$f(x) \in \mathbb{F}[x]$ $\quad \mathbb{F} \subseteq \mathbb{K}$

$f(x) = \alpha (x-\alpha_1) \cdot \dots \cdot (x-\alpha_n)$

$\alpha, \alpha_1, \dots, \alpha_n \in \mathbb{F}$

$f(x) = x^2 + 1 \quad \in \mathbb{R}[x]$

$f(x) = (x-i)(x+i) \in \mathbb{C}[x]$

$\mathbb{R} \hookrightarrow \mathbb{C}$

$\phi(x) \in \mathbb{F}_p[x]$ $\quad p$ prime

$= \sum a_i x^i$

$\mathbb{K} = \mathbb{F}_p[x]/(\phi)$

$\mathbb{Z}/n = \{0, \dots, n-1\}$

$= \left\{ r(x) = \sum_{i=0}^{k} a_i x^i \;\middle|\; a_i \in \mathbb{F}_p \right\}$

$$= \sum_{i=0}^{k} a_i x^i \mid k < n \}$$

$a_i \in \mathbb{F}_p$

$\mathbb{K}$ w/ $+ \bmod \phi$

$\cdot \bmod \phi$

is a field $\Leftrightarrow$

$$r_0(x) + r_1(x) \cdot X + \dots + r_n(x) X^n$$

$\mathbb{F}_p \subseteq \mathbb{K} \Rightarrow$

$$\sum a_i X^i = \phi(X) \in \mathbb{K}[X]$$

$$\phi(X) = (X - \alpha) \cdot \psi(X)$$

$$\mathbb{F}_p \subseteq \mathbb{K} \subseteq \mathbb{K}_1 \subseteq \dots$$

$\mathbb{K}$ finite field

Def: Let $\mathbb{F}$ be a field.

A polynomial in two variables over $\mathbb{F}$ is an expression of the form

$$f(x,y) = \sum_{i,j=0}^{n} a_{ij} \cdot x^i \cdot y^j \quad \text{w/}$$

$$a_{ij} \in \mathbb{F}$$

$\boxed{\mathbb{F}[x,y]}$

eg: over $\mathbb{R}$

a_{21} a_{02} a_{10}

$f(x,y) = 3x^2y + 2y^2 + 1\cdot x$

$+\ g(x,y) = y^2 + 5x$

$f+g = 3x^2y + 3y^2 + 6x$

On $\mathbb{F}[x,y]$ we have addition and mult.

Last time

For a set X, an equivalence relation is a subset $R \subseteq X \times X$

$$R = \{(a_1, b_1), \dots, (a_n, b_n), \dots\}$$

(denote $a \sim b$ if $(a, b) \in R$)

satisfying

1) Reflexivity: $\forall a \in X$

$(a, a) \in R$

$(a \sim a)$

2) Symmetry: $\forall a, b \in X$

$a \sim b \iff b \sim a$

3) Transitivity: $\forall a, b, c \in X$

if $a \sim b$ and $b \sim c$

then $a \sim c$

$\Rightarrow$ If $\sim$ is an equivalence relation on X and $a \in X$

we denote

$$[a] = \{ b \in X \mid a \sim b \}$$

"equivalence class" of a.

