Rings: commutative by default (0 is additive identity, 1 mult iden)

E.g.
- Any field K ($\mathbb{R}, \mathbb{C}, \mathbb{Z}/p$)
- $\mathbb{Z}$
- $F[x]$ or $F[x_1, \dots, x_n]$
- $R \subset S$ subring & $a_1, \dots, a_n \in S \longrightarrow R[a_1, \dots, a_n] \subset S$ → smallest subring containing R & $a_1, \dots, a_n$ ↳ intersection
- zero ring $\bar{0}$ is legit. (if $1=0$ then this)

Units
- $x \in R$ is a unit if $\exists y \in R$ so $xy = 1$
  ↳ if so y is unique. we write $y = x^{-1}$
- collection of units $R^\times$ forms a subgrp under mult.
  ↳ unit grp.
- R is a field $\iff R^\times = R \setminus \{0\}$ & $1 \neq 0$

E.g.
- $\mathbb{Z}^\times = \{\pm 1\} \cong \mathbb{Z}/2$
- $F[x]^\times = F^\times$ (F a field)
- $\mathbb{F}_p^\times \cong \mathbb{Z}/_{p-1}$
- $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} = \{\pm 1, \pm i\} \cong \mathbb{Z}/4$
- $\mathbb{Z}[\sqrt{2}]^\times = \{\pm 1 (\sqrt{2} \pm 1)^n\} \cong \mathbb{Z}/2 \times \mathbb{Z}$

Nilpotents
- $x \in R$ is nilpotent if $x^n = 0$ for some $n \geq 1$
- R is reduced if only nilp 0.

E.g.
- $\mathbb{Z}$, $F[x]$ reduced
- $\mathbb{Z}/4$ is not as 2 is nilp
- $\mathbb{Z}/n$ is reduced $\iff$ is sq free.

Prop | If x is nilp & $y \in R \implies xy$ is nilp ①

$x+y$ is nilp if y nilp ②

Pf | ① $x^n = 0 \implies (xy)^n = x^n y^n = 0$ ✓

② $x^n = 0$ $y^m = 0 \implies (x+y)^{n+m} = \sum_{i+j=n+m} \binom{n+m}{i+j} x^i y^j$

$i \geq n$ or $j \geq m$ are zero.

$= 0$

$\implies$ nilp elts are dead.

Idempotent | • $e \in R$ is idempotent if $e^2 = e$

• If e idem $\implies 1-e$ is also $(1-e)^2 = 1 - 2e + e^2 = 1 - e$

also, $(1-e)e = e - e^2 = e - e = 0$

• If e is idempotent then $eR = \{ex \mid x \in R\} \subset R$ is closed under mult & add (within itself)

$e \in eR$ & $ex = x$ $\forall x \in eR$

$\implies eR$ is a ring w mult id elt e (but not nec subring, e might not be 1)

• $R \cong eR \times (1-e)R$ ring iso.

$x \mapsto (ex, (1-e)x)$

• If $R \cong S_1 \times S_2$ $(1,0) \in S_1 \times S_2$ corr to idem e

$e \mapsto (1,0)$ $eR \cong S_1$

e.g. • $\mathbb{Z}/6 \cong \mathbb{Z}/2 \times \mathbb{Z}/3$

$3 \longmapsto (1, 0)$

$4 \longmapsto (0, 1)$

(rings with no idem called connected)

Zero divisors

- $x \in R$ is a zero div if $\exists y \in R \setminus \{0\}$ s.t. $xy = 0$
- 0 is a zero div if $R \neq 0$
- A ring is a domain if $R \neq 0$ & only zero div is 0
- If x is nilp, $R \neq 0 \Rightarrow x$ is zero div

  if $x^n = 0$ w/ n minimal

  $\Rightarrow x^{n-1} \neq 0$ & $x x^{n-1} = 0$.

- Domain $\Rightarrow$ Reduced

e.g.

