) Prove that the intersection of an arbitrary nonempty collection ofsubgroups of G is again a subgroup of G (do not assume the collection is countable).

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

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

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

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

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

(a) $\{a^n \,|\, a \in A\}$

(b) $\{a \in A \,|\, a^n = 1\}$.

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

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

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

    Inductive Proof.

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

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

2.2 Centralizers and Normalizers, Stabilizers and Kernels

Definition 2.2.1 (Centralizer)**.** Define $C_G(A) = \{g \in G \,|\, gag^{-1} = a, \forall a \in A\}$. This subset of G is called the ***centralizer*** of A in G. Since $gag^{-1} = a$ if and only if $ga = ag, C_G(A)$ is the set of elements of G which commute with every element of A.

Note: The centralizer is the set of gs that commute with EVERY element in A.

Definition 2.2.2 (Center)**.** Define $Z(G) = \{g \in G \,|\, gx = xg, \forall x \in G\}$, the set of elements commuting with all the elements of G. This subset of G is called the ***center*** of G.

Definition 2.2.3 (Normalizer)**.** Define $gAg^{-1} = \{gag^{-1} \,|\, a \in A\}$. Define the ***normalizer*** of A in G to be the set $N_G(A) = \{g \in G \,|\, gAg^{-1} = A\}$.

Note: the normalizer is the set of gs whose commute in any $a \in A$ is also in A but not necessarily equal.

Definition 2.2.4 (Stabilizer)**.** The ***stabilizer*** of $s \in G$ is the set

$$G_s = \{g \in G \,|\, g \cdot s = s\}.$$

Note: given some point s this is the set of elements in G that have no effect on it.

Definition 2.2.5 (Kernel)**.** The ***kernel*** of an action is a subgroup, where the kernel of the action of G on S is defined as

$$\{g \in G \,|\, g \cdot s = s, \forall s \in S\}.$$

Note: the kernel depends on the entire set S and it is the subgroup of G that doesn't effect it (set of stabilizers).

2.2.1 Exercises

1. Prove that $C_G(A) = \{g \in G \,|\, g^{-1}ag = a, \forall a \in A\}$.

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

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

$$\begin{aligned} C_G(A) &= \{g \in G \,|\, gag^{-1} = a, \forall a \in A\} \\ N_G(A) &= \{g \in G \,|\, gAg^{-1} = A\} \end{aligned}$$

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

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

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

   (a) $G = S_3$ and $A = \{1, (\begin{array}{ccc} 1 & 2 & 3 \end{array}), (\begin{array}{ccc} 1 & 3 & 2 \end{array})\}$.

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

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

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.

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

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

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

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

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

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

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

12. Let R be the set of al polynomials with integer coefficients in teh independendent variables x_1, x_2, x_3, x_4, i.e., the numbers of R are finite sums of elements of the form $Ax_1^{r_1}x_2^{r_2}x_3^{r_3}x_r^{r_4}$, where a is any integer and $r_1, \ldots, r_4$ are nonnegative integers. For example,

$$12x_1^5x_3 2^7x_4 - 18x_2^3x_3 + 11x_1^g x_2 x_3^3 x_4^{23}$$

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

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

for all $p(x_1, x_2, x_3, x_4) \in \mathbb{R}$ (i.e., σ simly permutes the indices of the variables). For example, if $\sigma =$(1 2)(3 4) and $p(x_1, x_2, x_3, x_4)$ is the polynomial in (*) above, then

$$\begin{aligned}\sigma \cdot p(x_1, x_2, x_3, x_4) &= 12x_2^5x_1^7x_3 - 18x_1^3x_4 + 11x_2^6x_1x_4^3x_3^{23} \\ &= 12x_1^7x_2^5x_3 - 17x_1^3x_4 + 11x_1x_2^6x_3^{23}x_4^3.\end{aligned}$$

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

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

   (c) Exhibit all permutations in S_4 that stabilize x_4 and prove that they form a subgoup 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.

   (e) Exhibit all permutations in S_4 that stabilize the elements $x_1x_2 + x_3x_4$ and prove that they form a subgroup isomorphic to the diheral group of order 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) are the subgroup that stabilizes them awill play an imporant rolebin the study of roots of quartic equationsi in Section 14.6.)

13. Let n be a positive integer and let R be the set of all polynomials with integer coefficients in the independnent variables $x_1, x_2, \ldots, x_n$, i.e., the members of R are finite sums of elements of the from $ax_1^{r_1}x_2^{r^2} \cdots x_n^{r_n}$, where a is any integer and $r_1, \ldots, r_n$ are nonnegative integers. For each $\sigma \in S_n$ define a map

$$\sigma : R \to R \text{ by } \sigma p(x_1, x_2, x_3, x_4) = p(x_{\sigma 1}, x_{\sigma 2}, \ldots, x_{\sigma n}).$$

   Prove that this defines 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.

2.3 Cyclic Groups and Cyclic Subgroups

Definition 2.3.1 (Cyclic Group)**.** A group H is ***cyclic*** if H can be generated by a single element, i.e., there is some element $x \in H$ such that $H = \{x^n \,|\, n \in \mathbb{Z}\}$ (where as usual the operation is multiplication). We shall write $H = \langle\, x \,\rangle$ and say H is *generated* by x (and x is a *generator* of H).

Proposition 2.3.2. If $H = \langle\, x \,\rangle$, then $|H| = |x|$ (where if one side of this equality is infinite, so is the other). More specifically:

1. if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all the distinct elements of H, and
2. if $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b$. (Note: infinite and distinct elements, countable?).

Proposition 2.3.3. Let G be an arbitrary group, $x \in G$ and let $m, n \in \mathbb{Z}$. If $x^n = 1$ and $x^m = 1$, then $x^d = 1$, where $d = (m, n)$. In particualr, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m.

Theorem 2.3.4. *Any two cyclic groups of the same order are isomorphic. More specifically,*

1. *if $n \in \mathbb{Z}^+$ and $\langle\, x \,\rangle$ and $\langle\, y \,\rangle$ are both cyclic groups of order n, then the map*

$$\begin{aligned} \varphi : \langle\, x \,\rangle &\to \langle\, y \,\rangle \\ x^k &\mapsto y^k \end{aligned}$$

is well defined and is an isormophism.

2. *if $\langle\, x \,\rangle$ is an infinite cyclic group, the map*

$$\begin{aligned} \varphi : \mathbb{Z} &\to \langle\, x \,\rangle \\ k &\mapsto x^k \end{aligned}$$

is well defined and is an isomorphism.

Proposition 2.3.5. Let G be a group, let $x \in G$ and let $a \in \mathbb{Z} - \{0\}$.

1. If $|x| = \infty$, then $|x^a| = \infty$.
2. If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$.
3. In particular, if $|x| = n < \infty$ and a is a positive integer dividing n, then $|x^a| = \frac{n}{a}$.

Proposition 2.3.6. Let $H = \langle\, x \,\rangle$.

1. Assume $|x| = \infty$. Then $H = \langle\, x^a \,\rangle$ if and only if $a = \pm 1$.
2. Assume $|x| = n < \infty$. Then $H = \langle\, x^a \,\rangle$ if and only if $(a, n) = 1$. In particular, the number of generators of H is $\varphi(n)$ (where φ is Euler's φ-funtion).

Theorem 2.3.7. *Let $H = \langle\, x \,\rangle$ be a cyclic group.*

1. *Every subgroup of H is cyclic. More precisely, if $K \leq H$, then either $K = \{1\}$ or $K = \left\langle\, x^d \,\right\rangle$, where d is the smallest positive integer such that $x^d \in K$.*
2. *$|H| = \infty$, then for any distinct nonnegative integers a and $b, \langle\, x^a \,\rangle \neq \left\langle\, x^b \,\right\rangle$. Furthermore, for every integer $m, \langle\, x^m \,\rangle = \left\langle\, x^{|m|} \,\right\rangle$, where $|m|$ denotes the absolute value of m, so that the nontrivial subgroups of H correspond bijectively with the integers $1, 2, 3, \ldots$.*
3. *if $|H| = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of H of order a. This subgroup is the cyclic group $\left\langle\, x^d \,\right\rangle$, where $d = \frac{n}{a}$. Furthermore, for every integer $n, \langle\, x^m \,\rangle = \left\langle\, x^{(n,m)} \,\right\rangle$, so that the subgroups of H correspond bijectively with the positive divisors of m.*

Remark 2.3.8 (Notation)*.* For each $n \in \mathbb{Z}^+$, let $\mathbb{Z}_n$ be the cyclic group of order n. Also, notice that $\mathbb{Z}/n\mathbb{Z}$ is the set of equivalence classes $\overline{k} \equiv k \bmod n$ for all $k \in \mathbb{Z}$.

