Abstract Algebra I

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 341

Subsection 1

Basic Axioms and Examples

Binary Operations

Definition (Binary Operation, Associativity, Commutativity)

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

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

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

Examples of Binary Operations

(1) $+$ (usual addition) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$).

(2) $\times$ (usual multiplication) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$).

(3) $-$ (usual subtraction) is a noncommutative binary operation on $\mathbb{Z}$, where $-(a, b) = a - b$.
The map $a \mapsto -a$ is not a binary operation (not binary).

(4) $-$ is not a binary operation on $\mathbb{Z}^+$ (nor $\mathbb{Q}^+$, $\mathbb{R}^+$) because, for $a, b \in \mathbb{Z}^+$, with $a < b$, $a - b \notin \mathbb{Z}^+$, i.e., $-$ does not map $\mathbb{Z}^+ \times \mathbb{Z}^+$ into $\mathbb{Z}^+$.

(5) Taking the vector cross-product of two vectors in 3-space $\mathbb{R}^3$ is a binary operation which is not associative and not commutative.

Closure Under an Operation

- Suppose that $\star$ is a binary operation on a set G and H is a subset of G. If the restriction of $\star$ to H is a binary operation on H, i.e., for all $a, b \in H$, $a \star b \in H$, then H is said to be **closed under** $\star$

  Example: $-$ is a binary operation on $\mathbb{R}$. $\mathbb{Z}$ is a subset of $\mathbb{R}$. Clearly, $\mathbb{Z}$ is closed under $-$.

  $-$ is a binary operation on $\mathbb{R}$. $\mathbb{N}$ is a subset of $\mathbb{R}$. However, $\mathbb{N}$ is not closed under $-$.
- If $\star$ is an associative (respectively, commutative) binary operation on G and $\star$ restricted to some subset H of G is a binary operation on H, then $\star$ is automatically associative (respectively, commutative) on H as well.

Definition of Group

Definition (Group)

(1) A **group** is an ordered pair $(G, \star)$, where G is a set and $\star$ is a binary operation on G satisfying the following axioms:
   (i) $(a \star b) \star c = a \star (b \star c)$, for all $a, b, c \in G$, i.e., $\star$ is associative;
   (ii) There exists an element e in G, called an **identity** of G, such that, for all $a \in G$, we have $a \star e = e \star a = a$;
   (iii) For each $a \in G$, there is an element a^{-1} of G, called an **inverse** of a, such that $a \star a^{-1} = a^{-1} \star a = e$.

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

- We usually say G is a group under $\star$ if $(G, \star)$ is a group, or just G is a group when the operation $\star$ is clear from the context.
- Also, we say G is a **finite group** if, in addition, G is a finite set.
- Note that axiom (1)(ii) ensures that a group is always nonempty.

Examples of Groups

(1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are groups under $+$ with $e = 0$ and $a^{-1} = -a$, for all a.

(2) $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, $\mathbb{C} - \{0\}$, $\mathbb{Q}^+$, $\mathbb{R}^+$ are groups under $\times$, with $e = 1$ and $a^{-1} = \frac{1}{a}$, for all a.

Note that $\mathbb{Z} - \{0\}$ is not a group under $\times$ because, although $\times$ is an associative binary operation on $\mathbb{Z} - \{0\}$, the element 2 (for instance) does not have an inverse in $\mathbb{Z} - \{0\}$.

- For now, we take for granted the fact that the associative law holds in all these familiar examples.

(3) The axioms for a vector space V include those axioms which specify that $(V, +)$ is an abelian group (the operation $+$ is called **vector addition**). Thus any vector space, such as $\mathbb{R}^n$, is, in particular, an additive group.

Examples of Groups (Cont'd)

(4) For $n \in \mathbb{Z}^+$, $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under the operation $+$ of addition of residue classes. For now, we take the facts that $+$ is well defined and associative for granted. The identity in this group is the element $\overline{0}$ and for each $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, the inverse of $\overline{a}$ is $\overline{-a}$.
When we talk about the group $\mathbb{Z}/n\mathbb{Z}$ it will be understood that the group operation is addition of classes mod n.

(5) For $n \in \mathbb{Z}^+$, the set $(\mathbb{Z}/n\mathbb{Z})^\times$ of equivalence classes $\overline{a}$ which have multiplicative inverses mod n is an abelian group under multiplication of residue classes. For now, we take for granted that this operation is well defined and associative. The identity of this group is the element $\overline{1}$ and, by definition of $(\mathbb{Z}/n\mathbb{Z})^\times$, each element has a multiplicative inverse.
When we talk about the group $(\mathbb{Z}/n\mathbb{Z})^\times$, it will be understood that the group operation is multiplication of classes mod n.

Examples of Groups: Direct Products

(6) If $(A, \star)$ and $(B, \diamond)$ are groups, we can form a new group $A \times B$, called their **direct product**:

- Its elements are those in the Cartesian product

$$A \times B = \{(a, b) : a \in A, b \in B\};$$

- Its operation is defined componentwise:

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2).$$

Example: If we take $A = B = \mathbb{R}$ (both operations addition), $\mathbb{R} \times \mathbb{R}$ is the familiar Euclidean plane.

- The proof that the direct product of two groups is again a group is easy:
  - $(a_1, b_1)((a_2, b_2)(a_3, b_3)) = (a_1, b_1)(a_2 \star a_3, b_2 \diamond b_3) =$ $(a_1 \star (a_2 \star a_3), b_1 \diamond (b_2 \diamond b_3)) = ((a_1 \star a_2) \star a_3, (b_1 \diamond b_2) \diamond b_3) =$ $(a_1 \star a_2, b_1 \diamond b_2)(a_3, b_3) = ((a_1, b_1)(a_2, b_2))(a_3, b_3)$.
  - Identity of $A \times B$ is (e_A, e_B).
  - Inverse of (a, b) is (a^{-1}, b^{-1}).

Properties of Identities and Inverses

Proposition

If G is a group under the operation $\star$, then:

(1) The identity of G is unique;

(2) For each $a \in G$, a^{-1} is uniquely determined;

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

(4) $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$;

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

(1) If f and g are both identities, then, since g is an identity, $f \star g = f$ and, since f is an identity, $f \star g = g$. Thus $f = g$, and the identity is unique.

Proof of the Proposition (Cont'd)

(2) Assume b and c are both inverses of a and let e be the identity of G. Then $a \star b = e$ and $c \star a = e$. Thus,
$c = c \star e = c \star (a \star b) = (c \star a) \star b = e \star b = b$.

(3) To show $(a^{-1})^{-1} = a$ is exactly the problem of showing a is the inverse of a^{-1}. By the definition of a^{-1}, with the roles of a and a^{-1} interchanged, it follows that a is the inverse of a^{-1}.

