Last time

Correction : $n = \{0, \dots, n-1\}$

$= n-1 \cup \{n-1\}$

$0 := \emptyset$

$1 := \emptyset \cup \{\emptyset\} = \{\emptyset\}$

$2 := \{\emptyset\} \cup \{\{\emptyset\}\}$

$= \{\emptyset, \{\emptyset\}\}$

inj map $f : A \to B$

$\Leftrightarrow \forall\, a \neq a' \in A$

s.th

$$f(a) \neq f(a').$$

surj map $f: A \to B$

$\forall\, b \in B \quad \exists\, a \in A$ s.th

$$f(a) = b.$$

bijective = inj $\wedge$ surj.

Prop: If $f: A \to B$ is bijective $\exists\, f^{-1}: B \to A$ s.th $f^{-1} \circ f = id_A$

and $f \circ f^{-1} = id_B$.

Note: The converse is also true: if $\exists\, f^{-1}: B \to A$ s.th $f^{-1} \circ f = id_A$

$\wedge$ $f \circ f^{-1} = id_B$

then f is bijective

Proof: f is inj : if

$a \neq a' \in A \quad a = f^{-1}(f(a))$

$f^{-1}(f(a')) = a'$

so it cannot be that

$f(a) = f(a')$

Exercise: f is surj. //

Meta principle

Notions of type of functions (eg inj, surj) are closed under composition

ie

if $A \xrightarrow{f} B \xrightarrow{g} C$

and both f & g are

inj (surj) then

$g \circ f$ is inj (surj).

Proof: suppose $a \neq a' \in A$.

then $f(a) \neq f(a')$

(f inj) and

$g(f(a)) \neq g(f(a'))$

(g inj) $\Rightarrow$ $g \circ f$ inj.

Aside: Cantor's thm.

Thm: There is no surj map

$\mathbb{N} \longrightarrow \mathbb{R}$.

Proof: Suppose by contradiction

that $\exists\ f : \mathbb{N} \to \mathbb{R}$

that is surj.

Write $f(n) = x^{(n)}$

w/ $x^{(n)} = x_1^{(n)} . x_2^{(n)} x_3^{(n)} \cdots$

where $x_1^{(n)} \in \mathbb{Z}$

and $\forall 1<i$, $x_i^{(n)} \in \{0, \cdots, 9\}$.

$$1 \mapsto x^{(1)} = x_1^{(1)} . x_2^{(1)} \cdots x_n^{(1)} \cdots$$

$$2 \mapsto x^{(2)} = x_1^{(2)} x_2^{(2)} \cdots x_n^{(2)} \cdots$$

$$\vdots$$

$$n \mapsto x^{(n)} = x_1^{(n)} . x_2^{(n)} \cdots x_n^{(n)} \cdots$$

$\vdots$

define $y \in \mathbb{R}$ as follows:

$$y = y_1 . y_2 \cdots y_n \cdots$$

$$y_1 = x_1^{(1)} + 1$$

$$y_2 = \begin{cases} x_2^{(2)} + 1 & , \text{ if } x_2^{(2)} \neq 9 \\ x_2^{(2)} - 1 & , \text{ if } x_2^{(2)} = 9. \end{cases}$$

$$y_n = \begin{cases} x_n^{(n)} + 1, & \text{if } x_n^{(n)} \neq 9 \\ x_n^{(n)} - 1, & \text{if } x_n^{(n)} = 9. \end{cases}$$

Note for any n, $y \neq x^{(n)}$ bcs $y_n \neq x_n^{(n)}$.

Thus f is not surj - contradiction. //

Example: Choose a programming language and let $\bar{\mathcal{P}}$ be all programs.

Let $\mathcal{P} \subseteq \bar{\mathcal{P}}$ be the set of all programs that print a decimal rep'n.

(*) eg. 1) print "0."

(2) While true:
print "3".

For such a program $P \in \mathcal{P}$ the theoretical print output is an element $\in \mathbb{R}$

(*) "0.33....." $= \frac{1}{3} \in \mathbb{R}$

Claim: $\exists$ a real number $x \in \mathbb{R}$ that is not obtained as a theoretical output of any program.

