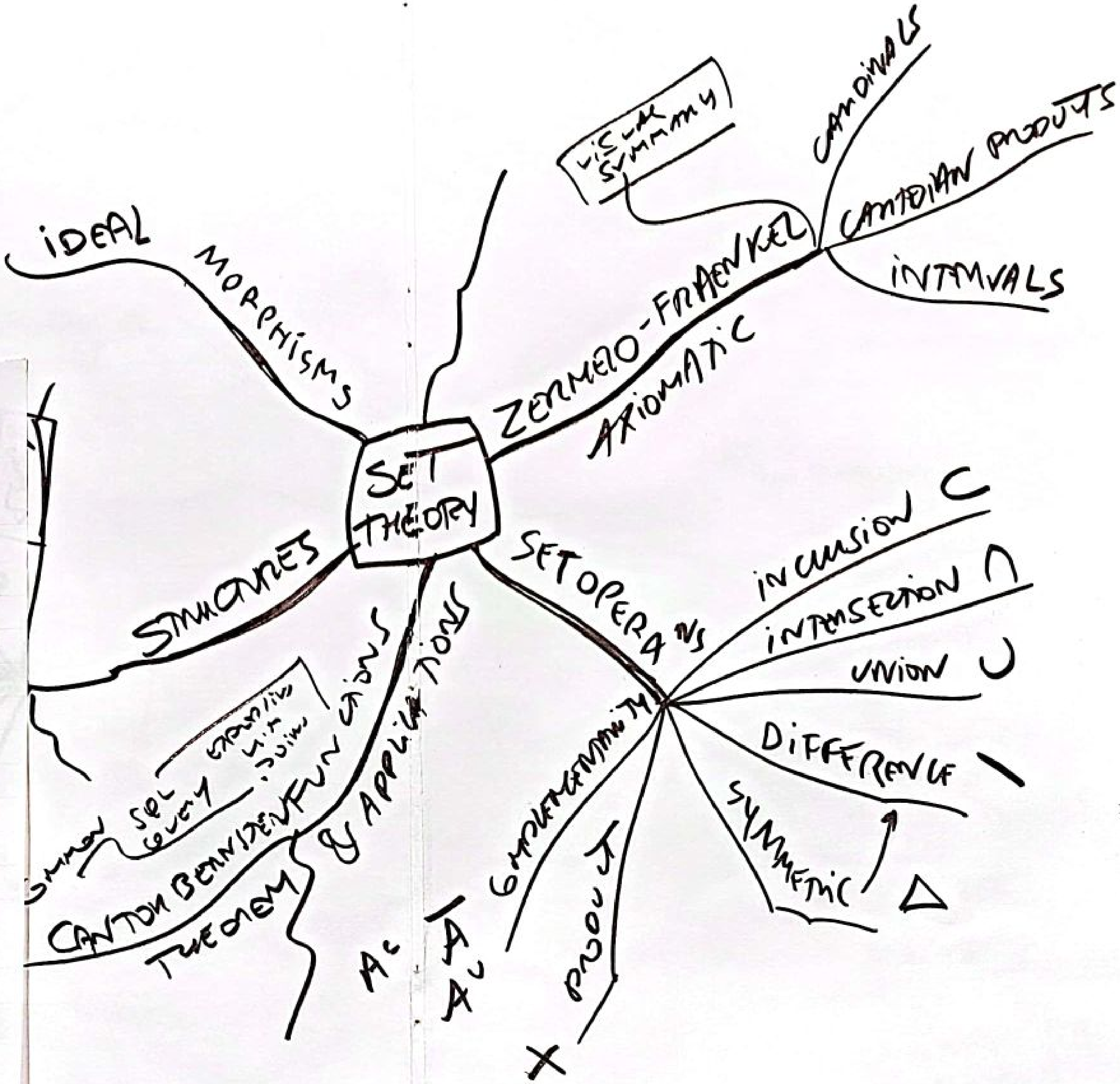
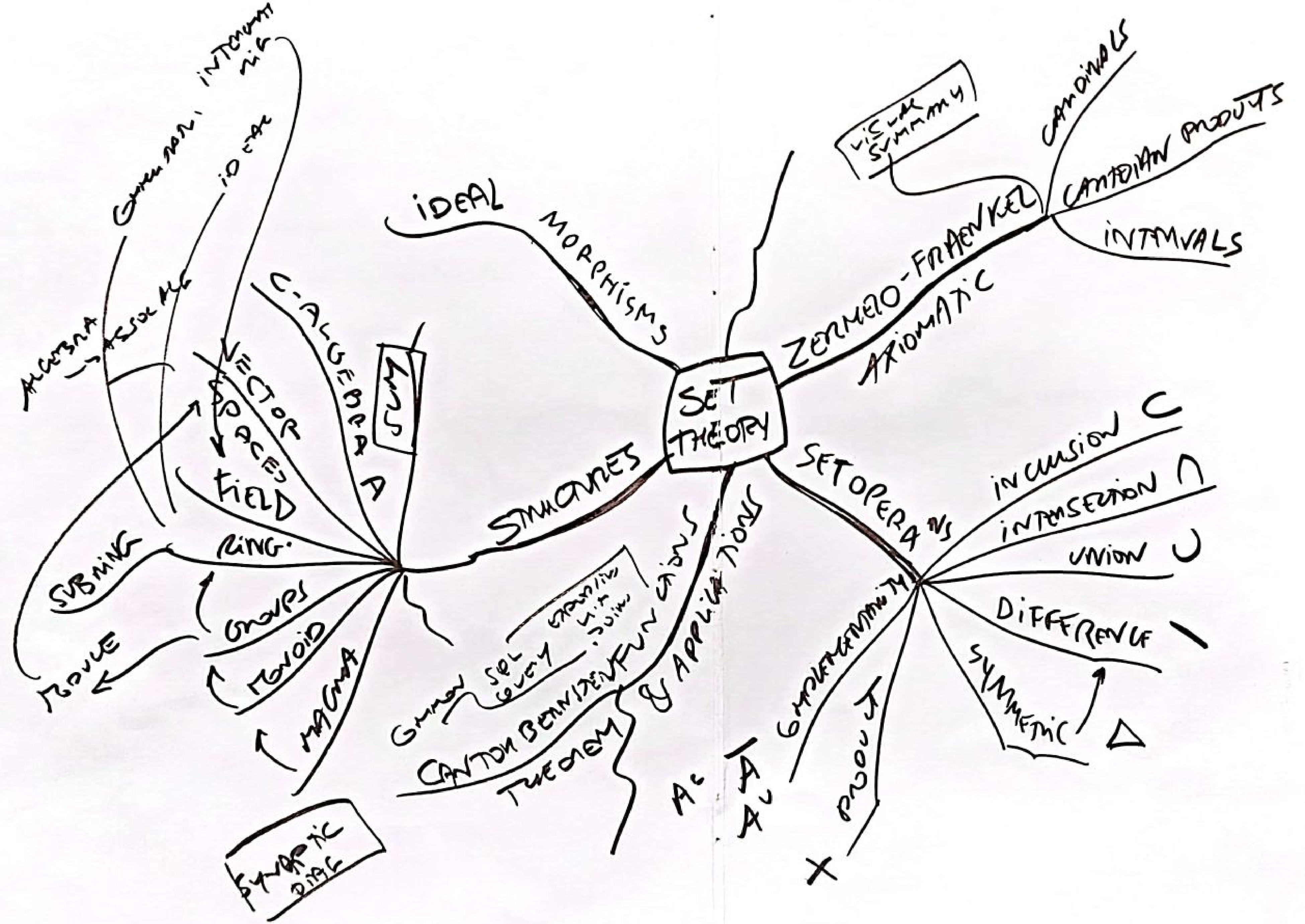


ISO2 SET THEORY


SET THEORY
ZERMELO-FRAENKEL
AXIOMATIC
VISUAL SUMMARY
CARDINALS
CARTESIAN PRODUCTS
INTERVALS
SET OPERATIONS
INCLUSION ⊂
INTERSECTION ∩
UNION ∪
DIFFERENCE \
SYMMETRIC Δ
COMPLEMENTARITY
PRODUCT
×
FUNCTIONS & APPLICATIONS
CANTOR BERNSTEIN THEOREM
STRUCTURES
MORPHISMS
IDEAL
C-ALGEBRA
SUM
VECTOR SPACES
FIELD
RING
GROUPS
MONOID
MAGMA
SUBRING
MODULE
ALGEBRA
SYNOPTIC DIAG

