35003 MODERN ALGEBRA

Prof Murray Elder, UTS

Week 1:

Lauritzen 2.1, 2.2

DEFINITION

Let G be a set.

A map $\circ\colon G \times G$ to G is called a *composition* on G.

$\circ(g_1, g_2) \in G$

$G = \mathbb{Z}$ $\{\ldots -2, -1, 0, 1, 2 \ldots\}$

$3 + 7$

$3 \div 7$

$\frac{3}{7}$ $\times$

$+ (3, 7)$

$= 10$

DEFINITION

Let G be a set.

A map $\circ\colon G \times G$ to G is called a *composition* on G.

We write $\circ(x, y)$ as $x \circ y$ or just xy when the map is understood.

Let G be a set.

A map $\circ : G \times G$ to G is called a *composition* on G.

We write $\circ(x, y)$ as $x \circ y$ or just xy when the map is understood.

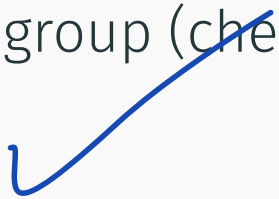
Definition (2.1.1)

A pair $(G, \circ)$ consisting of a set G and a composition $\circ$ on G is called a *group* if :

1. the composition is *associative*: $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$
2. $\exists e \in G$ with the property that $e \circ a = a \circ e = a$ for all $a \in G$, we call e an *identity* for $(G, \circ)$
3. $\forall a \in G \exists b \in G$ such that $a \circ b = e = b \circ a$, we call b an *inverse* for a

EG

$\mathbb{Z}$ with the operation of addition: $(\mathbb{Z}, +)$ is a group (check the axioms)



EG

$\mathbb{Z}$ with the operation of addition: $(\mathbb{Z}, +)$ is a group (check the axioms)

$(\mathbb{N}, +)$ is not a group (no inverses)

$\mathbb{Z}$ with the operation of addition: $(\mathbb{Z}, +)$ is a group (check the axioms)

$(\mathbb{N}, +)$ is not a group (no inverses)

2. Je =

Matrices of the same size with entries in $\mathbb{R}$ with addition of matrices?

$$\begin{bmatrix} \pi & 3 \\ -7.2 & 0 \\ 1 & \sqrt{} \end{bmatrix} + \begin{bmatrix} -\pi & -3 \\ 7.2 & 0 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} \pi & 3 \\ -7.2 & 0 \\ 1 & 1 \end{bmatrix}$$

3×2

$A + (-1A)$

EG

$\mathbb{Z}$ with the operation of addition: $(\mathbb{Z}, +)$ is a group (check the axioms)

$(\mathbb{N}, +)$ is not a group (no inverses)

Matrices of the same size with entries in $\mathbb{R}$ with addition of matrices?

Square matrices of the same size with entries in $\mathbb{R}$ with multiplication of matrices?

Eg: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 4 & 2 \\ -4 & -2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

LEMMA 1

Unique.

If $(G, \circ)$ is a group, then it has exactly one element e which satisfies $e \circ a = a \circ e = a$ for all $a \in G$.

Proof: Contradiction

Suppose $\exists e, f \in G$ distinct both satisfy Ax. 2.

$e = e \circ f = f$ which is a contrad.

treat f as in Ax 2

treating e as in Ax 2.

LEMMA 1

If $(G, \circ)$ is a group, then it has exactly one element e which satisfies $e \circ a = a \circ e = a$ for all $a \in G$.

Proof: Suppose f also satisfies this and $f \neq e$, then

$$\begin{aligned} f &= e \circ f \quad \text{where } e \text{ is acting like the identity, and } f \text{ is arbitrary} \\ &= e \quad \text{where } f \text{ is acting like the identity, and } e \text{ is arbitrary} \end{aligned}$$

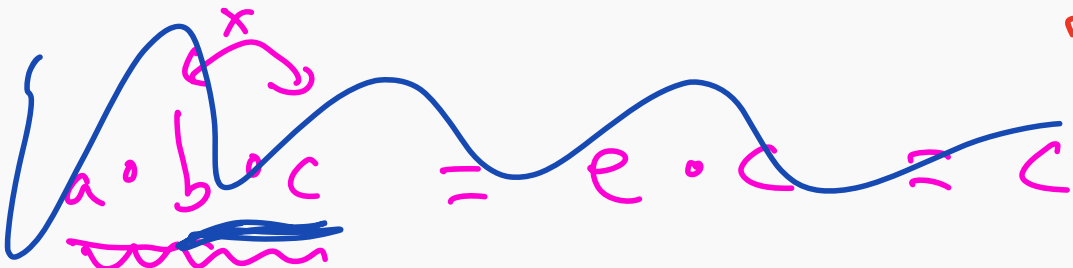
which contradicts that $f \neq e$.

