

The Chinese remainder theorem

Ex ①: I have some pebbles

into 3 piles \rightarrow 1 remaining 4, 7, 10, 13, ...

into 5 piles \rightarrow 2 remaining 7, 12, 17, 22

Question: how many pebbles do I have

A1: 7

A2: 22

Conjecture: $7 + 15n$ for any $n \in \mathbb{Z}$

Ex ②: Add another condition

in piles of 7 \rightarrow 3 remaining

A1: 52

A2: $52 + 3 \cdot 7 \cdot 5 = 157$

Ex ③: Conditions

piles of 4 \rightarrow 2

piles of 6 \rightarrow 4

10 works

Ex ④: piles of 4 \rightarrow 1 1, 5, 9, 13, ...

piles of 6 \rightarrow 4 4, 10, 16, 22, ...

Chinese remainder theorem: (OG version)

Suppose m_1, m_2, \dots, m_N are pairwise relatively prime

Then the system $x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

\vdots

$x \equiv a_N \pmod{m_N}$

has a unique solution modulo $m_1 m_2 \dots m_N$

Proof For each $1 \leq k \leq N$, let

$$M_k = \frac{m_1 m_2 \dots m_N}{m_k} = m_1 m_2 \dots \overset{\text{omit}}{\overbrace{m_k}^{\wedge}} \dots m_N$$

then $\gcd(M_k, m_k) = 1$

so M_k has an inverse mod m_k , call it y_k
(multiplicative inverse)

the $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_n M_n y_n$ is a solution (not the smallest)
to check

$$x \equiv a_1 0 y_1 + a_2 0 y_2 + \dots + a_k M_k y_k + \dots + a_n 0 y_n \pmod{m_k} \\ \equiv a_k (M_k y_k) \equiv a_k \cdot 1 = a_k \pmod{m_k}$$

Ex: (5)

$$x \equiv 15 \pmod{37}$$

$$x \equiv 7 \pmod{61}$$

$$M_1 = 61 \quad M_2 = 37$$

$$M_1 = 61 \equiv 24 \pmod{37}$$

$$M_2 = 37 \equiv 37 \pmod{61}$$

what is the inverse of 24 mod 37?

$$\text{Divide: } 37 = 1 \cdot 24 + 13$$

$$24 = 1 \cdot 13 + 11$$

$$13 = 1 \cdot 11 + 2$$

$$11 = 5 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$\gcd(37, 24) = \gcd(24, 13)$$

$$\text{reverse: } 1 = 11 - 5 \cdot 2$$

$$= 1 - 5(13 - 1 \cdot 11)$$

$$= 6 \cdot 11 - 5 \cdot 13$$

$$= 6(24 - 1 \cdot 13) - 5 \cdot 13$$

$$= 6 \cdot 24 - 11 \cdot 13$$

$$= 6 \cdot 24 - 11(37 - 1 \cdot 24)$$

$$= 17 \cdot 24 - 11 \cdot 37$$

$$\text{mod } 37: \quad 1 \equiv 17 \cdot 24 \pmod{37}$$

$$\text{so } y_1 = 17$$

to get the remainder of 37 mod 61:

$$61 = 37 + 24$$

$$37 = 24 + 13$$

$$24 = 13 + 11$$

$$13 = 11 + 2$$

$$11 = 5 \cdot 2 + 1$$

$$2 = 1 + 0$$

$$1 = 11 - 5 \cdot 2$$

$$1 = 11 - 5(13 - 11)$$

$$= -4 \cdot 11 + 5 \cdot 13$$

$$= -4(24 - 13) + 5 \cdot 13$$

$$= -4 \cdot 24 + 9 \cdot 13$$

$$y_2 = -29 \equiv 33 \pmod{61}$$

More modern: Desired remainders

$$a_1 \pmod{m_1}, \dots, a_n \pmod{m_n}$$

\Downarrow

$$a_1 \in \mathbb{Z}/m_1\mathbb{Z} \quad \dots \quad a_n \in \mathbb{Z}/m_n\mathbb{Z} \Leftrightarrow (a_1, a_2, \dots, a_n) \in \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z}$$