Quotient set

$X/_{\sim} := \{ [a] \mid a \in X \}$

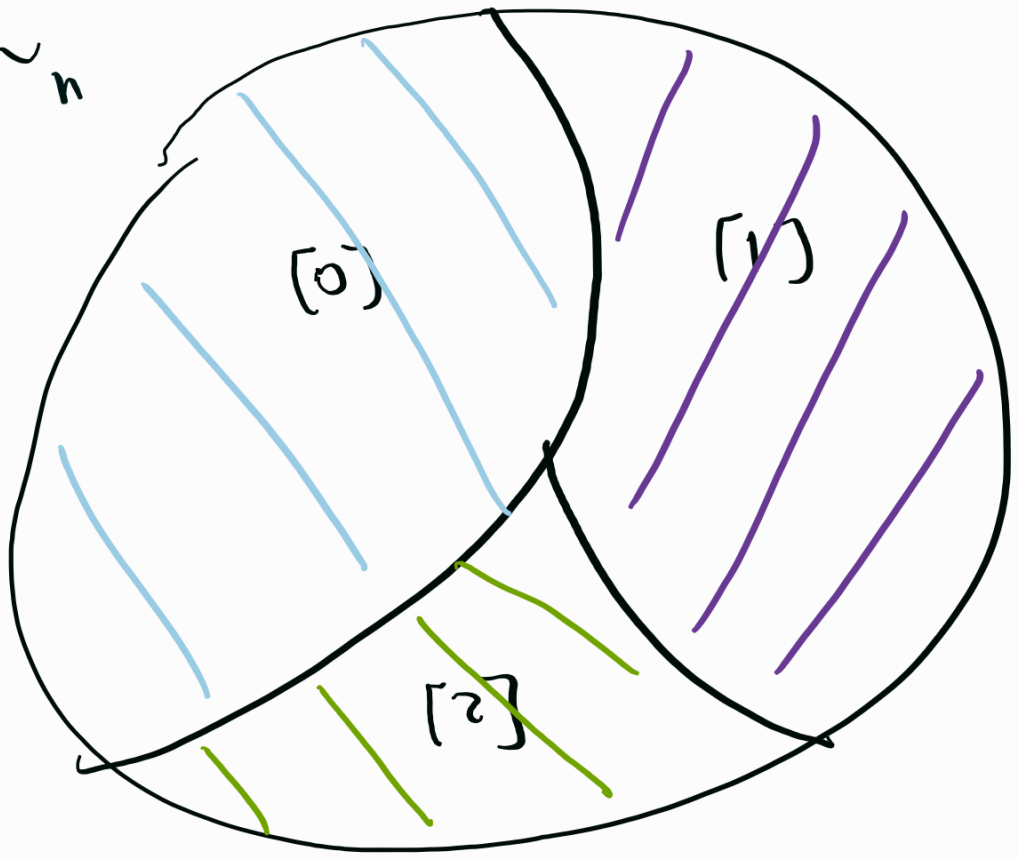
e.g $X = \mathbb{Z}$

$\sim_n \; = \; \text{mod } n$

$n = 3$

$(\text{mod } \emptyset)$

$\mathbb{Z}/\sim_n$



$\mathbb{Z}/\sim_n$ has "induced

op`n " + , ·

$$\begin{cases} [a] \overset{+}{=} [b] := [a+b] \\ [a] \overset{\cdot}{=} [b] := [a \cdot b] \end{cases}$$

is it a well-defined op`n?

If $\boxed{\begin{array}{l} a \sim a' \\ b \sim b' \end{array}}$ and

$$\left(\Rightarrow \begin{array}{l} [a] = [a'] \\ [b] = [b'] \end{array} \right)$$

need

$[a]+[b] = [a+b]$

$=$

$[a']+[b'] = [a'+b']$

$[a] + [b] = [a+b]$

In $\mathbb{Z}$ $\sim_n$ it is so

$a \sim_n a' \iff$

$a = qn + r$

$a' = q'n + r'$

$r = r'$

$b \sim_n b'$

More formally, "well-defined" mean

$$+ : \mathbb{Z}/\sim_n \times \mathbb{Z}/\sim_n \longrightarrow \mathbb{Z}/\sim_n$$

$$([a], [b]) \longmapsto [a+b]$$

$a \sim a'$ $\quad ([a], [b]) \mapsto [a+b]$

$b \sim b'$ $\quad \Big(\!\Big($ $\qquad \qquad \qquad \qquad \qquad \qquad \| $

$$([a'], [b']) \mapsto [a'+b']$$

Non example

define on $\mathbb{Z}$

the relation

$0 \sim 1$ and

$\forall a \in \mathbb{Z} \quad a \sim a$

$$\mathbb{Z}/\sim$$

<u>Proposition</u>: 1) $\mathbb{Z}/\sim_n$ is

a ring wrt the induced

binary op'n $+_{\text{mod}n}$, $\cdot_{\text{mod}n}$

2) $\mathbb{Z}/\sim_n \;\cong\; \mathbb{Z}_n$

$\{[0], \ldots, [n-1]\} \quad \{0, \ldots, n-1\}$

$f : \mathbb{Z}/\sim_n \to \mathbb{Z}_n$

$f([a]) = a \bmod n$

In polynomials F a field

$(\deg f = n)$ $f(x) \in F[x]$ arbitrary

$F[x]/(f)$

$$= \left\{ r(x) = \sum_{i=0}^{k} a_i x^i \;\middle|\; \begin{array}{l} a_i \in \mathbb{F} \\ k < n \end{array} \right\}$$

