Beyond Sets: Equip a set with "algebraic structure"

- nonempty set A (or more)
- operations (start with a binary operation) $* : A \times A \to A$
  (could have a collection of operations of finite arity.
  eg. ternary $* : A \times A \times A \to A$
  unary $* : A \to A$
  0-ary $e : \{\bullet\} \to A$
  in other words $e \in A$. "zero inputs"
- identities axioms

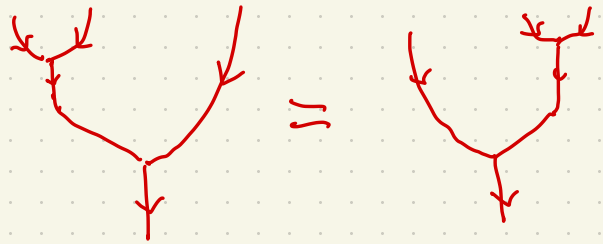
$* : A \times A \to A$

Ex 1 MAGMA $(A, *)$ binary operation, no laws

eg. $(\mathbb{R}, x * y = xy^2 + 3x - y)$

Ex 2: SEMIGROUP $= (A, *)$ ASSOCIATIVE LAW HOLDS

$$(a * b) * c = a * (b * c)$$



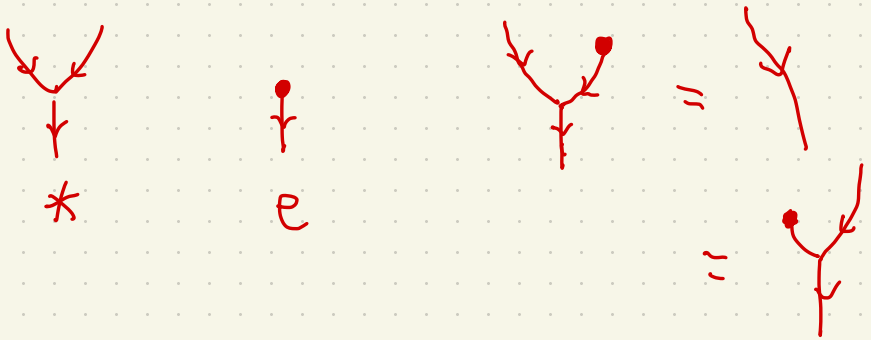
Ex3: MONOID $(A, *, e)$ SEMIGROUP

WITH IDENTITY i.e. $e \in A$

$$e * a = a * e = a \quad \forall\, a \in A$$

$(\mathbb{Z}, \cdot, 1)$ MONOID

$(\mathbb{Z}, +, 0)$ MONOID.



Ex. GROUP $(G, *, e, i)$

$(G, *, e)$ MONOID

i unary "inversion"

$g \in G$

$i(g) = g^{-1}$ is the inverse of g i.e.

$$g^{-1} * g = e = g * g^{-1}$$

(Show: the inverse is unique when it exists)

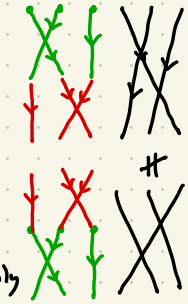
e.g. $(Bij(X,X), \circ, I_X)$ inversion of Bijct.

In case $X = B_n$, $Bij(B_n, B_n) = S_n$ the permutation group.

note this group not commutative. $f \circ g \neq g \circ f$

when $*$ is commutative ($a * b = b * a \ \forall a, b$.) we call G an

ABELIAN GROUP



Ex.: Ring.

Ex: Field

$f \circ g \overset{?}{=} g \circ f$ not necessarily the case.

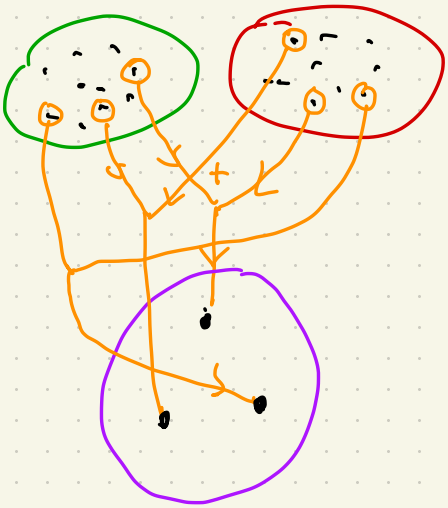
Example of an abelian group

$(\mathbb{Z}, +, 0, \text{inv}_+ : n \mapsto -n)$

- $\mathbb{Z}$: binary operation, assoc. + commutative
- $+$: Identity element.
- 0: inversion: every elt has inverse.
- $\text{inv}_+ : n \mapsto -n$

$\mathbb{Z} = \{ \cdots -3\ -2\ -1\ 0\ 1\ 2\ 3\ 4 \cdots \}$.

Construct some finite groups from $\mathbb{Z}$: define an equivalence relation which partitions $\mathbb{Z}$ into equivalence classes in such a way that



is compatible with partition.

As a result, the partition itself i.e. the set of equivalence classes becomes a group

Define equivalence relation $\sim$

Choose a positive integer n.

We'll define an equivalence relation $\sim_n$

If $a, b \in \mathbb{Z}$ then $a \sim_n b$

when $b - a$ is divisible by n.

e.g.: If $n = 10$ then $\begin{cases} 1 \sim_{10} 11 \sim_{10} 21 \\ -5 \sim_{10} 5 \\ 0 \sim_{10} 10 \end{cases}$

$7863 \sim_{10} 7873$

$\sim_{10} 3$

In fact, every integer is equivalent to a unique elt of $\{0, 1, \ldots, n-1\}$.