(4) Let $c = (a \star b)^{-1}$. By definition of c,

$$
\begin{aligned}
(a \star b) \star c = e \;&\Rightarrow\; a \star (b \star c) = e \\
&\Rightarrow\; a^{-1} \star (a \star (b \star c)) = a^{-1} \star e \\
&\Rightarrow\; (a^{-1} \star a) \star (b \star c) = a^{-1} \\
&\Rightarrow\; e \star (b \star c) = a^{-1} \;\Rightarrow\; b \star c = a^{-1} \\
&\Rightarrow\; b^{-1} \star (b \star c) = b^{-1} \star a^{-1} \\
&\Rightarrow\; (b^{-1} \star b) \star c = b^{-1} \star a^{-1} \\
&\Rightarrow\; e \star c = b^{-1} \star a^{-1} \;\Rightarrow\; c = b^{-1} \star a^{-1}.
\end{aligned}
$$

Proof of the Proposition (Conclusion)

(5) We show by induction on n that, regardless of bracketing, the expression $a_1 \star \cdots \star a_n$ evaluates to the expression that is left-parenthesized: $((a_1 \star a_2) \star \cdots \star a_{n-1}) \star a_n$.

For $n = 3$, we have $a_1 \star (a_2 \star a_3) = (a_1 \star a_2) \star a_3$ by associativity.

Suppose that, for all $k < n$, we have
$a_1 \star \cdots \star a_k = ((a_1 \star a_2) \star \cdots \star a_{k-1}) \star a_k$.

Then we obtain:

$$\begin{aligned}
&(a_1 \star a_2 \star \cdots \star a_i) \star (a_{i+1} \star \cdots \star a_n) \\
&= (a_1 \star a_2 \star \cdots \star a_i) \star ((a_{i+1} \star a_{i+2}) \star \cdots \star a_{n-1}) \star a_n) \\
&= ((a_1 \star a_2 \star \cdots \star a_i) \star ((a_{i+1} \star a_{i+2}) \star \cdots \star a_{n-1})) \star a_n \\
&= (((a_1 \star a_2) \star \cdots \star a_{n-2}) \star a_{n-1}) \star a_n.
\end{aligned}$$

Some Commonly Used Notation

(1) For abstract groups G, H, etc., we write the operation as $\cdot$ and $a \cdot b$ as ab. In view of the generalized associative law, products of three or more group elements need not be bracketed. For an abstract group G, with operation $\cdot$, we denote the identity of G by 1.

(2) For any group G, with operation $\cdot$, $x \in G$ and $n \in \mathbb{Z}^+$, since the product $\underbrace{xx \cdots x}_{n \text{ terms}}$ does not depend on how it is bracketed, we shall denote it by x^n. Denote $\underbrace{x^{-1}x^{-1} \cdots x^{-1}}_{n \text{ terms}}$ by x^{-n}. Let $x^0 = 1$, the identity of G.

- When we are dealing with specific groups, we shall use the natural operation. For example, when the operation is $+$:
  - the identity will be denoted by 0;
  - for any element a, the inverse a^{-1} will be written $-a$;
  - $\underbrace{a + a + \cdots + a}_{n > 0 \text{ terms}}$ will be written na; $\underbrace{-a - a \cdots - a}_{n \text{ terms}}$ will be written $-na$; and $0a = 0$.

Solving Equations and the Cancelation Laws

Proposition

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 cancelation laws hold in G:

(1) If $au = av$, then $u = v$;

(2) If $ub = vb$, then $u = v$.

- To solve $ax = b$, multiply on the left by a^{-1} and simplify to get $x = a^{-1}b$. Since a^{-1} is unique so is x. Similarly, if $ya = b$, $y = ba^{-1}$.

  If $au = av$, multiply both sides on the left by a^{-1} to get $u = v$.

  Similarly, the right cancelation law holds.
- Useful consequences:
  - If $a \in G$ is such that, for some $b \in G$, $ab = e$ or $ba = e$, then $b = a^{-1}$, i.e., we do not have to show both equations hold.
  - If, for some $b \in G$, $ab = a$ (or $ba = a$), then b must be the identity of G, i.e., we do not have to check $bx = xb = x$, for all $x \in G$.

The Order of an Element in a Group

Definition (Order of an Element)

For G a group and $x \in G$, define the **order** of x to be the smallest positive integer n, such that $x^n = 1$. This integer is denoted by $|x|$ and x is said 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**.

- The symbol for the order of x should not be confused with the absolute value symbol; especially when $G = \mathbb{R}$, care is needed to distinguish the two.

  Examples:

  (1) An element of a group has order 1 if and only if it is the identity.
  (2) In the additive groups $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$, every nonzero (i.e., nonidentity) element has infinite order.
  (3) In the multiplicative groups $\mathbb{R} - \{0\}$ or $\mathbb{Q} - \{0\}$, the element -1 has order 2 and all other nonidentity elements have infinite order.

Additional Examples of Order

- Some additional examples drawn from modular arithmetic:

(4) In the additive group $\mathbb{Z}/9\mathbb{Z}$:

$$\begin{aligned}&\overline{6} \neq \overline{0};\\ &\overline{6}+\overline{6}=\overline{12}=\overline{3}\neq\overline{0};\\ &\overline{6}+\overline{6}+\overline{6}=\overline{18}=\overline{0}.\end{aligned}$$

So, the element $\overline{6}$ has order 3.

(5) In the multiplicative group $(\mathbb{Z}/7\mathbb{Z})^{\times}$:
The powers of the element $\overline{2}$ are: $\overline{2}, \overline{4}, \overline{8}=\overline{1},$ the identity in this group.
So $\overline{2}$ has order 3.

- Similarly, for the element $\overline{3}$:

$$\begin{aligned}&\overline{3};\qquad &&\overline{3}^4\equiv\overline{18}\equiv\overline{4};\\ &\overline{3}^2\equiv\overline{9}\equiv\overline{2};\qquad &&\overline{3}^5\equiv\overline{12}\equiv\overline{5};\\ &\overline{3}^3\equiv\overline{6};\qquad &&\overline{3}^6\equiv\overline{15}\equiv\overline{1}.\end{aligned}$$

So $\overline{3}$ has order 6 in $(\mathbb{Z}/7\mathbb{Z})^{\times}$.

Multiplication or Group Table

Definition (Multiplication or Group Table)

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 $g_i g_j$.

- For a finite group the multiplication table contains, in some sense, all the information about the group.

  Example: Consider the group G, with elements $1, a, b, c$. Its multiplication $\cdot$ is completely specified by the group table:

$\cdot$	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Subsection 2

Dihedral Groups

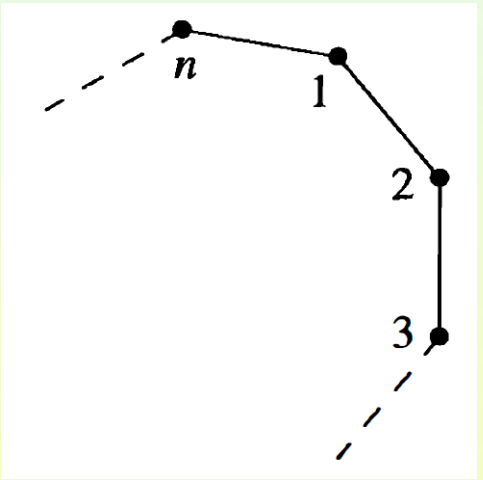
Symmetries of a Regular n-gon

- An important family of examples of groups is the class of groups whose elements are symmetries of geometric objects.

  The simplest subclass is when the geometric objects are regular planar figures.
- A **symmetry** of an n-gon is any rigid motion of the n-gon which can be effected by:
  - taking a copy of the n-gon;
  - moving it in any fashion in 3-space;
  - placing it back on the original so it exactly covers it.
- For each $n \in \mathbb{Z}^+$, $n \geq 3$, let D_{2n} be the set of symmetries of a regular n-gon.

