Lecture 4

Congruences and Residue Class Rings

Def. If X is a set, a map $\circ$

$$\circ : X \times X \to X$$

which sends a pair (x_1, x_2) of elements from X to the element $x_1 \circ x_2$ is called an operation on X.

Examples

1. $X = \mathbb{R}$ $\quad \circ = +$ (addition)
2. $X = \mathbb{R}$ $\quad \circ = \cdot$ (multiplication)

Def On the set $X = \mathbb{Z}/m\mathbb{Z}$ of the residue classes mod m we introduce two operations:

Let $a+m\mathbb{Z}$, $b+m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ are two residue classes.

- The sum of these residue classes is

$$a+m\mathbb{Z} + b+m\mathbb{Z} = (a+b)+m\mathbb{Z}$$

- The product of these two classes is

$$(a+m\mathbb{Z})\cdot(b+m\mathbb{Z}) = (a\cdot b)+m\mathbb{Z}.$$

In this definition we use representative elements of each class (in fact it is possible to select any other representative elements.) this definition is independent of the representatives.

Ex $(3+5\mathbb{Z}) + (4+5\mathbb{Z}) = 2+5\mathbb{Z}.$

$(3+5\mathbb{Z})\cdot(4+5\mathbb{Z}) = 2+5\mathbb{Z}.$

Def. Let $\circ$ be an operation on the set X. It is called associative if

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

holds for all $a, b, c \in X$.

It is called commutative if

$$a \circ b = b \circ a$$

for all $a, b \in X$.

Ex. Addition and multiplication in $\mathbb{Z}/m\mathbb{Z}$ are associative and commutative.

Def. A pair $(H, \circ)$ consisting of a set H and an associative operation $\circ$ on H is called a semigroup. This semigroup is called commutative or abelian if the operation $\circ$ is commutative.

Example. Let X is a set of $n \times n$ matrices, $M = (m_{ij})$ - matrix $m_{ij} \in \mathbb{R}$

- Operation $+$ is associative and commutative

$$A + (B + C) = (A + B) + C$$

$$A + B = B + A$$

- Operation $\cdot$ (multiplication) is associative but in general not commutative

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

A sufficient condition for matrices to be commutative

- A and B are symmetric
- $A \cdot B$ is also symmetric

Then : $AB = BA$.

Proof.

$$AB = (AB)^T = B^T \cdot A^T$$

$$= B \cdot A .$$

Examples.

Commutative semigroups

1. $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}/m\mathbb{Z}, +)$, $(\mathbb{Z}/m\mathbb{Z}, \cdot)$

2. $(M, \cdot)$ is a semigroup, but not an Abelian semigroup

T. Let $(H, \circ)$ be semigroup, and set for $a \in H$, $n \in \mathbb{N}$

$$a^1 = a, \quad a^{n+1} = a \circ a^n.$$

The following are true:

$$a^n \circ a^m = a^{n+m}, \quad (a^n)^m = a^{nm},$$

$n, m \in \mathbb{N}$.

If $a, b \in H$ and $a \circ b = b \circ a$ then

$$(a \circ b)^n = a^n \circ b^n. \qquad (*)$$

If the semigroup is commutative then $(*)$ is true in general

Proof of $(*)$ by using mathematical induction method.

1) $n = 1$

$$(a \circ b)^1 \overset{def}{=} a \circ b \overset{def}{=} a^1 \circ b^1$$

2) Let's assume that $(*)$ is true for

$\forall k$, $1 \leq k \leq n$.

Then

$$(a \circ b)^{n+1} \overset{def}{=} (a \circ b) \circ (a \circ b)^n$$

$$\overset{induct.}{=} (a \circ b) \circ (a^n \circ b^n)$$

$$\overset{associat.}{=} a \circ (b \circ a^n) \circ b^n$$

Let's consider

$$b \circ a^n \overset{def}{=} b \circ (a \circ a^{n-1}) = (b \circ a) \circ a^{n-1}$$

$$\overset{commut}{=} (a \circ b) \circ a^{n-1} = a \circ (b \circ a^{n-1})$$

$$= a \circ (b \circ a \circ a^{n-2}) = a \circ a \circ (b \circ a^{n-2})$$

$$= a^2 \circ (b \circ a^{n-2}) = \dots = a^n \circ b$$

$$(a \circ b)^{n+1} = a \circ (a^n \circ b) \circ b^n$$

$$= (a \circ a^n) \circ (b \circ b^n) \overset{def}{=} a^{n+1} \circ b^{n+1}$$ ▷

Def. A neutral element of the semigroup $(H, \circ)$ is an element $e \in H$ which satisfies

$$e \circ a = a \circ e = a \quad \text{for all } a \in H.$$

If the semigroup contains a neutral element, then it is called **monoid**.

A semigroup has at most one neutral element. (give a proof).

Def. If e is the neutral element of the semigroup $(H, \circ)$ and $a \in H$, then $b \in H$ is called an inverse of a of

$$a \circ b = b \circ a = e.$$

If a has an inverse, then it is called invertible in H.

Examples.

1. $(\mathbb{Z}, +)$ the neutral element is $e = 0$.

The inverse of a is $(-a)$

2. $(\mathbb{Z}, \cdot)$ the neutral element is $e = 1$.

The only invertible elements are $1, (-1)$.

$$1 \cdot 1 = 1 \quad , \quad (-1) \cdot (-1) = 1.$$

3. $(\mathbb{Z}/m\mathbb{Z}, +)$ the neutral element is the ~~zero~~ residue class $m\mathbb{Z}$.

The inverse of $a + m\mathbb{Z}$ is $(-a) + m\mathbb{Z}$.

4. $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ the neutral element is $1 + m\mathbb{Z}$. The inverse element exist not always

We will see later how to find the inverse element of $a + m\mathbb{Z}$:

$b + m\mathbb{Z}$ such that

$$(a \cdot b) + m\mathbb{Z} = 1 + m\mathbb{Z}.$$

Equation for $a + m\mathbb{Z}$:

$$a \cdot b \equiv 1 \mod m$$

has a solution if and only if.

$$\gcd(a, m) = 1$$

The the euclidean algorithm can be used to solve equation

$$ax + my = 1. \quad \text{and} \quad b = x.$$

Take $3 + 5\mathbb{Z}$, then $\gcd(3, 5) = 1$

and for $3x + 5y = 1$

the solution $x = 2, y = 1$

The inverse element

$$2 + 5\mathbb{Z}.$$

Groups

Def. A **group** is a monoid (it has a neutral element in semigroup) in which any element is invertible.

The group is called **commutative** (or **abelian**) if the monoid is commutative

Ex.

1. The monoid $(\mathbb{Z}, +)$ is an abelian group.
2. The monoid $(\mathbb{Z}, \cdot)$ is not a group, because not every element is invertible.
3. The monoid $(\mathbb{Z}/m\mathbb{Z}, +)$ is an abelian group.
4. $(\mathbb{Z}/m\mathbb{Z}, \cdot)$ is not always a group.

Let's give a sufficient condition to define a group.

If m is a prime number, then

$\forall a \in \{1, 2, \dots, m\}$

$$\gcd(a, m) = 1$$

and inverse a^{-1} exists.

Def. The order of a group (or a semigroup) is the number of its elements.

Ex.
1. $(\mathbb{Z}, +)$ has infinite order
2. $(\mathbb{Z}/m\mathbb{Z}, +)$ has order m.