Functions and Relations

Functions (map, mapping) $f: A \to B$
$x \mapsto f(x)$

injective: $x \neq y \Rightarrow f(x) \neq f(y)$
surjective: for all $y \in B$ there is $x \in A$: $f(x) = y$
or: $f(A) = B$
bijective: injective + surjective
(one-to-one)

$|A| = |B| \iff$ exists bijective mapping $f: A \to B$
A, B finite

Examples:		inj	surj	bij
	$- f: A \to A,\ x \mapsto x$ (identity mapping)	x	x	x
	$- \sin: \mathbb{R} \to [-1, 1]$		x	
	$- f: \mathbb{N} \to \mathbb{N},\ x \mapsto x+1$	x		

Relations S a set, relation is written as "$\sim$".
For $x, y \in S$ either $x \sim y$ (relation holds)
or $x \not\sim y$ (" does not hold)

Examples: $S = \mathbb{R}$, "$\sim$" = "$=$" or "$\sim$" = "$\leq$"

Equivalence relation: for $x, y, z \in S$

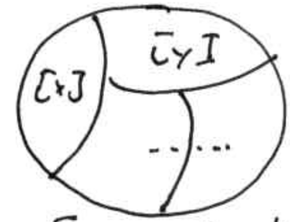
a.) $x \sim x$ reflexive
b.) $x \sim y \Rightarrow y \sim x$ symmetric
c.) $x \sim y$ and $y \sim z \Rightarrow x \sim z$ transitive

equivalence class: $[x] = \{y \in S \mid y \sim x\}$
$\uparrow$ representative

$x, y \in S$: either $[x] \cap [y] = \emptyset$ (when $x \not\sim y$)
or $[x] = [y]$ (when $x \sim y$)

As a consequence, $\sim$ yields a "partition" of S:

$$S = \bigcup_{x \in S} [x], \qquad S:$$



Partition: A set of subsets $S_\alpha \subset S$ such that

$$S_\alpha \cap S_\beta \neq \emptyset \quad \text{for } \alpha \neq \beta$$

$$\bigcup_\alpha S_\alpha = S$$

$$\text{all } S_\alpha \neq \emptyset$$

Notation: $S/_\sim = \{[x] \mid x \in S\}$ is the partition induced by $\sim$

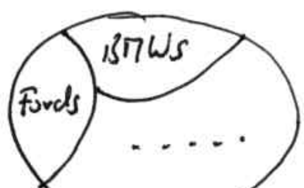
Conversely, let $S = \bigcup_\alpha S_\alpha$ be a partition of S.
Then $x \sim y \iff x, y \in S_\alpha$ for some α
is an equ. rel.

$$\boxed{\text{equivalence relations on } S \iff \text{partitions of } S}$$

Examples:

- $S = \{\text{cars}\}$, "$\sim$" = "is the same make as"

  partition $S/_\sim$:

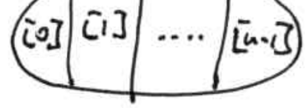


- $S = \mathbb{R}$, "$\sim$" = "$=$", $[x] = \{x\}$
- $S = \mathbb{R}$, "$\sim$" = "$\leq$", reflexive ✓, transitive ✓, symmetric ↯
- $S = \mathbb{Z}$, $x \sim y \iff n \mid (x-y)$

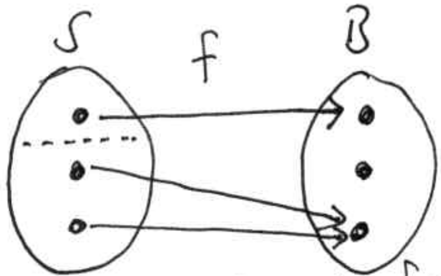
  $[x] = \{\ldots x-n, x, x+n, x+2n, \ldots\}$ a residue class modulo n

partition:

$$\mathbb{Z}/_\sim = \underbrace{\mathbb{Z}/_{n\mathbb{Z}}}_{\text{explained later}} :$$



- $f: S \to B$ a function, $x \sim y \iff f(x) = f(y)$
(equ. rel. induced by f)
$[x] = \{ y \in S \mid f(y) = f(x) \}$