Set theory

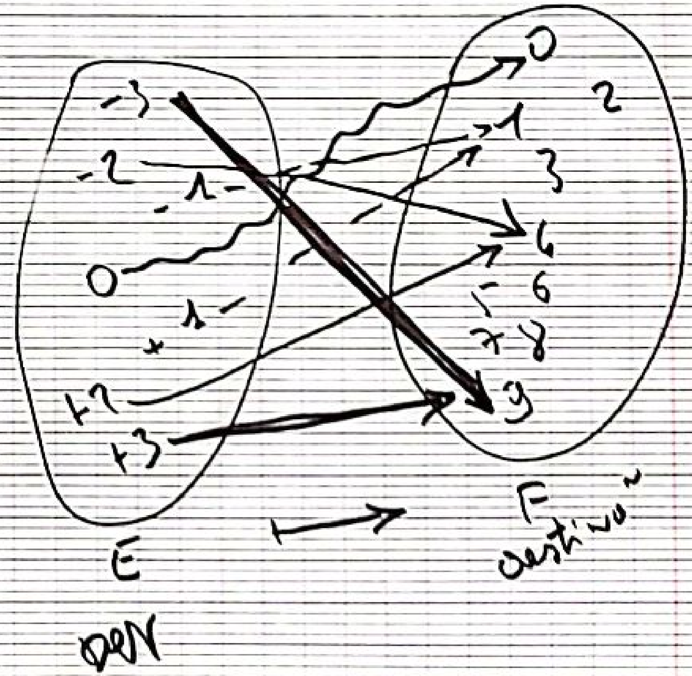
5/11 begins

... storing them in separate categories

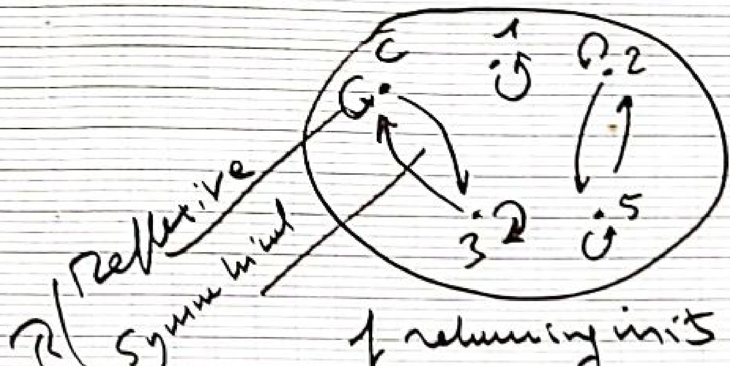
D "arrow diag" = "sagittal diag"
→ showing a correspondence btw 2 sets of comp connected wholly or partially by a set of arrows

~~circles~~ → Venn diag

EX



R, E to E $E \mapsto E$



f returning into a new set of obj

D if target set is ident to original set
"binary R"

internal rigor frame — contradictory or consistent
framework

D_1 "set" any list, collection or gathering of well def.d objects, explicitly or implicitly

D_2 "Universe" U is an ~~set~~ object whose constituents are sets
not a set!
= a model that satisfies to the axioms of sets ‖ ★

instead ~~of~~ talk about the set of all sets
(because this is ~~set~~ a ~~set~~) ...

D3 "elts" or "members of the S"

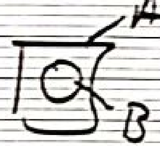
objects belonging to the set

$x \in A$

contrary case $x \notin A$

if B is a "part" of A or "subset" of A

we write $B \subset A$ or $A \supset B$



Thus $\forall x, x \in B \Rightarrow x \in A$

E1 $A = \{1, 2, 3\}$

E2 $X = \{x \mid x \text{ is a } \oplus \text{ ve int}\}$

D4 can provide sets with a ~~set~~ set of R

that compare (useful sometimes) their elts

or to compare some of their properties

"comparison R"

or "order R"

R1 Str ordered set has originally been set up in framework of works of CANTOR & ...

R2 $\mathbb{N}\ \mathbb{Z}\ \mathbb{Q}\ \mathbb{R}$ tot^y ord^{ed} by $\geq \leq$

$<$ strict ~~ord~~ R : ~~...~~

divides by / partial

R3 if R ord on $E \& F$,

restriction ~~R~~ to F = ord on F

"order induced by R in F"

R4 If R order on E,

R' defined by

$x R' y \Leftrightarrow y R x$

is an order on E "reciprocal order" of R

$\leq \rightarrow \geq$

divides by $\mathbb{N}$

is a multiple of

S = basic math^al^ entity whose existence is defined:
it is not defined as itself by but by its properties, given by the axioms
it uses a human process: a kind of categorization feature which allows thought to distinguish several independent qualified elts

T nb of subsets of a S of card n is 2^n

Pf $\emptyset$ 0 items chosen from n i.e C_0^n

$$C_n^k = \vec{v} = \binom{n}{k} = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)}$$

Car Σ of all bin coef

$$\mathrm{Card}(P(E)) = \sum_{k=0}^{n} C_n^k$$

$$(x+y)^n = \sum_{k=0}^{n} C_n^k 1^k 1^{n-k} = (1+1)^n = 2^n$$

EX $\{x_1, x_2, x_3\} = S$

$\{\} = \emptyset$

singletons x_1 x_2 x_3

duets $x_1 x_2$
$x_1 x_3$
$x_2 x_3$

itself $\{x_1, x_2, x_3\}$

$P(S) = \{\emptyset, \{x_1\} \{x_2\} \{x_3\} \{x_1 x_2\} (\ ) (\ ) S$

Card $P(S) = 8$

R order in which elts are differentiated does not come into account when counting parts of the original S

Applied → sets of numbers → limit*

ZF Axiomatic   ZF-C axioms

considered most natural

Strictly technically speaking, are "statements of calcula" for the 1st order predicate calculus in a lang with only one primitive symbol for membership (∈ in R) ..

following should ∴ only be seen as an attempt (...) to express in english the expected significance of these axioms

(A1) Extensionality

$$A = B \iff (\forall x \in A, x \in B) \wedge (\forall x \in B, x \in A)$$

(A2) Empty S exists

$\emptyset$ has no elt   card $\emptyset = 0$

This A can be deduced from another A* →

(A3) Pairing

if

then $\exists$ C containing A & B above and comp as $\{A, B\}$

From the perspective of the sets considered elts, that gives

$$\forall A \forall B \exists C : A \in C \wedge B \in C$$

also shows the $\exists$ence of "singleton" a set $\{X\}$

only elts is X → card = 1

we simply need to apply the axiom asking equality btw A & B

(A4) Sum "Union" → merge of any family of set is a ... set

$\bigcup_i A_i$ or if we take some of its elts $\bigcup_{x \in A} x_i$

(A5) subsets

any set A, the set of all its parts P(A) exists

So for any S A, we can associate a S B which contains exactly the parts C (verbatim C) of the first

$$\boxed{\forall A \exists B \forall C : (C \in B \Leftrightarrow C \subset A)}$$

(A6) infinity

there exist an ∞ S then named "auto successor S" A containing $\emptyset$ such that if x belongs to A, then also $x \cup \{x\}$ belongs to A

(thus perm)

$$\boxed{A \text{ is auto successor} \Leftrightarrow (\emptyset \in A) \wedge (x \in A \Rightarrow (x \cup \{x\}) \in A)}$$

expresses for ex that S int exists

$\mathbb{N}$ is so the smallest auto suc S in a the sense of inclusion

$\mathbb{N} = \{\emptyset, \{\emptyset, \{\emptyset, \dots\}\}\}$ by conv

$0 = \emptyset$

$1 = \{\emptyset\}$

$2 = \{\emptyset, \{\emptyset\}\}$

(A7) regularity = foundation

just eliminate possibility of having A as part of itself

Thus for any non empty S A ~~then~~ there exists a S B which is a elt of A such that no elt of A is a elt of B

(≠ level lang used, a set & its elts have not the same status!)

$$\forall A \neq \emptyset : \exists B \in A, A \cap B = \emptyset$$

and thus result we expected to have

$$\boxed{\forall A, A \notin A}$$

PF $A \in A$

$\{A\}$ Axiom fund

$A \cap \{A\} = \phi$ contradict...

(A8) Replacement schema of

for any S

if a formula f is a functional of then for any SA, there is a SB consisting precisely of the images of A by this f

+ formally

A of elts a & bin Rf

there exists B b such that

$f(a,b)$ is True

If f is a f where b is not free that it means that $\neq b = f(A)$ and $B = f(A)$

$\forall A, \exists a \in A \; \exists! f : f(a,b) \Rightarrow \exists B \; \forall a \in A \; \exists b \in B \; f(a,b)$

So for every set A and any item its contains, then one and only one b defined by the f^al f such that there exists a SB which any elt belonging to SA this is a b belonging to set B defined by the f^al f

EX bin predicate that for the value of any a from A determines the value of any b of B

$P(a,b) = (a=1 \wedge b=2) \vee (a=3 \wedge b=4)$

Sub of A

(A9) Selection comprehension schema

any A & any property B, Sof all elts of A satisfying P $\exists$

any f^{al} ϕ that does not include a as free variable

$\forall A \exists B \forall a : a \in B \Leftrightarrow a \in A \wedge \phi$

→ even $\{a \in \mathbb{N} \mid \exists b \in \mathbb{N}, a = 2b\}$

eliminate paradox naive set $\mathcal{T}$

(Russell (Cantor

R of all sets that don't contain themselves / that we prove a P of R without specifying what is the set

$R = \{E : E \notin E\}$

A10 Choice

Given a set A of non empty mutually disjoint sets, there exists a set B (the set of choice for A) containing exactly one elt for each member A

Ghent

Is' some continuum hyp:

if we can put 2 S_s of nbs in cor term to term, they have the same nb of elts (cardinal)

We can thus map all $\mathbb{N}$ with $\mathbb{Q}$ same card

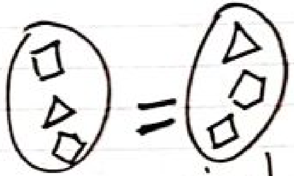
$\mathbb{R}$

then is S whose nb of elts would be located ~~tt~~ btw the two or not.