$+ \underline{\text{mod } f}$, $\cdot \underline{\text{mod } f}$

eg to do $r_1(x) \cdot r_2(x)$

write

$$r_1(x) \cdot r_2(x) = f(x) \cdot q(x) + \underline{r(x)}$$

and set

$$r_1 \cdot_{\text{mod } f} r_2 := r$$

This defines a ring str.

on $\mathbb{F}[x]/$

$/_{(f)}$

Alternatively, f induces an equivalence relation $\sim_f$ on $\underline{F[x]}$ namely

$\alpha(x) \sim_f \beta(x)$ iff

$\alpha \equiv \beta \mod f$

(ie if $\alpha = q_1 f + r_1$

$\beta = q_2 f + r_2$

then $\alpha \sim_f \beta$ $(=)$

$r_1 = r_2$)

Then

$$F[x]/\sim_f$$

$$= \left\{ [\alpha] \;\middle|\; \alpha(x) \in F[x] \right\}$$

$$= \left\{ [r] \;\middle|\; \begin{array}{l} r(x) \in F[x] \\ \deg r < \deg f = n \end{array} \right\}$$

---

or $F[x]/\sim_f$

we have a ring str.

$$[\alpha] + [\beta] := [\alpha + \beta]$$

$$[\alpha] \cdot [\beta] := [\alpha \cdot \beta]$$

Proposition: $F[x]/$

Proposition $F[x]/\sim_f$

is a ring and

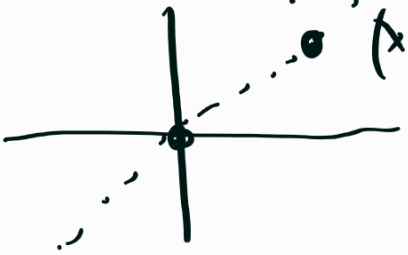
$$F[x]/\sim_f \;\cong\; F[x]/(f)$$

$$\{[r] \mid r \in F[x],\ \deg r < n\} \qquad \{r \mid r \in F[x],\ \deg r < n\}$$

Projective line

Consider the punctured plane.

$$X = \mathbb{R}^2 \setminus \{(0,0)\}$$



define a relation on X

as $(x,y) \sim (x',y') \iff$

$\exists\ 0 \neq \lambda \in \mathbb{R}$ s.th

$$(x, y) = (\lambda x', \lambda y').$$

$\sim$ is an equivalence relation

Ref : $\lambda = 1$

Sym: if $(x, y) \sim (x', y')$

$\exists\ 0 \neq \lambda$ s.th

$$(x, y) = (\lambda x', \lambda y')$$

but then

$$(x', y') = \left(\frac{1}{\lambda} x, \frac{1}{\lambda} y\right)$$

$$\Rightarrow (x', y') \sim (x, y).$$

Transitivity: if

$(x,y) \sim (x',y')$ $(x,y) = (\lambda x', \lambda y')$ and

$(x',y') \sim (x'',y'')$ $(x',y') = (\delta x'', \delta y'')$

$\Downarrow$ then

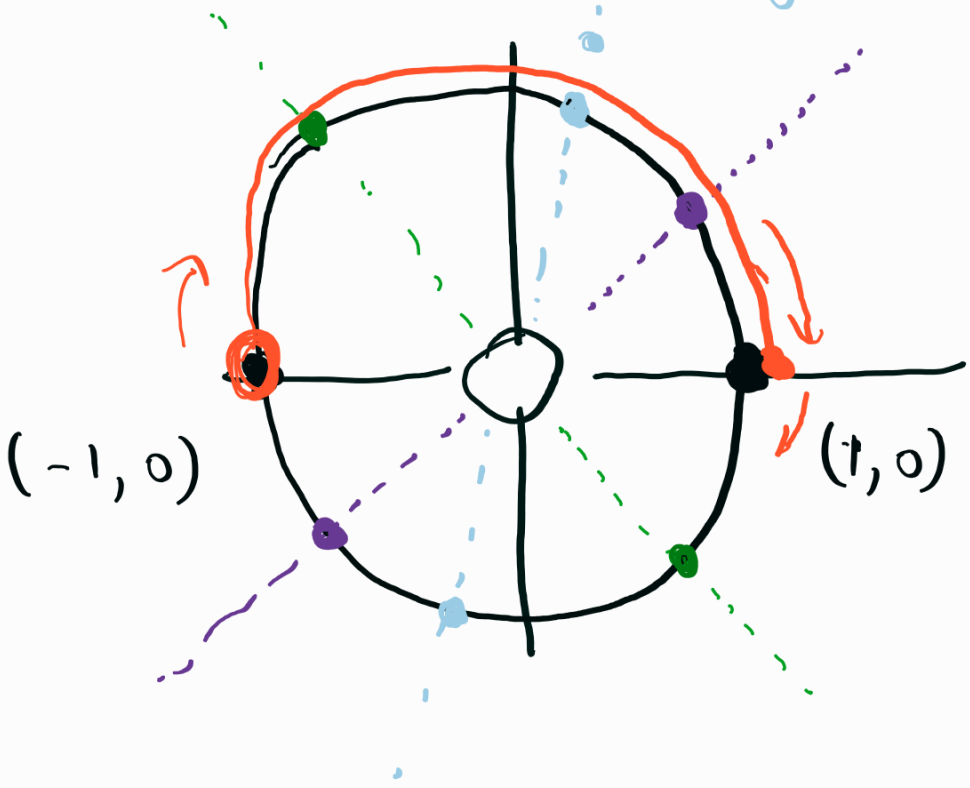
$(x,y) \sim (x'',y'')$ $(x,y) = (\lambda\delta x'', \lambda\delta y'')$

