§3.1 Definition of a Group

Shaoyun Yi

MATH 546/701I

University of South Carolina

Spring 2022

Review

- Permutation $\sigma \in \mathrm{Sym}(S)$ (or S_n)
- $\#|S_n| = n!$
- Composition (Product) $\sigma\tau$ & Inverse σ^{-1}
- Cycle of length k: $\sigma = (a_1 a_2 \cdots a_k)$ has order k.
- Disjoint cycles are commutative
- $\sigma \in S_n$ can be written as a **unique** product of disjoint cycles.
- The order of σ is the **lcm** of the lengths (orders) of its disjoint cycles.
- A **transposition** is a cycle $(a_1 a_2)$ of length two.
- $\sigma \in S_n$ can be written as a product of transpositions. (NOT unique)
- Even Permutation & Odd Permutation
- A cycle of odd length is even. & A cycle of even length is odd.

Motivation

Symmetry occurs frequently and in many forms in nature.

Example 1

Each coefficient of a poly. is a symmetric function of the poly.'s roots.

$$f(x) = (x - r_1)(x - r_2)(x - r_3) = x^3 + bx^2 + cx + d$$

$$r_1 + r_2 + r_3 = -b, \quad r_1 r_2 + r_2 r_3 + r_3 r_1 = c, \quad \text{and} \quad r_1 r_2 r_3 = -d.$$

$\star$ The coefficients remain unchanged under any permutation of the roots.

$\rightsquigarrow$ With respect to symmetry, the **operation** of shifting the roots among themselves is the most important and not the roots themselves.

Binary Operation

A **binary operation** $*$ on a set S is a function

$$*: S \times S \to S$$

from the set $S \times S$ of all ordered pairs of elements in S into S.

- The operation $*$ is said to be **associative** if

$$a * (b * c) = (a * b) * c \qquad \text{for all } a, b, c \in S.$$

- An element $e \in S$ is called an **identity** element for $*$ if

$$a * e = a \quad \text{and} \quad e * a = a \qquad \text{for all } a \in S.$$

- If $*$ has an identity element e and $a \in S$, then $b \in S$ is an **inverse** for a if

$$a * b = e \quad \text{and} \quad b * a = e.$$

Examples

1) *Multiplication* defines an associative binary operation on $\mathbf{R}$.
   - 1 serves as an **identity** element.
   - only nonzero element a has the **inverse** $1/a$.
2) *Multiplication* defines an associative binary operation on $S = \{x \in \mathbf{R} | x \geq 1\}$
   - 1 serves as an **identity** element.
   - only 1 has the **inverse** 1.
3) Multiplication does not define a binary operation on $S = \{x \in \mathbf{R} | x < 0\}$.
4) *Matrix multiplication* defines an associative binary operation on $M_n(\mathbf{R})$.
   - the identity matrix serves as an **identity** element.
   - a matrix has a *multiplicative* **inverse** iff its determinant is nonzero.
5) *Matrix addition* defines an associative binary operation on $M_n(\mathbf{R})$.
   - the zero matrix serves as an **identity** element.
   - each matrix has an *additive* **inverse**, i.e., its negative.
6) Matrix multiplication does not define a binary operation on the set of nonzero matrices in $M_n(\mathbf{R})$. e.g., $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

Example: Well-definedness of a Binary Operation

If $a, b \in \mathbf{Q}$ with $a = \dfrac{m}{n}$ and $b = \dfrac{s}{t}$, then we define multiplication $ab = \dfrac{ms}{nt}$.

Check the **well-definedness** of multiplication:

To show that the multiplication does not depend on how we represent a, b.

Suppose that we also have $a = \dfrac{p}{q}$ and $b = \dfrac{u}{v}$, then we need to check

$$\frac{ms}{nt} = \frac{pu}{qv}, \quad \text{that is,} \quad (qv)(ms) = (pu)(nt).$$

$$a = \frac{m}{n} = \frac{p}{q} \quad \Rightarrow mq = np$$

$$\Longrightarrow mqsv = nptu \quad \Rightarrow (qv)(ms) = (pu)(nt)$$

$$b = \frac{s}{t} = \frac{u}{v} \quad \Rightarrow sv = tu$$

Associative Binary Operation $*$ on a set S

Let $*$ be an **associative** binary operation on a set S.

i) The operation $*$ has at most one identity element.

ii) If $*$ has an identity element, then any element has at most one inverse.

