Rings

- extension of groups to two operation $+, \times$.
- they are coupled by the dist^n law.

① Add^n operatio
- Abelian ~~group~~

- closure
- assoc'y
- identity
- inverses.

② Mult^n:

Required:

① Closure: $a \times b \in R \quad \forall a, b \in R$

② Associativity: $a \times (b \times c) = (a \times b) \times c = a \times b \times c$

like a group but not quib.

③ Distributivity: $a \times (b + c) = a \times b + a \times c$ (left dis'y)

$(b + c) \times a = b \times a + c \times a$ (right ")

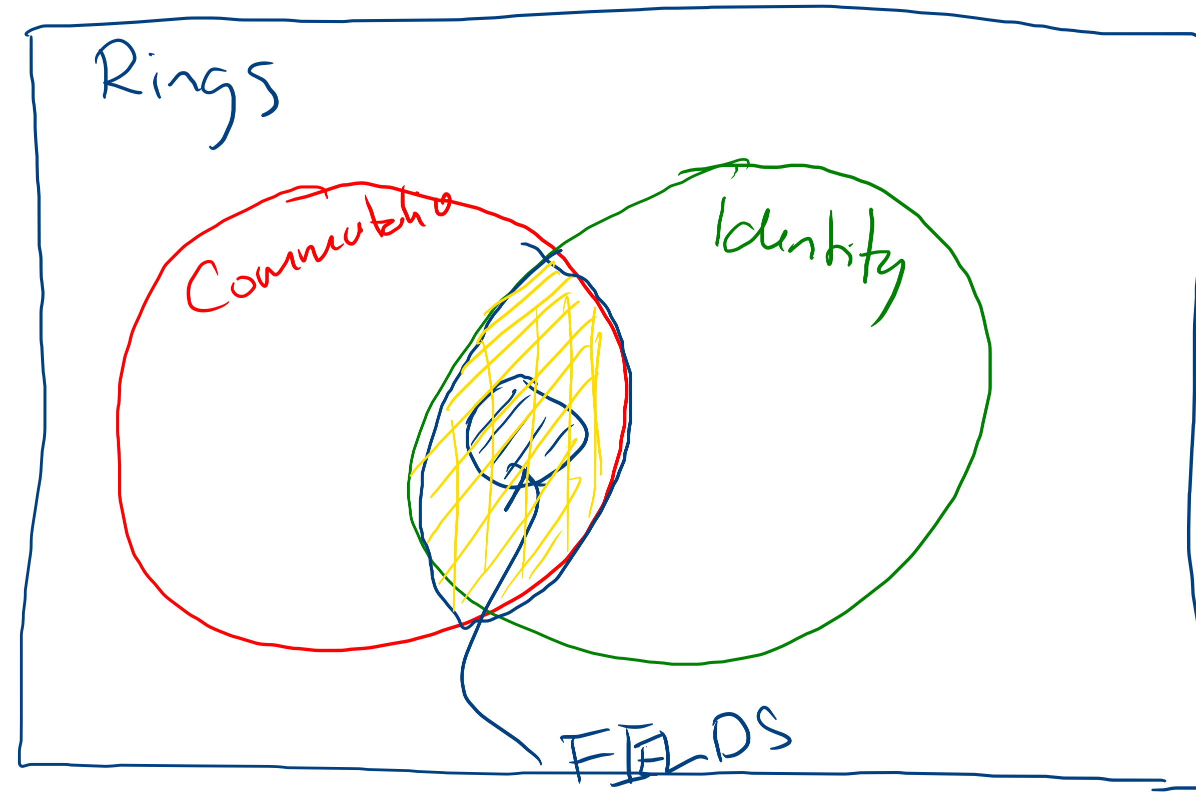
Optional:

① commutative
② identity
③ inverses are not guarenteed.

0 is never invertable.
1 is always invertible
- all other elts $\Rightarrow$ it depend.

Commutative ring (with identity)

$\Rightarrow$ If all elts are invertible
$\Rightarrow$ FIELD



(9) Notation - adjoining an element to a ring.

Ring R

Adjoin elt x to R : $R[x]$ — R adjoin x

What do the elts in the new ring $R[x]$ look like?