~~now~~ but we can say the opposite

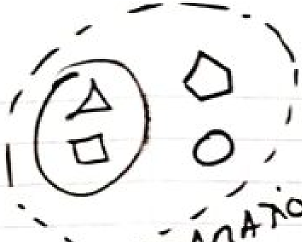
In fact is linked in a more = way we could thing to the C which can also be formulated as follows:

if C is a collection of non empty S_s
then we can select any elt of each S of
the col
if C has a finite set of elts or a countable
set of sets elts, C seems pretty trivial:
We can sort and number the sets of C and
the selection of an elt in each S is simple
- Complicated when C has the power of cont:
how to choose the elts if it's not possible to
number them?
- 1938 (Godel) shows that set T is consistent
with C and without the cont hyp as well, as well!
Cohen 1963 C at CH not related



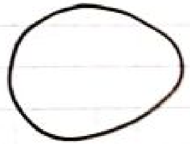
EXTENSION

if 2 Ss have the same elts, then they are =



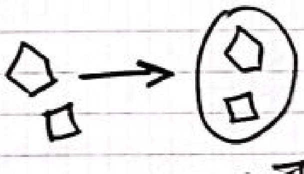
SEPARATION

We can form a SubS of a S, which consists of some elts

 { } ∅

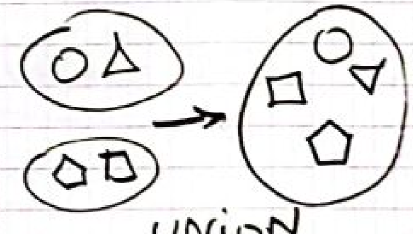
EMPTY S

This is a S with no members,



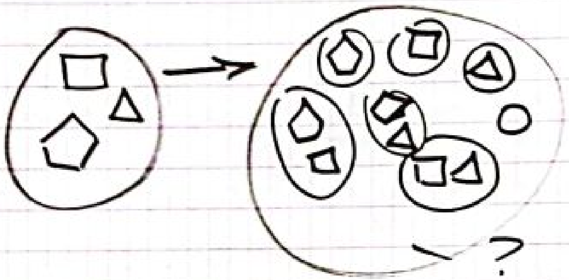
PAIR-SET

Given 2 objects x & y we can form a S $\{x,y\}$



UNION

We can form the $\cup$ of 2 or more Ss

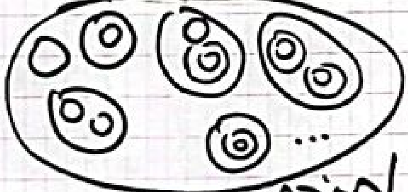


POWER SET

Given any S, we can form the S of all SubSs (the power set)

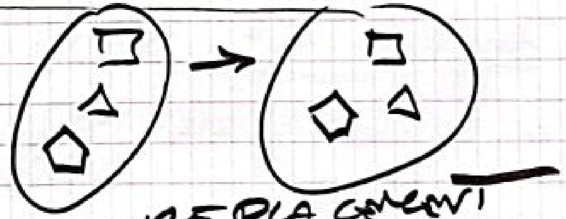
INFINITY

This is a S with infinitely many elts



FOUNDATION

Ss are built from simpler Ss, meaning that every (non-empty) S has a minimal member



REPLACEMENT

if we apply a function to every elt in a S, the answer is still a S

Cardinals

D S_s "equipot"
If there exists a bij btw
thus they have same cardinal
card(S) Card(S) $|S| \neq S$
thus more rigour " a card (which quantifies the nb of items in the set) is an equivalence class for the R of equipot

R (Cantor) real novelty it lets talk about ∞ precisely to def "equipot"

$c_1 = c_2$
" "
Card(A) card(B)
cards can be compared total ordering
Pf that order is complete use Axiom choice
Antisym = Cantor Bernstein T

Say that $c_1 < c_2$ means
A is equip to a proper part of B
But B is not equip to any own part of A
[Card(A) ≤ card(B)
if there is a injection of A into B

Transfinite nbs, that a equipot set (or bij) to N was told to "countable set"

A set, if ~~then~~ there is an int n such that there is at least for each ~~et~~ elt of A a corr item in {1, 2, ... n}
then Card(A) is a "finite cardinal" = n
otherwise ~~Card~~ Card(A) = +∞
infinite

. A is countable if there is bij A ~~CB~~ & N
A Set of numbers A is count if there is bij btw A & part of (N)
maximum

therefore :: TG

check following proposals:

P1 A part of a count set is at most count

P2 A set containing a non count set is also not count

P3 Product of 2 count is count

$R^* = R \setminus \{\emptyset\}$

$R_+ = \{x / x \in R \text{ and } x \geq 0\}$

So any infinite subset of N is equipotent to N itself

even int = int $f(n) = 2n$

N → P a many relative nbs

int .

$\text{Card}(N) = \text{Card}(Z) = \text{Card}(Q) = \aleph_0$

any ∞ part of Q is count

Thus

any ∞ set :: has an ∞ countable part

Since we have proved that set of R has the "power of continuum"

& N has transfinite card $\aleph_0$

Cantor → ? Whether there was a card btw $\aleph_0$ & card R?

in oth words

∞ amount of int & even greater amount R

Does ∃ an ∞ greater than infinite of int & smaller ... R?

. $\aleph_0$ card(N) $\aleph_1$ = card (R) & offering to claim or contradict that

$\aleph_1 = 2^{\aleph_0}$

~~[illegible]~~

It is in vain to prove this result
"continuum hyp"

1300 Hilbert 23 maj issues

solved
1st 1938 Gödel
hyp was not refutable
never prove that it was false
1963 Cohen
demonstrat that we could
never prove that it was true

Cartesian product

D $E \times F = \{(e,f) \mid e \in E \wedge f \in F\}$

$E \times E = E^2$
"set of pairs of elts of E"

$E_1 \times E_2 \times \dots \times E_n$
n-tuples E^n ...

$\text{Card}(E \times F) = \text{Card}(E) \cdot \text{Card}(F)$

$\text{Card}(E_1 \times E_2 \times \dots \times E_n) = \prod_{i=1}^{n} \text{Card}(E_i)$

$\text{Card}(E^n) = [\text{Card}(E)]^n$

Ex
E1 $\mathbb{R}^2$ in plane every pt has the coordinates that are an elt of $\mathbb{R}^2$

E2 2 dice $E = \{1,2,3,4,5,6\}$
outcome elt de E^2 card $= 36$

R the initial basis of $\mathbb{R}^d$ ... ~~intervals~~

~~[illegible]~~

~~7 [illegible]~~

INTERVALS

M of any nbs

$\mathbb{R}$ (particular but freq ex)

D1 $x \in \mathbb{R}$ "upper bound" of M

if $x \geq m$ for $\forall m \in M$

Conversely "lower

≠ terminal!

D2 Given $M \subset \mathbb{R}$, $M \neq \emptyset$, $x \in \mathbb{R}$

"smallest ub"

$x = \sup M$

of M if x is an ub of M and

if for any ub $y \in \mathbb{R}$ we have $x \leq y$

Conversely "smallest lb" $x = \inf M$

equiv in context of analysis

D of I subset of $\mathbb{R}$

$f : E \longrightarrow \mathbb{R}$

$x_0 \in \mathbb{R}$

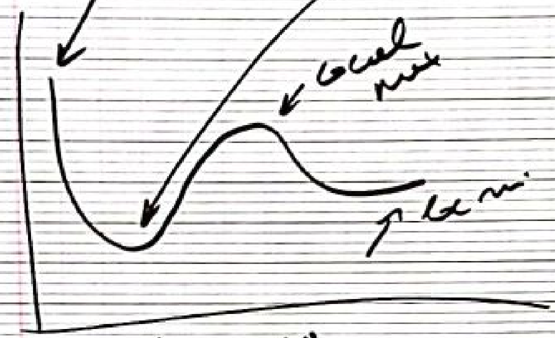
D1 f has a "global maximum" on x_0 if:

