MATH 2022 Linear and Abstract Algebra

LECTURE 03 Thursday 27/02/2020

Introducing groups

Recall that a field F is an arithmetic with $+, \cdot$ having at least two elements (in fact $1 \neq 0$) satisfying six axioms:

(1) $(\forall a, b, c \in F) \quad (a+b)+c = a+(b+c), \quad (ab)c = a(bc)$

(associativity)

(2) $(\forall a, b \in F) \quad a+b = b+a, \quad ab = ba$

(commutativity)

(3) $(\forall a, b, c \in F) \quad (a+b)c = ab + ac$

(distributivity)

(4) $(\exists\, 0,1 \in F)(\forall a \in F) \quad a+0 = 0+a = a, \quad a1 = 1a = a$

(existence of additive & multiplicative identity elements)

(5) $(\forall a \in F)(\exists b \in F) \quad a+b = b+a = 0$

(existence of negatives, $b = -a$)

(6) $(\forall a \in F \setminus \{0\})(\exists b \in F) \quad ab = ba = 1$

(existence of multiplicative inverses of nonzero elements, $b = a^{-1}$)

Subtraction in F: Define, for $a, b \in F$,

$$\boxed{a - b = a + (-b)}.$$

In particular,

$$a - a = a + (-a) = 0.$$

Division in F: Define for $a \in F$, $b \in F \setminus \{0\}$,

$$\boxed{a \div b = \frac{a}{b} = ab^{-1}}.$$

In particular,

$$b \div b = \frac{b}{b} = bb^{-1} = 1.$$

Focussing attention on just one operation leads to the notion of a group.

A group G is an arithmetic with respect to a binary operation $*$ satisfying

(1) $(\forall a, b, c \in G) \quad (a*b)*c = a*(b*c)$

(associativity)

(2) $(\exists e \in G)(\forall a \in G) \quad a*e = e*a = a$

(existence of an identity element e)

(3) $(\forall a \in G)(\exists b \in G) \quad a*b = b*a = e$

(existence of inverses $b = a^{-1}$)

A group G is an arithmetic with respect to a binary operation $*$ satisfying

(1) $(\forall a,b,c \in G) \quad (a*b)*c = a*(b*c)$

(associativity)

(2) $(\exists e \in G)(\forall a \in G) \quad a*e = e*a = a$

(existence of an identity element e)

(3) $(\forall a \in G)(\exists b \in G) \quad a*b = b*a = e$

(existence of inverses $b = a^{-1}$)

If $*$ is commutative, that is,

(4) $(\forall a,b \in G) \quad a*b = b*a$

then G is called abelian (after Abel (1802-29))

From conditions (1), (2), (4), (5) listed earlier for a field F, we have

> $(F, +)$ is an abelian group, with identity element 0, and group inverses are negatives.

From conditions (1), (2), (4), (6) for a field F,

> $(F \setminus \{0\}, \cdot)$ is an abelian group, with identity element 1, and group inverses are reciprocals.

In the case of modular arithmetic, where $n \in \mathbb{Z}^+$,

$(\mathbb{Z}_n, +)$ is an abelian group, with identity element 0, and group inverses are negatives.

can reach everything by adding 1 to itself successively:

$$1,\ 1+1=2,\ 1+1+1=3,\ \dots,\ \underbrace{1+1+1+\cdots+1}_{n-1 \text{ times}} = n-1,$$

$$\underbrace{1+1+1+\cdots+1+1}_{n \text{ times}} = 0,$$ and then the cycle repeats.

In the case of modular arithmetic, where $n \in \mathbb{Z}^+$,

$(\mathbb{Z}_n, +)$ is an abelian group, with identity element 0, and group inverses are negatives.

can reach everything by adding 1 to itself successively:

$1,\ 1+1=2,\ 1+1+1=3,\ \dots,\ \underbrace{1+1+1+\dots+1}_{n-1 \text{ times}} = n-1,$

$\underbrace{1+1+1+\dots+1+1}_{n \text{ times}} = 0$, and then the cycle repeats.

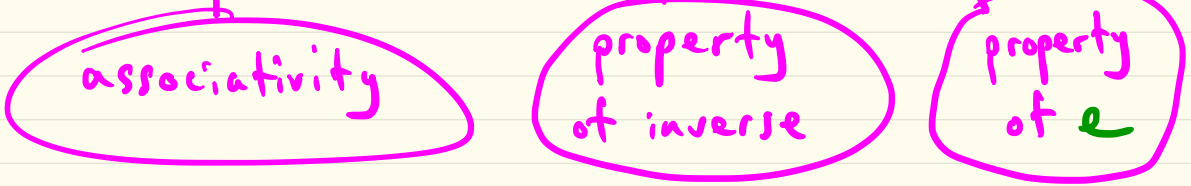
We say $(\mathbb{Z}_n, +)$ is a cyclic group with generator 1.