Proof: i) Suppose e and e' are identity elements for $*$. To show $e = e'$.

$$\left.\begin{array}{lcl} e \text{ is an identity element} & \Rightarrow & e * e' = e' \\ e' \text{ is an identity element} & \Rightarrow & e * e' = e \end{array}\right\} \Rightarrow e = e'$$

ii) e: the identity element. Let b and b' be inverses for a. To show $b = b'$.

$$b' = e * b' = (b * a) * b' = b * (a * b') = b * e = b \qquad \square$$

Let e be the identity element, and a, b have inverses a^{-1} and b^{-1}. Then

iii) the inverse of a^{-1} exists and is equal to a, and

iv) the inverse of $a * b$ exists and is equal to $b^{-1} * a^{-1}$.

Proof: iii) ✓ iv) $(a * b) * (b^{-1} * a^{-1}) = \ldots = e$ & $(b^{-1} * a^{-1}) * (a * b) = e$

Group $(G, *)$

Let $(G, *)$ be a nonempty set G together with a binary operation $*$ on G. Then $(G, *)$, or just G, is called a **group** if the following properties hold.

i) **Closure**: For all $a, b \in G$, $a * b$ is a well-defined element of G.

ii) **Associativity**: For all $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$.

iii) **Identity**: There exists an **identity** element (unique) $e \in G$:

$$a * e = a \quad \text{and} \quad e * a = a \qquad \text{for all } a \in G.$$

iv) **Inverses**: For each $a \in G$ there exists an **inverse** element $a^{-1} \in G$:

$$a * a^{-1} = e \quad \text{and} \quad a^{-1} * a = e.$$

- **R** is a group under the standard addition.
- **R** is not a group under the standard multiplication.

A group is a nonempty set G with an **associative** binary operation $*$, s.t. G contains an **identity** element e, and each element has an **inverse** in G.

Symmetric Group

Recall: The set of all permutations of a set S is denoted by $\mathrm{Sym}(S)$.
The set of all permutations of $\{1, 2, \ldots, n\}$ is denoted by S_n.

$\mathrm{Sym}(S)$ is a group under the operation of composition of functions.

Proof: Let $f, g \in \mathrm{Sym}(S)$ be any two one-to-one and onto functions.

i) **Closure:** $f \circ g \in \mathrm{Sym}(S)$

ii) **Associativity:** $\circ$ is associative.

iii) **Identity:** the identity function 1_S

iv) **Inverses:** f is 1-1 and onto $\Leftrightarrow$ the inverse function f^{-1} is 1-1 and onto

- $\mathrm{Sym}(S)$ is called the **symmetric group** on S.
- S_n is called the **symmetric group of degree** n.

Example: Multiplication Table for S_3

$\circ$	(1)	(123)	(132)	(12)	(13)	(23)
(1)	(1)	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	(1)	(13)	(23)	(12)
(132)	(132)	(1)	(123)	(23)	(12)	(13)
(12)	(12)	(23)	(13)	(1)	(132)	(123)
(13)	(13)	(12)	(23)	(123)	(1)	(132)
(23)	(23)	(13)	(12)	(132)	(123)	(1)

- In each row, each element in S_3 occurs **exactly once**.
- In each column, each element in S_3 occurs **exactly once**.

⋆ This phenomenon occurs in any such group table! (cancellation law)

Cancellation law for Groups

From now on, we drop the notation $a * b$, and simply write ab instead.

Let G be a group, and let $a, b, c \in G$.

i) If $ab = ac$, then $b = c$.

ii) If $ac = bc$, then $a = b$.