$\uparrow$ n elts $\uparrow$

the resulting equivalence classes are called

$$\{\underbrace{[0]}_{[n]}, \underbrace{[1]}_{[1+n]}, \dots, [n-1]\} = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$$

this finite set "inherits" the operation $+$:

$n = 10$

$$\begin{array}{ccccc} 1 & + & 2 & = & 3 \\ \wr & & \wr & & \wr \\ 211 & + & 12 & = & 223 \end{array}$$

i.e. if we define the sum as follows

$$[a] +_{\mathbb{Z}_n} [b] = [a +_{\mathbb{Z}} b]$$

↑ trying to define

for this to be a definition, must check that it does not depend on the choices of representatives a, b

if $[a'] \overset{①}{=} [a]$ and $[b'] \overset{②}{=} [b]$

then show $[a' +_{\mathbb{Z}} b'] = [a +_{\mathbb{Z}} b]$

① $\Rightarrow \quad a' - a = k_1 n \qquad k_1 \in \mathbb{Z}$

② $\Rightarrow \quad b' - b = k_2 n \qquad k_2 \in \mathbb{Z}.$

$\Rightarrow (a'+b') - (a+b) = (a'-a) + (b'-b)$

want this to be mult of n.

$= k_1 n + k_2 n$

$= (k_1 + k_2) \cdot n.$

$\Rightarrow [a'+b'] = [a+b]$ □.

$\Rightarrow \left(\mathbb{Z}_n, +, [0], \text{inv}([n]) = [-n]\right).$

(set of size n.)

a new abelian group $\mathbb{Z}_n$

"the group of integers modulo n"

---

note: $a, b \in \mathbb{Z} \qquad a \sim_n b$

" $a \equiv b \pmod n$ "

Beyond groups:

Rings: Rig Rng

$((R, +, 0, i), \cdot, 1)$

- $(R, +, 0, i)$: abelian group, "the addition"
- $\cdot$: additional associative binary op. (may be non-commutative), "the multiplication"
- 1: multiplic. identity element.

Compatibility axiom between $+, \cdot$:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

Distributive axiom.

E.g.

(1) $((\mathbb{Z}, +, 0, \text{inv}_+), \cdot, 1)$ ← multiplic. identity elt.

↑ multiplication

there do not necess. exist inverses of elts using $\cdot$ eg. $\frac{1}{2} \notin \mathbb{Z}$

but there is a mult. identity. 1

$$1 \cdot n = n$$

Eg 2 $\mathbb{Z}_n$ is a ring for any $n \in \{2,3,4,\dots\}$

- we saw already that $(\mathbb{Z}_n, +, [0])$ is an abelian group.
- The multiplication operation $[k]\cdot[l] = [k\cdot l]$ (mult. in $\mathbb{Z}_n$ ↓, multiplication in $\mathbb{Z}$ ↓)

  is well-defined: if $[k'] = [k]$ and $[l'] = [l]$ are alternative representatives, i.e. $k' = k + an$, $l' = l + bn$ for some $a, b \in \mathbb{Z}$,

  then $k'l' - kl = k'l' - kl' + kl' - kl$
  $= (k'-k)l' + k(l'-l)$

  is divisible by n since these are
- $[1]$ is the multiplicative identity
- check the distributive law

this means $(\mathbb{Z}_n, +, [0], \cdot, [1])$ is a Ring

In fact this ring is commutative since $a\cdot b = b\cdot a \ \forall a,b$.

eg.: $\mathbb{Z}_3$

+	0	1	2
0	0	1	2
1		2	0
2			1

·	0	1	2
0	0	0	0
1		1	2
2			1

$\mathbb{Z}_4$

+	0	1	2	3
0	0	1	2	3
1		2	3	0
2			0	1
3				2

·	0	1	2	3
0	0	0	0	0
1		1	2	3
2			0	2
3				1

notice that $[2]\cdot[2] = [0]$ in $\mathbb{Z}_4$. This happens because $4 = 2\cdot 2$ is not prime!

Def^n A **field** is a commutative ring where every nonzero element is invertible.

"zero" means the additive identity element

Summary of all **structure** + **axioms** of a field:

structure: $(F, +, 0, \cdot, 1)$

- F: set
- $+$: addition
- 0: additive identity
- $\cdot$: multiplication
- 1: multiplicative identity

axioms:

Axioms for $(F, +, 0)$

$\forall a, b, c \in F$

$(a+b)+c = a+(b+c)$	associative
$a+b = b+a$	commutative
$a+0 = a$	0 is additive identity
$\exists d \in F : a+d = 0$	all elements have additive inverse

Axioms for $(F, \cdot, 1)$

$\forall a, b, c \in F$

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$	associative
$a \cdot b = b \cdot a$	commutative
$1 \cdot a = a$	1 is multiplicative identity
if $a \neq 0$ $\exists d \in F : ad = 1$	nonzero elements have multiplicative inverses

Compatibility Axiom:

$\forall a, b, c \in F, \quad a \cdot (b+c) = a \cdot b + a \cdot c$ distributivity

Examples of Fields:

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ familiar fields
- $\mathbb{Z}_p$ for p prime (why?!)

$\mathbb{Q} \subseteq \mathbb{R}$ and $\mathbb{R} \subseteq \mathbb{C}$ are examples of **subfields**:

Def^n A **subfield** of F is a subset S which "inherits" the structure of F. This means that S contains $0, 1$ and the sums, products, and (both kinds of) inverses of elements in S. This makes $(S, +, 0, \cdot, 1)$ into a field.