Sketch: if it wasn't the case

$\exists$ surj map

$$f : \mathcal{P} \longrightarrow \mathbb{R}$$
$$P \longmapsto \text{output}(P)$$

$\rightsquigarrow$

$$\bar{f} : \bar{\mathcal{P}} \longrightarrow \mathbb{R}$$

$$\bar{f}(P) = \begin{cases} 0, & \text{if } P \notin \mathcal{P} \\ \text{output}(P) \text{ if} \end{cases}$$

$\bar{f}$ surj

$P \in \mathcal{P}$

Furthermore, we can order $\bar{\mathcal{P}}$ in a lexicographic order

$\Rightarrow \quad \bar{g} : \mathbb{N} \to \bar{\mathcal{P}}$

$\bar{g}(1) = "a"$

$\bar{g}(24) = "z"$

$\bar{g}(25) = "aa"$ ..

$\bar{g}$ is surj.

$\Rightarrow \quad \mathbb{N} \xrightarrow{\bar{g}} \bar{\mathcal{P}} \xrightarrow{\bar{f}} \mathbb{R}$

$\bar{f} \circ \bar{g} : \mathbb{N} \to \mathbb{R}$

is surj $\perp$ //

Def. A ... is {set G data

Def: A group is

together with a binary op'n

$$\mu : G \times G \longrightarrow G, \quad (x,y) \longmapsto \mu(x,y)$$

$$i : G \to G, \quad x \mapsto x^{-1}$$

and a unit/neutral ellement $e \in G$

Cond. such that:

(1) $\forall x \in G, \quad \mu(x,e) = x = \mu(e,x)$
(unitarity)

(2) $\forall x,y,z \in G$

$$\mu(\mu(x,y),z) = \mu(x,\mu(y,z))$$

(associativity).

(3) $\forall x \in G \quad \exists x^{-1} \in G$ s.th

$\mu(x, i(x)) = e = \cdots$

$$\mu(x,x^{-1}) = e = \mu(x^{-1},x).$$

(existence of inverse).

Meta principle: Math notions can be described by

(1) data : collection of sets

(2) conditions that this data satisfies.

Notations (1) "$\cdot$" instead of μ

$$\cdot : G \times G \longrightarrow G$$
$$(x, y) \longmapsto x \cdot y \equiv xy.$$

(1) $x \cdot e = x = e \cdot x \quad \forall x \in G$

(2) $\forall x, y, z \in G \quad (xy)z = x(yz)$

(3) $\forall x \in G, \exists \bar{x}^1 \in G$ s.th
$x \cdot \bar{x}^1 = e = \bar{x}^1 \cdot x.$

Famous groups

(1) take an object e,
then $G = \{e\}$
trivial gp ($\emptyset$ is not a gp)

(2) $(\mathbb{R}, +, 0)$ inverse of

$x \in \mathbb{R}$ is $-x$

Note: $(\mathbb{N} \cup \{0\}, +, 0)$

is not a group:

(3) $(\mathbb{Z}_n = \{0, \cdots, n-1\}, +_{(\mathrm{mod}\, n)}, 0)$

if $a \in \mathbb{Z}_n$ then

$-a := n - a$ since

$a + n - a = n \pmod n$

$= 0$

Exercise: $\forall a, b, c \in \mathbb{Z}_n$.