- add^n, mult^n.
- by multing elts of R $\to$ other elts of R
  $\to$ $\boxed{R = (r_0, r_1, r_2 \dots)}$
- by multing by x.
  $\to$ $x \cdot 0 = 0$
  $x \cdot 1 = x$
  $x \cdot r_2 = r_2 x$

  $\boxed{rx}$ where $r \in R$

- multing $x \times x = x^2$
- take $x^2 \to$ multing by R.

  $\boxed{rx^2}$

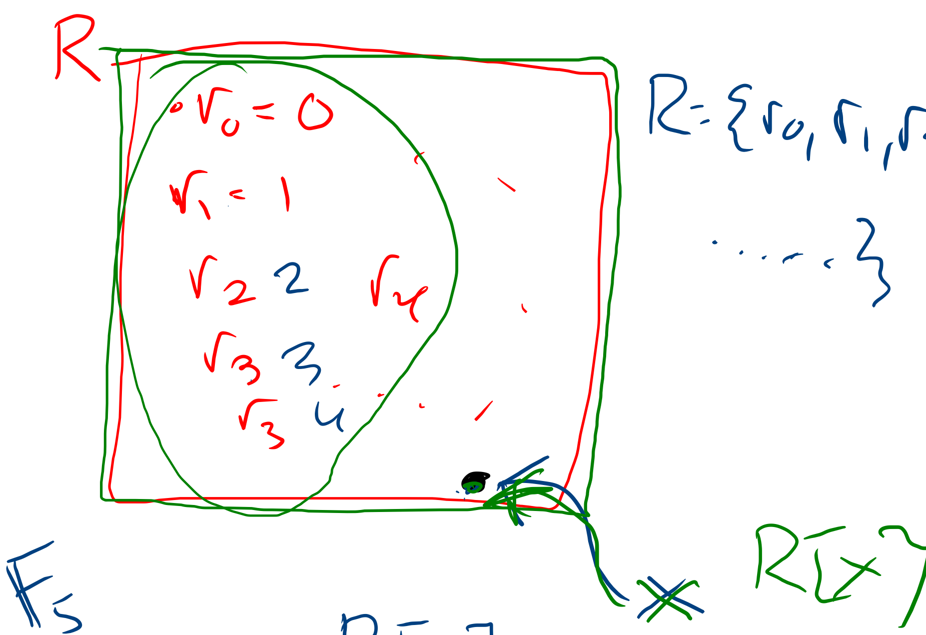
$0, 1, 2, 3, -4, \dots \in R$

$$\boxed{s_0 + s_1 x + s_2 x^2 + s_3 x^3 + \dots}$$

$s_0 \in R$

Finite. Sum $\in R[x]$

Polynomials rings.



$R = \{r_0, r_1, r_2 \dots \}$

$\mathbb{Z}_5 = \mathbb{F}_5$

$R[x]$

$= \{ s_0 + s_1 x + s_2 x^2 + \dots + s_n x^n \}$

For $s_i \in R$ $\to$ polynomials.

If $R = \mathbb{Z}$

$\mathbb{Z}[x] = \{ 3x + 5x^3, -2x^2 + x^5 + \dots \}$

$\mathbb{Q}[x] = \{ \quad \}$

(9) Notation - adjoining an element to a ring

Ring R

Adjoin elt x to R: $R[x]$ — R adjoin x

What do the elts in the new ring $R[x]$ look like?

- add^n, mult^n.
- by mult'ing elts of R $\to$ other elts of R
  $\to$ $\boxed{R = (r_0, r_1, r_2 \cdots)}$
- by mult'g by x.
  $\to$ $x \cdot 0 = 0$
  $x \cdot 1 = x$
  $x \cdot r_2 = r_2 x$
  $\boxed{rx}$ when $r \in R$

- mult'g $x \times x = x^2$
- take $x^2 \to$ mult'y by R. $\to$ polynomials.
  $\boxed{rx^2}$