2.3.1 Exercises

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

   45 is a composite number which decomposes into the following primes $5 * 3 * 3$. This means that we have all of the combinations of these three numbers: 3, 5, 9, 15. And these will generate the following subgroups:

   - 3: {0,3,6,9,12,15,18,21,24,27,30,33,36,39,42}
   - 5: {0,5,10,15,20,25,30,35,40}

- 9: {0,9,18,27,36}
- 15: {0,15,30}

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.

   From Proposition 2.3.2, every element $y \in H$ is represented by some element x^k for some $k \in \mathbb{Z}$. Thus, $H = \langle\, x \,\rangle$
   Let $G = \mathbb{Z}$. Then $|G| = \infty$ and it is clear that $2 \in \mathbb{Z}, |2| = \infty$ and that $3 \notin \langle\, 2 \,\rangle$.

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

   48 is a composite number whose prime decomposition is 48=2*2*2*2*3. Any combination of these primes will divide 48 and, hence, be a generator for $\mathbb{Z}/48\mathbb{Z}$. Namely, 2,4,8,16,3,6,12,24.

   - 2: {0,2,4,6,8,10,12,14,16,18,20,22,24,26,28,30,32,34,36,38,40,42,44,46}
   - 4: {0,4,8,12,16,20,24,28,32,36,40,44}
   - 8: {0,8,16,24,32,40}
   - 16: {0,16,32}
   - 3: {0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45}
   - 6: {0,6,12,18,24,30,36,42}
   - 12: {0,12,24,36}
   - 24: {0,24}
   - note that
     - $\langle\, 16 \,\rangle \leq \langle\, 8 \,\rangle \leq \langle\, 4 \,\rangle \leq \langle\, 2 \,\rangle$
     - $\langle\, 24 \,\rangle \leq \langle\, 12 \,\rangle \leq \langle\, 6 \,\rangle \leq \langle\, 2 \,\rangle$
     - $\langle\, 24 \,\rangle \leq \langle\, 12 \,\rangle \leq \langle\, 6 \,\rangle \leq \langle\, 3 \,\rangle$

   OOPS. These are the subgroups of $\mathbb{Z}/48\mathbb{Z}$ not the generators. The generators are the relative primes between to 48 which are less than 48.
   The relative primes in $\mathbb{Z}/48\mathbb{Z}$ of 48 are 1, 5,7,11,13,17,23,31,37,41,43,47. Each of these generates $\mathbb{Z}/48\mathbb{Z}$.

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

   The relative primes of $\mathbb{Z}/202\mathbb{Z}$.

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

   what is $\varphi(49000)$?

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

   see Exercise 3

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

   See Exercise 3

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

   Reworded: Given x, a relative prime of 48, for which integers a does x^a equal another relative prime?

9. Let $\mathbb{Z}_{36} = \langle\, x \,\rangle$. 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 $\mathbb{Z}_{36}$. Can ψ_a ever be a surjective homomorphism?

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

    $\langle\, \overline{30} \,\rangle = \{0, 30, 6, 36, 12, 42, 18, 48, 24\}$ and $|\langle\, \overline{30} \,\rangle| = 9$
    Or by the Theorem $|\langle\, \overline{30} \,\rangle| \, \frac{54}{(30,54)} = \frac{54}{6} = 9$

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

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

    (a) $\mathbb{Z}_2 \times \mathbb{Z}_2$.
    If it were cyclic then there would exist an x such that $\langle\, x \,\rangle = \mathbb{Z}_2 \times \mathbb{Z}_2$ That is given any element $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ we would need to find $x^d = (a, b)$ for some d.

    (b) $\mathbb{Z}_2 \times \mathbb{Z}$.

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

Ultimately, all of these are Linearly Independent two dimensional spaces which cannont be defined by a single varialbe.

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

    (a) $\mathbb{Z} \times \mathbb{Z}_2$ and $\mathbb{Z}$.

    (b) $\mathbb{Q} \times \mathbb{Z}_2$ and $\mathbb{Q}$.

    Ultimately, all of these are Linearly Independent two dimensional spaces which cannont befined by a single varialbe.

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: $a = 13, , 6, 626, 1195 - 6, -81, -570$ and -1211.

    We must understand that $\sigma^{12} = \sigma$. Thus $\sigma^a = \sigma^{a \bmod 12}$.

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

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

17. Find a presentation for $\mathbb{Z}_n$ with one generator.

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

    $\mathbb{Z}_n = \{x^a \bmod n \,|\, x|n = 1, a \in \{0.1. \dots, n-1\}\, \}$

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

20. Let p be a prime and let n be a positive integer. Show that if x is an element of the group G such that $x^{p^n} = 1$ then $|x| = p^m$ 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 $(1+p)^{p^{n-1}} \equiv 1 (\bmod\, p^n)$ but $(1+p)^{p^{n-2}} \not\equiv 1 (\bmod\, p^n)$. Deduce that $1 + p$ is an element of order p^{n-1} in the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

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

23. Show that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for any $n \geq 3$. [Find two distinc subgroups of order 2.]

24. Let G be a finite group and let $x \in G$.

    (a) Prove that if $g \in N_G(\langle\, x \,\rangle)$ then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.
    Let $g \in N_G(\langle\, x \,\rangle)$ and $n = |N_G(\langle\, x \,\rangle)|$. Let there exist $a, b \in \mathbb{Z}$ such that $gx^ag^{-1} = x^a$ and $gx^bg^{-1} = x^b$. Then $x^ax^b = gx^ag^{-1}gx^bg^{-1} = gx^ax^bg^{-1} = x^{a+b \bmod n}$.

    (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 ay integer k, so that $g \langle\, x \,\rangle g^{-1} \leq \langle\, x \,\rangle$. If x has order n, show that the element $gx^ig^{-1}, i = 0, 1, \dots, n-1$ are distinct, so that $|g \langle\, x \,\rangle g^{-1}| = |\langle\, x \,\rangle| = n$ and conclude that $g \langle\, x \,\rangle g^{-1} = \langle\, x \,\rangle$.]

    Note that this cuts down some of the work in computing normalizers of cyclic subgroups since one does not have to check $ghg^{-1} \in \langle\, x \,\rangle$ for every $h \in \langle\, x \,\rangle$

25. Let G be a cyclic group of order n and let k be an intger 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 some k each element has a k^{th} root in G. It follows from Cauchy's Theorem in Section 3.2 that if k is not relatively prime to the order of G then the map $x \mapsto x^k$ is not surjective.)

26. Let $\mathbb{Z}_n$ be a cyclic group of order n and for each integer a let

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

    (a) Prove that σ_a is an automorphism of $\mathbb{Z}_n$ if and only if a and n are relatively prime (automorphisms were introduced in Exercise 20, Section 1.6).

    (b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b (\bmod\, n)$.

    (c) Prove that *every* automorphism of $\mathbb{Z}_n$ is equal to σ_a for some integer a.

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

2.4 Subgroups generated by Subsets of a Group

Proposition 2.4.1. If $\mathcal{A}$ is any nonempty collection of subgroups of G, then the intersection of all mumbers of $\mathcal{A}$ is also a subgroup of G.

Definition 2.4.2 (Subgroup of G generated by A)**.** If A is any subset of a group G define

$$\langle A \rangle = \bigcap_{A \subseteq H, H \leq G} H.$$

This is called the ***subgroup of*** G ***generated by*** A.***Note: the intersection of all subgroups that contain*** A.

Definition 2.4.3 (Closure of A)**.** The set which is the ***closure of*** A under the group operation (and the process of taking inverses). Let

$$\overline{A} = \{a_1^{\epsilon_1}, a_2^{\epsilon_2}, \ldots, a_n^{\epsilon_n} \mid n \in \mathbb{Z}, n \geq 0 \text{ and } a_i \in A, \epsilon_i = \pm 1 \text{ for each } i\}$$

where $\overline{A} = \{1\}$ if $A = \emptyset$, so that $\overline{A}$ is the set of all finite products (called *words*) of elements of A and inverses of elements of A. Not that the a_i's need not be distinct, so a^2 is written aa in the notation defining $\overline{A}$. Note also that A is not assumed to be a finite (or even countable) set.