Describing Symmetries

- We can describe the symmetries by first choosing a labeling of the n vertices:
  Each symmetry s can be described uniquely by the corresponding permutation σ of $\{1, 2, 3, \ldots, n\}$, where, if the symmetry s puts vertex i in the place where vertex j was originally, then σ is the permutation sending i to j.



  Example: If s is a rotation of $\frac{2\pi}{n}$ radians clockwise about the center of the n -gon, then σ sends i to $i+1$, $1 \leq i \leq n-1$, and $\sigma(n) = 1$.

The Group Structure

- We make D_{2n} into a group by defining st for $s, t \in D_{2n}$ to be the symmetry obtained by first applying t then s to the n-gon.

  We are viewing symmetries as functions on the n-gon, so st is just function composition, read, as usual, from right to left.
- If s, t effect the permutations σ, τ, respectively, on the vertices, then st effects $\sigma \circ \tau$.
  - The binary operation on D_{2n} is associative since composition of functions is associative.
  - The identity of D_{2n} is the identity symmetry (which leaves all vertices fixed), denoted by 1.
  - The inverse of $s \in D_{2n}$ is the symmetry which reverses all rigid motions of s. So, if s effects permutation σ on the vertices, s^{-1} effects σ^{-1}.
- We will show that $|D_{2n}| = 2n$.

  So D_{2n} is called the **dihedral group of order** $2n$.

Order of D_{2n}

- We determine the order $|D_{2n}|$:
  - Given any vertex i, there is a symmetry which sends vertex 1 into position i.
  - Since vertex 2 is adjacent to vertex 1, vertex 2 must end up in position $i+1$ or $i-1$ (where $n+1$ is 1 and $1-1$ is n, i.e., the integers labeling the vertices are read mod n).
  - By following the first symmetry by a reflection about the line through vertex i and the center of the n-gon, we see that vertex 2 can be sent to either position $i+1$ or $i-1$ by some symmetry.

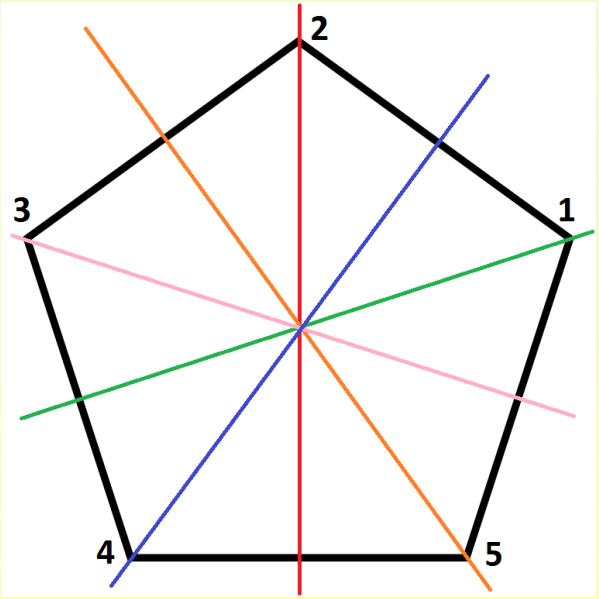
Thus there are $n \cdot 2$ positions the ordered pair of vertices 1, 2 may be sent to upon applying symmetries.

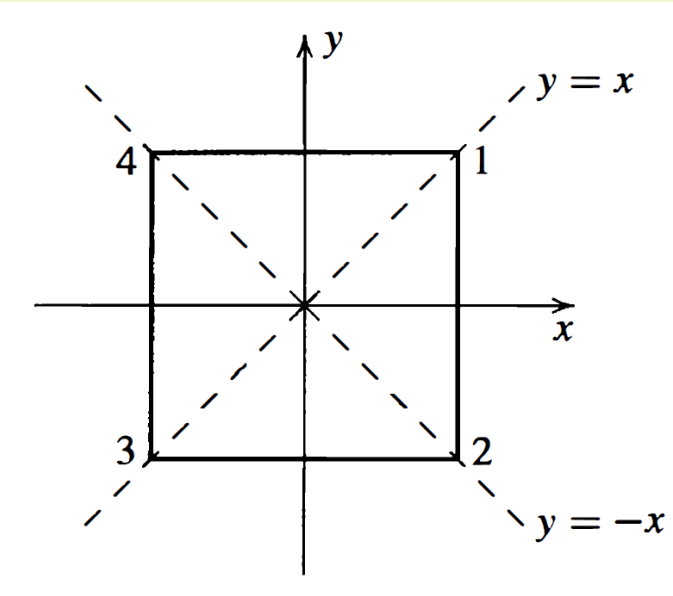
Since symmetries are rigid motions, once the position of the ordered pair of vertices 1, 2 has been specified, the action of the symmetry on all remaining vertices is completely determined.

Thus, there are exactly $2n$ symmetries of a regular n-gon.

Exhibiting the Symmetries in D_{2n}

- We can explicitly exhibit the $2n$ symmetries that we proved exist:
  - The n rotations about the center through $\frac{2\pi}{n}$ radian, $0 \leq i \leq n-1$;
  - The n reflections through the n lines of symmetry;
    - If n is odd, each symmetry line passes through a vertex and the mid-point of the opposite side;
    - If n is even, there are $\frac{n}{2}$ lines of symmetry which pass through 2 opposite vertices and $\frac{n}{2}$ which perpendicularly bisect two opposite sides.





Notation

- Fix a regular n-gon centered at the origin in an x, y-plane and label the vertices consecutively from 1 to n in a clockwise manner.
- Let r be the rotation clockwise about the origin through $\frac{2\pi}{n}$ radian.
- Let s be the reflection about the line of symmetry through vertex 1 and the origin.
  (1) $1, r, r^2, \ldots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$.
  (2) $|s| = 2$.
  (3) $s \neq r^i$, for any i.
  (4) $sr^i \neq sr^j$, for all $0 \leq i, j \leq n-1$, with $i \neq j$.

  So we get that

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}.$$

  I.e., each element can be written uniquely in the form $s^k r^i$, for some $k = 0$ or 1 and $0 \leq i \leq n-1$.

Operations involving s and Powers of r

- We saw that

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}.$$

(5) $rs = sr^{-1}$. This shows, in particular, that r and s do not commute, so that D_{2n} is non-abelian.

(6) $r^i s = sr^{-i}$, for all $0 \leq i \leq n-1$.
This can be shown by induction on i:

$$\begin{aligned} r^{i+1}s &= (rr^i)s = r(r^i s) = r(sr^{-i}) = (rs)r^{-i} \\ &= (sr^{-1})r^{-i} = s(r^{-1}r^{-i}) = sr^{-(i+1)}. \end{aligned}$$

It provides a method for commuting s with powers of r.

Multiplying Elements of D_{2n}

- The complete multiplication table of D_{2n} can be written in terms of r and s alone, since all the elements of D_{2n} have a (unique) representation in the form $s^k r^i, k = 0, 1$, and $0 \leq i \leq n-1$.