- $\mathbb{Z}$, $F[x]$ domains
- $\mathbb{Z}/6$ not a domain but is reduced.
- $\mathbb{Z}/n$ is a domain $\Leftrightarrow$ n is prime $(n=0)$

Ideals

An ideal of a ring is an additive subgp $\mathfrak{a}$ closed under mult by arb elts in ring R.

i.e. $x \in R$, $y \in \mathfrak{a} \Rightarrow xy \in \mathfrak{a}$

- Given $y_1, \ldots, y_n \in R$ $\quad (y_1, \ldots, y_n) = \{x_1 y_1 + \cdots + x_n y_n \mid x_1, \ldots, x_n \in R\}$ (lin comb)

  This is an ideal ~ ideal gen'd by $y_1, \ldots, y_n$

  More gen can consider ideal by any set of elts (a.k.a. jazz)

- An ideal $\mathfrak{a}$ is fin gen if $\exists x_1, \ldots, x_n$ if $\mathfrak{a} = (x_1, \ldots, x_n)$
- $\mathfrak{a}$ is principal if $\mathfrak{a} = (x)$

e.g.

- $n\mathbb{Z} = (n)$ is an ideal & all ideals of $\mathbb{Z}$ is like that

  $\hookrightarrow$ so $\mathbb{Z}$ is a PID (Principal ideal dom)

  $(3,5) = (1) = \mathbb{Z}$

- $(1) = R$ is the unit ideal & $(0) = \{0\}$ zero ideal.
- The (nil) radical of R, $\operatorname{rad}(R)$ - set of nilp's is an ideal
- if $f: R \to S$ ring homo $\Rightarrow$ $\ker f$ is an ideal $\quad 1 \mapsto 1$

Pf) $x \in R$ $y \in \ker f$ $\Rightarrow$ $f(xy) = f(x)f(y) = \cdot\, 0 = 0$

$x, y \in \ker f$ $\Rightarrow$ $f(x+y) = f(x)+f(y) = 0+0 = 0$.

- A ring R is a field $\Leftrightarrow$ $R \neq 0$ & $(0), (1)$ only ideals.

Pf) $(0), (1)$ only ideals ($\Leftarrow$ triv)

let $x \neq 0$ is in R $\Rightarrow (x) = (1)$

so $1 \in (x) \Rightarrow 1 = yx$ for some y $\Rightarrow$ $x \in R^{\times}$.

Operation on ideals) • if $\mathfrak{a}, \mathfrak{b} \subset R$ ideals, $\underbrace{\mathfrak{a} + \mathfrak{b} = \{x+y \mid x \in \mathfrak{a}, y \in \mathfrak{b}\}}_{\text{ideal}}$

- more gen given $\underbrace{\{\mathfrak{a}_i\}_{i \in I}}_{\text{ideals}}$ $\Rightarrow$ $\sum_{i \in I} \mathfrak{a}_i$ ideal
- $(x_1, \dots, x_n) = (x_1) + \dots + (x_n)$
- $\mathfrak{a} \cap \mathfrak{b}$ is an ideal (also inf int)
- $(2), (3) \subset \mathbb{Z}$ $(2) \cup (3)$ not ideal of $\mathbb{Z}$ $(5 \notin (2) \cup (3))$

unions okay w/ chain

(but)

- Given ideals $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$ then $\bigcup_{i \geq 1} \mathfrak{a}_i$ ideal
- $\mathfrak{a}\mathfrak{b} = \left\{ x_1 y_1 + \dots + x_n y_n \;\middle|\; \begin{matrix} x_1, \dots, x_n \in \mathfrak{a} \\ y_1, \dots, y_n \in \mathfrak{b} \end{matrix} \right\}$ prod ideal.

E.g) • $R = \mathbb{C}[x_1, x_n, \dots]$ $\mathfrak{a} = (x_1, x_2, \dots)$
is an ideal not fin gen

- consider chain $(x_1) \subset (x_1, x_2) \subset \dots$ $\mathfrak{a} = \bigcup_{j \geq 1} (x_1, \dots, x_j)$

Quotient) • If $\mathfrak{a} \subset R$ an ideal $\rightsquigarrow R/\mathfrak{a}$ to coset rep stuff

- $\pi : R \to R/\mathfrak{a}$ & $\ker \pi = \mathfrak{a}$
$x \mapsto x + \mathfrak{a}$

E.g) • $\mathbb{Z}/n\mathbb{Z}$ is quot of $\mathbb{Z}$ by (n)

Ideal corr thm

$$\left\{\begin{array}{c}\text{ideals of } R\\ \text{containing } \mathfrak{a}\end{array}\right\} \xleftrightarrow{\text{bij}} \{\text{ideals of } R/\mathfrak{a}\}$$

$$\mathfrak{b} \longmapsto \pi(\mathfrak{b})$$

$$\pi^{-1}(\mathfrak{c}) \longleftarrow \mathfrak{c}$$

Types of ideals

- **Maximal ideal**: an ideal m of R is max'll if $m \neq (1)$ & $m \subset \mathfrak{a} \subset (1) \Rightarrow \mathfrak{a} = (1)$ or m — if R a field 0 max'll.
- m is max'll $\iff R/m$ a field

Pf m is max'll $\iff (0)$ & (1) only ideals R/m (corr thm)

$\iff R/m$ a field.