Proposition 2.4.4. $\overline{A} = \langle A \rangle$, that is the closure of A is also the smallest subgroup containing A.

Definition 2.4.5. Misc.

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

2.4.1 Exercises

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

   suppose that there were an $x \in \langle H \rangle$ but $x \notin H$. The $|\langle H \rangle| > |H|$. However, H is a group hence $\langle H \rangle$ is not the smallest possible subgroup in G.

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 $\langle A \rangle = \langle B \rangle$.

   The elements of S_3 that are of order 2 are (1 2), (2 3) and (1 3). Any two of this will utilize every one of the base elements. Further the product/powers of these two elements will generate the remaining elements of S_3.

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

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

   Essentially, every subgroup contains 1 and the smallest sugroup containing all of the elements of H except one contains 1.

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

   The only elements of order two are transpositions and there are only 3 of them (1 2), (2 3), (1 3). Any two of these will require all 3 of the base elements to be part of the closure. Hence, S_3.

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

   (1 2) has order 2.
   (1 2)(3 4) has order 2.
   (1 2)(1 2)(3 4) = (3 4) which has order 2.
   (1) is necessary to make it group (must have identity.
   That makes 4 elements.

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

   $D_8 = \left\langle r, s \mid r^4 = s^2 = 1, rs = sr^{-1} \right\rangle$. Notice that that $\left|(\ 1 \quad 2\ )\right| = 2$ now show that $\left|(\ 1 \quad 3\ )(\ 2 \quad 4\ )\right| = 4$ Will this be enough? I think that we still have to demonstrate a 1-to-1 relationship between the elements of D_8 and S_4.

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

   Demonstrate that each generates a subgroup whose intersection is (1)

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

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_3)$. Hence $\det(A) = ad - bc = 1$ Since $a, b, c, d \in \{0, 1, 2\}$ This is true when

$$\begin{aligned} ad - bc = 2 - 1, & \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \\ = 1 - 0, & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}, \\ & \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix} \\ = 0 - (-1), & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ = -1 - (-2), & \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -2 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix} \\ & \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -2 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 2 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 2 & 1 \end{pmatrix}, \end{aligned}$$

10. Prove that the subgroup $SL_2(\mathbb{F}_3)$ 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]

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

Demonstrate that $SL_2(\mathbb{F}_3)$ had order 24. Then demonstrate that there cannot be a one-to-one correspondence that suports the operations

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.]

Given any A of interest it will have the form $\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}$ and the fact that $adf \neq 0$. Thus, $a, d, f \in \{1\}$ and $b, c, e \in \{0, 1\}$.

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

Clearly, to include every inverse of $\frac{1}{p}$ would include all prime numbers as well, Multiplication of any two of these would be of the form $\frac{p}{q}$ where p, q are primes. Any multiplicative combination will describe any object $\frac{a}{b}$ where $a, b \in \mathbb{Z}$.

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.

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

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

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

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 subgoup 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.

    $D_{2n} = \{r, s \mid r^n = s^2 = 1, rs = sr^{-1}\}$ The set of rotations are $H = \{1, r, r^2, \ldots, r^{n-1}\}$. Suppose that there exits a subgroup K such that $H < K < D_{2n}$ then there must exist $y \in G$ and $y \notin K$. Let $x \in K$ and $x \notin H$. $x = sr^k$ for some k which means that $x^{-1} = sr^{n-k}$, further it implies $s \in K$ which extrapolates K to all of D_{2n}. Therefore, $K = D_{2n}$, hence H is maximal.

(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.
Let p be prime such that $p|n$ and k be such that $kp = n$. Since, $G = \langle\, x \,\rangle$ then $x^n = 1$ and

$$1 = x^n = x^{pk} = (x^p)^k \implies x^p = 1$$

Let $n = 100$ and $x = 12$ and $G = \langle\, 12 \,\rangle$ where all elements of G are less than or equal to 1200. $100 = 2 \cdot 2 \cdot 5 \cdot 5$ and $12^2 = 144$ and $\langle\, 144 \,\rangle$ is maximal under G. Notice that $\left\langle\, 12^{25} \,\right\rangle$ will have fewer elements in it than $\left\langle\, 12^5 \,\right\rangle$ and that that $\left\langle\, 12^{25} \,\right\rangle \subseteq \left\langle\, 12^5 \,\right\rangle$. Intuitively speaking, the largest proper subgroups of a cycle are those generted by x^p where p is a prime and $p|n$.

17. This is an exerecise involving Zorn's Lemma (see Appendix I) to prove that every nontrival finitely generated group possesses maximal subgroups. Let G be a finitely generated group, say $G = \langle\, g_1, g_2, \ldots, g_n \,\rangle$, 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.

    (b) Prove that H is *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 defintiion of a chain to arrive at a contradiction.]

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

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

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

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

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

    (d) $\mathbb{Z}$ is not finitely generated.

19. A nontrivial abelian group A (wrtiten 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 in A).

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

    (b) Prove that 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.

2.5 The Lattice of Subgroups of a Group

Chapter 3

Quotient Groups and Homomorphisms

3.1 Definitions and Examples

Definition 3.1.1 (Kernel)**.** If φ is a homomorphism $\varphi : G \to H$, the ***kernel*** of φ is the set

$$\ker(\varphi) \equiv \{g \in G \,|\, \varphi(g) = 1\}$$

and will be denonted $\ker \varphi$ (here 1 is the identity of H).

Proposition 3.1.2. Let G and H be groups and let $\varphi : G \to H$ be a homomorphism.

1. $\varphi(1_G) = 1_H$, where 1_G and 1_H are the identities of G and H, respectively.
2. $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.
3. $\varphi(g^n) = \varphi(g)^n$ for all $n \in \mathbb{Z}$.
4. $\ker \varphi$ is a subgroup of G.
5. $\operatorname{Im} \varphi$, the image of G under φ, is a subgroup of H.

Definition 3.1.3 (Quotient Group or Factor Group)**.** Let $\varphi : G \to H$ be a homomorphism with the kernel K. The ***quotient group or factor group***, G/K (read G *modulo* K or simply $G \bmod K$) is the group whose elements are the fibers of φ with group operation defined above; namely if X is the fiber above a and Y is the fiber above b then the product X with Y defined to be the fiber above the product ab.

Proposition 3.1.4. Let $\varphi : G \to H$ be a homomorphism of groups with kernel K. Let $X \in G/K$ be the fiber above a, i.e., $X = \varphi^{-1}(a)$. Then

1. For any $u \in X$. $X = \{uk \,|\, k \in K\}$
2. For any $u \in X$. $X = \{ku \,|\, k \in K\}$

Definition 3.1.5 (Coset)**.** For any $N \leq G$ and any $g \in G$ let

$$gN = \{gn \,|\, n \in N\} \text{ and } Ng = \{ng \,|\, n \in N\}$$

called respectively a ***left coset*** and a ***a right coset*** of N in G. Any element of a coset is called a ***representative*** for the coset.
Note: **cosets** are another name for **fibers** without needing to define a homomorphism. It will later be shown that given a set of cosets to a subgroup, there will exist a homomorphism that defines them as fibers Proposition 3.1.11.

Theorem 3.1.6. *Let G be group and let K be the kernel of some homomorphism from G to another group. Then the set whose elements are the left cosets of K in G with operation defined by*

$$uK \circ vK = (uv)K$$

forms a group, G/K. In particular, this operation is well defined in the sense that if u_1 is any element in uK and v_1 is any element in vK, then $u_1v_1 \in uvK$, i.e.,e $u_1v_1K = uvK$ so that the multiplication does not depend on the choice of representatives for the cosets. The same statement is true with "right cosets" in place of "left cosets".

Proposition 3.1.7. Let N be any subgroup of the group G. The set of left cosets of N in G form a partition of G. Furthermore, for all $u, v \in G, uN = vN$ if and only if $v^{-1}u \in N$ and in particular, $uN = vN$ if and only if u and v are representatives of the same coset.

Proposition 3.1.8. Let G be a group and let N be a subgroup of G.

1. The operation on the set of left cosets of N in G described by
$$uN \cdot vN = (uv)N$$
is well defined if and only if $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$.

