Rings

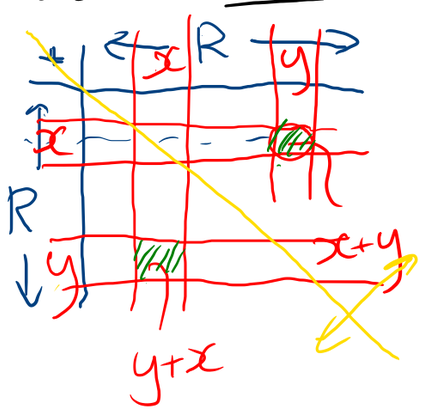
Abstract Algebra;

- groups → set c/ 1 comp^ rule. + o
- rings → " c/ 2 comp^ rules + x
- fields → rings → inverses
- vector spaces - eigenstract (mut)
- modules - vector space c/ scalar are from rings.

RING:

① Start c/ a set symbols $R = \{\dots\}$

② Define two composition laws:



Addition

- Abelian group - commutative.
  - closure
  - assoc'v
  - identity
  - inverse
  - commutative: a+b = b+a

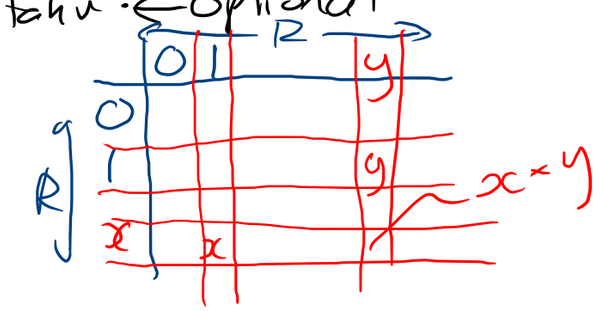
0

Mult^: - composition rule.

1. closure: $x \times y \in R \quad \forall x, y \in R$
2. associativ: $(x \times y) \times z = x \times (y \times z) = x \times y \times z$.

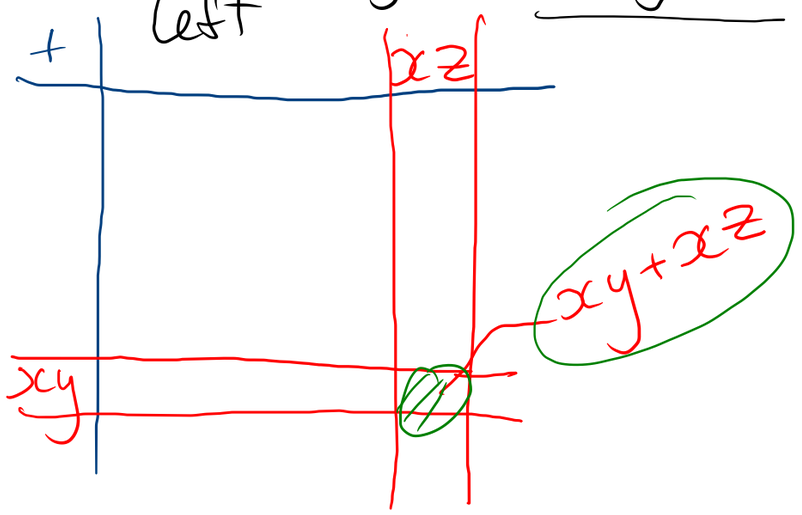
3. Identity: 1 ⇐ optional

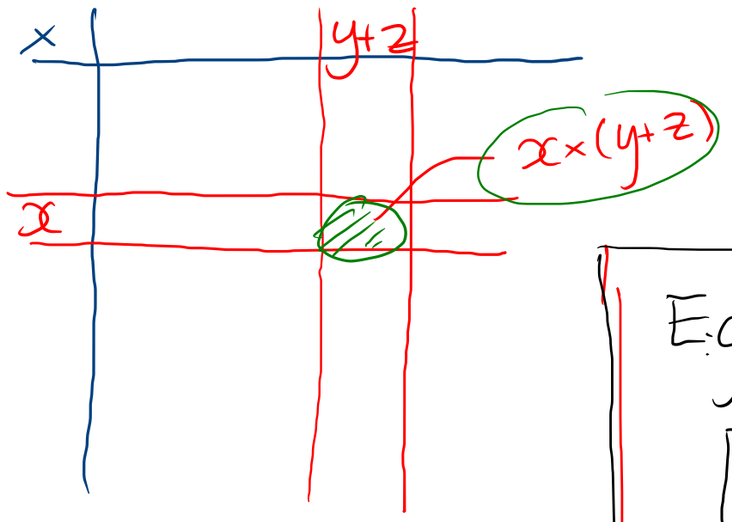
4) Commutativ: ⇐ optional



5) distributivity: $x \times (y+z) = xy + x \times z = (xy) + (xz)$ - convention order of operations.

left





right distrib: $(y+z)x = yx + zx$

$AB \neq BA$ ⇐

- commutative ring ⇐
- rings & identity ⇐

$[\ ]_{2\times 3}\ [\ ]_{2\times 2}$

Eg. of rings: matrices $n \times n$ 2×2

$\begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix} + \begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix} = \begin{bmatrix} \square & \square \\ \square & \square \end{bmatrix}$

$A + B = C$

$B + A = C$

$\begin{bmatrix} 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \end{bmatrix} + A = A$

$A \longrightarrow -A$

Mult^n:

closure

- $[\ ]_{n\times m} \times [\ ]_{n\times n} = [\ ]_{n\times n}$
- $ABC = (AB)C = A(BC)$ assoc.

identity: yes · inverses ✗ · commutin ✗

Mult conditions:

① commutativity → not necessary
② multive inverses → not nessecary

} optional.