$0, 1, 2, 3, -4, \ldots \in R$

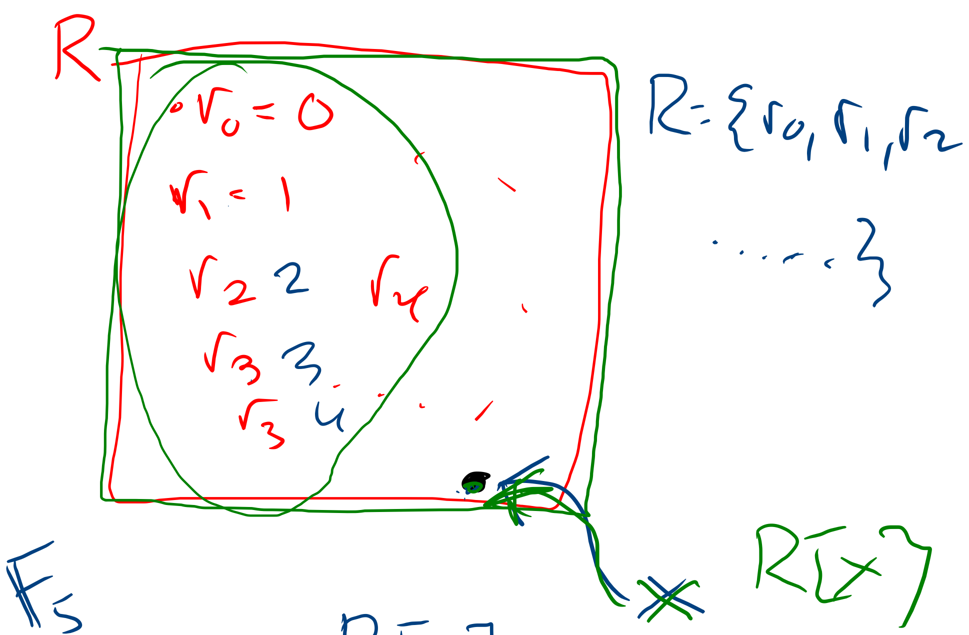
$$\boxed{s_0 + s_1 x + s_2 x^2 + s_3 x^3 + \cdots}$$

$s_0 \in R$

Finite.

Sum $\in R[x]$

Polynomials rings.



$R = \{r_0, r_1, r_2 \ldots\}$

$\mathbb{Z}_5 = \mathbb{F}_5$

$\{ \ldots$

$R[x] = \{s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n\}$

For $s_i \in R$

If $R = \mathbb{Z}$

$\mathbb{Z}[x] = \{3x + 5x^3, -2x^2 + x^5 + \cdots\}$

$\mathbb{Q}[x] = \{ \quad \}$

Usually this is just a definitn.

$R[x]$ is the set of all polynomials with coefficients in R.

$\mathbb{Z}[x]$: go from $\mathbb{Z} = \{0, 1, -1, 2, -2\}$

$$\downarrow$$

$$\mathbb{Z} = \{\underbrace{0, 1, -1, \dots}_{\mathbb{Z}}, x, 2x, -2x, \dots, x^2, x^3, -x+-x^2, \dots$$

$3x^3 + 2x - 1$ → it's not function like in high school.

→ it's an element in $R[x]$.

(10) Ring of Subsets

- Defn: Power set of a set
  $\to$ set of all subsets.

$\mathcal{P}(X) = \{\text{all subsets of } X\} = \{A \mid A \subset X\}$

$X = \{0, 1, 2\} \to n = 3$

$\mathcal{P}(X) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}$

$|\mathcal{P}(X)| = 8 \to 2^3$

cardinality of X
- num. of elts.

$$\boxed{\begin{array}{l} \text{If } |X| = n \\ \to |\mathcal{P}(X)| = 2^n \end{array}}$$

$|\mathcal{P}(\mathbb{R})| =$

$\mathbb{R}$

$X = \{a, b, c, d, e\}$

a	b	c	d	e	
1	0				
0	0	0	0	0	$\to \emptyset$
0	0	0	0	1	$\to e$
0	0	0	1	0	$\to d$
⋮					
0	1	1	0	0	$\to \{b, c\}$
0	0	1	1	1	$\to \{c, d, e\}$

$\to n$ bits

gives you 2^n possibilities.

Claim: $R[x]$ - ~~ring~~ set of all poly^n's $\bar{c}$ coefficents in R

real- $\mathbb{R}$

R - ring.

$R[x]$ is a ring:

extension ring.

• Add^n: Abelian group?