2. If the above operation is well defined, then it makes the set of left cosets of N in G into a group. In particular the identiy of this group is the coset $1N$ and the inverse of gN is the coset $g^{-1}N$ i.e, $(gN)^{-1} = g^{-1}N$.

Definition 3.1.9 (Conjugate, Normal, Normalize)**.** The element gng^{-1} is called the ***conjugate*** of $n \in N$ by g. The element g is said to ***normalize*** N if $gNg^{-1} = N$. A subgroup N of a group G is called ***normal*** if every element of G normalizes N, i.e., if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G we shall write $N \trianglelefteq G$

Theorem 3.1.10. *Let N be a subgroup of the group G. The following are equivalent:*

1. $N \trianglelefteq G$
2. $N_G(N) = G$ *(recall $N_G(N)$ is the normalizer of G of N)*
3. $gN = Ng$ *for all* $g \in G$
4. *the operation on left cosets of N in G described in previous proposition makes the set of left cosets into a group*
5. $gNg^{-1} \subseteq N$ *for all* $g \in G$.

Proposition 3.1.11. A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.

Definition 3.1.12. Let $N \trianglelefteq G$. The homomorphism $\pi : G \to G/N$ defined by $\pi(g) = gN$ is called ***natural projection (homomorphism)*** of G onto G/N. If $\overline{H} \leq G/N$ is a subgroup of G/N, the ***complete preimage*** of $\overline{H}$ in G is the preimage of $\overline{H}$ under the natural projection homomorphism.

3.1.1 Exercises

Let G and H be groups.

1. Let $\varphi : G \to H$ be a homomorphism and let E be a subgroup of H. Prove that $\varphi^{-1}(E) \leq G$ (i.e., the preimage or pullback of a subgroup under a homomorphism is a subgroup). If $E \trianglelefteq H$ prove that $\varphi^{-1}(E) \trianglelefteq G$. Deduce that $\ker\varphi \trianglelefteq G$.

   Given $a, b \in E$ and let $x, y \in G$ such that $\varphi(x) = a, \varphi(y) = b$, hence $x, y \in \varphi^{-1}(E)$. Since E is a group $ab \in E$. Thus, $\varphi(x)\varphi(y) = ab$ and $\varphi(xy) \in E$ because φ is a homomorphism. Thus, $xy \in \varphi^{-1}(E)$
   $E \trianglelefteq H$ means that $hah^{-1} = a$ for all $h \in H$. Hence, $\varphi^{-1}(a) = \varphi^{-1}(hah^{-1}) = \varphi^{-1}(h)\varphi^{-1}(a)\varphi^{-1}(h^{-1})$ for all $h \in H$ hence $\varphi^{-1}(E) \trianglelefteq G$.

2. Let $\varphi : G \to H$ be a homomorphism of groups with kernel K and let $a, b \in \varphi(G)$. Let $X \in G/K$ be the fiber above a and let Y be the fiber above b, i.e., $X = \varphi^{-1}(a), Y = \varphi^{-1}(b)$. Fix an element u of X (so $\varphi(u) = a$). Prove that if $XY = Z$ in the quotient group G/K and w is any member of Z, then there is some $v \in Y$ such that $uv = w$. [Show $u^{-1}w \in Y$.]

   Let $u \in X$ and $v \in Y$. Since $XY = Z \in G/K$ and $w \in Z$. Now, $\varphi(uv) = \varphi(u)\varphi(v) = ab$ and $\varphi(w) = ab$ therefore $\varphi(w) = \varphi(u)\varphi(v)$ and hence $\varphi(u)^{-1}\varphi(w) = \varphi(v)$ and $u^{-1}w = v \in Y$.

3. Let A be an abelian group and let B be a subgroup of A. Prove that A/B is abelian. Give an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.

4. Prove that in the quotient group G/N, $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.

   Inductive proof: notice that $(gN)^2 = gNgN = ggNN = g^2N$

5. Use the preceding exercise to prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $g^n \in N$ (and gN is infinite order if no such positive integer exists). Give an example to show that the order of gN in G/N may be strictly smaller than the order of g in G.

   Notice that in $G = \mathbb{Z}/84\mathbb{Z}$ we choose the subgroup $N = \mathbb{Z}/21\mathbb{Z}$. Given any number, say 6, then $6N = \{0, 126, 252, 378\} = \{0, 21, 42, 63\} = \{0, 42, 0, 42\}$ hence, of order 2.
   84, 168, 252, 336

6. Define $\varphi : \mathbb{R}^\times \to \{\pm 1\}$ by letting $\varphi(x)$ be x divided by the absolute value of x. Describe the fibers of φ and prove that φ is a homomorphism.

$$\begin{aligned}\varphi(x) &= \frac{x}{|x|}\\ &= \begin{cases} 1 : x = |x| \\ -1 : -x = |x| \end{cases}\\ &\text{and}\\ \varphi(xy) &= \frac{x}{|x|}\frac{y}{|y|} = \frac{xy}{|x||y|} = \frac{xy}{|xy|}\end{aligned}$$

which is true for all $x, y \in \mathbb{R}^{\times}$ and there are two fibers, those less than zero and those greater than zero.

7. Define $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\pi((x, y)) = x + y$. Prove that π is a surjective homomorphism and describe the kernel and fibers of π geometrically.

   It is surjective because any real number is the sum of two other real numbers. The kernel is $x + y = 1$ which is a line through the point (0,-1) at a 135°. The fibers are all lines 135° to the x-axis.

8. Let $\varphi : \mathbb{R}^{\times} \to \mathbb{R}^{\times}$ be the map sending x to the absolute value of x. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ.

$$\begin{aligned}\varphi : \mathbb{R}^{\times} &\to \mathbb{R}^{\times}\\ x &\mapsto |x|\end{aligned}$$

$$\varphi(xy) = |xy| = |x||y| = \varphi(x)\varphi(y)\, \forall x, y \in \mathbb{R}^{\times}$$

   The kernel is the graph the line of 45° from the origin to the upper left and the graph of the line 45° from the origin to the upper right. The fibers are the set of numbers and their negative. That is $\{(x, -x) \,|\, x \in \mathbb{R}^{\times}\}$

9. Define $\varphi : \mathbb{C}^{\times} \to \mathbb{R}^{\times}$ by $\varphi(a + bi) = a^2 + b^2$. Prove that φ is a homomorphism and find the image of φ. Describe the kernel and the fibers of φ geometrically (as subsets of the plane).

$$\begin{aligned}\varphi : \mathbb{C}^{\times} &\to \$^{\times}\\ a + bi &\mapsto a^2 + b^2\end{aligned}$$

$$\begin{aligned}\varphi((a + bi)(c + di)) &= \varphi(ac - bd + i(bc + ad))\\ &= (ac - bd)^2 + (bc + ad)^2\end{aligned}$$

10. Let $\varphi : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ by $\varphi(\overline{a})$. Show that this is a well defined, surjective homomorphism and describe its fibers and kernel explicitly (showing that φ is well defined involves the fact that $\overline{a}$ has a different meaning in the domain and range of φ).

    $\ker\varphi = \{g \in \mathbb{Z}/8\mathbb{Z} : \varphi(g) =\} = \{\overline{1}, \overline{4}\}$.

11. Let F be a field and let $G = \left\{ \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \middle| \; a, b, c \in F, ac \neq 0 \right\} \leq GL_2(F)$.

    (a) Prove that the map $\varphi : \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \mapsto a$ is a surjective homomorphism from G onto $F^{\times}$(recall that $F^{\times}$ is the multiplictive group of nonzero elements in F). Describe the fibers and kernel of φ.

    (b) Prove that the map $\psi : \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \mapsto (a, c)$ is a surjective homomorphism from G onto $F^{\times} \times F^{\times}$. Describe the fibers and kernel of ψ.

    (c) Let $H = \left\{ \left(\begin{array}{cc} 1 & b \\ 0 & 1 \end{array} \right) \middle| \; b \in F \right\}$. Prove that H is isomorphic to the additive group F.

12. Let G be the additive group in real numbers, let H be the multiplicative group of complex numbers of absolute value 1 (the unit circle S^1 in the complex plane) and let $\varphi : G \to H$ be the homomorphism $\varphi : r \mapsto e^{2\pi i r}$. draw the points on a real line which lie in the kernel of φ. Describe similarly the elements in the fibers of φ above the point -1,i, and $e^{4\pi i/3}$ of H. Figure 1 of the text for this homomorphism φ is usually depicted using the following diagram [See Fig. 5 on page 84(99)].