  Any product of two elements in this form can be reduced to another in the same form using only "relations" (1), (2) and (6).

  Example: If $n = 12$,

$$\begin{aligned} (sr^9)(sr^6) &= s(r^9 s)r^6 = s(sr^{-9})r^6 \\ &= s^2 r^{-9+6} = r^{-3} = r^9. \end{aligned}$$

Generators of a Group

- A subset S of elements of a group G with the property that every element of G can be written as a (finite) product of elements of S and their inverses is called a set of **generators** of G. This is indicated by writing $G = \langle S \rangle$. We say G is **generated by** S or S **generates** G.

  Example: The integer 1 is a generator for the additive group $\mathbb{Z}$ of integers since every integer is a sum of a finite number of $+1$'s and -1's, so $\mathbb{Z} = \langle 1 \rangle$.

  Example: By the preceding discussion, the set $S = \{r, s\}$ is a set of generators of D_{2n}, so $D_{2n} = \langle r, s \rangle$.
- We will see later that, in a finite group G, the set S generates G if every element of G is a finite product of elements of S (i.e., it is not necessary to include the inverses of the elements of S as well).

Generators and Relations of a Group

- Any equations in a general group G that the generators satisfy are called **relations** in G.

  Example: In D_{2n} we have relations: $r^n = 1, s^2 = 1$ and $rs = sr^{-1}$.

  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.
  This follows from the fact that we can determine exactly when two group elements are equal by using only these three relations.

Presentations Through Generators and Relations

- If some group G is generated by a subset S and there is some collection of relations, say $R_1, R_2, \ldots, R_m$ (each R_i is an equation in the elements from $S \cup \{1\}$), such that any relation among the elements of S can be deduced from these, we call these generators and relations a **presentation** of G and write

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

Example: One presentation for the dihedral group D_{2n} is then

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

Characterization of D_{2n}

- We proved geometrically that there is a group of order $2n$ with generators r and s and satisfying the relations in

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

  Thus, a group with only these relations must have order at least $2n$.
- On the other hand, using with the commutation relation $rs = sr^{-1}$, it can be shown that any group defined by this set of generators and relations has order at most $2n$.
- It follows that the group with that presentation has order exactly $2n$ and that it is the group of symmetries of the regular n-gon.

Subsection 3

Symmetric Groups

The Symmetric Groups

- Let Ω be any nonempty set and let S_Ω be the set of all bijections from Ω to itself, i.e., the set of all permutations of Ω.
- The set S_Ω is a group under function composition $\circ$.
  $\circ$ is a binary operation on S_Ω since, if $\sigma : \Omega \to \Omega$ and $\tau : \Omega \to \Omega$ are both bijections, then $\sigma \circ \tau$ is also a bijection from Ω to Ω.
  - Since function composition is associative in general, $\circ$ is associative.
  - The identity of S_Ω is the permutation 1 defined by $1(a) = a$, for all $a \in \Omega$.
  - For every permutation σ, there is a (2-sided) inverse function $\sigma^{-1} : \Omega \to \Omega$ satisfying $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = 1$.

  Thus, all the group axioms hold for $(S_\Omega, \circ)$. It is called the **symmetric group on the set** Ω.
- Note that the elements of S_Ω are the permutations of Ω, not the elements of Ω itself.
- In the special case when $\Omega = \{1, 2, 3, \ldots, n\}$, the symmetric group on Ω is denoted S_n, the **symmetric group of degree** n.

The Order of S_n

Claim: The order of S_n is $n!$.

The permutations of $\{1, 2, 3, \ldots, n\}$ are precisely the injective functions of this set to itself because it is finite.

To count the number of injective functions, note that an injective function σ can send:

- the number 1 to any of the n elements of $\{1, 2, 3, \ldots, n\}$;
- $\sigma(2)$ can then be any one of the elements of this set except $\sigma(1)$, so there are $n - 1$ choices for $\sigma(2)$;
- $\sigma(3)$ can be any element except $\sigma(1)$ or $\sigma(2)$, so there are $n - 2$ choices for $\sigma(3)$, and so on.

Thus, there are precisely $n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!$ possible injective functions from $\{1, 2, 3, \ldots, n\}$ to itself.

Hence there are precisely $n!$ permutations of $\{1, 2, 3, \ldots, n\}$, i.e., precisely $n!$ elements in S_n.

The Cycle Decomposition

- An efficient notation for writing elements σ of S_n is called the **cycle decomposition**.
- A **cycle** is a string of integers which represent the element of S_n which cyclically permutes these integers (and fixes all other integers).

  The cycle $(a_1\ a_2 \dots a_m)$ is the permutation which sends a_i to a_{i+1}, $1 \leq i \leq m-1$ and sends a_m to a_1.

  Example: (2 1 3) is the permutation which maps 2 to 1, 1 to 3 and 3 to 2.
- For each $\sigma \in S_n$, the numbers from 1 to n will be rearranged and grouped into k cycles of the form

$$(a_1\ a_2 \dots a_{m_1})(a_{m_1+1}\ a_{m_1+2} \dots a_{m_2}) \cdots (a_{m_{k-1}+1}\ a_{m_{k-1}+2} \dots a_{m_k}),$$

  from which the action of σ on any number from 1 to n can be read.

Permutation Represented by a Cycle Decomposition

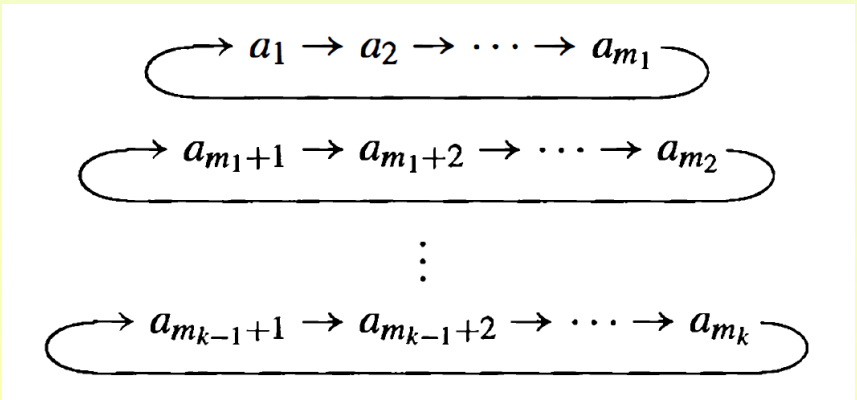
- In the representation of σ as

$$(a_1\ a_2 \dots a_{m_1})(a_{m_1+1}\ a_{m_1+2} \dots a_{m_2}) \cdots (a_{m_{k-1}+1}\ a_{m_{k-1}+2} \dots a_{m_k}),$$

the action on any number from 1 to n can be read as follows:

For any $x \in \{1, 2, 3, \dots, n\}$, first locate x in the above expression.

- If x is not followed immediately by a right parenthesis, i.e., x is not at the right end of one of the k cycles, then $\sigma(x)$ is the integer appearing immediately to the right of x.
- If x is followed by a right parenthesis, then $\sigma(x)$ is the number which is at the start of the cycle ending with x, i.e., if $x = a_{m_i}$ for some i, then $\sigma(x) = a_{m_{i-1}+1}$.



- The product of all the cycles is called the **cycle decomposition** of σ.