$[(a+b) \bmod n + c] \pmod n$

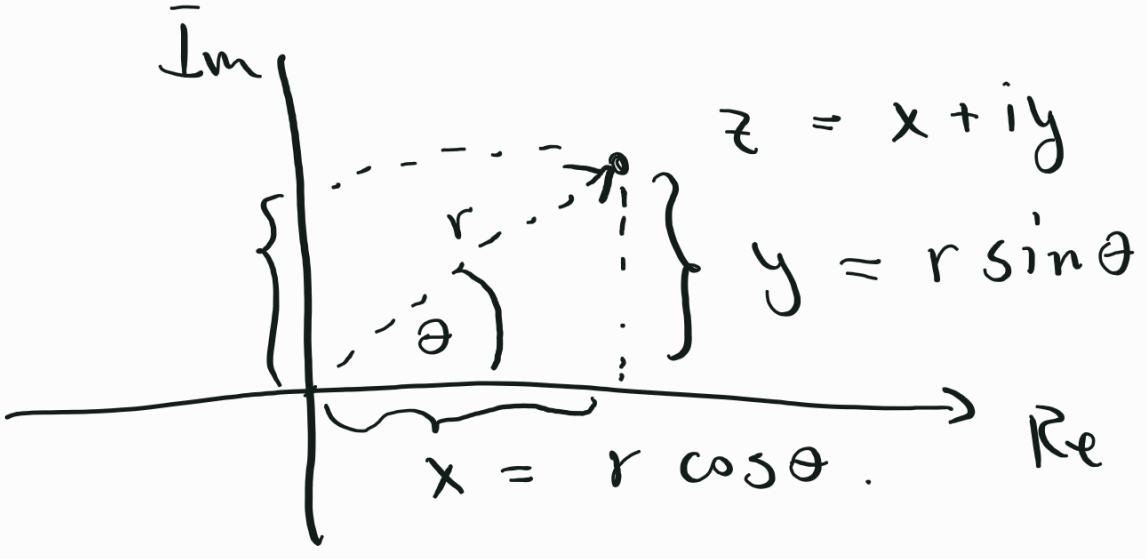
$= [a + (b+c) \pmod n] \pmod n$

(4) $\mathbb{C} = \{ x + iy \mid x, y \in \mathbb{R} \}$

$z = x + iy$

$z' = x + iy'$

$\mathbb{C} \ni z \cdot z' = (xx' - yy') + i(xy' + x'y)$



$|z| = r$ and $z = r \cdot (\cos\theta + i\sin\theta)$

$\equiv r\,cis(\theta)$

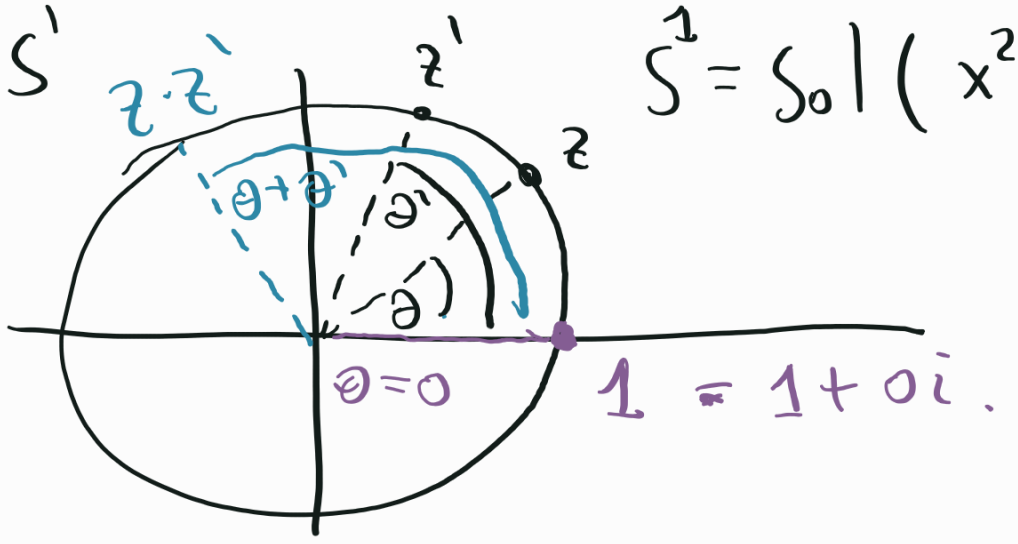
$z = r\,cis(\theta)$

$z' = r'\,cis(\theta')$

$z \cdot z = r r'\,cis(\theta + \theta')$

$= r \cdot r' (\cos(\theta + \theta') + i \sin(\theta + \theta'))$

$$\mathbb{C} \supseteq S^1 = \{ z \mid |z| = 1 \}$$



$S^1 = S_0 | (x^2+y^2-1)$

$\rightsquigarrow \quad z \cdot z'$

Obs: $(S^1, \cdot, 1)$ is a gp.

if $z = \text{cis}(\theta)$

$z^{-1} = \text{cis}(2\pi - \theta)$

$\rightsquigarrow \quad z \cdot z^{-1} = \text{cis}(2\pi) = 1$.