What maps to 1 in φ? Hence,

$$\begin{aligned} &1 = e^{2\pi i r} \implies 2\pi i r \in \{0, 2\pi, 4\pi, \dots\} \\ &r \in \{0, 1, 2, \dots\} = \mathbb{N} \end{aligned}$$

13. Repeat the preceding exercise with the map φ replaced by the map $\varphi : r \mapsto e^{4\pi i r}$.

14. Consider the additive quotient group $\mathbb{Q}/\mathbb{Z}$.

   (a) Show that every coset of $\mathbb{Z}$ in $\mathbb{Q}$ contains exactly one representative $q \in \mathbb{Q}$ in the range $0 \leq q < 1$.
   Given any $q \in Q$ then the left-coset $q + \mathbb{Z} = \{\dots, q-2, q-1, q, q+1, q+2, \dots\}$. Let $x, y \in q + \mathbb{Z}$ and $0 \leq x, y < 1$. There there exists $a, b \in \mathbb{Z}$ such that $x = q + a, y = q + b$. Notice that $x - y = q + a - (q + b) = a - b$. $a - b$ must be an integer and if $a - b \geq 1$ then $x - y \geq 1$ and hence one of them is not in the range $[0, 1)$. Therefore, $a - b = 0$ and $x = y$.

   (b) Show that every element of $\mathbb{Q}/\mathbb{Z}$ has finite order but that there are elements of arbitrarily larger order.
   The identity of $\mathbb{Q}/\mathbb{Z}$ is $\mathbb{Z}$. Notice that $\frac{1}{2}\mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ and that $\left|\frac{1}{2}\mathbb{Z}\right| = 2$. In fact, in general, for every $n \in \mathbb{Z}, \left|\frac{1}{n}\mathbb{Z}\right| = n$. Notice further that for any $n, m \in \mathbb{Z}, \left|\frac{m}{n}\mathbb{Z}\right| = n$. Thus, any $q \in \mathbb{Q}$ can be defined as $q = \frac{m}{n}$ an hence $|q\mathbb{Z}| = n$ and finite, yet, arbitrarily large.

   (c) Show that $\mathbb{Q}/\mathbb{Z}$ is the torsion subgroup of $\mathbb{R}/\mathbb{Z}$ (cf. Exercise 6, Section 2.1).
   A torsion subgroup is $\{g \in G \mid |g| < \infty\}$. The question is, does $\mathbb{Q}/\mathbb{Z}$ contain ALL finite order elements of $\mathbb{R}/\mathbb{Z}$?

   (d) Prove that $\mathbb{Q}/\mathbb{Z}$ is ismorphic to the multiplicative group of root of unity in $\mathbb{C}^\times$.

   $$\text{WTS } \mathbb{Q}/\mathbb{Z} \cong \mathbb{C}^\times, \exists \varphi : \mathbb{Q}/\mathbb{Z} \to \mathbb{C}^\times \implies \varphi(q) = z, |z| = 1$$

   and φ is surjective and injective.

   $$\text{Let } \varphi(m/n) = e^{2\pi i m/n}$$

   need to show it is 1-to-1 and onto.

15. Prove that a quotient of a divisilbe abelian group by any proper subgroup is also divisible. Deduce that $\mathbb{Q}/\mathbb{Z}$ is divisible(cf Exercise 19, Section 2.4).

16. Let G be a group, let N be a normal subgroup of G and let $\overline{G} = \langle \overline{x}, \overline{y} \rangle$. Prove more generally that if $G = \langle S \rangle$ for any subset S of G, then $\overline{G} = \langle \overline{S} \rangle$.

17. Let G be the dihedral grup of order 16 (whose lattice appears in Section 2.5):

   $$G = \langle r, s \mid r^8 = s^2 = 1, rs = sr^{-1} \rangle$$

   and let $\overline{G} = G/\langle r^4 \rangle$ be the quotient of G by the subgroup generated by r^4 (this subgroup is the center of G, hence is normal)

   (a) Show that the order of $\overline{G}$ is 8.
   $\overline{1} = \langle r^4 \rangle = (1, r^4) = r^4 \langle r^4 \rangle = \overline{r^4}$ is the kernel
   $\overline{r} = r \langle r^4 \rangle = (r, r^5) = r^5 \langle r^4 \rangle = \overline{r^5}$
   $\overline{r^2} = r^2 \langle r^4 \rangle = (r^2, r^6) = r^g \langle r^4 \rangle = \overline{r^6}$
   $\overline{r^3} = r^3 \langle r^4 \rangle = (r^3, r^7) = r^7 \langle r^4 \rangle = \overline{r^7}$
   each of these can be multiplied by s giving 4 more.

   (b) Exhibit each element in $\overline{G}$ in the form $\overline{s}^a \overline{r}^b$, for some integers a and b.

   (c) Find the order of each of the elements of $\overline{G}$ exhibited in (b)

   (d) Write each of the following elements of $\overline{G}$ in the form $\overline{s}^a \overline{r}^b$ and b as in (b): $\overline{rs}, \overline{sr^{-2}s}, \overline{s^{-1}r^{-1}sr}$.

   (e) Prove that $\overline{H} = \langle \overline{s}, \overline{r}^2 \rangle$ is a normal subgroup of $\overline{G}$ and$\overline{H}$ is isomorphic to the Klein 4-group. Describe the isomorphism type of the complete preimage of $\overline{H}$ in G.

   (f) Find the center of $\overline{G}$ and describe the isomorphism type of $\overline{G}/Z(\overline{G})$.

18. Let G be a quasidihedral group of order 16 (whose lattice was computed in Exercise 11 of Section 2.5)

   $$G = \{ \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \}$$

   and let $\overline{G} = G/\langle \sigma^4 \rangle$ be the quotient of G by the subgroup generated by σ^4 (this subgroup is the center of G, hence is normal).

(a) Show that the order of $\overline{G}$ is 8.

(b) Exhibit each element of $\overline{G}$ in the form $\overline{\tau}^a, \overline{\sigma}^b$, for some integers a and b.

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

(d) Write each of the following elements of $\overline{G}$ in the form $\overline{\tau}^a, \overline{\sigma}^b$, for some integers a and$b$ as in (b): $\overline{\sigma\tau}, \overline{\tau\sigma^{-2}\tau}, \overline{\tau^{-1}\sigma^{-1}\tau\sigma}$.

(e) Prove that $\overline{G} \cong D^8$.

19. Let G be the modular group of order 16 (whose lattice was computed in Exercise 14 of Section 2.5)

$$G = \{\ u, v \mid u^2 = v^8 = 1, vu = uv^5\ \}$$

and let $\overline{G} = G/\langle\, v^4 \,\rangle$ be the quotient of G by the subgroup generated by v^4 (this subgroup is contained in the center of G, hence is normal).

(a) Show that the order of $\overline{G}$ is 8.

(b) Exhibit each element of $\overline{G}$ in the form $\overline{u}^a, \overline{v}^b$, for some integers a and b.

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

(d) Write each of the following elements of $\overline{G}$ in the form $\overline{u}^a, \overline{v}^b$, for some integers a and$b$ as in (b): $\overline{uv}, \overline{uv^{-2}u}, \overline{u^{-1}v^{-1}uv}$.

(e) Prove that $\overline{G} \cong \mathbb{Z}_2 \times \mathbb{Z}^4$.

20. Let $G = \mathbb{Z}/24\mathbb{Z}$ and let $\tilde{G} = G/\langle\, 12 \,\rangle$, where for each integer a we simplify notation by writing $\tilde{\bar{a}}$ as $\tilde{a}$.

(a) Show that $\tilde{G} = \{\tilde{0}, \tilde{1}, \ldots, \tilde{11}\}$.

(b) Find the order of each element of $\tilde{G}$.

(c) Prove that $\tilde{G} \cong \mathbb{Z}/12\mathbb{Z}$. (Thus $(\mathbb{Z}/24\mathbb{Z})/(12\mathbb{Z}/24\mathbb{Z}) \cong \mathbb{Z}/12\mathbb{Z}$, just as if we inverted and cancelled the 24$\mathbb{Z}$'s.)

21. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ be given in terms of the following generators and relations:

$$G = \langle\, x, y \mid x^4 = y^4 = 1, xy = yx \,\rangle$$

Let $\overline{G} = G/\langle\, x^2y^2 \,\rangle$ (note that every subgroup of the abelian group G is normal).