- closed : $p+q \Rightarrow \in R[x]$
- associa $p+q+r$ ✓ ✓
- identity ~ 0
- inverse ~ $p \longrightarrow -p$
- commu'ue ~ $p+q = q+p$

0 $\quad x$ $\quad \cancel{0}$

1 $\quad x$

2 $\quad 2x$

$R[\mathbb{Z}] =$

$R[x]$ - all poly^{n}s in x $\bar{c}$ coeff's from R

• Multi^n

• closure. $p \cdot q \overset{?}{\in} R[x]$ ✓

• associ'y $(p\cdot q)r = p(q r)$ ✓

• disti'v $p(q+r) = pq + pr$ ✓

$\frac{1}{x^2-1}$ $\quad$ $\frac{1}{x^3+2x+5}$

$\mathbb{Z}_3$

$\dot{0}\ \dot{1}\ \dot{2}$		x			
$0 \cdot x$	=	0	x^2	x^3	x^4
$1 \cdot x$	=	x	$2x^2$	$2x^3$	
$2x$	=	$2x$		x^3	

$\Downarrow$

$R[x]$

• identy? $\rightarrow 1 \cdot p \rightarrow p$ (1) ✓

• commu'ue $\rightarrow pq = qp$

X • inverses $\rightarrow$

$$\frac{x^3+2x+3}{x^2-1} = (x^2-1)^{-1} \cdot x^3+2x+3.$$

take as our ring the set of subsets of a set.

$\{\emptyset, \{a\}, b, c, ab, ac, bc, abc\}$

Union: $\cup$

Intersection $\cap$ ✓

$(a,b) \cup (a) = ab$

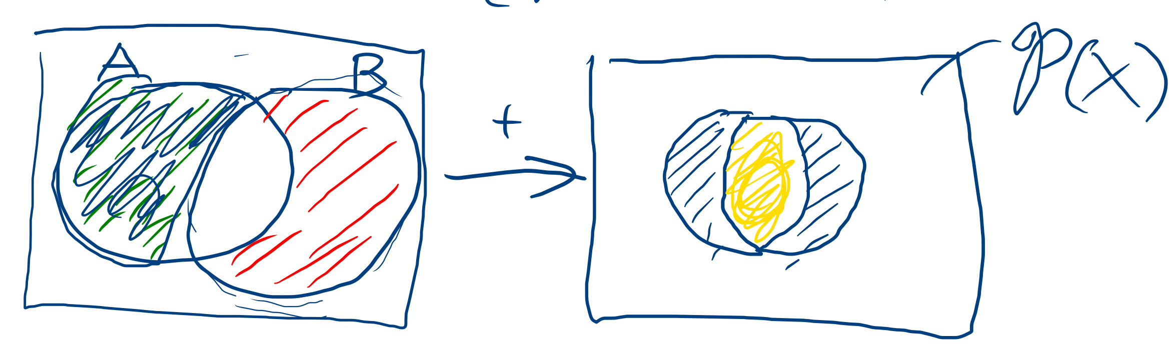
$\{bc\} \cap \{c\} = \{c\}$.

Define: Sum : symmetric difference of sets

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

Mult^n: : Intersection

$$A \times B = A \cap B$$



Add^n: $A + B = (A \setminus B) \cup (B \setminus A)$

$= (A \cap B^c) \cup (B \cap A^c)$

$=$

Closure ✓

$S \longrightarrow \mathcal{P}(S) \Rightarrow R$

$+$ symm.

$\times$ intersect

ax^3

$\underset{R}{\mathcal{P}(S)[x]} \equiv \{ \emptyset \cdot x, \{a\} \cdot x^2, \boxed{\{a,c\} x^3 + \{c\} x^2 + \{a\}} \}$

$(\alpha x^2 + \beta)(\delta x + \delta) =$

Ring of

$\mathbb{Z}[\sqrt{2}]$ $\sqrt[3]{3}$

2 4

Ring of $n \times n$ matrices

$R = \{2 \times 2 \text{ matrices}\}$

$R[x] = \{ [\ \ ]x^3 + [\ \ ]x + 1,\ [\ \ ]x^2 + [\ \ ]x + 5,\ \ldots\ \ldots \}$

$$\left(\begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix} x + 1 \cdot \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \right) \left(\begin{bmatrix} 5 & 4 \\ 1 & 2 \end{bmatrix} x + 5 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot 5 \right)$$

$$\begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix} \begin{pmatrix} 5 & 4 \\ 1 & 2 \end{pmatrix} x^2 + \begin{bmatrix} 1 & \\ & 1 \end{bmatrix} \begin{bmatrix} 5 & 4 \\ 1 & 2 \end{bmatrix} x +$$