$\forall x \in E : f(x) \leq f(x_0)$

minimum $\geq$

global extremum

D2



D3 "upper bounded"

if there is a real number M such as $\forall x \in I$

$f(x) \leq M$

$\sup_I f$

$\inf f$

bounded

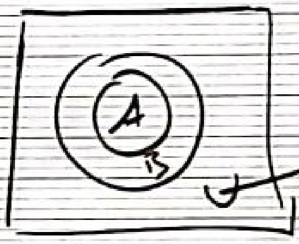
Set operations

~~Set~~ from at least

$A \subset B \subset 3$

inclusion

$$\boxed{A \subset B \Leftrightarrow \forall x \, [x \in A \Rightarrow x \in B]}$$



cantor universe

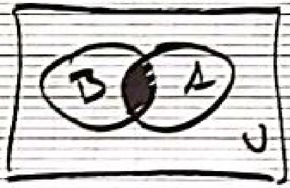
P1 If $A \subset B$ & $B \subset A$ then it implies $A = B$

P2 ——— $\subset$ ——— $A \subset C$ & vice versa

intersection

$A \cap B = \{x \mid x \in A \wedge x \in B\}$

Both



If (A_i) family of sets indexed by $i \in I$

$\cap$ of (A_i), $i \in I$ is

$$\bigcap_{i \in I} A_i$$

explicitly sets are

$$\bigcap_{i \in I} A_i = \{x \mid \forall i \in I \; x \in A_i\}$$

"disjoint" $A \cap B = \emptyset$

furthermore

$A \cap B = \emptyset \Leftrightarrow$ Card ~~Set~~ $(A \cup B) = \text{Card}(A) + \text{Card}(B)$

$A \sqcup B$, "disjoint union"

D A collection $S = \{S_i\}$ of non empty set forms a "partition" of a set A if the following holds

P1 $\forall S_i, S_j \in S$ and $i \neq j \Rightarrow S_i \cap S_j = \emptyset$

P2 $A = \bigcup_{S_i \in S} S_i$

ex Set even nbs & — odd — are a partition of $\mathbb{Z}$

$A \cap B = B \cap A$

Union "merge"

$$A \cup B = \{x \mid x \in A \lor x \in B\}$$

Distributive Property

$$\left(\bigcup_{i \in I} A_i\right) \cap B = \bigcup_{i \in I} (A_i \cap B)$$

$\cap \quad \cup \quad \cap \quad \cup$

Com $\quad A \cup B = B \cup B$

"Idempotence laws"

$$A \cap A = A$$
$$A \cup A = A$$

"Absorptions laws"

$$A \cap (A \cup B) = A$$
$$A \cup \quad \cap \quad = A$$

Assoc

$$A \cap (B \cap C) = (A \cap B) \cap C$$

$\cup \quad \cup \quad\quad \cup \quad \cup$

Dist

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$\cup \quad \cap \quad\quad \cup \quad \cap \quad \cup$

$\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B) - \mathrm{Card}(A \cap B)$

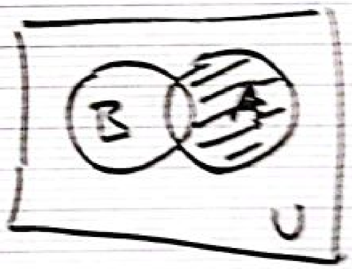
Hence if $A \cap B = \emptyset$

$\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B)$

Difference

$$A \setminus B = \{x \mid x \in A \land x \notin B\}$$

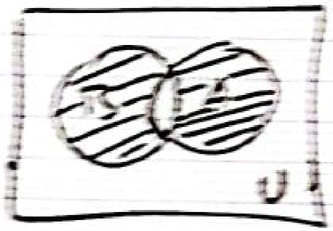
$A \setminus B$



Symmetric diff

U For any $A, B \subseteq U$

$A \Delta B = (A \setminus B) \cup (B \setminus A)$



$= (A \cup B) \setminus (A \cap B)$

P1 Com $A \Delta B = B \Delta A$

P2 [$A^c \Delta B^c = A \Delta B$

P3 $A \Delta B = (A \cup B) \setminus (A \cap B)$

Product set = cartesian

$A \times B = \{(x,y) \mid x \in A \wedge y \in B\}$

f of two real variables which gives real output will be written

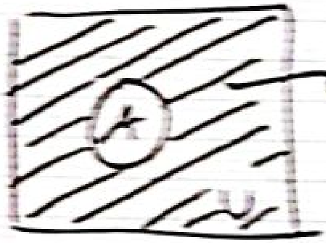
$f(x,y) \to z$

$f: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$

$f(x,y) = z$

Complementarity

$\forall A \subset U \quad \bar{A} = \{x \mid x \in U \mid x \notin A\}$



$A^U = A^c = {}^cA^c$

$\overline{U \setminus A}$

$\left(\bigcup_{i \in I} A_i\right)^c = \bigcap_{i \in I} A_i^c$

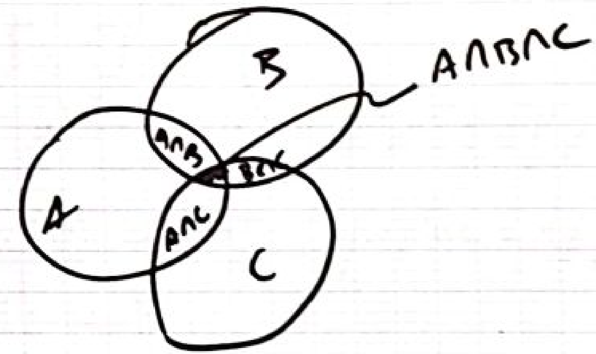
$\cap \quad \cup$

$\bar{\bar{A}} = A$

$A \cap \bar{A} = \emptyset$

$A \cup \bar{A} = U$

The are ~~st~~ also applied to Boolean logic



$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

$A \setminus B \setminus C = (A \setminus B) \cup (A \cap B)$

De Morgan laws in set form

$\overline{A \cap B} = \overline{A} \cup \overline{B}$

∪ ∩

SQL language

query expression with Join

Functions / Applications

D function is the information
A linealy of 2 sets

E F
departure arrival
image de E

x image of x by y

"antécédents" $f(x)$
$f(E)$
images

$f : E \longmapsto F$

arguments in E values in F

n
f often ~~is~~ used for applicaⁿ with scalar numeric values real or complex
that is to say when the arrival set is $\mathbb{R}$ or $\mathbb{C}$
we speak then of "real f" or "complex f"
in the ~~sole~~ case of vector we prefer to use the word "applicaⁿ"

E1 $f(\vec{x},\vec{\alpha},\vec{s}) = \sum_{i=1}^{n} \frac{\alpha_i x_i}{(x_i+s_i)^2}$

$\vec{x} \in \mathbb{R}^n$

$\vec{\alpha} \in [0,1]^n$

$s \in \mathbb{R}_+^n$

$: \mathbb{R}^n \times [0,1]^n \times \mathbb{R}_+^n \longrightarrow \mathbb{R}$

D1 graph = plot = graphic = representation

$f / E \longrightarrow F$

= subset of $E \times F$

$(x, f(x))$ for x varying in E

Set of pairs ... pairing set

(any two pairs ... same ... element ... image (graph of ... ?)

D2 if $f(E,F,\Gamma)$ is a f

$\Gamma \subset (E \times F)$

Source — purpose — graph

$Df = I = \{x \in E \mid \exists y \in F, (x,y) \in \Gamma\}$

definition set

D3 EFG

any f $E \times F \to G$

= composition law

of f $E \times F$ ... G

D4 internal ICL

$E \times E \longrightarrow E$

R ... ICL

+ ICL

D5 external

$F \times E \longrightarrow E$

separate set of E

= "scalar set"

ex $\vec{V}$ space — $\vec{V}$ x real scalar — = ECL

R

= ECL of F on E

Field operations

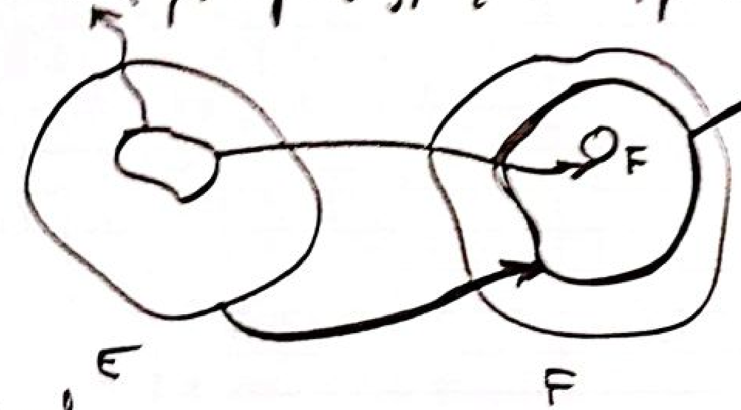
F operate on E

D5

$\mathrm{Im}(f) = f(E) = \{y \in E \mid \exists x \in E, y = f(x)\}$

collection of $f(x)$ for x browsing E — <u>subset of F</u>

~~Kern~~ $\mathrm{Ker}(f) = f^{-1}(\{0\}) = \{x \in E \mid f(x) = 0\}$



R1 Kernel

R2 Im Ker reserved group homomorph~~ism~~ rings, ~~fiel~~ fields and to lin applic^{n} ~~btw~~ btw V space and modules etc