(a) Show that the order of $\overline{G}$ is 8.

(b) Exhibit each element of $\overline{G}$ in the form $\overline{x}^a, \overline{y}^b$, for some integers a and b.

(c) Find the order of each of the elements of $\overline{G}$ exhibited in (b).

(d) Prove that $\overline{G} \cong \mathbb{Z}_4 \times \mathbb{Z}^2$.

22. (a) Prove that if H and K are nomal subgroups of a group G then their intersection $H \cap K$ is also a normal subgroup of G.

Let $x \in H \cap K$ then $xg = gx$ for all $g \in G$ because $x \in H$ as well as because $x \in K$. Hence, $H \cap K \trianglelefteq G$.

(b) Prove that the intersection of an arbitrary nonempty collection of normal subgroups of a group is a normal subgroup (do not assume the collection is countable).

23. Prove that the join (cf. Section 2.5) of any nonempty collection of normal subgroups of a group is a normal subgroup.

24. Prove that if $N \trianglelefteq G$ and H is any subgroup of G then $N \cap H \trianglelefteq H$.

Given $x \in N \cap H$. Then, $xg = gx$ for all $g \in G$. If $h \in H$ then we know that $xh = hx$, hence

25. (a) Prove that a subgroup N of G is normal if and only if $gNg^{-1} \subseteq N$ for *all* $g \in G$.

(b) Let $G = GL_2(\mathbb{Q})$, let N be the subgroup of upper triangular matrices with integer entries and 1's on the digonal, and let g be the diagonal matrix with entries 2,1. Show that $gNg^{-1} \subseteq N$ but g does *not* normalize N.

26. Let $a, b \in G$.

(a) Prove that the conjugate of the product of a and b is the product of the conjugate of a and the conugate of b. Prove that the order of a and that the order of any conjugate of a are the same.

The conjugate of ab is $gabg^{-1}$ for some $g \in G$. Notice that $gag^{-1}gbg^{-1} = gabg^{-1}$.
Let $|a| = n$ then $a^n = 1. \rightarrow (gag^{-1})^n = gag^{-1} \cdot gag^{-1} \cdot gag^{-1} \cdots gag^{-1} = ga \cdot a \cdot a \cdots ag^{-1} = ga^n g^{-1} = gg^{-1} = 1$

(b) Prove that the conjugate of a^{-1} is inverse of the conjugate of a.

$(gag^{-1})^{-1} = g^{-1}a^{-1}g$

(c) Let $N = \langle\, S \,\rangle$ for some subset S of G. Prove that $N \trianglelefteq G$ if $gSg^{-1} \subseteq N$ for all $g \in G$.

(d) Deduce that if N is cyclic group $\langle\, x \,\rangle$ then N is normal in G if and only if for each $g \in G, gxg^{-1} = x^k$ for some $k \in \mathbb{Z}$.

(e) Let n be a positive integer. Prove that the subgroup N of G generated by all the elements of G of order n is a normal subgroup of G.

27. Let N be a *finite* subgroup of a group G. Show that $gNg^{-1} \subseteq N$ if and only if $gNg^{-1} = N$. Deduce that $N_G(N) = \{\, g \in G \mid gNg^{-1} \subseteq N \,\}$.

28. Let N be a *finite* subgroup of a group G and assume $N = \langle\, S \,\rangle$ for some subset S of G. Prove that an element $g \in G$ normalizes N if and only if $gSg^{-1} \subseteq N$.

29. Let N be a *finite* subgroup of G and suppose $G = \langle\, T \,\rangle$ and $N = \langle\, S \,\rangle$ from some subsets S and T of G. Prove that N is normal in G if and only if $tSt^{-1} \subseteq N$ for all $t \in T$.

30. Let $N \leq G$ and let $g \in G$. Prove that $gN = Ng$ if and only if $g \in N_G(N)$.

31. Prove that if $H \leq G$ and N is a normal subgroup of H then $H \leq N_G(N)$. Deduce that $N_G(N)$ is the largest subgroup of G in which N is normal (i.e., is the join of all subgroups H for which $N \trianglelefteq H$).

32. Prove that every subgroup of Q_8 is normal. For each subgroup find the isomorphism type of its corresponding quotient. [You may use the lattice of subgroups for Q_8 in Section 2.5]

33. Find all normal subgroups of D_8 and for each of these find the isomorphism type of its corresponding quotient. [You may use the lattice of subgroups for D_8 in Section 2.5.]

34. Let $D_{2n} = \left\langle\, r, s \mid r^n = s^2 = 1, rs = sr^{-1} \,\right\rangle$ be the usual presentation of the dihedreal group of order $2n$ and let k be a positive integer dividing n.

    (a) Prove that $\left\langle\, r^k \,\right\rangle$ is a normal subgroup of D_{2n}.

    (b) Prove that $D_{2n}/\left\langle\, r^k \,\right\rangle \cong D_{2k}$

35. Prove that $SL_n(F) \trianglelefteq GL_n(F)$ and describe the isormophism type of the quotient group (cf. Exercise 9, Section 2.1).

36. Prove that if $G/Z(G)$ is cyclic then G is abelian. [If $G/Z(G)$ is cyclic with generator $xZ(G)$, show that every element of G can be written in the from $x^a z$ for some integer $a \in \mathbb{Z}$ and some element $z \in Z(G)$.]

37. Let A and B be groups. Show that $\{(a, 1) \mid a \in A\}$ is a normal subgroup of $A \times B$ and the quotient of $A \times B$ by this subgroup is isomorphic to B.

38. Let A be an abelian group and let D be the (diagonal) subgroup $\{(a, a) \mid a \in A\}$ of $A \times A$. Prove that D is a normal subgroup of $A \times A$ and $(A \times A)/D \cong A$.

39. Suppose A is the non-abelian group S_3 and D is the diagonal subgroup $\{(a, a) \mid a \in A\}$ of $A \times A$. Prove that D is not normal in $A \times A$.

40. Let G be a group, let N be a normal subgroup of G and let $\overline{G} = G/N$. Prove that $\overline{x}$ and $\overline{y}$ commute in $\overline{G}$ if and only if $x^{-1}y^{-1}xy \in N$. (The element $x^{-1}y^{-1}xy$ is called the *commutator* of x and y and is denoted by $[x, y]$.)

41. Let G be a group. Prove that $N = \left\langle\, x^{-1}y^{-1}xy \mid x, y \in G \,\right\rangle$ is a normal subgroup of G and G/N is abelian (N is called the *commutator subgroup* of G).

42. Assume both H and K are normal subgroups of G with $H \cap K = 1$. Prove that $xy = yx$ for all $x \in H$ and $y \in K$. [Show that $x^{-1}y^{-1}xy \in H \cap K$.]

43. Assume $\mathcal{P} = \{A_i \mid i \in I\}$ is any partition of G with property that $\mathcal{P}$ is a group under the "quotient operation" defined as follows: to compute the product of A_i with A_j take any element a_i of A_i and any element a_j of A_j and let A_iA_j be the element $\mathcal{P}$ containing a_ia_j (this operation is assumed to be well defind). Prove that the element of $\mathcal{P}$ that contains the identity of G is a normal subgroup of G and the elements of $\mathcal{P}$ are the cosets of this subgroup (so $\mathcal{P}$ is just a quotient group of G in the usual sense).

3.2 More on Cosets and Lagrange's Theorem

Theorem 3.2.1 (Lagrange's Theorem). *If G s a finite group and H is a subgroup of G, then the order of H divides the order of G (i.e., $|H| \mid |G|$) and the number of left cosets of H in G equals $\frac{|G|}{|H|}$.*

Remark 3.2.2. The *full converse* of Lagrange's Theorem is *not* true: namely, if G is a finite group and n divides $|G|$, then G need not have a subgroup of order n.

Definition 3.2.3. If G is a group (possibly infinite) and $H \leq G$, the number of left cosets of H in G is called the *index* of H in G and is denoted by $|G : H|$.