Def a gp G is abelian

if $\forall\, x, y \in G$

$$x \cdot y = y \cdot x.$$

(S) Let $[n] = \{1, \ldots, n\}$

and $S_n = \left\{ [n] \xrightarrow{\sigma} [n] \;\middle|\; \begin{array}{l}\sigma \text{ is} \\ \text{bijective}\end{array} \right\}$

symmetric group

$$\sigma \cdot \tau := \sigma \circ \tau \in S_n$$

assoc: $\sigma \cdot (\tau \cdot \rho) = \sigma \circ (\tau \circ \rho)$

$$= (\sigma \circ \tau) \circ \rho = (\sigma \cdot \tau) \cdot \rho$$

unit $id_{[n]} : [n] \to [n]$

inverse of σ is

σ^{-1} (exists since

σ is bijective).

Exercise find σ, τ

s.t. $\sigma \cdot \tau \neq \tau \cdot \sigma$.

Thm (Fermat's little thm):

If p a prime and

$1 \leq a \leq p-1$, then $a^{p-1} \equiv 1 \pmod{p}$

Lemma: Consider $\mathbb{F}_p = \{0, \dots, p-1\}$

w/ $+ \pmod{p}$ and $\cdot \pmod{p}$

Then $\forall n$ and any $x, y \in \mathbb{F}_p$,

$$\boxed{(x+y)^p = x^p + y^p \pmod{p}}$$

Proof:

$$\underbrace{(x+y) \cdot (x+y) \cdots (x+y)}_{p\text{-times}}$$

$$= \sum_{i=0}^{p} \binom{p}{i} \cdot x^i y^{p-i}$$

$$\binom{p}{i} = \frac{p!}{i!\,(p-i)!}$$

$$\binom{p}{i} = \frac{}{i! \cdot (p-i)!}$$

for $0 < i < p$

since p is prime

$$p \nmid i! \quad \wedge \quad p \nmid (p-i)!.$$

but $p \mid p! \Rightarrow$

$$p \mid \binom{p}{i} \Rightarrow \binom{p}{i} = 0 \pmod p$$

$$\rightsquigarrow \quad (x+y)^p = x^0 \cdot y^p + x^p y^0 =$$

$$x^p + y^p \pmod p. \quad //$$

Proof of Fermat's little thm

Want: $a^{p-1} = 1 \pmod p \quad \forall a \in \{1, \dots, p-1\}$

$$\iff \underline{a^p = a \pmod p}$$

By induction on a.

$a = 1$ clear

suppose $a^p = a \pmod p$.

Then $(a+1)^p \overset{\text{Fermat}}{=} a^p + 1^p = a+1$

↑ Induction (mod p)

Example: $\mathbb{F}_p^\times = \{1, \dots, p-1\}$

- $(\mathrm{mod}\ p)$ is a gp.

Want $\forall\ a \in \mathbb{F}_p^\times \quad \exists\ \bar{a}^{-1}$

s.th $a \cdot \bar{a}^{-1} = 1$.

take $\bar{a}^{-1} = a^{p-2}$.

Then $a \cdot \bar{a}^{-1} = a^{p-1} = 1$.

Example: Suppose $(G, \cdot_G, e_G), (H, \cdot_H, e_H)$ are groups. Then

$$G \times H = \{ (x, y) \mid x \in G, y \in H \}$$

for $(x, y), (x', y') \in G \times H$

$$(x, y) \cdot (x', y') := (x \cdot_G x', y \cdot_H y')$$

and

$$e_{G \times H} := (e_G, e_H) \in G \times H.$$

$_{G\times H}$

$$(x,y)^{-1} = (x^{-1}, y^{-1})$$

Exercise: $G \times H$ w/ these op'n is a gp.

$$\times : \text{Group} \times \text{Group} \longrightarrow \text{Group}$$

$$(G, H) \longrightarrow G \times H$$

Note: $\#(G \times H) = \#G \cdot \#H$.