(5) What are the rows & cols for the 0 elt in the mult table.

· left dist'y.

$$x(y+z) = xy + xz$$

· let $z = 0$

$$\Rightarrow x(y+0) = xy + x0$$

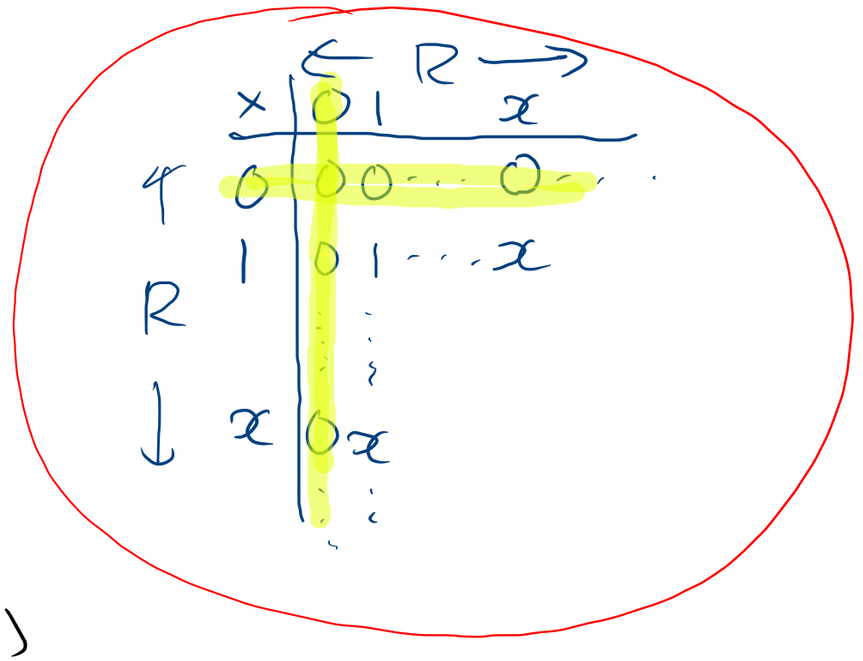
$$xy = xy + x0$$

$$xy + (-xy) = xy + x0 + (-xy)$$

$$0 = x0 + 0$$

$$\boxed{0 = x0}$$

$$\boxed{0 = 0x}$$



0-ring

×	0
0	0

+	0
0	0

$R = \{0\}$

⑥ Extended Distrivy

- Consider $x(y_1 + [y_2 + y_3 + \cdots y_n]) =$

$$x(y_1 + [\ \ ]) = xy_1 + x[y_2 + \cdots y_n]$$

$$= xy_1 + xy_2 + x(y_3 + \cdots y_n)$$

$$\vdots$$

$$= xy_1 + xy_2 + \cdots xy_n$$

- consider $(x_1 + [x_2 + \cdots + x_m])(y_1 + y_2 + \cdots + y_n)$

$$= x_1y_1 + x_1y_2 + \cdots + x_1y_n$$
$$+ x_2y_1 + \cdots x_ny_n$$
$$+ \ \ \vdots$$
$$= \sum_{i=1}^{m} \sum_{j=1}^{n} x_iy_j$$

⑦ Terminology

① unit – an element of R is called a unit if it has a multiplicative inverse.

e.g. integers $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$.

units of $\mathbb{Z}$: $\{1, -1\}$

rationals $\mathbb{Q} = \{0, 1/2, 2/3, 7/8, 15/4, \dots\}$.

units $= \mathbb{Q} \setminus 0$. $\Rightarrow$ FIELD – a ring with all units except 0.

② Note: if an elt is a unit, its inverse is unique.

Proof: suppose $x \in R$ has two inverses a & b.

$a = a \cdot 1$

$= a \cdot (x\, b)$

$= (a x)\, b$

$= 1 \cdot b$

$= b$

II.) Examples of Rings.

① Ring of integers - prototype

$R = \{0, 1, -1, 2, -2, \ldots\}$,

Add^n: Abelian group. ✓

Mult^n: • closure ✓

• assoc'y $(xy)z = x(yz)$ ✓

• distve. $x(y+z) =$ ✓

- mult'v idety ✓ 1
- inverses - No
- units 1, -1

② Ring of Rationals -

- mult'v idt - 1
- inverses - YES

units: $\mathbb{Q} \setminus 0$

Field

③ Reals & Complex ~ FIELDS.

④ Zero ring

$R = \{0\}$.

⑤ $n \times n$ matrices

- identity I.
- inverses? No
- units? - set of invertible matrices. ✓

⑥ $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$: integers mod n.

$\mathbb{Z}_n$ - Abelian under add^n.

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$ add^n mod 4

mult^n.

- closure ✓ $2 \times 3 = 6 \bmod 4$
  $= 2$
- assoc. ✓
- disty.
- identy: 1
- inverses: No in general for general n

⑦ $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ where p is prime.

$\Rightarrow$ all elts (except 0) have inverse.

$\{0,1,2\}$ mod 3 $\rightarrow$ have invers.

$\mathbb{Z}_p$ where p is prime is <u>finite field</u>

⑧ $n\mathbb{Z} = \{0, n, -n, 2n, -2n, 3n, -3n, \ldots\}$

e.g. $2\mathbb{Z} = \{0, 2, -2, 4, -4, 6, -6, \ldots\}$.

Add^n: closed? ✓ assoc: ✓
identy ✓ 0 inverse ✓
comm'ce ✓

Multⁿ: closed ✓ assoc'e ✓
dist. ✓

- identity - No ⇒ comm'e YES
- inverse - NO