Corollary 3.2.3.1. *If G is a finite group and $x \in G$, then the order of x divides the order of G. In particular $x^{|G|} = 1$ for all x in G.*

Corollary 3.2.3.2. *If G is a group of prime order p, then G is cyclic, hence $G \cong \mathbb{Z}_p$.*

Theorem 3.2.4 (Cauchy's Theorem)**.** *If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.*

Theorem 3.2.5 (Sylow)**.** *If G is a finite group of order $p^\alpha m$, where p is prime and p does not divide m, then G has a subgroup of order p^α.*

Definition 3.2.6. Let H and K be subgroups of a group and define

$$H\,K = \{hk \,|\, h \in H, k \in K\}$$

Proposition 3.2.7. If H and K are finite subgroups of a group then

$$|H\,K| = \frac{|H||K|}{|H \cap K|}$$

Note:

$$H\,K = \bigcup_{h \in H} h\,K$$

Proposition 3.2.8. If H and K are subgroups of a group, $H\,K$ is a subgroup if and only if $H\,K = K\,H$

Definition 3.2.9. If A is any set of $N_G(K)$ (or $C_G(K)$), we shall say A *normalizes* K (*centralizes* K, respectively).[1]

3.2.1 Exercises

Let G be a group.

1. Which of the following are permissible orders for subgroups of a group of order 120: 1,2,5,7,9,15,60,240? For each permissible order give the corresponding index.

   1, 2, 5 are all prime and divide 120. These are permissilble.
   7,9 do not divide 120 so they are not permissible.
   The order of a subgroup can't be bigger than the group so 240 is not permissible.
   60 has an index of 2, therefore it is permissible.
   Is 15 a permissible order of a subgroup of 120?
   a group of order three is $H = (0,\ 40,\ 80)$ a subgroup of order 5 is $K = (0,\ 24,\ 48,\ 72,\ 96)$. Then we can see that $H \cap K = \{0\}$ and $|H \cap K| = 1$ therefore $|H\,K| = 15$ and is a subgroup.

2. Prove that the lattice of subgroups of S_3 in Section 2.5 is correct (i.e., prove that it contains all subgroups of S_3 and that their pairwise joins and intersections are correctly drawn).

3. Prove that the lattice of subgroups of Q_8 in Section 2.5 is correct.

4. Show that if $|G| = pq$ for some primes p and q (not necessarily distinct) then either G is abelian or $Z(G) = 1$. [See Exercise 36 in Section 1.]

   Since $|G| = pq$ we know that there exists a subgroup H such that $|H| = p$ and a subgroup K such that $|K| = q$. From this we can see that $H \cong \mathbb{Z}_p, K \cong \mathbb{Z}_q$. Then, for any $h \in H$ there exists an $n \in \mathbb{Z}$ such that $h = p^n$ and for any $k \in K$ there exists an $m \in \mathbb{Z}$ such that $k = q^m$. From the theorem, under what conditions are $h = k$? $p^n = q^m$ can only be true when $p = q$ or when $n = m = 0$ because each is prime. Thus, $\frac{|H||K|}{|H \cap K|} = \frac{pq}{pq} = 1$ or $\frac{pq}{1} = pq$ which implies that the group is abelian or $Z(G) = 1$.

5. Let H be a subgroup of G and fix some elements $g \in G$.

   (a) Prove that gHg^{-1} is a subgroup of G of the same order as H.

   Let $h_1, h_2 \in H$. Then $gh_1g^{-1}gh_2g^{-1} = gh_1h_2g^{-1} \in gHg^{-1}$. Therefore a group. Which implies that the order is the same. If H is unique than it commutes with all elements $g \in G$ and is therefore normal.

   (b) Deduce that if $n \in \mathbb{Z}^+$ and H is the unique subgroup of G of order n then $H \trianglelefteq G$.

6. Let $H \leq G$ and let $g \in G$. Prove that if the right coset Hg equals *some* left coset of H in G then it equals the left coset gH and g must be in $N_G(H)$.

[1] *centralize* means that each element commutes with every element in G. *normalize* means that each element in G will commute 'in some way' with elements in the normalized group.

7. Let $H \leq G$ and define a relation $\sim$ on G by $a \sim b$ if and only if $b^{-1}a \in H$. Prove that $\sim$ is an equivalence relation and describe the equivalence class of each $a \in G$. Use this to prove Proposition 4.

   We must show that $\sim$ is reflexive, symmetric and transitive.

   - Reflexive ($a \sim a$): $a \sim a \implies a^{-1}a = 1 \in H$. TRUE.
   - Symmetric ($a \sim b \iff b \sim a$): $a \sim b \implies b^{-1}a \in H$. Notice $(a \sim b)^{-1} = (b^{-1}a)^{-1} = a^{-1}b = b \sim a \in H$. TRUE
   - Transitive ($a \sim b, b \sim c \implies a \sim c$):

   $$\begin{aligned} a \sim b &\implies b^{-1}a \in H \\ b \sim c &\implies c^{-1}b \in H \\ (b \sim c)(a \sim b) &= (c^{-1}b)(b^{-1}a) = c^{-1}bb^{-1}a = c^{-1}a = c \sim a \in H \end{aligned}$$

   and since $\sim$ is symmetric $a \sim c \in H$. TRUE.

8. Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.

   From this we can see that $H \cong \mathbb{Z}_p, K \cong \mathbb{Z}_q$. Then, for any $h \in H$ there exists an $n \in \mathbb{Z}$ such that $h = p^n$ and for any $k \in K$ there exists an $m \in \mathbb{Z}$ such that $k = q^m$. From the theorem, under what conditions are $h = k$? $p^n = q^m$ can only be true when $p = q$ or when $n = m = 0$ because each is prime. Thus, $\frac{|H||K|}{|H \cap K|} = \frac{pq}{pq} = 1$.

9. This exercise outlines a proof of Cauchy's Theorem due to James McKay (*Another proof of Cauchy's group theorem* Amer. Math. monthly, 66(1959), p. 119). Let G be a finite group and let p be a prime dividing $|G|$. Let $\mathcal{S}$ denote the set of p-tuples of elements of G the product of whose coordinates is 1:

   $$\mathcal{S} = \{(x_1, x_2, \ldots, x_p) \,|\, x_i \in G \text{ and } x_1x_2\cdots x_p = 1\}$$

   (a) Show that $\mathcal{S}$ has $|G|^{p-1}$ elements, hence has order divisible by p.[2]

   (b) Show that a cyclic permutation of an element of $\mathcal{S}$ is again an element of $\mathcal{S}$.

   (c) Prove that *sim* is an equivalence relation on $\mathcal{S}$.

   (d) Prove that an equivalence class contains a single element if and only if it is of the form $(x, x, \ldots, x)$ with $x^p = 1$.

   (e) Prove that every equivalence class has order 1 or p (this uses the fact that p is a *prime*). Deduce that $|G|^{p-1} = k + pd$, where k is the number of classes of sie 1 and d is the number of classees of size p.

   (f) Since $\{(1, 1, \ldots, 1)\}$ is an equivalence class of size 1, conclude that from (e) that there must be a nonidentity element x in G with $x^p = 1$, i.e., G contains an element of order p. [Show $p \,|\, k$ and so $k > 1$.]

10. Suppose H and K are subgroups of finite index in the (possibly infinite) group of G with $|G : H| = m$ and $|G : K| = n$. Prove that $\operatorname{lcm}(m, n) \leq |G : H \cap K| \leq mn$. Deduce that if m and n are relatively prime then $|G : H \cap K| = |G : H| \cdot |G : K|$.

    (this is a start) From Lagrange's Theorem we have, at least for finite groups, we have

    $$\begin{aligned} m = |G : H| &= \frac{|G|}{|H|} \\ n = |G : K| &= \frac{|G|}{|K|} \\ mn &= \frac{|G|}{|H|} \cdot \frac{|G|}{|K|} \\ |G : H \cap K| &= \frac{|G|}{|H \cap K|} \leq \frac{|G|}{|H|} \text{ and } \frac{|G|}{|K|} \end{aligned}$$

    $|H \cap K|$ must divide $|G|$ and $|H \cap K|$ must divide both $|H|$ and $|K|$ therefore $\operatorname{lcm}(|H|, |K|) \leq |G : H \cap K|$

11. $H \leq K \leq G$. Prove that $|G : H| = |G : K| \cdot |K : H|$ (do not assume G is finite).

    $$\begin{aligned} |G : H| = \frac{|G|}{|H|}, |G : K| &= \frac{|G|}{|K|} \text{ and } |K : H| = \frac{|K|}{|H|} \\ |G| &= |G : H||H| = |G : K||K| \text{ and } |K : H||H| = |K| \\ |G : H||H| &= |G : K||K : H||H| \\ |G : H| &= |G : K||K : H| \end{aligned}$$

[2] Define the relation $\sim$ on $\mathcal{S}$ by letting $\alpha \sim \beta$ if β is a cyclic permutation of α.