LEMMA 2

If $(G, \circ)$ is a group and $a \in G$, then there is exactly one element b which satisfies $b \circ a = e = a \circ b$.

Proof: Suppose $\exists\ c$ also acting like inverse of a.

$b \neq c$



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

$b \circ e = b$ assoc. 1. inv. 3. ident. 2.

$(\mathbb{Z}, +)$

$7 + (-7)$

So $b = c$ contradiction

LEMMA 2

If $(G, \circ)$ is a group and $a \in G$, then there is exactly one element b which satisfies $b \circ a = e = a \circ b$.

Proof: Suppose c also satisfies this and $c \neq b$. Then

$$\begin{aligned} b &= b \circ e \\ &= b \circ (a \circ c) && \text{where } c \text{ is acting like the inverse of } a \\ &= (b \circ a) \circ c && \text{associativity} \\ &= e \circ c && \text{where } b \text{ is acting like the inverse of } a \\ &= c \end{aligned}$$

which contradicts that $b \neq c$.

We call a group $(G, \circ)$ *abelian* if $a \circ b = b \circ a$ for all $a, b \in G$.

EG $(\mathbb{Z}, +)$

$(M_{n,m}, +)$

$(M_{n,n}$ with $\det \neq 0$ over $\mathbb{R}$, $\times$ matrix mult$)$ $GL_n(\mathbb{R})$

ABELIAN

We call a group $(G, \circ)$ *abelian* if $a \circ b = b \circ a$ for all $a, b \in G$.

Eg: $(\mathbb{Z}, +)$

ABELIAN

We call a group $(G, \circ)$ *abelian* if $a \circ b = b \circ a$ for all $a, b \in G$.

Eg: $(\mathbb{Z}, +)$

$n \times n$ matrices over $\mathbb{R}$ with determinant equal to 1 and
$\circ$ =multiplication of matrices?

not abelian

ORDER OF A GROUP

size

$|G|$ (the cardinality of the set G) is called the *order* of the group $(G, \circ)$.

$(\mathbb{Z}, +)$ countably inf.

$(\mathbb{R}, +)$ uncountably inf.

ORDER OF A GROUP

$|G|$ (the cardinality of the set G) is called the *order* of the group $(G, \circ)$.

It is interesting to study

- finite groups (classify all of them up to isomorphism)

ORDER OF A GROUP

$|G|$ (the cardinality of the set G) is called the *order* of the group $(G, \circ)$.

It is interesting to study

- finite groups (classify all of them up to isomorphism)
- countably infinite groups (discrete groups)

ORDER OF A GROUP

$|G|$ (the cardinality of the set G) is called the *order* of the group $(G, \circ)$.

It is interesting to study

- finite groups (classify all of them up to isomorphism)
- countably infinite groups (discrete groups)
- uncountable groups (here ideas from Topology help)

ORDER OF AN ELEMENT

If $a \in G$, we can define $a \circ a$ to be $a^2 \in G$, then $a \circ (a^2)$ can be defined as a^3, and so on.

ORDER OF AN ELEMENT

If $a \in G$, we can define $a \circ a$ to be $a^2 \in G$, then $a \circ (a^2)$ can be defined as a^3, and so on.

We can also define $a^0 = e$.

a^{-1} the element from Ex. 3. inverse.

$a^{-2}, a^{-1}, a^0, a^1, a^2, a$

$(a^{-1} \circ a^{-1}) \circ (a \circ a)$

e

$= e$

ORDER OF AN ELEMENT

$(\mathbb{Z}, +)$

If $a \in G$, we can define $a \circ a$ to be $a^2 \in G$, then $a \circ (a^2)$ can be defined as a^3, and so on.