Def the projective line is the quotient set

$$\mathbb{R}^2 \setminus \{(0,0)\} / \sim$$

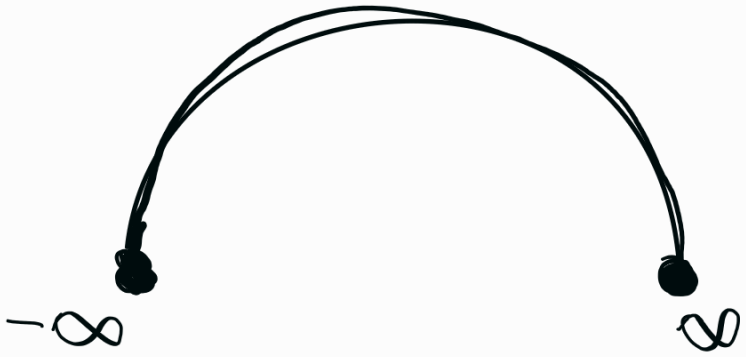
To represent the quotient set geometrically, $\forall\ \lambda \neq 0$

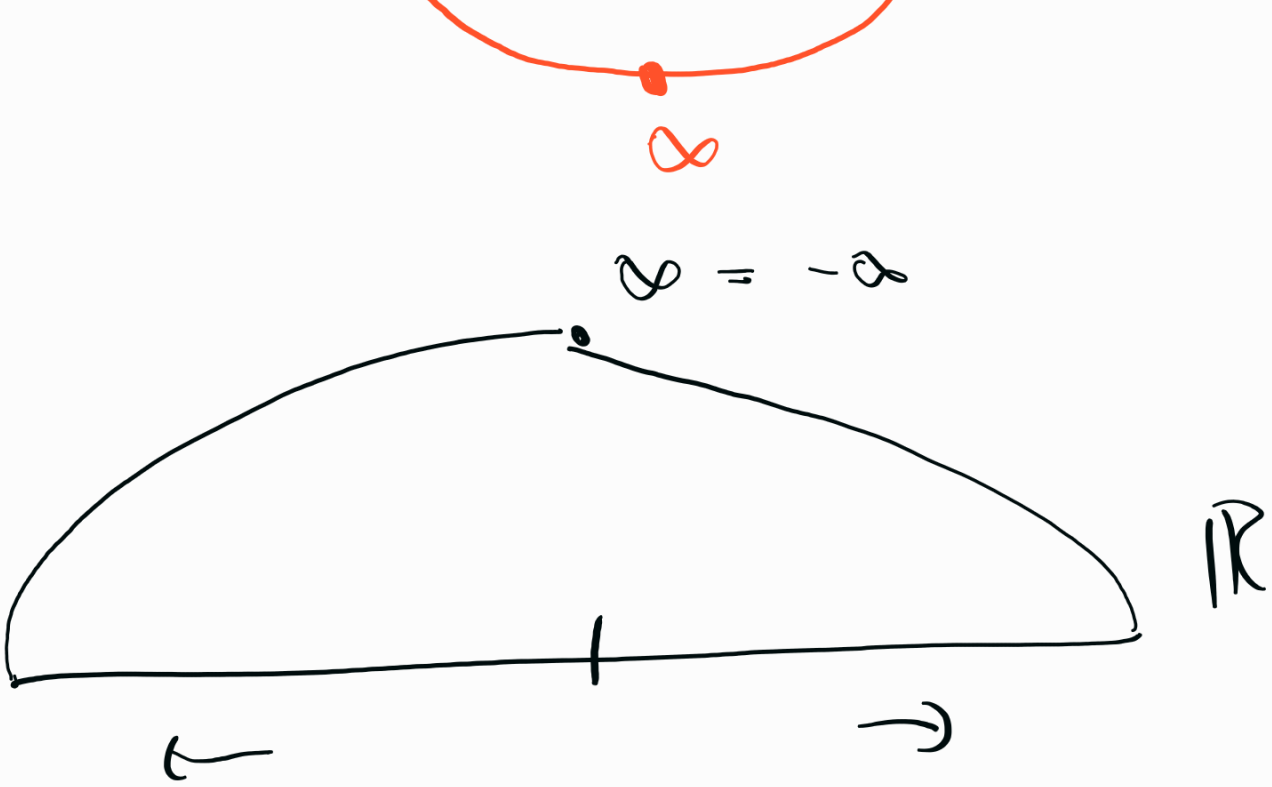
$(x,y) \sim (\lambda x, \lambda y)$



$\mathbb{Z}/\sim_n =$

$\{[0], \ldots, [n-1]\}$

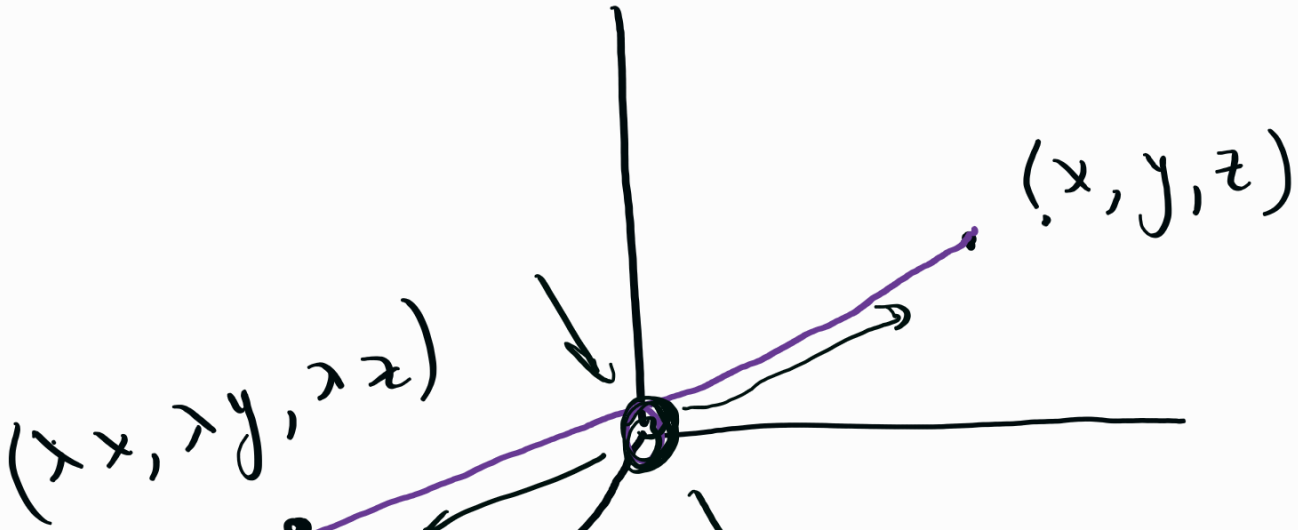