Computing the Cycle Decomposition of a Permutation

- We now give an algorithm for computing the cycle decomposition of an element σ of S_n.

  Running Example: Let $n = 13$ and let $\sigma \in S_{13}$ be defined by

$$\begin{array}{lllll} \sigma(1) = 12, & \sigma(2) = 13, & \sigma(3) = 3, & \sigma(4) = 1, & \sigma(5) = 11, \\ \sigma(6) = 9, & \sigma(7) = 5, & \sigma(8) = 10, & \sigma(9) = 6, & \sigma(10) = 4, \\ \sigma(11) = 7, & \sigma(12) = 8, & \sigma(13) = 2. & & \end{array}$$

- **The Cycle Decomposition Algorithm**:
  - To start a new cycle pick the smallest element of $\{1, 2, \ldots, n\}$ which has not yet appeared in a previous cycle - call it a; if just starting, $a = 1$; begin the new cycle: $(a$

    In the Example, we have (1
  - Read off $\sigma(a)$ from the given description of σ - call it b;
    - If $b = a$, close the cycle with a right parenthesis (without writing b down); this completes a cycle - return to step 1.
    - If $b \neq a$, write b next to a in this cycle: $(a\ b$

  $\sigma(1) = 12 = b$, $12 \neq 1$ so write: (1 12

Computing the Cycle Decomposition (Cont'd)

- Read off $\sigma(b)$ from the given description of σ - call it c;
  - If $c = a$, close the cycle with a right parenthesis to complete the cycle - return to step 1.
  - If $c \neq a$, write c next to b in this cycle: $(a\ b\ c$

  Repeat this step using the number c as the new value for b until the cycle closes.

  $\sigma(12) = 8$, $8 \neq 1$ so continue the cycle as: $(1\ 12\ 8$

This process stops when all the numbers from $\{1, 2, \ldots, n\}$ have appeared in some cycle.

Example: For the particular σ in the example

$$\begin{array}{lllll} \sigma(1) = 12, & \sigma(2) = 13, & \sigma(3) = 3, & \sigma(4) = 1, & \sigma(5) = 11, \\ \sigma(6) = 9, & \sigma(7) = 5, & \sigma(8) = 10, & \sigma(9) = 6, & \sigma(10) = 4, \\ \sigma(11) = 7, & \sigma(12) = 8, & \sigma(13) = 2, & & \end{array}$$

$$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(3)(5\ 11\ 7)(6\ 9).$$

Final Step of the Cycle Decomposition Algorithm

- The **length** of a cycle is the number of integers which appear in it. A cycle of length t is called a t-**cycle**.
- Two cycles are called **disjoint** if they have no numbers in common. Example: $\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(3)(5\ 11\ 7)(6\ 9)$ is the product of 5 (pairwise) disjoint cycles: a 5-cycle, a 2-cycle, a 1 -cycle, a 3-cycle, and another 2-cycle.
- We adopt the convention that 1-cycles will not be written: If some integer i does not appear in the cycle decomposition of a permutation σ, it is understood that $\sigma(i) = i$, i.e., σ fixes i.
- The identity permutation of S_n has cycle decomposition $(1)(2)\cdots(n)$ and will be written simply as 1.
- **Final Step of the Algorithm**: Remove all cycles of length 1. Example: The cycle decomposition for the particular σ in the example is therefore

$$\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9).$$

Advantage of Dropping 1-Cycles

- The convention of not writing 1-cycles in the cycle decomposition has the advantage that the cycle decomposition of an element σ of S_n is also the cycle decomposition of the permutation in S_m for $m \geq n$ which acts as σ on $\{1, 2, 3, \ldots, n\}$ and fixes each element of $\{n+1, n+2, \ldots, m\}$.

  Example: (1 2) is the permutation which interchanges 1 and 2 and fixes all larger integers whether viewed in S_2, S_3 or S_4, etc.

  Example: The 6 elements of S_3 have the cycle decompositions:

Values of σ	Cycle Decomposition of σ
$\sigma_1(1) = 1, \sigma_1(2) = 2, \sigma_1(3) = 3$	1
$\sigma_2(1) = 1, \sigma_2(2) = 3, \sigma_2(3) = 2$	(2 3)
$\sigma_3(1) = 3, \sigma_3(2) = 2, \sigma_3(3) = 1$	(1 3)
$\sigma_4(1) = 2, \sigma_4(2) = 1, \sigma_4(3) = 3$	(1 2)
$\sigma_5(1) = 2, \sigma_5(2) = 3, \sigma_5(3) = 1$	(1 2 3)
$\sigma_6(1) = 3, \sigma_6(2) = 1, \sigma_6(3) = 2$	(1 3 2)

Inverses and Compositions in Cycle Representation

- For any $\sigma \in S_n$, the cycle decomposition of σ^{-1} is obtained by writing the numbers in each cycle of the cycle decomposition of σ in reverse order.

  Example: If $\sigma = (1\ 12\ 8\ 10\ 4)(2\ 13)(5\ 11\ 7)(6\ 9)$ is the element of S_{13}, then $\sigma^{-1} = (4\ 10\ 8\ 12\ 1)(13\ 2)(7\ 11\ 5)(9\ 6)$.
- Computing products is straightforward, keeping in mind that when computing $\sigma \circ \tau$ in S_n one reads the permutations from right to left. One simply "follows" the elements under the successive permutations.

  Example: In the product $(1\ 2\ 3) \circ (1\ 2)(3\ 4)$ the number 1 is sent to 2 by the first permutation, then 2 is sent to 3 by the second permutation. Hence the composite maps 1 to 3.

  To compute the cycle decomposition of the product we need next to see what happens to 3, etc. We have $(1\ 2\ 3) \circ (1\ 2)(3\ 4) = (1\ 3\ 4)$.
- Note that $(1\ 2) \circ (1\ 3) = (1\ 3\ 2)$ and $(1\ 3) \circ (1\ 2) = (1\ 2\ 3)$. Thus S_n is a non-abelian group for all $n \geq 3$.

Rearrangements of a Cycle Decomposition

- Each cycle $(a_1\ a_2 \ldots a_m)$ in a cycle decomposition can be viewed as the permutation which cyclically permutes $a_1, a_2, \ldots, a_m$ and fixes all other integers.
- Since disjoint cycles permute numbers which lie in disjoint sets, it follows that disjoint cycles commute.

  Thus, rearranging the cycles in any product of disjoint cycles (in particular, in a cycle decomposition) does not change the permutation.
- Also, since a given cycle $(a_1\ a_2 \ldots a_m)$ permutes $\{a_1, a_2, \ldots, a_m\}$ cyclically, the numbers in the cycle itself can be cyclically permuted without altering the permutation, i.e., $(a_1\ a_2 \ldots a_m) = (a_2\ a_3 \ldots a_m\ a_1) = (a_3\ a_4 \ldots a_m\ a_1\ a_2) = \cdots = (a_m\ a_1\ a_2 \ldots a_{m-1})$.
  Example: We have $(1\ 2) = (2\ 1)$ and $(1\ 2\ 3\ 4) = (3\ 4\ 1\ 2)$.
- By convention, the smallest number appearing in the cycle is usually written first.

Some Remarks on the Cycle Decomposition

- A permutation may be written in many ways as an arbitrary product of cycles!