Ex sine f has from its any a kernel that is $2\pi\mathbb{Z}$

a f

D1 <u>surjective</u> f

Any elt of ~~F~~ of F is the image by f of <u>at least</u> an elt of E

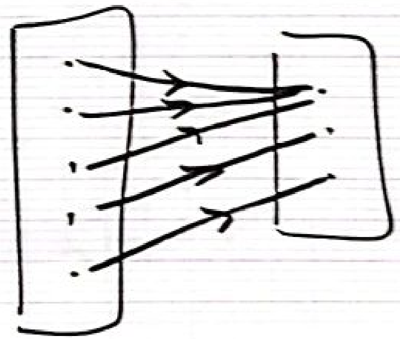
~~E~~ from E to F

<u>e or f</u> $f: E \longrightarrow F$

$\boxed{E \twoheadrightarrow F}$ $\twoheadrightarrow$

iff $F = \mathrm{Im} f$ in other words

$\forall y \in F, \exists x \in E : y = f(x)$



P2 "<u>injective</u>"   ~~surjec~~ sur- inj +

Any elt y of F is the image by f of <u>at most</u> a single elt ~~x~~ of E

$\Longrightarrow$

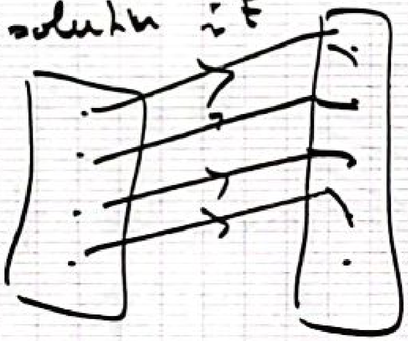
iff the relation $x_1, x_2 \in E$ & $f(x_1)=f(x_2)$ involve.

≠ 2 separate elts have distinct images
at least of one:

P1 $\forall x,y \in E^2: f(x)=f(y) \Rightarrow x=y$

P2 —— $x \neq y \Rightarrow f(x) \neq f(y)$

P3 $\forall y \in F$ eqn in x ≠ $y=f(x)$ has at least one solution in E



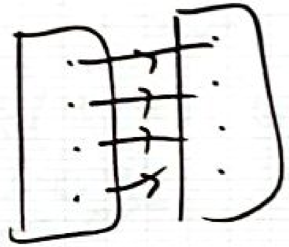
P3 ~~iff~~ "<u>bij</u>" = "total o/f"

both inj & ~~x~~ surj

any elt y of F, $y=f(x)$ admits in E a <u>single</u> (at ~~least~~ or ~~x~~ at) pre image x

$\Longleftrightarrow$

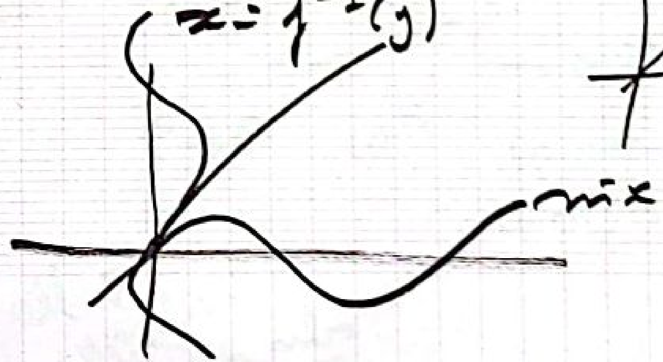
$\forall y \in F, \exists! x \in E : y=f(x)$

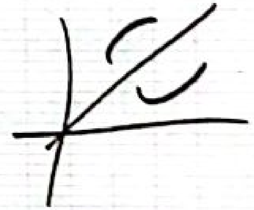


"inverse f" "reciprocal f" f^{-1} $\tilde{f}$

$y=f(x)$

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

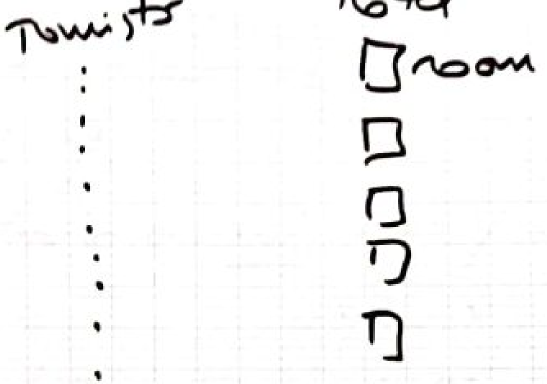




EX

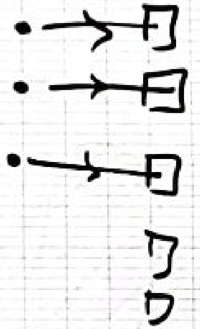
Tourists Hotel

room



• application
to each t is
assigned a room

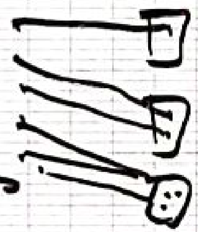
• t want a inj



each a Then
a single room

only possible if ~~nbt~~
nb $t_s \not> r_s$

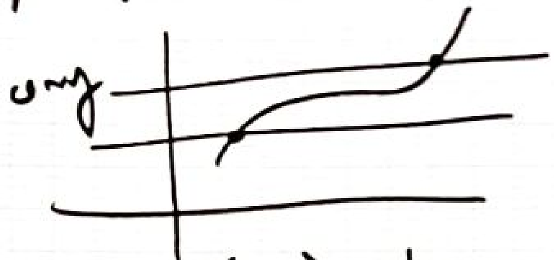
• manager hopes surj



each
room
occupied

~~nbt~~ only pos
if there are
at least as there are
at least as many tourists
than rooms

R1 f bij in $\mathbb{R}$



R2 cont y ↗ or ↘ at any pt in its domain..

PG "composite"

1 $\varphi \; E \to F$

1 $\psi \; F \to G$

$\psi(\varphi(x))$ "composed" a of φ and ψ

"$\psi \circ \varphi$"

χ a G in H

Assoc $\chi \circ (\psi \circ \varphi) = (\chi \circ \psi) \circ \varphi$

→ omit ( )

$E \to E$ $\quad \varphi^k$

~~$\varphi \circ \varphi \dots \varphi$~~

$\varphi \circ \varphi \circ \dots \circ \varphi$

all P applicable to nbs

Cantor - Bernstein T

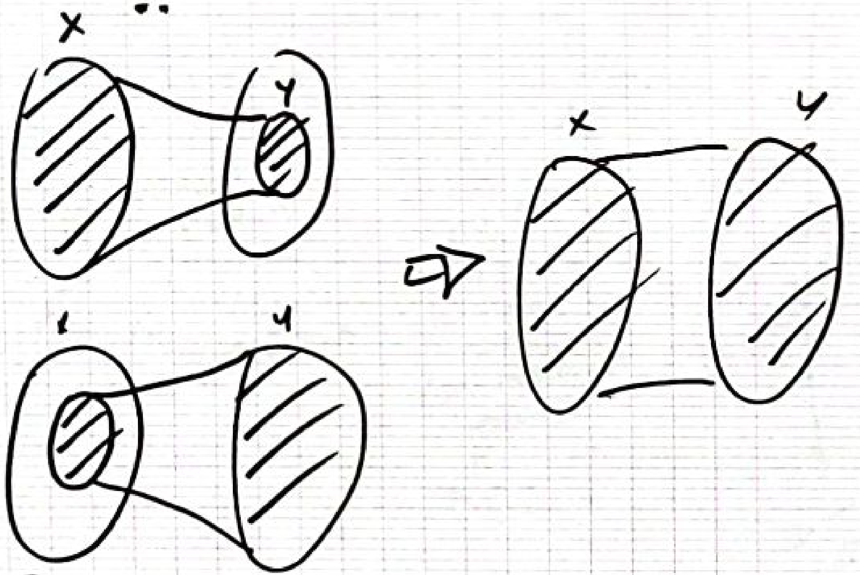
$X \quad Y$

If ther is an inj $X \to Y$ and another $Y \to X$

then both sets are in bij

It is therefore an antisym $\mathcal{R}$

$\therefore$



Formally said true

$card(Y) \leq card(X)$ ~~iff~~ and

$X \leq Y \iff card(X) = card(Y)$

+ tech Y

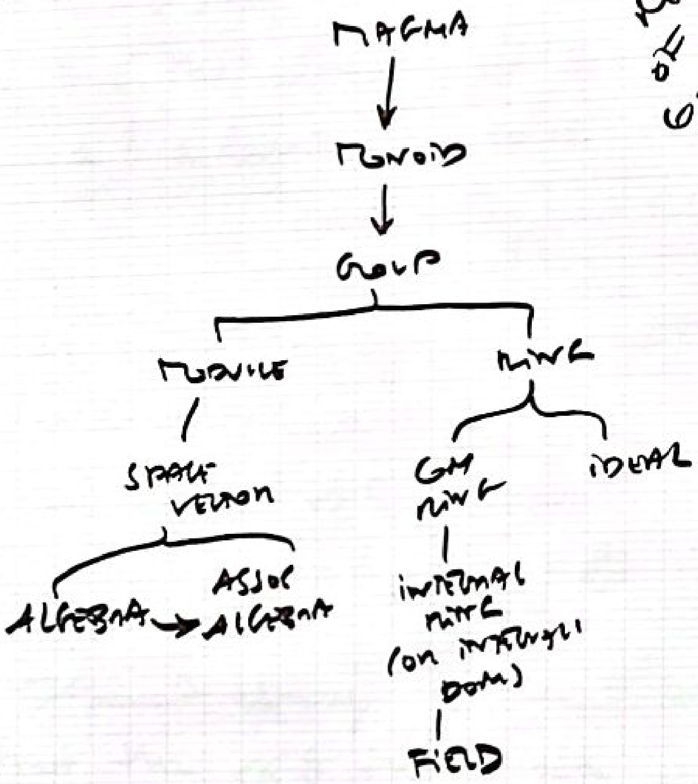
$(X \rightarrowtail Y) \wedge (Y \rightarrowtail X) \iff X \leftrightarrow Y$

Lemma

...

