Lecture 7:

Last time: • Isomorphism (of binary structures) of pairs $(S_1, *_1) \xrightarrow{\sim} (S_2, *_2)$.

it means that the binary structures are the same after "re-labeling".

Def: $(S_1, *_1)$ is isomorphic to $(S_2, *_2)$ if there is an (isomorphism) function $\varphi: S_1 \to S_2$ which:

- is a bijection
- satisfies
  $\forall x, y \in S_1 \quad \varphi(x_1 *_1 x_2) = \varphi(x_1) *_2 \varphi(x_2)$

A map which satisfies these is called an isomorphism.

Notation: we write $(S_1, *_1) \cong (S_2, *_2)$

Examples:

• $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, *)$ multiplication

we need to make an isomorphism $\varphi: \mathbb{R} \to \mathbb{R}_{>0}$

$\varphi(x) = e^x$.

• φ is a bijection: yes because φ has an inverse: $\log_e(\cdot)$

• $\varphi(x_1 + x_2) = e^{x_1 + x_2} = e^{x_1} \cdot e^{x_2}$
$= \varphi(x_1) \cdot \varphi(x_2)$ ✓

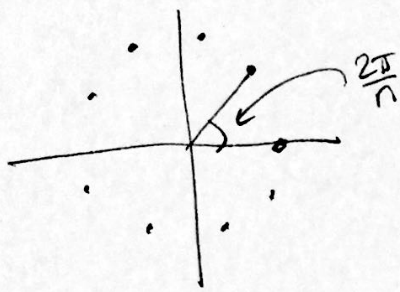
Hence, φ is an isomorphism (of set-operation pairs)

Example 2:

Let $U_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$

we already know these are the roots of unity:

$$U_n = \{ 1, e^{i 2\pi/n}, e^{i \frac{2\pi}{n} 2}, \dots, e^{i \frac{2\pi}{n}(n-1)} \}.$$



Claim: $(U_n, *)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$

proof: Let $\varphi : \mathbb{Z}/n\mathbb{Z} \to U_n$ be defined by $\varphi(\bar{k}) = e^{i \frac{2\pi}{n} k}$

- φ is one-to-one and onto:

$$\varphi(k_1) = \varphi(k_2) \Rightarrow e^{i \frac{2\pi}{n} k_1} = e^{i \frac{2\pi}{n} k_2}$$

so $\frac{2\pi}{n} k_1 = \frac{2\pi}{n} k_2 + 2k\pi$

for some k. So

$$k_1 - k_2 = kn$$

for some k, so $\bar{k}_1 = \bar{k}_2$.

- φ is onto: by definition.

(we also need to be careful that φ is well-defined, i.e. $\varphi(\bar{k}_1) = \varphi(\bar{k}_2)$ if $\bar{k}_1 = \bar{k}_2$ - exercise) finally, we check that φ respects the operation

$$\varphi(k_1+k_2) = e^{\frac{i2\pi}{n}(k_1+k_2)} = e^{i\frac{2\pi}{n}k_1} \cdot e^{i\frac{2\pi}{n}k_2}.$$

$\square$

Groups:

Definition: A group $(G, *)$ is a set G together with a binary operation $*: G\times G \to G$ such that the following (axioms) are satisfied:

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

$$(a*b)*c = a*(b*c)$$

ie $*$ is associative.

(2) There is an element $e\in G$ such that for all $x \in G$,

$$e*x = x*e = x$$

e is called the identity element.

(3) Corresponding to each $a \in G$, there is an element $a' \in G$ s.t.

$$a*a' = a'*a = e$$ a-prime.

a' is called the inverse of a, always denoted a^{-1}.

Examples:

(1) $\mathbb{Z}/n\mathbb{Z}$ is a group with $+$. ie $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group.

- $(\bar{a}+\bar{b})+\bar{c} = \bar{a}+(\bar{b}+\bar{c})$ ✓
- identity element $e = \bar{0}$.
- inverse of $\bar{a}$ is $\overline{-a}$.

$$\bar{a} + (\overline{-a}) = (\overline{-a}) + \bar{a} = \bar{0}.$$

(2) $(\mathbb{Z},+)$, $(\mathbb{R},+)$, $(\mathbb{Q},+)$, $(\mathbb{C},+)$

are groups.

(3) $(\mathbb{Z},\cdot)$, $(\mathbb{R},\cdot)$, $(\mathbb{Q},\cdot)$, $(\mathbb{C},\cdot)$

are not groups.

no inverses for 2 and 0, ...

no inverse for 0.

(4) $(\mathbb{R}\setminus 0,\cdot)$, $(\mathbb{Q}\setminus 0,\cdot)$, $(\mathbb{C}\setminus 0,\cdot)$

are groups.

(5) $(\mathbb{R}^n,+)$ is a group.

$e = \vec{0}$. $\vec{v}^{-1} = -\vec{v}$.