We can also define $a^0 = e$.

Suppose $a^j = a^i$ for some $0 \leqslant i < j$, that is, you take powers and at some point see the same element twice (and suppose this is the first repeat)

$\exists$ smaller $n \in \mathbb{N}_+$ so that $a^n = e$

$j - i$

$a^1 \quad a^2 \quad a^3 \quad \cdots \quad a^i \quad \cdots$

a^j

$a^{j-i} = a^j \circ a^{-i} = a^i \circ a^{-i} = e$

$a \circ a \circ a \cdots a \circ a^{-1} \circ a^{-1} \circ \cdots a^{-1}$

ORDER OF AN ELEMENT

If $a \in G$, we can define $a \circ a$ to be $a^2 \in G$, then $a \circ (a^2)$ can be defined as a^3, and so on.

We can also define $a^0 = e$.

Suppose $a^j = a^i$ for some $0 \leqslant i < j$, that is, you take powers and at some point see the same element twice (and suppose this is the first repeat)

Then if b is an inverse of a, $b^i a^j = a^{j-i} = e$ so the first repeated element you will see starting from $a^0 = e$ is e.

ORDER OF AN ELEMENT

If $a \in G$, we can define $a \circ a$ to be $a^2 \in G$, then $a \circ (a^2)$ can be defined as a^3, and so on.

We can also define $a^0 = e$.

Suppose $a^j = a^i$ for some $0 \leqslant i < j$, that is, you take powers and at some point see the same element twice (and suppose this is the first repeat)

Then if b is an inverse of a, $b^i a^j = a^{j-i} = e$ so the first repeated element you will see starting from $a^0 = e$ is e.

Definition

If $a \in G$ and $n \in \mathbb{N}_+$ is minimal so that $a^n = e$, we say a has *order* n, and otherwise if no such positive integer exists, we say a has infinite order.

EG

Eg $\mathbb{Z}/12\mathbb{Z} = \{0, \ldots, 11\}$

$1 + 2 \equiv 3$

$10 + 7 \equiv 5$

Define $\mathbb{Z}/c\mathbb{Z}$ to be the set $\{0, 1, \ldots, c-1\}$ with the operation $x \circ y = x + y \mod c$.

Order of 4 in $(\mathbb{Z}/12\mathbb{Z}, +\text{mod } c)$? 3

How about the same set with the operation $x \circ y = xy \mod c$?

Exercise.

$4 + 4 + 4 = 0$

order of 6 = 2

order of 7 = 12

$7 \quad 14 \quad 21 = 11$

$\quad 2 \quad 9 \quad 16$

ASSOCIATIVITY

In general, checking associativity axiom can be difficult.

ASSOCIATIVITY

In general, checking associativity axiom can be difficult.

Suppose G is a set of maps from X to X (where X is just some set) with $\circ$ defined by function composition

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

ASSOCIATIVITY

In general, checking associativity axiom can be difficult.

Suppose G is a set of maps from X to X (where X is just some set) with $\circ$ defined by function composition

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

Then $f(g(h(x)))$ clearly doesn't matter which order you apply the maps.

ASSOCIATIVITY

In general, checking associativity axiom can be difficult.

Suppose G is a set of maps from X to X (where X is just some set) with $\circ$ defined by function composition

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

Then $f(g(h(x)))$ clearly doesn't matter which order you apply the maps.

Eg: set of bijective maps which send $X = \{1, 2, 3\}$ to $\{1, 2, 3\}$ is called S_3. (Symmetric group.)

$$f: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad g: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$f \circ g(1) = f(g(1)) = f(3) = 3$$

ASSOCIATIVITY

In general, checking associativity axiom can be difficult.

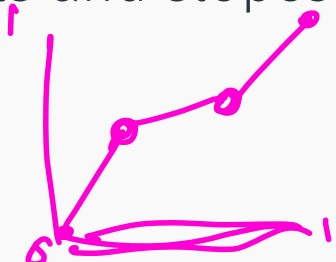
Suppose G is a set of maps from X to X (where X is just some set) with $\circ$ defined by function composition

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

Then $f(g(h(x)))$ clearly doesn't matter which order you apply the maps.

Eg: set of maps which send $X = \{1, 2, 3\}$ to $\{1, 2, 3\}$ is called S_3.