STRUCTURES

"mod alg" (Gauss)
"abstract" — (Galois)



Minimum of constraints = 1

=> maximum

★ o : operation

D Given ★ o iL to a given S E ×× then

D1 ★ "commutative law" if COMMUT

$a \star b = b \star a$

D2 ASSOC

$a \star (b \star c) = (a \star b) \star c$

D3 n is the "neutral elt" for ★ if

$a \star n = n \star a = a$

If this exists it is ! (unique)

D4 "symmetrical elt" — opposite + / inverse × a' of a for ★ if:

$a' \star a = a \star a' = n$

(! unique

~ . D to the Right

D5 o "distributive law" with respect to ⋆ if:

$$a \circ (b \star c) = (a \circ b) \star (a \circ c)$$
$$(a \star b) \circ c = (a \circ b) \star (b \circ c)$$

D6 b is the "absorbing elt" of for all a & a law ⋆ we have

$$\boxed{a \star b = 0}$$

R1 If a is its own sym with respect to the law ⋆ a is involutive

R2 If an elt b of E satisfies:

$$a \star b = b \star a = b$$

absorbing elt

R3 It must always be checked that the n & the s elts are such on the L & on the R thus

Ex $(\mathbb{Z}, -)$ 0 is n to the R

∵ $x - 0 = x$

but $0 - x = -x$

Magma

is components conditions it are operable with respect to an iL ⋆

$(M, \star)$ is a magma $\Leftrightarrow \begin{cases} \star \text{ is on opera}^{\sim} \text{ O} \\ \star \text{ iL} \end{cases}$

R1 ⋆ Cm — Com M

R2 ⋆ ASS — ASS M

R3 ⋆ possess a n

~~S~~ Smtms (unitary ASSOC M

n unitary Com M

D M an elt x is named "regular elt" or "simplifiable elt" to the L if for any pair $(a, b) \in E$

$$\boxed{x \star a = x \star b \Rightarrow a = b}$$

$\not{L}$ R ... to the Right

- thus an elt x is say to be <u>regular</u> if it regular to the R & to the L
- If Gm $\to$ G inv ible

$(M, \star)$

<u>Monoid</u>

$(M, \star)$ monoid $\Leftrightarrow \begin{cases} \star \text{ assoc} \\ \exists \text{ a neutral elt } n \in M \text{ for the law } \star \end{cases}$

R1 $\star$ Gm Abelian M

R3 Some text books <u>semigroup</u> with no assoc $\star$! + n

$\mathbb{N}$ $(+)$ and abelian monoids
+ $\times$

+ $\underline{i_0}$ $\forall a, b \in \mathbb{N}$

$a+b = c$

~~We can~~ We can prove

$c \in \mathbb{N}_a$

$$\sum_{i=1}^{a} 1 + \sum_{i=1}^{b} 1 = \sum_{i=1}^{a+b}$$

<u>Stable</u>

Does it exist in line with previous

ex for + a sym $\exists$ c such that $\forall a, b \in \mathbb{N}$ we have

$$\left(\sum_{i=1}^{a} 1 + \sum_{i=1}^{b} 1\right) + c = \left(\sum_{i=1}^{a+b} 1\right) + c = 0$$

with $c \in \mathbb{N}$?

$-c$

$a+b = -c$

+ <u>no sym</u> — <u>does not exist</u> !

ny add^{n} $\ominus^{ve}$ nb !

- Similarly

$a' \cdot a = n = 1$

$a' = \dfrac{1}{a}$ exist for 1 $\not\exists$ in $\mathbb{N}$

$\mathbb{N}$	+	−	×	/
IO (closure)	YES		YES	
COM	YES		YES	
N elt	YES (0)	NO	YES (1)	NO
Absorbing elt	NO		YES (0)	
sym	NO		NO	

P1 $(\mathbb{N}, \leq, \geq)$ completely ord est
just one op

P2 $(\mathbb{N},+)$ $(\mathbb{N},\times)$ Abelian M

P3 0 absorbing for

P4 − / $\nexists$ in $\mathbb{N}$

P5 $\mathbb{N}$ Abelian M tot ord with respect to + & ×
only one!

unique
order R

→ 4 M's $(\mathbb{N},+,\geq,\leq)$
×?

R1 poor

R2 algebraic str is tot ordered with respect to some laws

means that given a law *
& R a, b, c, d
then if aRb and cRd
imply $(a*c)R(b*d)$ *
$(S,*,R)$ (S,R)

Groups internal a law

$(G,*) \Leftrightarrow \begin{cases} * \text{ Assoc} \\ \exists \in G \text{ a N} \\ \forall x \in G \text{ has a symmetrical (inverse) for } * \end{cases}$

GANS
+ addition
e 0 its value
x −x

* Com Abelian G Com G

If th $\exists$ at least one elt a
such that every elt is a power of a
or of the sym of a Cyclic G of
finite "monogenic" generator a

Monogen^Y G

e not reduced only to {e}
will be monogeneous, if there ∃
a distinct from e such that
$G = \{e, a^1, a^2, \dots a^n, \dots\}$
will be cyclic, if there ∃ a nonzero
int n for which $a^n = e$
Smallest nonzero int satisfying this
is then the "order of G"

- Show whether

Z tot^Y ord^ed abel G + x
extension of N

Z	+	−	x	/
iO	YES	YES	YES	NO
A	YES	NO	YES	
C	YES	NO	YES	
N	YES (1)	(0) NO TO L	YES (1)	
ABS	NO	NO	YES (0)	
S	YES (opposite sign)	YES	NO	

P1 (Z, ≤, ≥) Comp^Y ord^ed
order of z

P2 (Z, +) comm G Ö n

P3 / ∄

P4 Abel G tot^Y ord wrt +

x ~~G^Y~~

. Z too ~~restricted~~ restricted conditions

$\mathbb{Q} = \{\frac{p}{q} \mid (p, q) \in \mathbb{Z} / q \neq 0\}$

$(\mathbb{N}, \mathbb{Z}) \subset \mathbb{Q}$

$(\mathbb{Q}, \leq, \geq)$ tot ord^ed
(+) Abelian G
what becomes interesting with $\mathbb{Q}$ is x
becomes an id & form a commutative
"multiplicative G" with respect to $\mathbb{Q}^*$

Scanné avec CamScanner

PF Let us prove that $\leq \exists$ for $\times$

$a \times a = n = 1$

Since in $\mathbb{Q}^*$ every elt can be put

$$a = \frac{p \in \mathbb{Z}}{q \in \mathbb{Z}^*}$$

So since $a' = \frac{1}{a} = \frac{1}{\left(\frac{p}{q}\right)} = \frac{q}{p}$

this is $\therefore$ a S to every elt in $\mathbb{Q}^*$ for $\times$

/ $\exists$ ASSOC

$\forall (p, q, r) \in \mathbb{Q}^*$

$\cancel{a}$ p

$\frac{q}{r} = \frac{p}{\frac{q}{r}}$

$\frac{a}{b} = \frac{b}{a} = \pm 1 \Rightarrow a = \pm b$

$\mathbb{Q}$	+	−	×	/
iL	Y	Y	Y	Y
A	Y	N	Y	N
C	Y	N	Y	N
N elt	Y(0)	N (0 to L)	Y (1)	Y (1 to R)
Abs elt	N	N	Y (0)	Y (0 at numerator)
S	Y (opp sign)	(opposite sign)	NO (exception in $\mathbb{Q}^*$)	N

P1 $(\mathbb{Q}, \geq, \leq)$ totally ordered

P2 $(\mathbb{Q}, +)$ $(\mathbb{Q}^*, \times)$ make totally non Abel G's

P3 0 ABS with respect $(\mathbb{Q}^*, \times)$

P4 Abelian G totally ordered WRT + $\times$

$(\mathbb{Q}, +, \leq, \geq)$ $(\mathbb{Q}^*, \times, \leq, \geq)$

Same P applicable to $\mathbb{C}$

≠ latter not orderable

$+ - \times /$ 2 rules types $x+iy$

$\mathbb{C} \longrightarrow \mathbb{C}$ ...