  Example: In S_3,

$$(1\ 2\ 3) = (1\ 2)(2\ 3) = (1\ 3)(1\ 3\ 2)(1\ 3) \text{ etc.}$$

- We will show that the cycle decomposition of each permutation is the unique way of expressing a permutation as a product of disjoint cycles (up to rearranging its cycles and cyclically permuting the numbers within each cycle).
  - Reducing an arbitrary product of cycles to a product of disjoint cycles allows us to determine at a glance whether or not two permutations are the same.
  - Another advantage is that the order of a permutation is the l.c.m. of the lengths of the cycles in its cycle decomposition.

Subsection 4

Matrix Groups

Fields

- A field is the "smallest" mathematical structure in which we can perform all the arithmetic operations $+, -, \times$ and $\div$ (division by nonzero elements).

  In particular every nonzero element must have a multiplicative inverse.

Definition (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);
- $(F - \{0\}, \cdot)$ is also an abelian group;
- The following distributive law holds:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

(2) For any field F, let $F^\times = F - \{0\}$.

The Set $\mathrm{GL}_n(F)$

- Let F be a field.
- The determinant of any matrix A with entries from F can be computed by the same formulas as when $F = \mathbb{R}$.
- For each $n \in \mathbb{Z}^+$, let $\mathrm{GL}_n(F)$ be the set of all $n \times n$ matrices whose entries come from F and whose determinant is nonzero:

$$\mathrm{GL}_n(F) = \{A : A \text{ is an } n \times n \text{ matrix with entries from } F \text{ and } \det(A) \neq 0\}.$$

- For arbitrary $n \times n$ matrices A and B, let AB be the product of these matrices, computed by the same rules as when $F = \mathbb{R}$.

  Example: A product in $\mathrm{GL}_2(\mathbb{R})$:

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} = \begin{bmatrix} 1 \cdot 5 + 2 \cdot 7 & 1 \cdot 6 + 2 \cdot 8 \\ 3 \cdot 5 + 4 \cdot 7 & 3 \cdot 6 + 4 \cdot 8 \end{bmatrix} = \begin{bmatrix} 19 & 22 \\ 43 & 50 \end{bmatrix}.$$

The General Linear Groups of Degree n

Claim: $\mathrm{GL}_n(F)$ is a group under matrix multiplication.

Since $\det(AB) = \det(A) \cdot \det(B)$, it follows that, if $\det(A) \neq 0$ and $\det(B) \neq 0$, then $\det(AB) \neq 0$, so $\mathrm{GL}_n(F)$ is closed under matrix multiplication.

- Matrix product is associative.
- For every matrix $A \in \mathrm{GL}_n(F)$, $AI = IA = A$, where I is the $n \times n$ identity matrix.
- $\det(A) \neq 0$ if and only if A has a matrix inverse (that can be computed by the same adjoint formula used when $F = \mathbb{R}$). So each $A \in \mathrm{GL}_n(F)$ has an inverse A^{-1} in $\mathrm{GL}_n(F)$, such that $AA^{-1} = A^{-1}A = I$.

- $\mathrm{GL}_n(F)$ is called the **general linear group of degree** n.

Subsection 5

The Quaternion Group

The Quaternion Group

Definition (The Quaternion Group)

The **quaternion group** Q_8 is defined by

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

with product $\cdot$ computed as follows:

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

- We write ab for $a \cdot b$.
- It is tedious to check the associative law, but the other group axioms are easily checked.
- Q_8 is a non-abelian group of order 8.

Subsection 6

Homomorphisms and Isomorphisms

Group Homomorphisms

- Two groups are isomorphic if they "look the same".
- A more relaxed notion is that of a homomorphism:

Definition (Homomorphism)

Let $(G, \star)$ and $(H, \diamond)$ be groups. A map $\varphi : G \to H$, such that

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

is called a **homomorphism**.

- When the group operations for G and H are not explicitly written, the homomorphism condition becomes simply

$$\varphi(xy) = \varphi(x)\varphi(y).$$

  - The product xy on the left is computed in G.
  - The product $\varphi(x)\varphi(y)$ on the right is computed in H.
- The idea is that φ is a homomorphism if it respects the group structures of its domain and codomain.

Group Isomorphisms

Definition (Isomorphism)

The map $\varphi : G \to H$ is called an **isomorphism** and G and H are said to be **isomorphic** or of the same **isomorphism type**, written $G \cong H$, if:

(1) φ is a homomorphism, i.e., $\varphi(xy) = \varphi(x)\varphi(y)$;

(2) φ is a bijection.

- The groups G and H are isomorphic if there is a bijection between them which preserves the group operations.
- In effect, G and H are the same group except that the elements and the operations may be written differently in G and H.
- It follows that any property which G has, which depends only on the group structure of G, also holds in H.

Isomorphism Classes

- Let $\mathcal{G}$ be any nonempty collection of groups.
  Claim: The relation $\cong$ is an equivalence relation on $\mathcal{G}$.
  - **Reflexivity**: Consider $G \in \mathcal{G}$. The identity map $i_G : G \to G$ is a bijection. Moreover, for all $a, b \in G$, $i_G(ab) = ab = i_G(a)i_G(b)$. So $i_G : G \to G$ is an isomorphism. This proves $G \cong G$.
  - **Symmetry**: Suppose $G_1 \cong G_2$. Then, there exists an isomorphism $f : G_1 \to G_2$. Since f is a bijection, it has an inverse $f^{-1} : G_2 \to G_1$. f^{-1} is a bijection. Moreover, for all $a_2, b_2 \in G_2$, there exist $a_1, b_1 \in G_1$, such that $f(a_1) = a_2$ and $f(b_1) = b_2$. Thus, we get $f^{-1}(a_2 b_2) = f^{-1}(f(a_1)f(b_1)) = f^{-1}(f(a_1 b_1)) = a_1 b_1 = f^{-1}(a_2)f^{-1}(b_2)$. Hence, $f^{-1} : G_2 \to G_1$ is also an isomorphism. This shows that $G_2 \cong G_1$.
  - **Transitivity**: Suppose $G_1 \cong G_2$ and $G_2 \cong G_3$. Then, there exist isomorphisms $f : G_1 \to G_2$ and $g : G_2 \to G_3$. Consider the bijection $g \circ f : G_1 \to G_3$. For all $a_1, b_1 \in G_1$, we have $(g \circ f)(a_1 b_1) = g(f(a_1)f(b_1)) = g(f(a_1))g(f(b_1)) = (g \circ f)(a_1)(g \circ f)(b_1)$. Thus, $g \circ f : G_1 \to G_3$ is an isomorphism. This shows that $G_1 \cong G_3$.
- The $\cong$-equivalence classes are called **isomorphism classes**.

Example: The Exponential Map

Example: The exponential map $\exp : \mathbb{R} \to \mathbb{R}^+$, defined by

$$\exp(x) = e^x,$$

where e is the base of the natural logarithm, is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$.

- exp is a bijection since it has an inverse function ln.
- exp preserves the group operations since $e^{x+y} = e^x e^y$.

Note both the elements and the operations are different, yet the two groups are isomorphic. Thus, as groups they have identical structures.