Eg: set of piecewise linear maps sending $[0, 1]$ to $[0, 1] \subset \mathbb{R}$ with breakpoints at dyadic rationals and slopes powers of 2, and $0 \mapsto 0, 1 \mapsto 1$.



Thompson's group F.

ASSOCIATIVITY

In general, checking associativity axiom can be difficult.

Suppose G is a set of maps from X to X (where X is just some set) with $\circ$ defined by function composition

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

Then $f(g(h(x)))$ clearly doesn't matter which order you apply the maps.

Eg: set of maps which send $X = \{1, 2, 3\}$ to $\{1, 2, 3\}$ is called S_3.

Eg: set of piecewise linear maps sending $[0, 1]$ to $[0, 1] \subset \mathbb{R}$ with breakpoints at dyadic rationals and slopes powers of 2, and $0 \mapsto 0, 1 \mapsto 1$.This is *Thompson's group F*.

DEFN: COMPOSITION TABLE

Question: how many "different" groups are there of size 3?

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$+ \bmod 3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$a^{-1} \circ a \circ a = a^{-1} \circ a$

$a = e$

$a \circ b = b$

$a = e$

$e \circ a = a$

$2 + 2 = 1$

$\mathbb{Z}/3\mathbb{Z}, +_{\bmod 3}$

$\{0, 1, 2\}$

$\mathbb{Z}/2\mathbb{Z}, +_{\bmod 2}$

DEFN: COMPOSITION TABLE

Question: how many “different” groups are there of size 3?

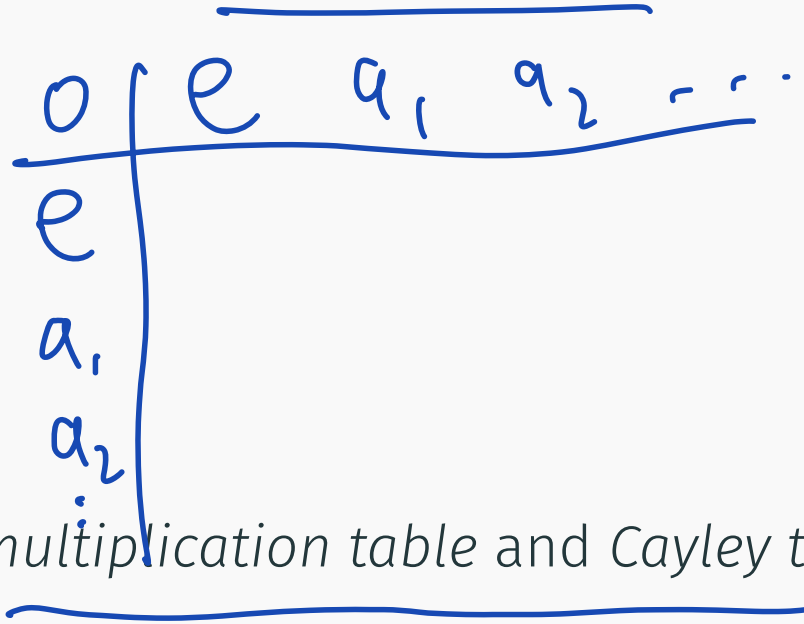
By “different” we will need to define it, but let’s say we don’t care what the “names” of the elements are (as long as the binary operation is preserved when you change element names)

DEFN: COMPOSITION TABLE

Question: how many "different" groups are there of size 3?

By "different" we will need to define it, but let's say we don't care what the "names" of the elements are (as long as the binary operation is preserved when you change element names)

To help answer this, Defn 2.1.4 is useful.