cyclic G

in $\mathbb{C}$ $G = \{1, i, -1, -i\}$

$(G, \times)$ Ab G

also monogenic : it is generated by the powers of one of its elts i or $(-i)$

finite → "cyclic G"

RING Heart of Gm alg

$+ - \times$

A Gm G is a ring 2nd IL of C

$(A, +, \times) \Leftrightarrow \begin{cases} (A,+) \text{ Ab G} \\ \times \text{ ASSOC} \\ \times \text{ DIST relat to } + \end{cases}$

0 1

R1 × Gm com Ring

∃ non Gm \ when st somets we must reinforce the pot

N 1

to be N on both to R & L

$1a = a1 = 1$

ex

Non Gm set square $n \times n$ mat with coef in .. $M_n(\mathbb{R})$

R2 If ∃ N for × unitary ring 1 unit of the ring

R3 If $a \times b = 0 \Rightarrow (a = 0 \text{ or } b = 0)$ regardless of elts a and b

"integral ring" = or without zero divisors

× zero

R4 factorial ring = unit & integral Gm in which fund T of arit using

D1 An elt a is a "unitary elt" if there is a $b \in A$ such that $ab = ba = 1$

If such a b exists it is ! (eny class)

D2 L zero divisor

$x \neq 0$ $ax = 0$ two sided

~~EX~~

E1 the only zero divisor of $\mathbb{Z}$ is 0

E2 If 2×2 Mat (over any nonzero A) we can find a and a nonzero x as following

$$\begin{pmatrix}1 & 1\\ 2 & 2\end{pmatrix}\begin{pmatrix}1 & 1\\ -1 & -1\end{pmatrix} = \begin{pmatrix}2 & 1\\ 2 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 2 & 2\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$$

R1 integral iff has zero divisors (excepted 0)

R2 Concepts of unit and zero are incompatible but one elt can be neither

ex $\forall$ int $\neq \{0, -1, +1\}$

these are neither units nor divisors from zero = "regular elements"

ex – polynomials
– any

E $(\mathbb{Z},+)$ $(\mathbb{Q},+)$ $(\mathbb{R},+)$ $(\mathbb{C},+)$ tot ordered

4 Ab G

Since / ring Assoc

We can restrict to studying for each of pair laws $\underline{+ \ \& \ \times}$

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

sub R

unitary & integral com rings

Sub ring A

P1 $a+b = a+c \Rightarrow (b=c) \quad \forall a,b,c \in A$

PF every elt has opp/sym indeed we ~~have~~ can add to $-a$

$(-a)+a+b = (-a)+a+c$

$0+b = 0+c$

P2 $0.a = 0 \quad \forall a \in A$

PF $\exists$ N $\exists$ sym DIST and

$0.a + a = 0.a + 1.a = (0+1).a = 1.a = a$

$0.a + a = a$

$0.a = 0$

P3 $(-1).a = -a$

SUBRING ~~A~~ A SCA

P1 $1 \in S$
P2 $a \in S \Rightarrow -a \in S$
P3 $(a,b) \in S \Rightarrow a+b \in S$
P4 $(a,b) \in S \Rightarrow a.b \in S$

E ~~x~~ $\mathbb{Z}$ is a sub ring of $\mathbb{Q}$ & $\mathbb{R}$

FIELD

$$D\ (F,+,\times) \Longleftrightarrow \begin{cases} (F,+,\times) \text{ is a unitary ring} \\ (F-\{0\},\times) \text{ is a G} \end{cases}$$

Hence Non zero ring in which any non zero elt is invertible or

Ring of which all non zero elts are unit elts is a F

R1 $\times$ Com

R2 Quaternions ~~Com~~ $+, \times$

$\mathbb{Z}, +\times$
$\mathbb{Q} + \times$
$\mathbb{R} + \times$
$\mathbb{C} + \times$

first determine which one do not Gingilike G_s with respect to $+$ $\times$

$\exists$ inverses ~~assumed~~

fundamental

$\times$ Com

$\mathbb{R}$ + ×
Com F tot ordered

$\mathbb{R}$ + ?
GMF

$\mathbb{R}$ +
GMG

+ — iL, ASS, COM
Thr ∃ n 0
Any real nb opposite

$\mathbb{R}$ ×
GMG

× — 1
inverse

× DIST rel to +

$\mathbb{R}$ ≤
tot ordered — Ref, Antisy, Trans

Thus Field $\mathbb{R}$ or $\mathbb{C}$ + - × ÷ ∈ F
(reproduce set operations) NO

$\mathbb{Z}$ cannot form a field

K-VECTOR SPACES EV

on the Field ~~K~~ K $\nearrow \mathbb{R}$ $\searrow \mathbb{C}$

$\mathbb{K}$

$(E,+,\cdot) \Leftrightarrow \begin{cases} (E,+) \text{ Abelian G} \\ \cdot \text{ external law} \end{cases}$

def by $\begin{cases} \cdot : E\times K \to E \\ (x,a) \longrightarrow a\cdot x \end{cases}$

~~(a,x)~~ R

$((x,a) \longrightarrow a\cdot x)$

NB!

À GAUCHE!

$\mathbb{K}\times E \to E$?

$(a,x) \longmapsto a\cdot x$

$(\lambda,\vec{u}) \longmapsto \lambda\vec{u}$

erreur ou lex ?

??!!

2 CL

1 iLC +

1.1 Assoc

$\forall \vec{x},\vec{y},\vec{z} \in E : (\vec{x}+\vec{y})+\vec{z} = \vec{x}+(\vec{y}+\vec{z})$

1.2 Com

$: \vec{x}+\vec{y} = \vec{y}+\vec{x}$

1.3 N elt

~~$\forall \vec{x} \in E, \exists \vec{x}' \in E : \vec{x}+\vec{x}' = \vec{0}$~~

~~1.4 opp elt~~

$\exists \vec{0} \in E : \forall x \in E, \vec{x}+\vec{0} = \vec{x}$

1.4 OPPOSITE elt

$\forall \vec{x} \in E, \exists \vec{x}' \in E : \vec{x}+\vec{x}' = \vec{0}$

2 ECL •

2.1 ASS

$\forall \lambda,\mu \in \mathbb{K}\ \forall \vec{x} \in E$

$\lambda\cdot(\mu\cdot\vec{x}) = (\lambda\cdot\mu)\cdot\vec{x}$

2.2 Dis on the R with respect to field K

$(\lambda+\mu)\cdot\vec{x} = \lambda\vec{x}+\mu\vec{x}$

R

2.3 L Dis with respect to E

$\lambda\cdot(\vec{x}+\vec{y}) = \lambda\cdot\vec{x}+\lambda\cdot\vec{y}$

L

2.4 N elt $1\cdot\vec{x} = \vec{x}$

10 Ps

"vectoriel algebraic str"

elt. = $\vec{v}$, K = scalars

R1 resx^4 iL + x

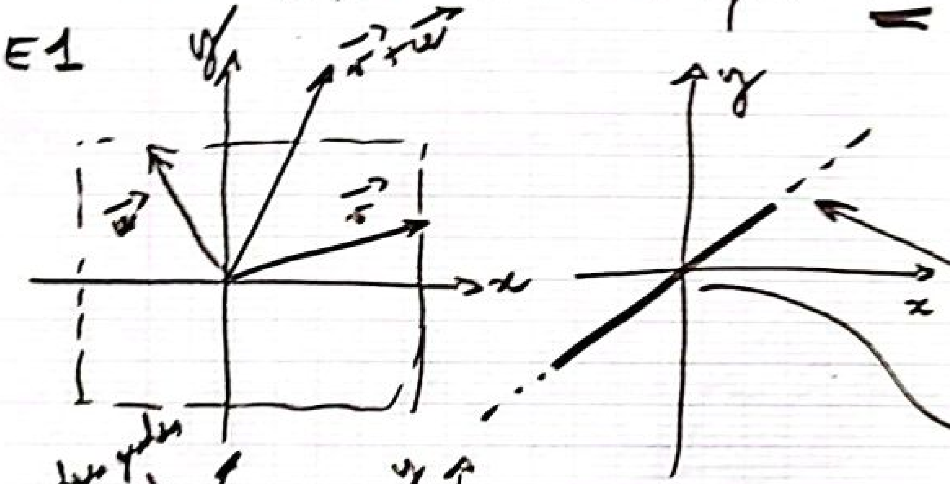
R2 K Field greek letter

E letter

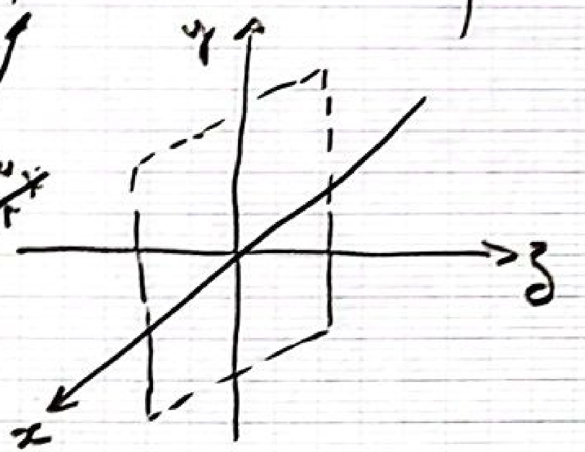
D subspace for $\mathbb{R}^n$

Some ~~subset~~ Subsets of $\mathbb{R}^n$??

