Sections 3+4

26/1/23

Last time: Binary operation on set S is function

$$* : S \times S \longrightarrow S$$

Binary algebraic structure: Pair $(S, *)$, • S set • $*$ bin. op. on S.

Isomorphism of binary alg. structures $(S, *)$ & $(S', *')$: Function $\phi : S \longrightarrow S'$ which is one-to-one, onto, and a "homomorphism": $\forall a, b \in S$, $\phi(a * b) = \phi(a) *' \phi(b)$.

Write $(S, *) \simeq (S', *')$ if isomorphism ϕ exists.

Example: $(\mathbb{R}, +) \simeq (\mathbb{R}^+, \cdot)$, where isomorphism is

$$\phi : \mathbb{R} \longrightarrow \mathbb{R}^+$$
$$\phi(x) = e^x.$$

To prove $(S, *) \simeq (S', *')$, find an isomorphism ϕ.

Question: How to prove that $(S, *)$ & $(S', *')$ are **not** isomorphic ($(S, *) \not\simeq (S', *')$)?

Find "structural property" that $(S, *)$ has and $(S', *')$ doesn't.

= property preserved under isomorphisms

Example: $(\mathbb{Z}, +) \not\simeq (\mathbb{Z}^+, +)$, since $(\mathbb{Z}, +)$ has an

$(\mathbb{Z}^+ = \{1, 2, 3, \dots\})$

identity element (0), while $\mathbb{Z}^+$ doesn't.

- $(\mathbb{R}, \cdot) \not\cong (\mathbb{C}, \cdot)$: For every $a \in \mathbb{C}$, the equation
  $$x \cdot x = a$$
  has solutions $x \in \mathbb{C}$,
  - Equation $x \cdot x = -1$ has no solution $x \in \mathbb{R}$.
- $(\mathbb{Z}, +) \not\cong (\mathbb{Z}, \cdot)$, since
  - $\forall a, b \in \mathbb{Z}$, the equation $x + a = b$ has a solution for $x \in \mathbb{Z}$
  - the equation $x \cdot 2 = 1$ has no solution for $x \in \mathbb{Z}$.

Groups (Norsk: Grupper)

Good property of a $(S, *)$: Every equation

$$x * a = b \qquad a, b \in S$$

admits unique solution in $x \in S$.

Example: $(\mathbb{Z}, +)$, $x + a = b$, $a, b \in \mathbb{Z}$, has solution $x \in \mathbb{Z}$.

Why? E.g. let's solve $x + 7 = 3$, and see what we use.

- There is an identity element $0 \in \mathbb{Z}$
- There is an element called $-7 \in \mathbb{Z}$, such that
  $$\underline{7 + (-7) = 0 = (-7) + 7}$$

$$x + 7 = 3$$
$$\Downarrow$$
$$(x+7) + (-7) = 3 + (-7)$$
$$\Downarrow$$

Associativity: $x+(7+(-7))=3+(-7)$

$\Downarrow$

$x+0=3+(-7)$

$\Downarrow$

$x=3+(-7)$.

Check that $x=3+(-7)$ works:

$$(3+(-7))+7=3+((-7)+7)=3+0=3.$$

<u>Def</u> A <u>group</u> is a binary algebraic structure $(G,*)$ satisfying:

- (G_1): $*$ is associative $[a*(b*c)=(a*b)*c]$

(G_2): There is an element $e\in G$ such that $e*a=a*e=a$ for all $a\in G$

(G_3): For all $a\in G$, there is an element $a'\in G$ such that

$$a*a'=a'*a=e.$$

<u>Example</u>: $(\mathbb{Z},+)$ is a group. (G_1): $+$ is associative $a+(b+c)=(a+b)+c$

(G_2): $0\in\mathbb{Z}$ is an identity element

(G_3): For $a\in\mathbb{Z}$, take $a'=-a$, then $a+(-a)=(-a)+a=0$.

- $(\mathbb{Q},\cdot)$ is <u>not</u> a group: G_1; yes, $\cdot$ is associative

G_2, yes, 1 is an identity element

G_3, no! For $0\in\mathbb{Q}$, there is no element $0'\in\mathbb{Q}$ such that $0'\cdot 0=1$.

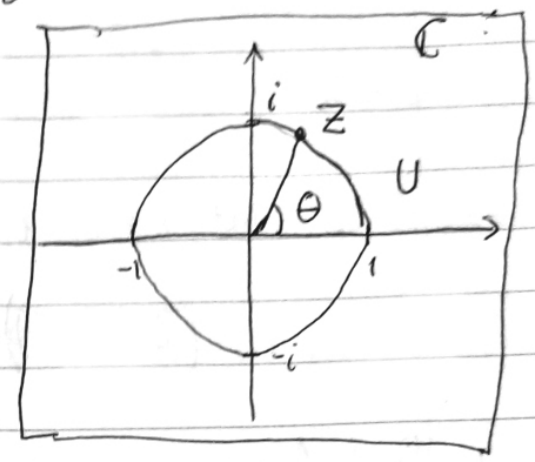
Important examples (see Section 1)

Consider $(\mathbb{C}, \cdot)$. Let $U = \{z \in \mathbb{C} \mid |z| = 1\}$.