The invertibility condition of a group G provides flexibility and movement:

If $a, b \in G$ then we can

"get from a to b":

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



This facilitates solving equations:

$$a * x = b \implies a^{-1} * (a * x) = a^{-1} * b$$

$$\implies (a^{-1} * a) * x = a^{-1} * b$$

$$\implies e * x = a^{-1} * b$$

$$\implies x = a^{-1} * b$$

analogous to manipulations involving invertible matrices

This facilitates solving equations:

$$a * x = b \implies a^{-1} * (a * x) = a^{-1} * b$$

$$\implies (a^{-1} * a) * x = a^{-1} * b$$

$$\implies e * x = a^{-1} * b$$

$$\implies x = a^{-1} * b$$

analogous to manipulations involving invertible matrices

Indeed, put

$$G = \{ \text{invertible } n \times n \text{ matrices over } F \}$$

where $n \in \mathbb{Z}^+$ and F is a field, and let $*$ be matrix multiplication.

Indeed, put

$$G = \{ \text{invertible } n \times n \text{ matrices over } F \}$$

where $n \in \mathbb{Z}^+$ and F is a field, and let $*$ be matrix multiplication.

If $A, B \in G$ then

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I$$

so that $AB \in G$ with inverse $(AB)^{-1} = B^{-1}A^{-1}$.

Indeed, put

$$G = \{ \text{invertible } n \times n \text{ matrices over } F \}$$

where $n \in \mathbb{Z}^+$ and F is a field, and let $*$ be matrix multiplication.

If $A, B \in G$ then

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I$$

so that $AB \in G$ with inverse $(AB)^{-1} = B^{-1}A^{-1}$.

$A^{-1} \in G$ since $(A^{-1})^{-1} = A$

Hence $*$ is a binary operation on G and the conditions defining a group are satisfied:

✓ (1) $*$ is associative.

✓ (2) I is the identity element.

✓ (3) $A \in G \Rightarrow A^{-1} \in G$ and $AA^{-1} = A^{-1}A = I$.

However, for $n \geq 2$, $*$ is not commutative,

e.g. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$

$\neq$ (not equal)

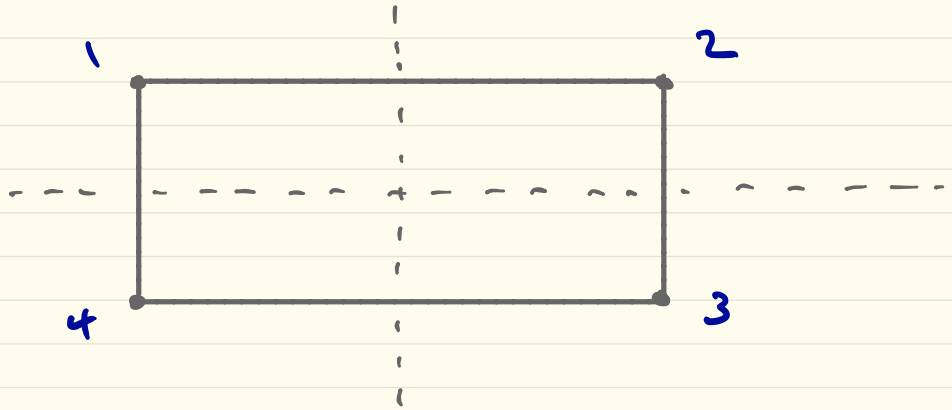
$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

so this G is <u>not</u> abelian.

(In fact, most groups are not abelian.)

Example: Consider the group

$G = \{$ symmetries of the rectangle $\}$.

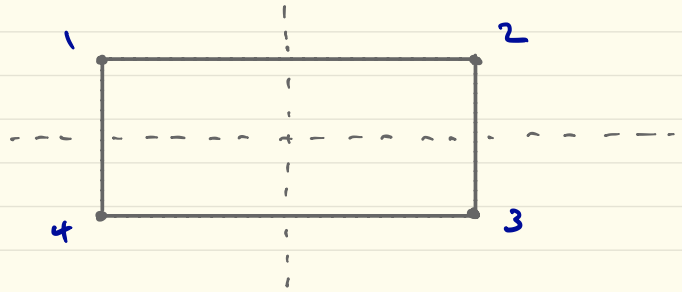


Operation on G is $*$, which is

composition of symmetries (following one after the other).

Example:

G = { symmetries of the rectangle }



$G = \{ 1, A, B, C \}$ where

1 = identity symmetry ("do nothing")

A = 180° rotation

B = reflection in vertical axis

C = reflection in horizontal axis

	1	A	B	C
1	1	A	B	C
A	A	1	C	B
B	B	C	1	A
C	C	B	A	1

The group is abelian (table symmetric about diagonal).