E1



vector yields region of $\mathbb{R}^3$



perspective

Example of a concept of vector space

This subset (~~of~~ the rectangle) is not a vector space !

among other things, 10 P (closure) of Ab G is ~~not~~ not satisfied.

Indeed

$\vec{v}, \vec{w}$ $\quad \vec{v}+\vec{w}$ may come out of rect.

on other hand, it is easy to see that the infinite line $\mathbb{R}^1$ follows all Ps → and a vector space

must pass → Origine,

otherwise P of Neut of Ab G would not be respected

no longer ∃

Scanné avec CamScanner

E2 "~~P~~ polynomial vector space" with ~~xx~~ real coef of degree two or less P^2

$x = t^2+2t+3$

$y = -t+5$

- we can form VS with sets of fs more ~~xxxx~~ general than 10Ps
- So defined, a VS E on K is an action of $(K,\times)$ on $(E,+)$ which is compatible with the G law (by ~~xx~~ extension an automorph

D E VS "~~#~~ vectorial subspace" F of E iff

$F \neq \emptyset$
$\forall (x,y) : \in F^2, x+y \in F$
$\forall \lambda \in K, \forall x \in F: \lambda x \in F$

$F \neq \emptyset$
$\forall (\vec{x},\vec{y}) \in F^2: \vec{x}+\vec{y} \in F$
$\forall \lambda \in K, \forall \vec{x} \in F: \lambda \vec{x} \in F$

C-ALGEBRA A

on field "K-ALGEBRA"

2 ICL $+$ $\times$ Gos product

1 EL $\bullet$ with operator domain $\mathbb{C}$ (multiplication by a scalar)

$(A,\mathbb{C},+,\cdot,\times) \iff$ iff
$(A,+,\cdot)$ is a $\mathbb{C}$-vector space
$(A,+,\times)$ — unitary ring
$\forall \lambda \in \mathbb{C}$
$\forall a,b \in A$:
$(\lambda a)\cdot b = a\cdot(\lambda b)$
$= \lambda(a\cdot b)$

Scanné avec CamScanner

E1 Euclidean $\mathbb{R}^3$

$+$

$\cdot$

$\times$ Cross product

Not assoc — Comm

$\mathbb{R}$-algebra

$(\mathbb{R}^3, \mathbb{R}, +, \cdot, \times)$

E2 $\mathbb{C}$ is a $\mathbb{R}$-algebra

Com → Loop / Quasi G

Loop	Quasi G
Closure	Closure
Id	Inv
Inv	

SUMMARY

	Magma	Semi G	Monoid	G	Ab G
Closure		•	•	•	•
ASS			•	•	•
Id el				•	•
Inv					•
Comm					

Closure

semi category

category

groupoid

CLOS	For all a, b in S, a+b dans S
ASS	$(a+b)+c = a+(b+c)$
ID	$\exists 0$ such a $0+a=a+0=a$
INV	each a $\exists -a$ $a+(-a)=-a+a=0$
Com	$a+b=b+a$ $\forall$

G additive sum $(S,+,0)$

$a \times b$

$(a\times b)\times c = a\times(b\times c)$

$1\times a = a\times 1 = a$

$1/a$ $a\times 1/a = 1/a \times a = 1$

$a\times b = b\times a$

$\times$ $(S,\times,1)$

$(A, *, e)$

$a * b$ — CL

$(a * b) * c = a * (b * c)$ — ASS

$e * a = a * e = a$ — Id

$a * (b) = b * a = e$ — In

$a * b = b * a$ — COM

FIELD

here we generalize our 3 inputs
defined above

- S becomes a specific instance of an input Set
- $+ \times$ —— spec inst of gen class of operator
- 0 and 1 —— gen class of Identity elts

√ Abelian G

Sets $\mathbb{N}\ \mathbb{Z}\ \mathbb{R}\ \mathbb{C}$	$\longrightarrow A$	Clos
		ASS
operators $\{+, -\ \text{mult}\}$	$\longrightarrow *$	Id elt
		inv —
Identity elts $\{0, 1, \{\} \ldots\}$	$\longrightarrow e$	Com

$\{F, +, 0, \times, 1\}$

CL $a + b \in F$

ASS $(a+b)+c = a+(b+c)$ holds

ID $\exists 0 \quad 0 + a = a + 0$

IN $(-a) \quad a + (-a) = -a + a = 0$

Com $a + b = b + a$

CL $\times$

ASS

ID 1

INV $1/a$

L DIST $a \times (b + c) = (a \times b) + (a \times c)$

R DIST $(a + b) \times c = (a \times c) + (b \times c)$

MORPHISMS

Str preserving map from 1 str → another

in SG morphisms = fn

LIN ALG → linear transform

GT Homomorph

TOPOLOGY → Cont fns

...

HOMOTOPY

f → nucleus "ideals"

→ identify one alg^c str to anoth

$D_1 (A, \star) (B, \circ)$ Magmas

$f : A \to B$

'just' homomorph of Magma = morph

if

$\boxed{f(a \star b) = f(a) \circ f(b) \quad \forall a, b \in A}$

Image of a comp^n in A is the comp of images in B

D_2 Monoid

$+ \quad f(1_B) = 1_B$

neutral

~~homom~~

D3 Rings

~~A~~ ~~A~~ E, x, T
F, □, O

$f : A \longmapsto B$

a, a' neutral with respect to "$\cdot$"

$f(1_A) = 1_B$

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

$f(a \cdot a') = f(a) f(a')$

Given $f : A \longmapsto B$ homomorph rings

P1 $f(0) = 0$

PF

P2 $f(-a) = -f(a)$

PF

P3 If a unit of A

then $f(A)$ is a unit of B

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

$\frac{*}{I}$ / powerful

A homomorph rings

$f : A \longmapsto B$

is inj

iff the elt 0 is the only preimage of 0 (i.e. $\ker f$) i.e.

$\ker(f) = \{0\}$

D4 $(A,+)$ $(B,\star)$ G_s

$f : A \longmapsto B$ homomorph of G

if
$$\begin{cases} f(x+y) = f(x) \star f(y) & \forall x,y \in A \\ f(1_A) = 1_B \\ f(x^{-1}) = (f(x))^{-1} & \forall x \in A \end{cases}$$

E exp f e is a morph of $(\mathbb{R}^+,+)$ on $(\mathbb{R}^+,.)$

D5 Field

if Ring

ltn 2 sth elts of F are all invertible

every is inj

D6 A B K-vector spaces

linear mapping or linear a

$f(x+y) = f(x) + f(y)$

$f(\lambda x) = \lambda f(x)$

$L(A,B)$ S of lin appn

R1 already def concept but dit not specify that

R2 = linear form iff $B = K$

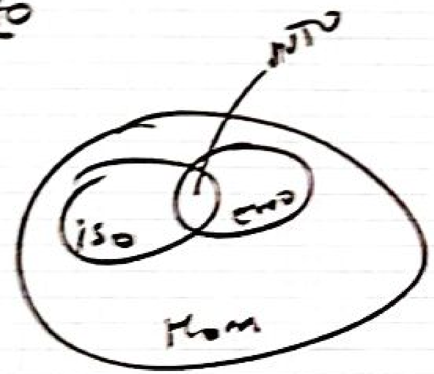
D7 homomorph bij → iso $A \simeq B$

allows identificat ~~of~~ of 2 Ss with an identical alg str but where elts are named in ≠ ways

D8
If f is a purely internal mapping
"endo"

R if Then f restricted to $I(f)$
$f(E) \subset E$
restrict = surj

D9 + bij auto



IDEAL

D A Com Ring ~~like~~ like $(\mathbb{R}, +, \cdot)$
$S \subset A$ is an ideal if

P1 For all $a, a' \in S$ $a + a' \in S$

P2 — a, r $r \cdot a \in S$

~~of~~ Closed subs for +
& Stable for $\cdot$ by any elt of A

E Set even nbs
$\mathbb{Z}_{2k}$ ideal of the S of $\mathbb{Z}$

R $S = \{0\}$ & $S = A$ "Trivial ideal"

To know if an ideal is equal to whole ring is useful

PF

D1 And $I \neq A$ of a ring A is named "principal ideal" if then $\exists\, a \in A$ such as $I = (a)$

D2 A ring of which $\forall I$ are princ "principal ring".

E $\mathbb{Z}$ is principal

...

D R $f: \mathbb{Z} \to \mathbb{R}$
$\text{char}(\mathbb{R}) = h = 0$

...