• let $\pi_k(x) = a_k$ when $\pi_k: \mathbb{Z} \rightarrow \mathbb{Z}/m_k\mathbb{Z}$

so $\pi(x) = (a_1, a_2, \dots, a_n)$ $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z}$

then "there always exist an x "



π is surjective

and "unique up to $m_1 m_2 \dots m_n$ "



$\ker(\pi) = m_1 m_2 \dots m_n \mathbb{Z} = (m_1 \mathbb{Z}) \dots (m_n \mathbb{Z})$

so 1st iso theorem says

$\mathbb{Z}/m_1 m_2 \dots m_n \mathbb{Z} \cong \mathbb{Z}/m_1 \mathbb{Z} \times \mathbb{Z}/m_2 \mathbb{Z} \times \dots \times \mathbb{Z}/m_n \mathbb{Z}$

more generally,

$R/I \times R/J \cong R/(I+J)$

A bit of informal category theory

A category C consists of

- 1) Collection of objects (often visualized as dots)
- 2) Collection of arrows (sometimes called morphisms) between objects

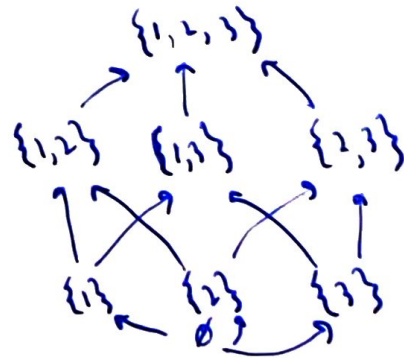
satisfying a few basic conditions (composition, associativity, unique identity arrow)

Ex 1: $X = \{1, 2, 3\}$

→ make a category C_X

• objects are subsets of X

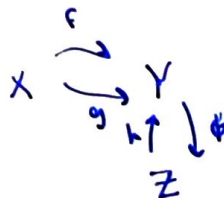
• arrows: $S \rightarrow T$
iff $S \subseteq T$



Ex 2 Set

• objects: sets

• arrows: functions between sets



Some others:

- Grp: objects: groups
arrows: group homomorphisms
- Ab: objects: abelian groups
arrows: group homomorphisms

Ring: objects: rings ($\neq 1$)
arrows: ring hom.

Vec _{\mathbb{R}} : objects: vector space of \mathbb{R}
arrows: linear transformations

Ex 3 (odd)

Mat _{\mathbb{R}} matrices with real entries

objects: natural numbers

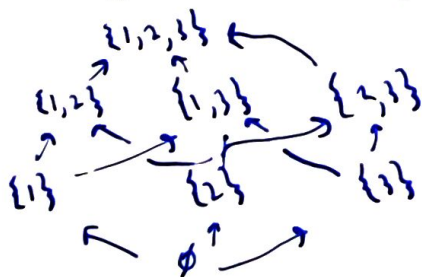
arrows:

$$i \xrightarrow{A} m$$

where A is an $n \times m$ matrix

New notion: "universal property"

Ex 4 In C_X where $X = \{1, 2, 3\}$



Suppose S, T are objects in C_X

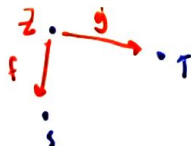
• T

• S

Q: Is there a single object in C_X that captures the information of this diagram

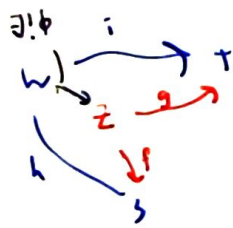
Alternatively: is there a single object closest to this diagram?