Proof: i) $ab = ac \quad \Rightarrow a^{-1}(ab) = a^{-1}(ac) \quad \ldots \quad \Rightarrow b = c$; ii) ✓ □

Let G be a group and $a, b \in G$. Then $(ab)^2 = a^2b^2$ if and only if $ba = ab$.

Proof: $(\Rightarrow)$ By $(ab)(ab) = (ab)^2 \overset{!}{=} a^2b^2 = (aa)(bb)$, we have

$$a(b(ab)) = a(a(bb)) \quad \rightsquigarrow b(ab) = a(bb) \quad \rightsquigarrow (ba)b = (ab)b \quad \rightsquigarrow ba = ab$$

$(\Leftarrow)$ $(ab)^2 = (ab)(ab) = a(b(ab)) = a((ba)b) \overset{!}{=} a((ab)b) = a(a(bb)) = (aa)(bb)$

There is no worry about "( )" by the associative law for the operation.

Proof: $(\Rightarrow)$ $abab = aabb \quad \rightsquigarrow ba = ab \qquad (\Leftarrow)$ $ba = ab \quad \rightsquigarrow abab = aabb$ □

Abelian Group $(G, +)$

A group G is said to be **abelian** if $ab = ba$ for all $a, b \in G$.

In an abelian group G, the operation is very often denoted additively.

Associativity: $a + (b + c) = (a + b) + c$ for all $a, b, c \in G$.

Identity: The identity element is 0 (**zero** element): $0 + a = a + 0 = a$

Inverses: The additive inverse of a is $-a$: $a + (-a) = (-a) + a = 0$

Example 2

$\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ are abelian groups under the ordinary addition.

(Cancellation law) Let G be an abelian group, and let $a, b, c \in G$.

$$a + b = a + c \;\; (\text{Equivalently, } b + a = c + a) \quad \Rightarrow b = c$$

For an abelian group G, let $a \in G$ and $n \in \mathbf{Z}_{>0}$, define $na := a + \cdots + a$.

Caution: "na" is not a multiplication in G, since n is not an element of G.

Finite Group v.s. Infinite Group

A group G is called a **finite group** if G has a finite number of elements.
In this case, the number of elements is called the **order** of G, denoted by $|G|$.
If G is not finite, it is said to be an **infinite group**.

$\mathbf{Z}_n$ is an abelian group under addition of congruence classes for $n \in \mathbf{Z}_{>0}$.
Moreover, the group $\mathbf{Z}_n$ is finite and $|\mathbf{Z}_n| = n$.

Closure: $[a] + [b] = [a + b]$ is well-defined & $[a + b] \in \mathbf{Z}_n$ for $[a], [b] \in \mathbf{Z}_n$.
Associative: $([a] + [b]) + [c] = [(a + b) + c] = [a + (b + c)] = [a] + ([b] + [c])$
Commutative: $[a] + [b] = [a + b] = [b + a] = [b] + [a]$
Identity: $[0] + [a] = [a] + [0] = [a + 0] = [a]$
Inverses: $[-a] + [a] = [a] + [-a] = [a - a] = [0]$

For each $a \in \mathbf{Z}$, $[a] = [r]$ for a unique $r \in \mathbf{Z}$ with $0 \leq r < n$. $\Rightarrow |\mathbf{Z}_n| = n$

Q: Is $\mathbf{Z}_n$ an abelian group under multiplication of congruence classes?

A: No! ($[a]$ has a multiplicative inverse in $\mathbf{Z}_n$ if and only if $(a, n) = 1$.)

$\mathbf{Z}_n^\times$: Group of Units Modulo n

$\mathbf{Z}_n^\times$ is an abelian group under multiplication of congruence classes for $n \geq 1$
Moreover, $\mathbf{Z}_n^\times$ is finite and $|\mathbf{Z}_n^\times| = \varphi(n)$, where $\varphi(n)$ is Euler's φ-function.