$S/_\sim = S/f$ (notation)

yields "canonical factorization" of f:

$$\begin{tikzcd} S \arrow[rr, "f"] \arrow[d, "f_1 : x \mapsto {[x]}"', "\text{surjective}"] & & B \\ S/f \arrow[rr, "f_2 : {[x]} \mapsto f(x)", "\text{bijective}"'] & & f(S) \arrow[u, "f_3 : x \to x"', "\text{injective}"] \end{tikzcd}$$

This is a "commutative diagram", i.e.
$$f = f_3 \circ f_2 \circ f_1$$

The issue of well-defined

Consider: $\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$

$$f: \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$$
$$[i] \mapsto [\mathrm{floor}(i/2)]$$

$[0] \mapsto [0]$, $[1] \mapsto [1]$, $[2] \mapsto [2]$

$\quad\quad\quad\;\; \| \quad\;\; \nparallel$

$\quad\quad\quad [4] \mapsto [2]$ inherent contradiction
f not "well-defined"

Cause of trouble:
The same element in $\mathbb{Z}/3\mathbb{Z}$ has different names
(i.e. " representations)

Other example:
set = collection of objects without repetition
is not well-defined ?! (Russell paradox)
set theory: 1874– (Georg Cantor 1845-1918)

Russell paradox: 1901 (Bertrand Russell 1872-1970)

S = set of all sets, $S = A \cup B$, $A \cap B = \emptyset$

$A = \{X \in S \mid X \in X\}$ $\qquad B \in A \Rightarrow B \in B$ $\lightning$

$B = \{X \in S \mid X \notin X\}$ $\qquad B \in B \Rightarrow B \notin B$ $\lightning$

(Abstract) algebra: Overview

(Binary) operation (two types):

a.) on a set S: $\quad \cdot : S \times S \to S$, $\quad (x,y) \mapsto xy$

could be $+, \circ, \dots$

b.) R operates on S: $\quad \cdot : R \times S \to S$, $\quad (x,y) \mapsto xy$

Examples:

$\mathbb{Z}, +$ ✓

$\mathbb{Z}, \cdot$ ✓

$\{0,1\}, \cdot$ ✓

$\{0,1\}, +$ $\lightning$

$\mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2$

$\alpha, \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \alpha \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x \\ \alpha y \end{pmatrix}$

$$\boxed{\text{Algebra studies algebraic structures} = \text{sets with operations}}$$

	group	ring	field	vector space	algebra (ring + vector space)	module
	$(G, \cdot)$	$(R, \cdot, +)$	$(F, \cdot, +)$	$(V, +)$, $\cdot : F \times V \to V$	$(A, +, \cdot)$, $\cdot : F \times A \to A$	$(M, +)$, $\cdot : A \times M \to M$
example:	$(\mathbb{Z}, +)$	$(\mathbb{Z}, \cdot, +)$	$(\mathbb{R}, \cdot, +)$	$F = \mathbb{R}$, $V = \mathbb{R}^2$	$F = \mathbb{R}$, $A = \mathbb{R}[x]$	$A = M = \mathbb{R}[x]$

set of polynomials with real coefficients

Groups

$\boxed{\text{Group definition}}$ $(G, \cdot)$, "$\cdot$" operation on G such that

a.) $a(bc) = (ab)c$ $\quad$ associative

b.) there is a neutral element e in G: $ae = ea = a$, $a \in G$

c.) for $a \in G$ there is an inverse a^{-1}: $aa^{-1} = a^{-1}a = e$

G is called "abelian" or "commutative" if

d.) $ab = ba$

Lemma: e and inverse are unique

Examples: $(\mathbb{Z},+)$, $(\mathbb{Q},\cdot)$, $(\mathbb{Z},\cdot)$ is not

$\boxed{\text{Generators}}$

- $\langle x\rangle_{grp} = \{\dots x^{-1}, x^0=1, x, x^2, \dots\} = C_\infty$ infinite cyclic group
- $\mathbb{Z}$ with "+" $= \langle 1\rangle_{grp}$
- $\langle x \mid x^4 = 1\rangle = \{x^0=1, x, x^2, \dots, x^{4-1}\} = C_4$ cyclic group of order 4

  x ↑ generator, $x^4=1$ ↑ relation; order ↑ size
- symmetry transformations of the square:

x: rotation by $90°$, $x^4=1$

y: reflection, $y^2=1$

further $xy = yx^{-1}$

group $D_8 = \langle x, y \mid x^4 = y^2 = 1,\ xy = yx^{-1}\rangle$