Def) Let R be a ring. A subset of a ring is a $S \subseteq R$ that is closed under $+, \cdot$ & $1 \in S$ is a subring

Note: ideals are closed under $+, \cdot$ but usually not subrings (b/c in fact the whole ring R is the only ideal that has 1 ($1 \cdot a = a \in I \ \forall a \in R$)

Let R a ring & $X \subseteq R$ is a subset.
The subring of R gen'd by X is a smallest subring of R containing X $= \bigcap_{\substack{X \subseteq S \\ S \text{ subring}}} S$

E.g 1) Gaussian integers

$\mathbb{Z}[i]$ = subring of $\mathbb{C}$ gen'd by $i = \sqrt{-1}$
$= \{a + bi \mid a, b \in \mathbb{Z}\}$

2) $R = \mathbb{C}[x,y]$ $\quad X = \mathbb{C} \cup \{x^2, xy, y^2\}$ coeff in $\mathbb{C}$

Subring gen'd by X → poly in x,y so each mono has total degree even $cx^i y^j$, $i+j \equiv 0 \bmod 2$

↳ Veronese Subring!

Recall) if R is a ring & I is an ideal of R then R/I naturally has a ring struct → called quotient ring.

Some prop) 1) Mapping Property: (everything is homo)

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\pi"'] & S \\ R/I \arrow[ur, dotted, "\psi"'] & \end{tikzcd}$$

quotient map ← π

given φ s.t. $I \subset \ker(\varphi)$
$\exists! \ \psi : R/I \to S$
so that the diagram commute

2) Corr thm for ideals!

$\{\text{ideals of } R/I\} \xleftrightarrow{\text{bij}} \{\text{ideals of } R \text{ cont } I\}$

$J \longmapsto \pi^{-1}(J)$

3) first iso thm. If $\varphi : R \to S$ is a surj of rings then φ induces isom
$\overline{\varphi} : R/\ker(\varphi) \xrightarrow{\sim} S$

Def) Given a ring R & elts $f_1, \dots, f_n \in R$ then the ideal of R gen'd by $f_1, \dots, f_n$
is $(f_1, \dots, f_n) = \{g_1 f_1 + \dots + g_n f_n \mid g_1, \dots, g_n \in R\}$
An ideal is principal if $I = (f)$ for $f \in R$

E.g) 1) Every ideal of $\mathbb{Z}$ is principal
2) If F is a field every ideal of $F[x]$ is principal!
3) Every ideal of Gaussian integers is principal!
4) The ideal (x,y) of $F[x,y]$ is not principal!

Def) A finite presentation of a ring R is an isom
$$\frac{\mathbb{Z}[x_1, \dots, x_n]}{(f_1, \dots, f_n)} \cong R$$
free ring on n things
for $f_1, \dots, f_n \in \mathbb{Z}[x_1, \dots, x_n]$

Def) More generally a (finite) pres of R rel to S is an isom
$$\frac{S[x_1, \dots, x_n]}{(f_1, \dots, f_n)} \cong R$$

Eg) Presentation for $\mathbb{Z}[i]$
$$\frac{\mathbb{Z}[x]}{(x^2+1)} \xrightarrow{\varphi} \mathbb{Z}[i]$$
1) $\exists$ ring map $\tilde{\varphi} : \mathbb{Z}[x] \to \mathbb{Z}[i]$
$x \longmapsto i$
mapping prop of polynomial
2) $\tilde{\varphi}(x^2+1) = i^2+1 = 0 \Rightarrow x^2+1 \subseteq \ker \tilde{\varphi}$

3) Mapping prop for quotients $\Rightarrow$

$\exists$ ring homo $\varphi : \frac{\mathbb{Z}[x]}{(x^2+1)} \longrightarrow \mathbb{Z}[i]$

s.t. $\varphi(\bar{x}) = i$

4) Clear φ (and thus φ) is surj

5) Every elt of $\frac{\mathbb{Z}[x]}{(x^2+1)}$ has $a\bar{x} + b \quad a,b \in \mathbb{Z}$

$$\text{Cos } x^5 = x^5 - x^3(x^2+1) + x^3(x^2+1)$$
$$\Rightarrow \bar{x}^5 = -\bar{x}^3 \longrightarrow \text{can reduce pow!}$$

Say $a\bar{x}+b \in \ker(\varphi) \Rightarrow 0 = \varphi(a\bar{x}+b) = ai+b$
$\Rightarrow a,b=0$

$\Rightarrow \ker(\varphi) = \{\bar{0}\}$

Def) A (comm) ring R is called an (integral) domain if
$xy=0 \Rightarrow x=0$ or $y=0$ (and $1 \neq 0$ in R)

e.g. 1. Any field is a domain

- $\mathbb{Z}$, $\mathbb{Q}[x]$, $\mathbb{C}[x]$, gaussian are integral domain!
- $\mathbb{Z}/6\mathbb{Z}$ not as $\overline{2} \cdot \overline{3} = \overline{0}$

(subrings of integral dom are integral domain) converse

We'll now see every integral domain embeds into a field

Given a domain R define a field
Frac(R) (fraction field of R)

an elt is an equiv cls of pairs (a,b) $a,b \in R$, $b \neq 0$

$(a,b) \sim (a',b') \iff ab' = a'b$

Notation $\Rightarrow \frac{a}{b} = \overline{(a,b)}$ define $(+,\cdot)$

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}, \quad \frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$$

integral important

Check well def field!

Natural injective ring homo $R \longrightarrow \text{Frac}(R)$
$a \longmapsto \frac{a}{1}$

E.g. $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$

$\mathrm{Frac}(\mathbb{Q}[x]) = \mathbb{Q}(x)$ → rational functions

E.g. $R = \dfrac{\mathbb{C}[x,y]}{(y^2 - x^3 - x)} \supset \mathbb{C}[x]$

this is an integral domain!

Frac(R) is a field

as $\mathbb{C}[x] \subset R \Rightarrow \underbrace{\mathbb{C}(x)}_{\text{rational}} \subset \mathrm{Frac}(R)$

$$\begin{array}{c} \mathrm{Frac}(R) \\ \uplus \\ y \end{array}$$

$y^2 = x^2 + x$ in Frac(R)