12. Let $H \leq G$. Prove that the map $x \mapsto x^{-1}$ sends each left coset of H in G onto a right coset of H and gives a bijection between the set of left coset and the set of right cosets of H in G (hence the number of left cosets of H in G equals the number of right cosets).

    Let $\varphi : G \to G$ such that $\varphi(x) = x^{-1}$. Then, let $K \in G/H$ and any coset gK implies that $\varphi(gk) = (gk)^{-1} = k^{-1}g^{-1}$. Which is clearly a bijection with right cosets on the right of the equation. This indicates that the number of left cosets equals the number of right cosets.

13. Fix any labelling of the vertices of a square and use this to identify D_8 as a subgroup o S_4. Prove that the elements of D_8 and $\langle (\; 1 \quad 2 \quad 3 \;) \rangle$ do not commute in S_4.

14. Prove that S_4 does not have a normal subgroup of order 8 or a normal subgroup of order 3.

15. Let $G = S_n$ and for fixed $i \in \{1, 2, \ldots, n\}$ let G_i be the stabilizer of i. Prove that $G_i \cong S_{n-1}$.

    The stablizer is defined as $G_s = \{g \in G \,|\, g \cdot s = s\}$. Where $\cdot$ is the composition operation. Thus, s would be any element of S_n with s in it.

16. Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove *Fermat's Little Theorem*: if p is a prime then $a^p \equiv a (\operatorname{mod} p)$ for all $a \in \mathbb{Z}$

    Let $G = \mathbb{Z}/n\mathbb{Z}$ for some $n \in Z^+$. Let $x \in G$ and we know that $|x| \,|\, n$. WTOG, we can select x such that $|x| = p$ where p is prime. Therefore $x^p \equiv x \bmod n$. If n is prime then p can be either 1 or n and since x is arbitrary this is true for all $x \in G$.

17. Let p be a prime and let n be a positive integer. Find the order of $\overline{p}$ in $(\mathbb{Z}/(p^n - 1)\mathbb{Z})^\times$ and deduce that $n \,|\, \varphi - 1$ (her φ is Euler's function).

18. Let G be a finite group, let H be a subgroup of G and let $N \trianglelefteq G$. Prove that if $|H|$ and $|G : N|$ are relatively prime then $H \leq N$.

19. Prove that if N is a normal subgroup of the finite group G and $(|N|, |G : N|) = 1$ then N is the unique subgroup of G of order $|N|$.

20. If A is an abelian group with $A \trianglelefteq G$ and B is any subgoup of G prove that $A \cap B \trianglelefteq AB$.

21. Prove that $\mathbb{Q}$ has no proper subgroups of finite index. Deduce that $\mathbb{Q}/\mathbb{Z}$ has no proper subgroups of finite index. [Recall Exercise 21, Section 1.6 and Exercise 15, Section 1.]

22. Use Lagrange's Theorem in the mutiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove *Euler's Theorem:* $a^{\varphi(n)} \equiv 1 \bmod n$ for every integer a relatively prime to n, where φ denotes Euler's φ-function.

23. Determine the last two digits of $3^{3^{100}}$. [Determine $3^{100} \bmod \varphi(100)$ and use the previous exercise.]

3.3 The Isomorphism Theorems

Theorem 3.3.1 (The First Isomorphsim Theorem). *if $\varphi : G \to H$ is a homomorphism of groups, then $\ker\varphi \trianglelefteq G$ and $G/\ker\varphi \cong \varphi(G)$.*

Corollary 3.3.1.1. *Let $\varphi : G \to H$ be a homomorphism of groups.*

1. *φ is injective if and only if $\ker\varphi = 1$.*

2. *$|G : \ker\varphi| = |\varphi(G)|$*

Theorem 3.3.2 (The Second or Diamond Isomorphism Theorem). *Let G be a group, let A and B be subgroups of G and assume $A \leq N_G(B)$. Then AB is a subgroup of G, $B \trianglelefteq AB, A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.*

Theorem 3.3.3 (The Third Isomorphism Theorem). *Let G be a group and let H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and*

$$(G/H)/(K/H) \cong G/K.$$

If we denote the quotient by H with a bar, this can be written

$$\overline{G}/\overline{K} \cong G/K.$$

Theorem 3.3.4 (The Fourth or Lattice Isomorphsm Theorem). *Let G be a group and let N be a normal subgroup of G. Then there is a bijectionfrom teh set of subgroups A of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N. In particular, every subgroup of $\overline{G}$is of the form A/N for som esubgroup A of G containing N (namely, its preimagein G under the natural projecton homomorphism from G to $/N$). This bijection has teh following properies: for all $A, B \leq G$ with $N \leq A$ and $N \leq B$,*

1. *$A \leq B$ if and only if $\overline{A} \leq \overline{B}$,*
2. *if $A \leq B$, then $|B : A| = |\overline{B} : \overline{A}|$.*
3. *$\overline{\langle A, B \rangle} = \langle \overline{A}, \overline{B} \rangle$,*
4. *$\overline{A \cap B} = \overline{A} \cap \overline{B}$, and*
5. *$A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$.*

3.3.1 Exercises

Let G be a group.

1. Let F be a finite field of order q and let $n \in \mathbb{Z}^+$. Prove that $|GL_n(F) : SL_n(F)| = q - 1$. [See Exercise 35, Section 1.]
2. Prove all parts of the Lattice Isomorphism Theorem.
3. Prove that if H is a normal subgroup of G of prime index p then for all $K \leq G$ either
   (a) $K \leq H$ or
   (b) $G = HK$ and $|K : K \cap H| = p$.
   First, according to the Diamond Isomorphism Theorem
   $$KH/H \cong K/(K \cap H)$$
   $$|KH/H| = |KH : H| = p$$
   $$|K : K \cap H| = \frac{|K|}{|K \cap H|}$$
4. Let C be a normal subgroup of the group A and let D be a normal subgroup of the group B. Prove that $(C \times D) \trianglelefteq (A \times B)$ and $(A \times B)/(C \times D) \cong (A/C) \times (B/D)$.
5. Let $QD_{16} = \langle \sigma, \tau \rangle$ be the quasidihedral group describe in Exercise 11 of Section 2.4. Prove that $\langle \sigma^4 \rangle$ is normal in QD_{16} and use the Lattice Isomorphism Theorem to draw the lattice of subgroups of $QD_{16}/\langle \sigma^4 \rangle$. Which group of order 8 has the same lattice as this quotient? Use generators and relations for $QD_{16}/\langle \sigma^4 \rangle$ to decide the isomorphism type of this group.
6. Let $M = \langle \mu, \nu \rangle$ be the modular group of order 16 escribe in Exercise 14 of Section 2.5. Prove that $\langle \nu^4 \rangle$ is normal in M and use the Lattice Isomorphism Theorem to draw the lattice of subgroups of $/\langle \nu^4 \rangle$. Which group of order 8 has the same lattice as this quotient? Use generators and relations for $\langle \nu^4 \rangle$ to decide the isomorphism type of this group.
7. Let M and N be normal subgroups of G such that $G = MN$. Pove that $G/M \cap N) \cong (G/M) \times (G/N)$.
8. Let p be a prime and let G be the grou pof p-power roots of 1 in $\mathbb{C}$ (cf. Exercise 18, Section 2.4). Prove that the map $z \mapsto z^p$ is a sujective homomorphism. Deduce that G is isomorphic to a proper quotient of itself.
9. Let p be a prime and let G be a group of order $p^a m$, where p does not divide m. Assume P is a subgroup of G of order p^a and N is a normal subgroup of G of order $p^b n$, where p does not divide n. Prove that $|P \cap N| = p^b$ and $|PN/N| = p^{a-b}$. (the subgroup P of G is called the *Sylow p-subgroup* of G. This exercise shows that the intersection of any Sylow p-subgroup of G with a normal subgroup N is a Sylow p-subgroup of N.)
10. Generealize the preceding exercise as follows. A subgroup H of a finite group G is called a *Hall subgroup* of G if its index in G is relatively prime to its order: $(|G : H|, |H|) = 1$. Prove that if H is a Hall subgroup of G and $N \trianglelefteq G$, then $H \cap N$ is a Hall subgroup of N and HN/N is a Hall subgroup of G/N.