Isomorphism Type of a Symmetric Group

Claim: Let Δ and Ω be nonempty sets. If $|\Delta| = |\Omega|$, the symmetric groups S_Δ and S_Ω are isomorphic.
Suppose $|\Delta| = |\Omega|$. Then there exists a bijection $\theta : \Delta \to \Omega$. Define the map $\phi : S_\Delta \to S_\Omega$ as follows: For all $\sigma : \Delta \to \Delta \in S_\Delta$, $\phi(\sigma) : \Omega \to \Omega$ is defined by

$$\phi(\sigma)(\omega) = \theta(\sigma(\theta^{-1}(\omega))), \text{ for all } \omega \in \Omega.$$

- $\phi(\sigma) : \Omega \to \Omega \in S_\Omega$, for all $\sigma \in S_\Delta$:
  Note that $\phi(\sigma) = \theta \circ \sigma \circ \theta^{-1}$. Since all three of $\theta, \sigma, \theta^{-1}$ are bijections and the composition of bijections is a bijection, we get that $\phi(\sigma) : \Omega \to \Omega$ is a bijection, i.e., $\phi(\sigma) \in \Delta_\Omega$.
- $\phi : S_\Delta \to S_\Omega$ is a bijection.
  Suppose $\phi(\sigma) = \phi(\tau)$. Then $\theta \circ \sigma \circ \theta^{-1} = \theta \circ \tau \circ \theta^{-1}$. Therefore, $\theta^{-1} \circ \theta \circ \sigma \circ \theta^{-1} \circ \theta = \theta^{-1} \circ \theta \circ \tau \circ \theta^{-1} \circ \theta$, i.e., $\sigma = \tau$. This shows that $\phi : S_\Delta \to S_\Omega$ is a bijection.
- $\phi : S_\Delta \to S_\Omega$ is a homomorphism.
  $\phi(\sigma \circ \tau) = \theta \circ (\sigma \circ \tau) \circ \theta^{-1} = \theta \circ \sigma \circ \theta^{-1} \circ \theta \circ \tau \circ \theta^{-1} = \phi(\sigma) \circ \phi(\tau)$.

Isomorphism Type of a Symmetric Group (Converse)

Claim: If $S_\Delta = S_\Omega$, then $|\Delta| = |\Omega|$.

We only show this in the finite case.

Any isomorphism between two groups G and H is a bijection between them. Thus, $|S_\Delta| = |S_\Omega|$. When Δ is a finite set of order n, then $|S_\Delta| = n!$. Similarly, if Ω is a finite set of order m, then $|S_\Omega| = m!$. Thus, if $S_\Delta \cong S_\Omega$, then $n! = m!$, whence $m = n$, i.e., $|\Delta| = |\Omega|$.

Some Properties Preserved by Isomorphisms

Proposition

If $\varphi : G \to H$ is an isomorphism, then:

(a) $|G| = |H|$;

(b) G is abelian if and only if H is abelian;

(c) For all $x \in G$, $|x| = |\varphi(x)|$.

(a) Since isomorphisms are bijections, if $G \cong H$, then $|G| = |H|$.

(b) Suppose G is abelian. Let $h_1, h_2 \in H$. Since φ is surjective, there exist $g_1, g_2 \in G$, such that $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$. Now we obtain: $h_1 \diamond h_2 = \varphi(g_1) \diamond \varphi(g_2) = \varphi(g_1 \star g_2) = \varphi(g_2 \star g_1) = \varphi(g_2) \diamond \varphi(g_1) = h_2 \diamond h_1$. Hence H is also abelian.

Suppose, conversely, that H is abelian. Let $g_1, g_2 \in G$. Then, we have $\varphi(g_1 \star g_2) = \varphi(g_1) \diamond \varphi(g_2) = \varphi(g_2) \diamond \varphi(g_1) = \varphi(g_2 \star g_1)$. But φ is injective, whence $g_1 \star g_2 = g_2 \star g_1$. Thus, G is also abelian.

(c) Assume that $|x| = n$ and $|\varphi(x)| = m$. Since $\varphi(x)^n = \varphi(x^n) = \varphi(1_G) = 1_H$, we have $m \leq n$. On the other hand, $\varphi(x^m) = \varphi(x)^m = 1_H = \varphi(1_G)$. Since φ is injective, $x^m = 1_G$, whence $n \leq m$.

Using Properties Preserved to Show Non-Isomorphism

- The properties that are preserved under isomorphisms, such as "being abelian", can be used to show that two groups are not isomorphic.
  - Show that one has the property and the other does not.

  Example: The groups S_3 and $\mathbb{Z}/6\mathbb{Z}$ are not isomorphic:
  - $\mathbb{Z}/6\mathbb{Z}$ is abelian;
  - S_3 is not abelian.

  Example: $(\mathbb{R} - \{0\}, \times)$ and $(\mathbb{R}, +)$ cannot be isomorphic:
  - In $(\mathbb{R} - \{0\}, \times)$ the element -1 has order 2;
  - $(\mathbb{R}, +)$ has no element of order 2.

Presentations and Homomorphisms

- Let G be a finite group of order n for which we have a presentation. Let $S = \{s_1, \ldots, s_m\}$ be the generators. Let H be another group and $\{r_1, \ldots, r_m\}$ be elements of H. Suppose that any relation satisfied in G by the s_i is also satisfied in H when each s_i is replaced by r_i. Then there is a (unique) homomorphism $\varphi : G \to H$ which maps s_i to r_i.
- If H is generated by the elements $\{r_1, \ldots, r_m\}$, then φ is surjective, since any product of the r_i's is the image of the corresponding product of the s_i's.
- If, in addition, H has the same finite order as G, then any surjective map is necessarily injective, i.e., φ is an isomorphism.
- Intuitively, we can map the generators of G to any elements of H and obtain a homomorphism, provided that the relations in G are still satisfied.

Example: Mapping D_{2n}

- Recall that $D_{2n} = \langle r, s \mid r^n = s^2 = 1, sr = r^{-1}s \rangle$.
- Suppose H is a group containing elements a and b with $a^n = 1$, $b^2 = 1$ and $ba = a^{-1}b$. Then there is a homomorphism from D_{2n} to H mapping r to a and s to b.
- Let k be an integer dividing n, with $k \geq 3$, say $n = km$, and let $D_{2k} = \langle r_1, s_1 \mid r_1^k = s_1^2 = 1, s_1 r_1 = r_1^{-1} s_1 \rangle$. Define $\varphi : D_{2n} \to D_{2k}$ by

$$\varphi(r) = r_1 \quad \text{and} \quad \varphi(s) = s_1.$$

. Since $r_1^k = 1$, also $r_1^n = (r_1^k)^m = 1$. Thus, the three relations satisfied by r, s in D_{2n} are satisfied by r_1, s_1 in D_{2k} Thus, φ extends (uniquely) to a homomorphism from D_{2n} to D_{2k}. Since $\{r_1, s_1\}$ generates D_{2k}, φ is surjective. If $k < n$, φ is not an isomorphism.

Example: Mapping D_6 to S_3

- Let $G = D_6 = \langle r, s \mid r^3 = s^2 = 1, sr = r^{-1}s \rangle$.

