LECTURE 7

September 20, 2023

Recall for $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ we define

(1) $a +_n b$ as the unique member of $\mathbb{Z}_n$ such that

$$a + b \equiv a +_n b \pmod{n}$$

(2) $a \cdot_n b$ as the unique member of $\mathbb{Z}_n$ such that

$$a \cdot b \equiv a \cdot_n b \pmod{n}$$

PROPOSITION 0.1. *Let $n \in \mathbb{N}$,*

(1) *The binary operation $+_n$ on $\mathbb{Z}_n$ satisfies the following:*
   (a) *$+_n$ is associative, i.e. for all $a, b, c \in \mathbb{Z}_n$,*

$$a +_n (b +_n c) = (a +_n b) +_n c$$

   (b) *0 is the identity element of $(\mathbb{Z}_n, +_n)$, i.e. for all $a \in \mathbb{Z}_n$, $0 +_n a = a +_n 0 = a$*
   (c) *Every $a \in \mathbb{Z}_n$ has an additive inverse, i.e. there exists a $b \in \mathbb{Z}_n$ such that $a +_n b = 0$.*

(2) *The binary operation $\cdot_n$ on $\mathbb{Z}_n$ satisfies the following:*
   (a) *$\cdot_n$ is associative, i.e. $a, b, c \in \mathbb{Z}_n$,*

$$a \cdot_n (b \cdot_n c) = (a \cdot_n b) \cdot_n c$$

   (b) *1 is the identity element of $(\mathbb{Z}_n, \cdot_n)$, i.e. for all $a \in \mathbb{Z}_n$, $1 \cdot_n a = a \cdot_n 1 = a$.*
   (c) *For $a \in \mathbb{Z}_n$, the following are equivalent:*
      (i) *a has a multiplicative inverse, i.e. there exists a $b \in \mathbb{Z}_n$ such that $a \cdot_n b = 1$.*
      (ii) $\gcd(a, n) = 1$

For example, in $\mathbb{Z}_4$, the multiplicative inverse of 3 is 3, since $3 \cdot 3 \equiv 1 \pmod{4}$, but 2 has no multiplicative inverse because $\gcd(2, 4) \neq 1$.

1. Multiplication and Addition Tables

We have formed tables for $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_4, \cdot_4)$ in the previous lecture:

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

2. Groups

Definition 2.1. Let G be a set with a binary operation $*$. The pair $(G, *)$ is called a group if the following are satisfied:

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

$$(a * b) * c = c * (a * b)$$

(2) There exists an identity element $e \in G$ of $(G, *)$, i.e. for any $a \in G$,

$$e * a = a * e = a$$

(3) Every member $a \in G$ has an inverse, usually denoted by $a^{-1} \in G$, such that

$$a * a^{-1} = a^{-1} * a = e$$

Example 2.2. $(\mathbb{Z}_n, +_n)$ is a group since

(1) $+_n$ is associative.
(2) 0 is an identity element.
(3) Every $a \in \mathbb{Z}_n$ has an inverse, usually denoted $-a \in \mathbb{Z}_n$, and we write $-a$ instead of a^{-1}.

Example 2.3. $(\mathbb{Z}_n, \cdot_n)$ is not a group. The first two conditions are satisfied, but there may not be any inverses. In particular, not all members have inverses.

Example 2.4. We want to show that $(\mathbb{Z}, +)$ is a group.

(1) $+$ is associative, i.e. $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{Z}$.
(2) 0 is the identity element, i.e. for all $a \in \mathbb{Z}$, $0 + a = a + 0 = a$.
(3) Every $a \in \mathbb{Z}$ has an additive inverse $-a \in \mathbb{Z}$ such that $a + (-a) = 0$.

Therefore, $(\mathbb{Z}, +)$ is a group.

Example 2.5. $(\mathbb{Z}, \cdot)$ is not a group since not all members have multiplicative inverses. Take $a = 7$, the only multiplicative inverse that will give us the identity 1, is $\frac{1}{7}$, which is not in $\mathbb{Z}$.

Notation 2.6. Let $(G, *)$ be a group. We call $|G|$ the order of G, i.e. the cardinality of G.

Example 2.7. The order of $(\mathbb{Z}_n, +_n)$ is n, while $(\mathbb{Z}, +)$ is of infinite order.

In this context, $(\mathbb{Z}_n, +_n)$ is a finite group of order n and $(\mathbb{Z}, +)$ is an infinite group.

Definition 2.8. A group $(G, *)$ is called *abelian* if the operation $*$ is commutative, i.e. for all $a, b \in G$,

$$a * b = b * a$$

EXAMPLE 2.9. The two groups $(\mathbb{Z}_n, +_n)$ and $(\mathbb{Z}, +)$ are both *abelian* since for all $a, b \in \mathbb{Z}_n$

$$a +_n b = b +_n a$$

and similar for $(\mathbb{Z}, +)$.

Note that not all groups are *abelian*. Recall that for $n \in \mathbb{N}$, $\mathcal{M}_n(\mathbb{R})$ denotes the set of all $n \times n$ matrices with real entries. With matrix multiplication and $\cdot$, this is not a group, because not all $A \in \mathcal{M}_n(\mathbb{R})$ has an inverse.

EXAMPLE 2.10. Take $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in \mathcal{M}_2(\mathbb{R})$, then $\det(A) = 0$, so A has no inverse.

NOTATION 2.11. For $n \in \mathbb{N}$, denote $GL_n(\mathbb{R})$ to be the set of all $n \times n$ invertible matrices with real entries.

EXAMPLE 2.12. $(GL_n(\mathbb{R}, \cdot)$ is a group. Indeed,

(1) $\cdot$ is associative, i.e. for all $A, B, C \in GL_n(\mathbb{R})$,

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)$$

(2) $I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$

(3) Every $A \in GL_n(\mathbb{R})$ has a multiplicative inverse $A^{-1} \in GL_n(\mathbb{R})$, i.e. $A \cdot A^{-1} = A^{-1} \cdot A = I_n$.

REMARK 2.13. $(GL_n(\mathbb{R}), \cdot)$ is not abelian. Indeed, take $n = 2$, $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, then

$$AB = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \quad BA = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$$

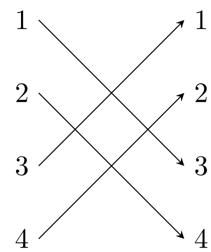
and so $AB \neq BA$, so $(GL_n(\mathbb{R}), \cdot)$ is not abelian.

3. Permutations

Let $X = \{a_1, a_2, ..., a_n\}$ be a set with distinct members. A bijection $\pi : X \to X$ is called a permutation. we will sometimes denote it as follows:

$$\pi = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ \pi(a_1) & \pi(a_2) & \pi(a_3) & \cdots & \pi(a_n) \end{pmatrix}$$

EXAMPLE 3.1. Let $X = \{1, 2, 3, 4\}$ and let $\pi : X \to X$. with the following:



Then

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

REMARK 3.2. When we shuffle the order of entries of π, we need to shuffle both the top and the bottom.

NOTATION 3.3. For a set X, denote S_X to be the collection of all permutations $\pi : X \to X$.

REMARK 3.4. If $|X| = n$, then $|S_X| = n!$.

EXAMPLE 3.5. If $X = \{1, 2\}$, then $S_X = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$.

EXAMPLE 3.6. If X is a nonempty set, the set $(S_X, \circ)$ is a group.