

Math103A  
Modern Algebra

seraph

October 14, 2024

# Contents

<b>1</b>	<b>Group and Subgroups</b>	<b>2</b>
1.1	Binary Operators . . . . .	2
1.2	Groups . . . . .	4
1.3	Abelian Groups . . . . .	5

# Chapter 1

## Group and Subgroups

### Lecture 2

#### 1.1 Binary Operators

**Definition 1.1.1.** A binary operation  $*$  on  $S$  is a function mapping every element in  $S \times S$  into  $S$

**Exercise.** Let  $M(\mathbb{R}) =$  set of all square matrices in  $\mathbb{R}$ , is  $+$  a binary operator on  $M$  ?

**Answer.** No, because different sized matrices cannot add together. ⊛

**Exercise.** Let  $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ , then we define  $a * b = c$  s.t.  $c$  is at least 5 more than  $a + b$ , is  $*$  a binary operator ?

**Answer.** No, because the output isn't unique.  $1 * 2 = \{8, 9, 10, \dots\}$ . ⊛

**Definition 1.1.2.** If  $(S, *)$  is a binary algebraic structure, then  $H \subseteq S$  is closed under this operation iff  $\forall a, b \in H, a * b \in H$

**Note.** If  $M_2(\mathbb{R})$  are all  $2 \times 2$  matrices over  $\mathbb{R}$ , then  $(M_2(\mathbb{R}), +)$  is a proper algebraic structure.

**Exercise.** If  $H \subseteq M_2(\mathbb{R})$ ,  $H = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$ , is  $H$  closed under  $+$  ?

**Answer.** Yes ⊛

**Proof.**  $\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} a+c & -(b+d) \\ b+d & a+c \end{bmatrix} \in H$  ■

**Exercise.** Let  $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ , is  $\mathbb{C}$  closed under addition and multiplication?

**Answer.** Yes, using Euler's formula we know that  $a + bi = \sqrt{a^2 + b^2}e^{i\theta}$ , so it will stay complex under  $+$  and  $\times$ . ⊛

**Exercise.** Let  $H \subseteq \mathbb{C}$  and  $H = \{a + bi : \sqrt{a^2 + b^2} = 1\}$ , is  $H$  closed under addition / multiplication?

**Answer.** It is closed under multiplication but not addition. ⊛

**Example.** Let  $(S, *)$  and  $(S', *)$  be two algebraic structures, we want to show whether they are the same.

**Answer.** Need to consider basic properties:  $*$  is commutative  $\Leftrightarrow a * b = b * a$

Let  $\mathcal{F}$  = the set of functions  $f : \mathbb{R} \rightarrow \mathbb{R}$ , we argue that  $f \circ g$  is not commutative ⊗

**Proof.**  $\circ$  is not commutative on  $\mathcal{F}$  because lets say  $h = \sin(x)$ ,  $g = e^x$ , then

$$h \circ g = h(g(x)) = \sin(e^x) \in \mathcal{F}$$

$$g \circ h = g(h(x)) = e^{\sin(x)} \in \mathcal{F}$$

but  $\sin(e^x) \neq e^{\sin(x)}$ , so back to the question, it may or may not be the same depending on what  $*$  is. ■

**Definition 1.1.3.** If we have a structure  $(\mathcal{F}, \circ)$ , then  $\circ$  is associative, i.e.  $f \circ (g \circ h) = (f \circ g) \circ h$

**Proof.** Computing them shows that they are equal

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x)))$$

■

**Exercise.**  $\mathbb{Z}^+ = \{1, 2, 3, 4, \dots\}$ , ans define  $a * b = 2^{a \cdot b}$ , is  $(\mathbb{Z}^+, *)$  1. commutative, 2. associative ?

**Answer.**

1. Yes,  $a * b = 2^{a \cdot b} = 2^{b \cdot a} = b * a$

2. No,  $2 * (3 * 4) \neq (2 * 3) * 4$  ⊗

**Exercise.** Given  $(S, *)$  where  $*$  is commutative and associative. Given  $H \subseteq S$  where  $H = \{a \in S : a * a = a\}$ , show that  $H$  is closed under  $*$ .

**Proof.**  $a * a = a$  and  $b * b = b$ , we can show  $[a * b] * [a * b] = [a * b]$  because by associativity and commutativity

$$[a * b] * [a * b] = a * b * a * b = a * a * b * b = a * b$$

■

## Lecture 3

**Definition 1.1.4.** Let  $(S, *)$  be an algebraic structure, and  $e \in S$  s.t.  $\forall a \in S, a * e = a = e * a$  Then  $e$  is called the identity element of  $S$ .