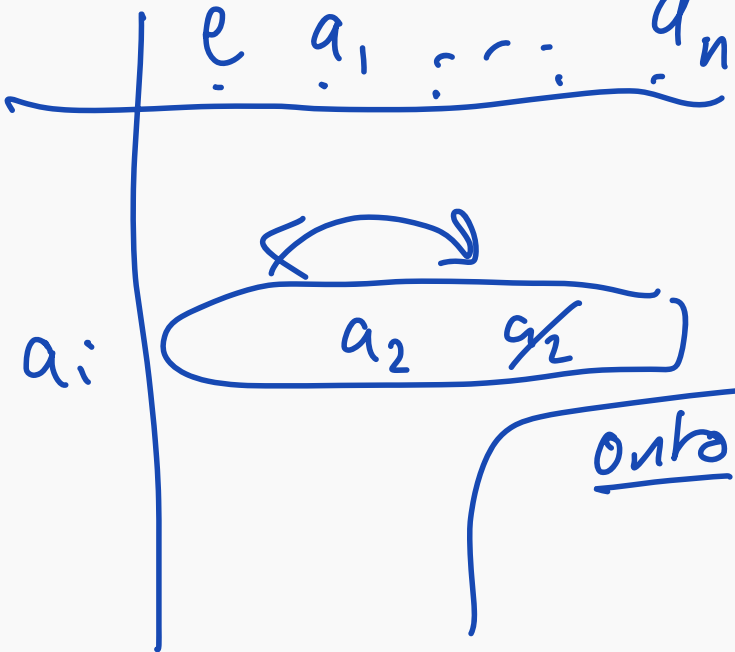
Also called *multiplication table* and *Cayley table*

LEMMA 3 (SUDOKU RULE)

If $(G, \circ)$ is a group and $g \in G$ then the map from G to G defined by $h \mapsto g \circ h$ is a bijection.

bijection = (a) one-to-one (b) onto

$\varphi_g(h) = g \circ h$



1-1

Proof

$\varphi_g(h_1) = \varphi_g(h_2)$

$\|$ $\|$

$g \circ h_1$ $g \circ h_2$

Apply g^{-1} on both sides on left

$g^{-1} \circ g \circ h_1 = g^{-1} \circ g \circ h_2$

$\|$ $\|$

$e \circ h_1 = h_1$ h_2

LEMMA 3 (SUDOKU RULE)

If $(G, \circ)$ is a group and $g \in G$ then the map from G to G defined by $h \mapsto g \circ h$ is a bijection.

bijection = (a) one-to-one (b) onto

Proof: Suppose $g \circ h_1 = g \circ h_2$, then since G is a group g has an inverse $b \in G$, then

$$h_1 = e \circ h_1 = (b \circ g) \circ h_1 = b \circ (g \circ h_1) = b \circ (g \circ h_2) = \ldots$$

LEMMA 3 (SUDOKU RULE)

If $(G, \circ)$ is a group and $g \in G$ then the map from G to G defined by $h \mapsto g \circ h$ is a bijection.

bijection = (a) one-to-one (b) onto

Proof: Suppose $g \circ h_1 = g \circ h_2$, then since G is a group g has an inverse $b \in G$, then

$$h_1 = e \circ h_1 = (b \circ g) \circ h_1 = b \circ (g \circ h_1) = b \circ (g \circ h_2) = \ldots$$

1-1, onto.

Application: each row (and column) of a Cayley table has one of each element of G (like a Sudoku)

HOMEWORK: EXPLORE MORE EXAMPLES

Isometries of $\mathbb{R}^2$ which preserve a square centred at $(0, 0)$ also called D_8

Matrix examples (GL, SL)

Important example for later (spend some time understanding the notation) S_3 (Lauritzen Example 2.1.6)

Ex: draw the composition table for S_3 for yourself (then check against Lauritzen)

Definition (2.2.1)

A *subgroup* of G is a non-empty subset $H \subseteq G$ such that the composition of G makes H into a group.

Claim (quick proof in your head): $H \subseteq G$ is a subgroup of G if and only if

1. $e \in H$
2. $x^{-1} \in H$ for every $x \in H$
3. $xy \in H$ for every $x, y \in H$.

Definition (2.2.1)

A *subgroup* of G is a non-empty subset $H \subseteq G$ such that the composition of G makes H into a group.

Claim (quick proof in your head): $H \subseteq G$ is a subgroup of G if and only if

1. $e \in H$
2. $x^{-1} \in H$ for every $x \in H$
3. $xy \in H$ for every $x, y \in H$.

Eg. (Prop 2.2.3) The only subgroups of $(\mathbb{Z}, +)$ are

$$H = d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\} = \{\dots, -2d, -d, 0, d, 2d, \dots\}$$

Proof:

NEXT:

Reading: 2.1, 2.2

Next week:

- coset
- normal subgroup
- homomorphism
- isomorphism