E.g.
- If $p \in \mathbb{Z}$ prime then (p) is prime as $\mathbb{Z}/p$ field
- $F[x_1, \ldots, x_n] = R$ then $(x_1, \ldots, x_n) = m$ is max as $R/m = F$

Rmk $R = \mathbb{C}(x_1, \ldots, x_m)$ given $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$
$\rightarrow (x_1 - \alpha_1, \ldots, x_m - \alpha_m)$ all the max'll ideals of R — for alg closed $\mathbb{C}$.

Rmk 2 Also require alg closed $\frac{\mathbb{Q}[x]}{(x^2+1)} \cong \mathbb{Q}[i]$ is a field

$\Rightarrow (x^2+1)$ max'll ideal.

Prop if $R \neq 0$ then R has max'll ideal

Pf Σ = all proper ideals of R $(\Sigma \neq \emptyset$ as $(0) \in \Sigma)$ — (0) prop as $R \neq 0$.

Say ascending chain in Σ $(\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots)\ \{\mathfrak{a}_i\}$

By earlier chain comment $\bigcup_{i \in I} \mathfrak{a}_i = \mathfrak{a}$ ideal

Cl $\mathfrak{a} \in \Sigma$ as $1 \notin \mathfrak{a}$ as not in any $\mathfrak{a}_i$

Bdd chain $\Rightarrow$ by Zorn done

$\square$

Corr 1) If $\mathfrak{a} \subset R$ ideal not (1) $\Rightarrow \mathfrak{a} \subset \mathfrak{m}$ for some max'l $\mathfrak{m}$

Pf) Can do earlier arg zorn with Σ being ideals cont $\mathfrak{a}$

or take max'l ideal of $R/\mathfrak{a}$ & ideal corr

Corr If $R \neq 0 \Rightarrow \exists$ ring homo $R \to F$ w/ F a field

Pf $F = R/\mathfrak{m}$ for some max'l ideal $\mathfrak{m}$ & π map

Prime Ideals An ideal $\mathfrak{p}$ is prime if $\mathfrak{p} \neq (1)$ &
$xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$

Prop $\mathfrak{p}$ ideal prime $\Leftrightarrow R/\mathfrak{p}$ domain.

Pf Say $xy = 0$ in $R/\mathfrak{p}$. let $\tilde{x}, \tilde{y} \in R$ map to x & y under π

$\pi(\tilde{x} \cdot \tilde{y}) = \pi(\tilde{x})\pi(\tilde{y}) = xy = 0 \Rightarrow \tilde{x}\tilde{y} \in \ker \pi = \mathfrak{p}$

so $\tilde{x} \in \mathfrak{p}$ or $\tilde{y} \in \mathfrak{p}$ $\to x = 0$ or $y = 0$

$\Rightarrow R/\mathfrak{p}$ domain

Conv similar

Cor Max'l ideal are prime.

e.g.
- In a PID ($\mathbb{Z}$, $F[x]$) a nonzero prime ideal is max'l
- (0) is prime $\Leftrightarrow R$ a domain
- $R = \mathbb{C}[x,y]$ let $f \in R$ be irred, non const

$\Rightarrow (f)$ is prime not max'l

$\hookrightarrow$ irred & unique fact

can argue proper containment.

max'l ideals of R are $(x-\alpha, y-\beta)$ and $\alpha, \beta \in \mathbb{C}$

When is $(f) \subset (x-\alpha, y-\beta) \Leftrightarrow \Phi(f) = 0 \Rightarrow f(\alpha,\beta) = 0$

obs $\dfrac{\mathbb{C}[x,y]}{(x-\alpha, y-\beta)} \cong \mathbb{C}$

$f \mapsto f(\alpha,\beta)$

$\Phi : \mathbb{C}[x,y] \to \mathbb{C}$ ring homo

$f \mapsto f(\alpha,\beta)$

$\ker \Phi = (x-\alpha, y-\beta)$