**Example.**

$(\mathbb{Z}, +)$  has identity element 0.

$(\mathbb{Z}^+, \times)$  has identity element 1.

$(\mathbb{Z}^+, +)$  has no identity element.

**Theorem 1.1.1.** If  $(S, *)$  has an identity element, it is unique.

**Proof.** For sake of contradiction, suppose  $e$  and  $e'$  are both identity elements of  $S$ . Then  $e = e * e' = e'$ . ■

**Definition 1.1.5.** Let  $(S, *)$  be an algebraic structure, and  $x \in S$ . If  $\exists x' \in S$  s.t.  $x * x' = x' * x = e$ , then  $x'$  is called the inverse of  $x$ .

**Example.**

- $(\mathbb{Z}, +)$ , the inverse of  $a$  is  $-a$ .
- $(\mathbb{Z}^+, +)$ , has no inverses
- $(\mathbb{Z}, \times)$ , the inverse of  $a$  is  $\frac{1}{a}$  if  $a \neq 0$ .

## 1.2 Groups

**Definition 1.2.1.** A group is an algebraic structure  $(G, *)$  if:

1.  $*$  is associative.
2.  $\exists$  an identity element  $e \in G$ .
3.  $\forall a \in G, \exists$  an inverse  $a' \in G$ .

**Example.**  $G = \{e, a, b\}$  where

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad a = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}, \quad b = \begin{bmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}$$

$(G, \times)$  where  $\times$  is standard matrix multiplication is a group.

$(G, +)$  where  $+$  is standard matrix addition is not a group because it is not closed under addition.

**Definition 1.2.2.** A group  $(G, *)$  is **abelian** if  $\forall a, b \in G, a * b = b * a$ .

**Example.** Consider  $(\mathbb{Q}^+, *)$  where  $*$  is defined by  $a * b = \frac{ab}{2}$ .

**Associativity:** For any  $a, b, c \in \mathbb{Q}^+$ ,

$$(a * b) * c = \left(\frac{ab}{2}\right) * c = \frac{\left(\frac{ab}{2}\right)c}{2} = \frac{abc}{4} = a * (b * c)$$

Thus,  $*$  is associative.

**Identity element:** We need  $e \in \mathbb{Q}^+$  such that  $\forall a \in \mathbb{Q}^+$ ,

$$a * e = \frac{ae}{2} = a \quad \text{and} \quad e * a = \frac{ea}{2} = a$$

Solving  $\frac{ae}{2} = a$  gives  $e = 2$ . Thus, 2 is the identity element.

**Inverses:** For any  $a \in \mathbb{Q}^+$ , we need  $a' \in \mathbb{Q}^+$  such that

$$a * a' = \frac{aa'}{2} = 2 \quad \text{and} \quad a' * a = \frac{a'a}{2} = 2$$

Solving  $\frac{aa'}{2} = 2$  gives  $a' = \frac{4}{a}$ . Thus, every element has an inverse.

Therefore,  $(\mathbb{Q}^+, *)$  is a group.

**Commutativity:** For any  $a, b \in \mathbb{Q}^+$ ,

$$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$$

Thus,  $(\mathbb{Q}^+, *)$  is an abelian group.

**Theorem 1.2.1.** Let  $(G, *)$  be a group. Then

1. The identity element is unique ([Theorem 1.1.1](#)).
2. Every element has a unique inverse .

**Proof.** Let  $a, a', a''$  be inverses of  $a \in G$ . Then  $a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$ . ■

**Corollary 1.2.1.** Let  $(G, *)$  be a group and  $a, b \in G$ . If  $a * b \in G$ , then the inverse of  $(a * b)$  is  $b' * a'$ , where  $b'$  is the inverse of  $b$  and  $a'$  is the inverse of  $a$ .

**Proof.**

$$\begin{aligned}(a * b) * (b' * a') &= a * (b * b') * a' = a * e * a' = a * a' = e \\ (b' * a') * (a * b) &= b' * (a' * a) * b = b' * e * b = b' * b = e\end{aligned}$$

■

## Lecture 4

### 1.3 Abelian Groups

**Example.**  $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$  is an abelian group under addition.

**Example.** Let  $\mathbb{R}^2 = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} : a, b \in \mathbb{R} \right\}$ ,  $(\mathbb{R}^2, +)$  is an abelian group.