Closure: $[a] \cdot [b] = [ab]$ is well-defined & $[ab] \in \mathbf{Z}_n^\times$ for $[a], [b] \in \mathbf{Z}_n^\times$.
Associative: $([a] \cdot [b]) \cdot [c] = [(ab)c] = [a(bc)] = [a] \cdot ([b] \cdot [c])$
Commutative: $[a] \cdot [b] = [ab] = [ba] = [b] \cdot [a]$
Identity: $[1] \cdot [a] = [a] \cdot [1] = [a]$
Inverses: $[a]$ has a multiplicative inverse $[a]^{-1} \Leftrightarrow (a, n) = 1$, i.e., $[a] \in \mathbf{Z}_n^\times$.
We have already seen $|\mathbf{Z}_n^\times| = \varphi(n)$. □

Revisit Solving Linear Congruence:

$ax \equiv b \pmod{n} \quad \rightsquigarrow a_1 x \equiv b_1 \pmod{n_1}$ [Divide both sides by $d = (a, n)$]

$\rightsquigarrow [a_1]_{n_1} [x]_{n_1} = [b_1]_{n_1} \quad \rightsquigarrow [x]_{n_1} = [a_1]_{n_1}^{-1} [b_1]_{n_1}$ [Find $[a_1]_{n_1}^{-1}$ in $\mathbf{Z}_{n_1}^\times$]

$\rightsquigarrow$ d distinct solutions modulo n: $x + kn_1 \pmod{n}$, $k = 0, 1, \ldots, d-1$.

Example: Multiplication Table of $\mathbf{Z}_8^\times$

$\cdot_{[\ ]}$	$[1]$	$[3]$	$[5]$	$[7]$
$[1]$	$[1]$	$[3]$	$[5]$	$[7]$
$[3]$	$[3]$	$[1]$	$[7]$	$[5]$
$[5]$	$[5]$	$[7]$	$[1]$	$[3]$
$[7]$	$[7]$	$[5]$	$[3]$	$[1]$

- In each row, each element of the group occurs **exactly once**.
- In each column, each element of the group occurs **exactly once**.
- The table is symmetric w.r.t. the diagonal since $(\mathbf{Z}_8^\times, \cdot_{[\ ]})$ is abelian.

Examples from Matrices

$M_n(\mathbf{R})$ forms a group under matrix addition.

closure: ✓; **associativity:** ✓; **identity:** zero matrix; **inverses:** its negative

Moreover, $(M_n(\mathbf{R}), +)$ is abelian. □

$\mathrm{GL}_n(\mathbf{R}) := \{A \in M_n(\mathbf{R})\colon A \text{ is invertible, i.e., } \det(A) \neq 0\}$ is a group under matrix multiplication, called the **general linear group** of degree n over $\mathbf{R}$.

Closure: well-defined (by definition) & $\det(AB) = \det(A)\det(B)$

Associativity: *you should already see the proof in linear algebra course.*

Identity: the identity matrix I_n

Inverses: A has a multiplicative inverse $A^{-1} \Leftrightarrow \det(A) \neq 0$ i.e. $A \in \mathrm{GL}_n(\mathbf{R})$

However, $(\mathrm{GL}_n(\mathbf{R}), \cdot)$ is not abelian. □

Conjugacy

R is an **equivalence relation** if and only if for all $a, b, c \in S$ we have

Reflexive law: $a \sim a$;

Symmetric law: if $a \sim b$, then $b \sim a$;

Transitive law: if $a \sim b$ and $b \sim c$, then $a \sim c$.

Let G be a group and let $x, y \in G$. Write $x \sim y$ if there exists an element $a \in G$ such that $y = axa^{-1}$. In this case we say that y is a **conjugate** of x.

In particular, the relation $\sim$ defines an equivalence relation on G.

Reflexive law: $x = exe^{-1}$ for all $x \in G \quad \Rightarrow x \sim x$.

Symmetric law: $y = axa^{-1} \quad \Rightarrow x = a^{-1}ya$, i.e., $x \sim y$ implies $y \sim x$.

Transitive law: $y = axa^{-1}, z = byb^{-1} \Rightarrow z = baxa^{-1}b^{-1} = (ba)x(ba)^{-1}$
i.e., $x \sim y$ and $y \sim z$ implies $x \sim z$. □