More precisely: is there an object Z with arrows to this diagram



Z is closest among all such contenders

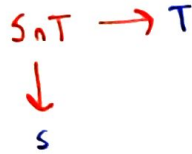
ie. $i \circ h$



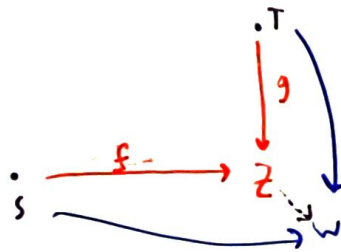
then there exists a unique arrow $\phi: w \rightarrow z$ such that $h = f \circ \phi$ and $i = g \circ \phi$

What is this magical set Z ?

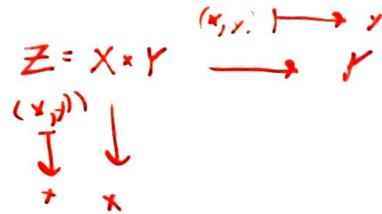
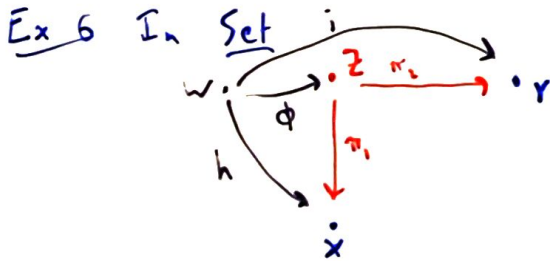
It's their intersection: $S \cap T$



"Dually"

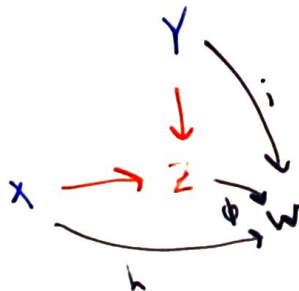


$$Z = S \cup T$$



$$\phi(w) = (h(w), i(w))$$

Similarly



$$Z = X \amalg Y \quad (\text{disjoint union})$$

ex: $A = \{a, b, c\}$ $Y = \{1, 2\}$

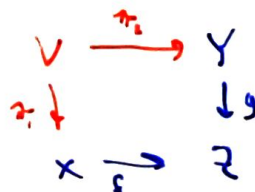
Up a notch (in Set)

Diagram

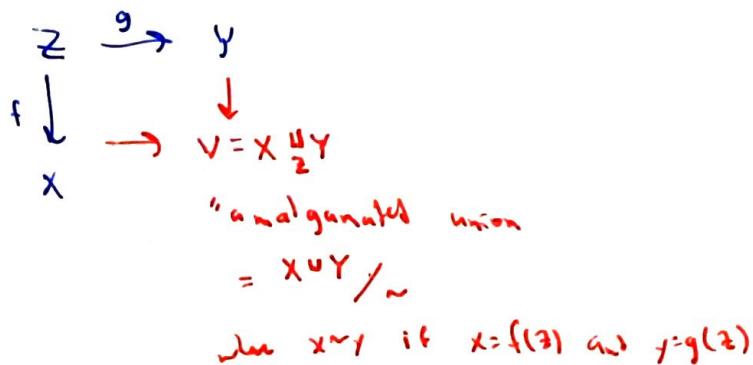
$$V = \{(x, y) : f(x) = g(y)\}$$

$$V = X \times_Y Y$$

"fiber product"



the other way



Back to Ring

"universal property of quotients"

For an ideal $I \subseteq R$ what is special about R/I

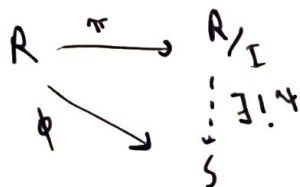
A: there is a hom. $\pi: R \rightarrow R/I$

with $I \subseteq \text{Ker}(\pi)$, i.e. $\pi(I) = 0$

This is universal

if $\phi: R \rightarrow S$ with $I \subseteq \text{Ker}(\phi)$

then



Lattice isomorphism theorem