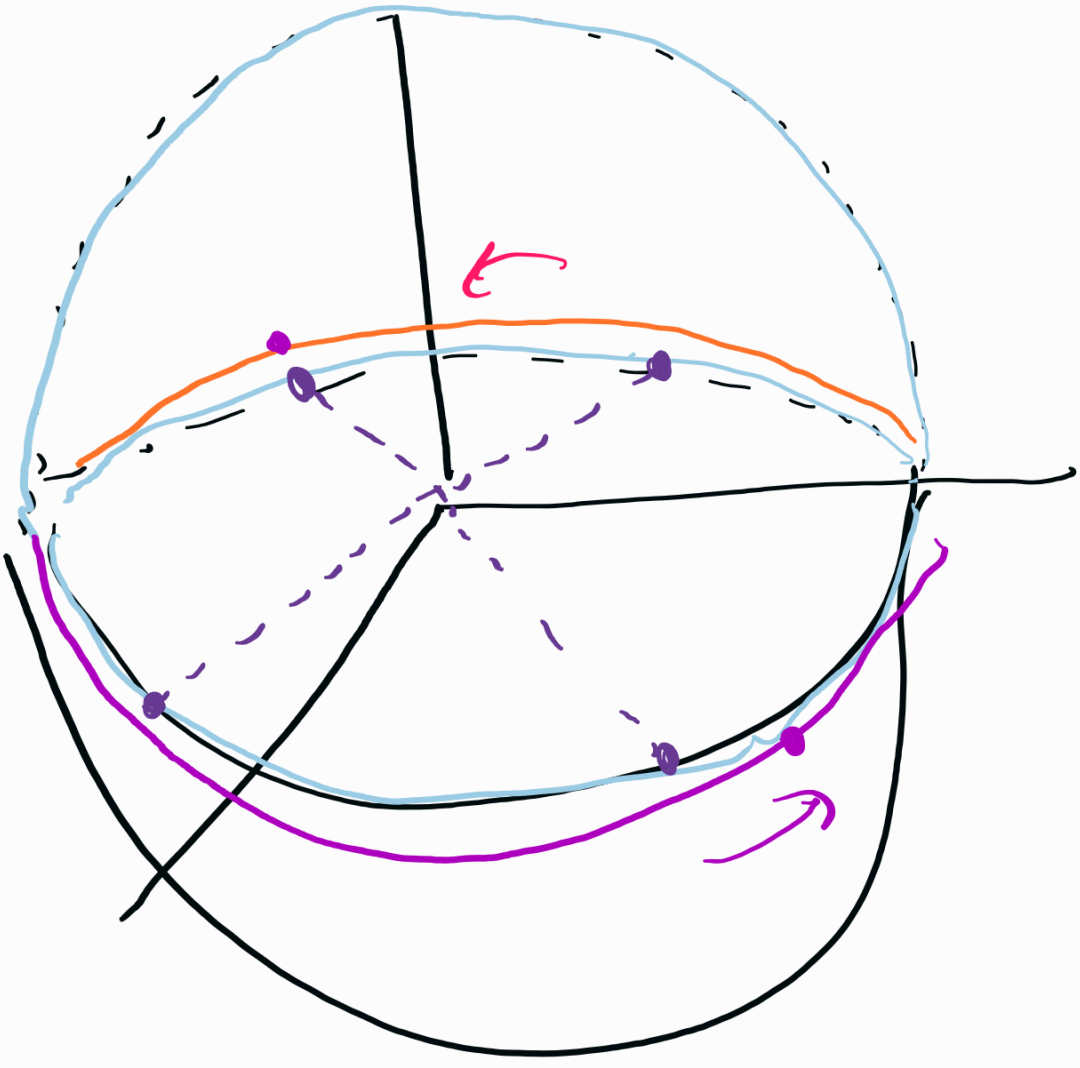


Projective plane

$$\mathbb{R}^3 \setminus \{(0,0,0)\}$$

$$(x,y,z) \sim (\lambda x, \lambda y, \lambda z)$$



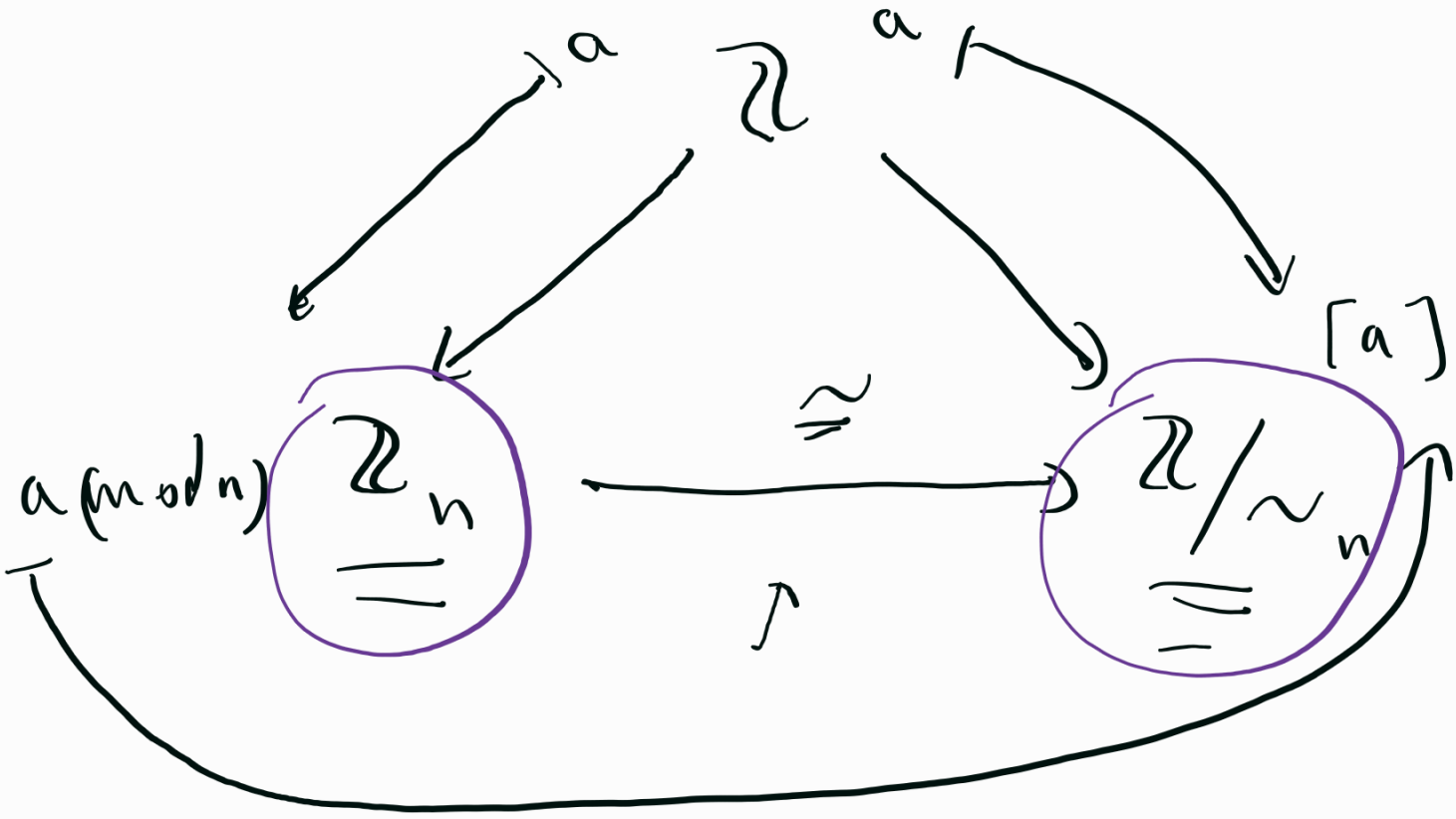


$$\mathbb{Z} \longrightarrow \mathbb{Z}_n$$

$$a \longmapsto a \bmod n$$

$$\mathbb{Z} \longmapsto \mathbb{Z}/\sim_n \quad \cong$$

$$a \longmapsto [a]$$



$$\begin{cases} 0 := \emptyset \\ 1 := \{\emptyset\} \\ \vdots \\ n := n-1 \cup \{n-1\} \end{cases}$$

$\mathbb{N}$ $\qquad n+1 = n \cup \{n\}$

... to define $\mathbb{Z}$

how to

Take $X = \mathbb{N} \times \mathbb{N}$

and define an equiv. relation on X by

$(a,b) \sim (c,d)$ iff

$a + d = c + b$ $\left(\Leftrightarrow a - b = c - d\right)$

(a,b) "$a - b$"

$\mathbb{Z} := \mathbb{N} \times \mathbb{N} / \sim$

$\mathbb{Z} \rightsquigarrow \mathbb{Q}$

$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$

$\underline{X} = \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$

$(a, b) \sim (c, d)$

$\Leftrightarrow \quad \underline{a \cdot d = b \cdot c}$

$\left(\text{"} \frac{a}{b} = \frac{c}{d} \text{"} \right)$

$\underline{\mathbb{Q}} := \mathbb{Z} \times \mathbb{Z} / \sim$

$\mathbb{R}$ – <u>dedeckind cut</u>