  In $H = S_3$, the elements $a = (1\ 2\ 3)$ and $b = (1\ 2)$ satisfy the relations: $a^3 = 1$, $b^2 = 1$ and $ba = ab^{-1}$. Thus, there is a homomorphism from D_6 to S_3 which sends $r \mapsto a$ and $s \mapsto b$.

  One may further check that S_3 is generated by a and b, so this homomorphism is surjective.

  Since D_6 and S_3 both have order 6, this homomorphism is an isomorphism: $D_6 \cong S_3$.

Subsection 7

Group Actions

Group Action

Definition (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 $g_1, g_2 \in G$, $a \in A$;

(2) $1 \cdot a = a$, for all $a \in A$.

- We say G is a group acting on a set A.
- The expression $g \cdot a$ will usually be written simply as ga when there is no danger of confusing this map with the group operation.
- Note that:
  - On the left hand side of the equation in Property (1), $g_2 \cdot a \in A$, so it makes sense to act on this by g_1.
  - On the right hand side, the product $(g_1 g_2) \in G$ and the resulting group element acts on the set element a.

Permutation Representations Associated with Actions

Claim: Let the group G act on the set A. For each fixed $g \in G$ we get a map σ_g defined by $\sigma_g : A \to A$, with $\sigma_g(a) = g \cdot a$. Then we have:

(i) For each fixed $g \in G$, σ_g is a permutation of A.

(ii) The map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism.

(i) To see that σ_g is a permutation of A, we show that, as a set map from A to A, it has a 2-sided inverse $\sigma_{g^{-1}}$. We have, for all $a \in A$, $(\sigma_{g^{-1}} \circ \sigma_g)(a) = \sigma_{g^{-1}}(\sigma_g(a)) = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1 \cdot a = a$. This proves $\sigma_{g^{-1}} \circ \sigma_g$ is the identity map from A to A. Interchange the roles of g and g^{-1} to get $\sigma_g \circ \sigma_{g^{-1}}$ is also the identity map on A. Thus, σ_g has a 2-sided inverse, and, hence, is a permutation of A.

(ii) Let $\varphi : G \to S_A$ be defined by $\varphi(g) = \sigma_g$. Part (i) shows that σ_g is indeed an element of S_A. To see that φ is a homomorphism we must prove $\varphi(g_1g_2) = \varphi(g_1) \circ \varphi(g_2)$. These are equal if and only if their values agree on every element $a \in A$. For all $a \in A$, $\varphi(g_1g_2)(a) = \sigma_{g_1g_2}(a) = (g_1g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = \sigma_{g_1}(\sigma_{g_2}(a)) = (\varphi(g_1) \circ \varphi(g_2))(a)$.

Actions Associated with Permutation Representations

- The process of associating a permutation of A with an action of a group G on A is reversible.

  Claim: 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

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

  satisfies the properties of a group action of G on A.

  We have, for all $g_1, g_2 \in G$ and all $a \in A$,
  - $g_1 \cdot (g_2 \cdot a) = \phi(g_1)(\phi(g_2)(a)) = (\phi(g_1) \circ \phi(g_2))(a) = \phi(g_1 g_2)(a) = (g_1 g_2) \cdot a$.
  - $1 \cdot a = \phi(1)(a) = 1(a) = a$.
- Thus, actions of a group G on a set A and the homomorphisms from G into the symmetric group S_A are in bijective correspondence (essentially the same notion, phrased in different terminology).

Trivial Actions

- Let G be a group and A a nonempty set.

  Define

  $$ga = a, \text{ for all } g \in G, a \in A.$$

  This forms a group action of G on A, called the **trivial action**.

  In this case G is said to **act trivially** on A.
- Distinct elements of G induce the same permutation on A, namely, the identity permutation.
- The associated permutation representation $G \to S_A$ is the trivial homomorphism which maps every element of G to the identity.

Faithful Actions and Kernel of an Action

- If G acts on a set B and distinct elements of G induce distinct permutations of B, the action is said to be **faithful**.

  Thus, a faithful action is one in which the associated representation is injective.
- The **kernel** of the action of G on B is defined to be

$$\{g \in G : gb = b, \text{ for all } b \in B\},$$

  i.e., consists of the elements of G which fix all elements of B.

  For the trivial action, the kernel of the action is all of G and this action is not faithful when $|G| > 1$.

Vector Spaces

- The axioms for a vector space V over a field F include the two axioms that the multiplicative group $F^\times$ act on the set V:
  - $(ab) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v})$, for all $a, b \in F^\times$ and all $\mathbf{v} \in V$;
  - $1 \cdot \mathbf{v} = \mathbf{v}$, for all $\mathbf{v} \in V$.

  Thus, vector spaces are familiar examples of actions of multiplicative groups of fields with additional structure (in particular, V must be an abelian group).
- In the special case when $V = \mathbb{R}^n$ and $F = \mathbb{R}$, the action is specified by

$$a(r_1, r_2, \ldots, r_n) = (ar_1, ar_2, \ldots, ar_n),$$

  for all $a \in \mathbb{R}$, $(r_1, r_2, \ldots, r_n) \in \mathbb{R}^n$, where ar_i is just multiplication of two real numbers.

Symmetric Groups

- For any nonempty set A, the symmetric group S_A acts on A by

$$\sigma \cdot a = \sigma(a), \text{ for all } \sigma \in S_A, a \in A.$$

- The associated permutation representation is the identity map from S_A to itself.

Dihedral Action

- If we fix a labeling of the vertices of a regular n-gon, each element α of D_{2n} gives rise to a permutation σ_α of $\{1, 2, \ldots, n\}$ by the way the symmetry α permutes the corresponding vertices.
  The map of $D_{2n} \times \{1, 2, \ldots, n\}$ onto $\{1, 2, \ldots, n\}$ defined by
  $$(\alpha, i) \mapsto \sigma_\alpha(i)$$
  defines a group action of D_{2n} on $\{1, 2, \ldots, n\}$.
- To simplify notation, we write αi in place of $\sigma_\alpha(i)$.
- This action is faithful.
  - When $n = 3$ the action of D_6 on the three vertices of a triangle gives an injective homomorphism from D_6 to S_3. Since these groups have the same order, this map must also be injective. So it is an isomorphism: $D_6 \cong S_3$.
  - The analogous statement is not true for any n-gon with $n \geq 4$. Just by order considerations we cannot have D_{2n} isomorphic to S_n, for any $n \geq 4$.

Left Regular Action

- Let G be any group and let $A = G$. Define a map from $G \times A$ to A by

$$g \cdot a = ga, \text{ for all } g \in G, a \in A,$$

where ga on the right hand side is the product of g and a in G.

- This gives a group action of G on itself, where each $g \in G$ permutes the elements of G by left multiplication:

$$g : a \mapsto ga, \text{ for all } a \in G.$$

- This action is called the **left regular action** of G on itself.

  Claim: The left regular action is faithful.

  Let $\varphi : G \to S_G$ be the representation associated by the left regular action. Suppose $\varphi(g_1) = \varphi(g_2)$, for some $g_1, g_2 \in G$. Then, for all $g \in G$, $\varphi(g_1)(g) = \varphi(g_2)(g)$, i.e., $g_1 g = g_2 g$. But, then $g_1 g g^{-1} = g_2 g g^{-1}$, giving $g_1 = g_2$. This shows that the action is faithful.