**Example.** Let  $\mathbb{P}_1 = \{ax + b : a, b \in \mathbb{R}\}$ . ,  $(\mathbb{P}_1, +)$  is an abelian group.

**Definition 1.3.1.** A **group isomorphism** is a bijective group homomorphism. Specifically, if  $(G, *_1)$  and  $(H, *_2)$  are groups, a function  $\phi : G \rightarrow H$  is called a group isomorphism if:

1.  $\phi$  is a homomorphism, i.e.,  $\forall a, b \in G, \phi(a *_1 b) = \phi(a) *_2 \phi(b)$ .
2.  $\phi$  is bijective, i.e.,  $\phi$  is both injective (one-to-one) and surjective (onto).

If such a function  $\phi$  exists, we say that  $G$  and  $H$  are **isomorphic** and write  $G \cong H$ .

**Exercise.** Let  $(\mathbb{Z}, +)$  and  $(2\mathbb{Z}, +)$  be groups under addition. Define the function  $\phi : \mathbb{Z} \rightarrow 2\mathbb{Z}$  by  $\phi(n) = 2n$  for all  $n \in \mathbb{Z}$ . Do we have an isomorphism between  $(\mathbb{Z}, +)$  and  $(2\mathbb{Z}, +)$ ?

1.  $\phi$  is a homomorphism: For all  $a, b \in \mathbb{Z}$ ,

$$\phi(a + b) = 2(a + b) = 2a + 2b = \phi(a) + \phi(b).$$

2.  $\phi$  is bijective:

- Injective: Suppose  $\phi(a) = \phi(b)$ . Then  $2a = 2b$ , which implies  $a = b$ . (For an output check if the input are the same)
- Surjective: For any  $m \in 2\mathbb{Z}$ , there exists  $n \in \mathbb{Z}$  such that  $m = 2n$ . Hence,  $\phi(n) = m$ .

Therefore,  $\phi$  is an isomorphism, and  $(\mathbb{Z}, +) \cong (2\mathbb{Z}, +)$ .

## Lecture 5

### 1.3.1 More Abelian Examples

**Example.**  $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$  where  $+_n$  is addition modulo  $n$ . When  $a, b \in \mathbb{Z}_n$ ,  $a +_n b = (a+b) \bmod n$ .

- Many groups are isomorphic to  $\mathbb{Z}_n$ .

**Remark (Fact).** Any group of size 1 is isomorphic to  $\mathbb{Z}_1$ .

**Example.** If we have a group  $\mathbb{Z}_2 = \{0, 1\}$  equipped with  $(\mathbb{Z}_2, +)$  and an abstract group  $G = \{e, a\}$ . Do these groups have the same structure?

**Answer.** We can check its operation table.

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \cong \begin{array}{c|cc} * & e & a \\ \hline e & e & a \\ a & a & e \end{array}$$

⊛

**Remark (Fact).** Any group of size 2 is isomorphic to  $\mathbb{Z}_2$ .

**Example.** Let  $G = \{I, A, B\}$  where  $I$  is the identity matrix,  $A = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$ , and  $B = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$ . Is this group isomorphic to  $\mathbb{Z}_3$ ?

**Answer.** This is also isomorphic to  $\mathbb{Z}_3$ .  
We can check it using the same method as above.

⊛

**Remark (Fact).** All groups on 3 elements is isomorphic to  $\mathbb{Z}_3$ .

**Theorem 1.3.1.** Let  $(G, *)$  be a group. If we fix  $a, b \in G$ , then:

1.  $a * x = b$  has a unique solution for  $x$ .
2.  $y * a = b$  has a unique solution for  $y$ .

**Example.**  $\mathbb{Z}_4 = \{0, 1, 2, 3\}$  and the Klein 4-group  $V_4 = \{e, a, b, c\}$  with their operation tables:

$$\begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array} \not\cong \begin{array}{c|cccc} * & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array}$$

**Proof.** Check the diagonals and it is clear that they are not isomorphic. ■

**Theorem 1.3.2.** Every group on 4 elements is isomorphic to either  $(\mathbb{Z}_4, +)$  or  $(V, *)$ .

**Partial proof.** Generate all possible tables and check if they are isomorphic to  $(\mathbb{Z}_4, +)$  or  $(V, *)$ . Turns out they will only be isomorphic to one of these two groups. ■