If $z_1, z_2 \in U$, then

$$|z_1 z_2| = |z_1||z_2| = 1 \cdot 1 = 1,$$

so $z_1 z_2 \in U$. So U is closed under $\cdot$, can talk of $(U, \cdot)$.



For $z \in U$, can write $z = e^{i\theta}$, $\theta \in [0, 2\pi)$.

If $z_1 = e^{i\theta_1}$, $z_2 = e^{i\theta_2}$, then $z_1 z_2 = e^{i(\theta_1 + \theta_2)}$.

If $\theta_1 + \theta_2 > 2\pi$, can write $z_1 z_2 = e^{i(\theta_1+\theta_2)} = e^{i(\theta_1+\theta_2-2\pi)}$.

Def $(\mathbb{R}_{2\pi}, +_{2\pi})$, "real numbers modulo 2π", defined by

$$\mathbb{R}_{2\pi} = [0, 2\pi)$$

For $a, b \in \mathbb{R}_{2\pi}$, $a +_{2\pi} b = \begin{cases} a+b & \text{if } a+b \in [0, 2\pi) \\ a+b-2\pi & \text{if } a+b \geq 2\pi. \end{cases}$

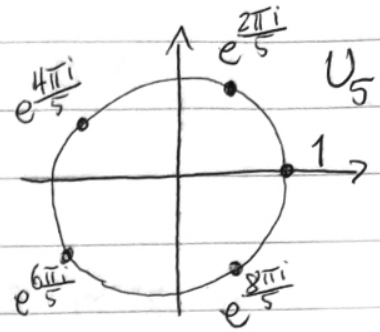
Function $\phi : \mathbb{R}_{2\pi} \to U$ is an isomorphism of $(\mathbb{R}_{2\pi}, +_{2\pi})$ with $(U, \cdot)$.
$\phi(a) = e^{ia}$

Def for $\mathbb{R}^+$ in def for $\mathbb{R}_{2\pi}$

V

Let $n \in \mathbb{Z}^+$, let $U_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$.

U_n closed under $\cdot$, so get binary alg. structure $(U_n, \cdot)$.



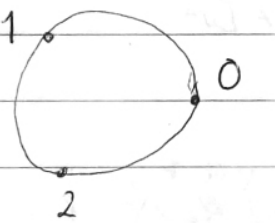
Def $(\mathbb{Z}_n, +_n)$, "integers modulo n", by

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

$$a, b \in \mathbb{Z}_n, \quad a +_n b = \begin{cases} a+b & \text{if } a+b \leq n-1 \\ a+b-n & \text{if } a+b \geq n. \end{cases}$$

Function $\phi : \mathbb{Z}_n \to U_n$, $\phi(a) = e^{a \cdot \frac{2\pi i}{n}}$ gives isomorphism from $(\mathbb{Z}_n, +_n)$ to $(U_n, \cdot)$.

Example: $(\mathbb{Z}_3, +_3)$



$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Prop $(U, \cdot)$, $(U_n, \cdot)$, $(\mathbb{R}_{2\pi}, +_{2\pi})$, $(\mathbb{Z}_n, +_n)$ are groups.

Proof $(U, \cdot)$: G_1, yes, $\cdot$ is associative
G_2, $1 \in U$ is identity element
G_3, for $z \in U$, $z^{-1} \in U$ is an inverse.

$(U_n, \cdot)$ similar.

$(\mathbb{R}_{2\pi}, +_{2\pi}) \cong (U, \cdot)$, so $(\mathbb{R}_{2\pi}, +_{2\pi})$ is group

$(\mathbb{Z}_n, +_n) \cong (U_n, \cdot)$, so $(\mathbb{Z}_n, +_n)$ is group.

Properties of groups

Def A group $(G, *)$ is abelian if $*$ is commutative
$a * b = b * a$ for all $a, b \in G$.

All groups above are abelian.

Example: Let $GL(n, \mathbb{R})$ = set of invertible real $(n \times n)$-matrices,
let $A * B = AB$ (matrix multiplication).
Then $(GL(n, \mathbb{R}), *)$ is a group:

G_1: $(AB)C = A(BC)$

G_2: $I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ is identity element

G_3: For $A \in GL(n, \mathbb{R})$, take $A^{-1} = A^{-1}$, $AA^{-1} = A^{-1}A = I_n$.

If $n \geq 2$, this is non-abelian, $AB \neq BA$.

The group with 2 elements: Let $G = \{a, b\}$, $*$ some binary operation. What can $*$ be if $(G, *)$ is group?

- Either a or b is identity element, let's make it b, and rename it e. So $G = \{e, a\}$, with multiplication table

$*$	e	a
e	e	a
a	a	?

What goes here? Note, a must have an inverse a^{-1}. e is not an inverse of a, hence $a^{-1} = a$, so $a * a = e$.

$*$	e	a
e	e	a
a	a	e

$+_2$	0	1
0	0	1
1	1	0

$(G, *) \simeq (\mathbb{Z}_2, +_2)$.