Example: $\mathbb{Z}[\sqrt{-5}]$ is the ring of integers in $\mathbb{Q}(\sqrt{-5})$.

$$2 \cdot 3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$$

irreducible in $\mathbb{Z}[\sqrt{-5}]$

distinct (don't differ by a unit).

(Check all of this using $N_{\mathbb{Q}(\sqrt{-5})/\mathbb{Q}}$).

Example: $\mathbb{Z} \longleftrightarrow \mathbb{F}_p[x] \longleftrightarrow \mathbb{C}[x]$.

Very similar.
- All are PIDs. ($\Rightarrow$ All integrally closed).
- All "1-dimensional"
  every non-zero prime ideal is maximal.

$\mathbb{C}[x] \sim$ polynomial functions on $\mathbb{C}$.

$f(x) \longrightarrow z \mapsto f(z)$.

$\mathbb{C}$: Affine line, 1-dimensional space.

Unique factorization + structure of irreducibles

$$\rightsquigarrow f(x) = c\,(x-z_1)^{k_1}(x-z_2)^{k_2}\cdots(x-z_n)^{k_n}.$$

$f \neq 0$

$c \in \mathbb{C}^*$ $\quad (x-z_i)$ $\quad z_i \in \mathbb{C}$ are the irreducibles in $\mathbb{C}[x]$.

$k_i =$ "order of vanishing of f at z_i"

i.e. if you write down the Taylor expansion of f at z_i then the first k_i terms are zero.

e.g. $k_i = 1$ $\quad f(x) = 0 + a_1(x-z_i) + a_2(x-z_i)^2 + \cdots$

$a_1 \neq 0$.

The unique factorization is encoded by the order of vanishing at each z.

$v_z(f)$ = order of vanishing of f at z.

Takes value in $\mathbb{Z}$.

Valuation corresponding to z ← Discrete valuation.

$$v_z(fg) = v_z(f) + v_z(g).$$
$$v_z(f+g) \geq \min(v_z(f), v_z(g)).$$

Idea: The existence of "order of vanishing" valuations corresponding to maximal ideal is the essential feature of rings of integers.

Example If $t \in \mathbb{Q}$

$t = \frac{r}{s}$ $r, s \in \mathbb{Z}$

If p is a prime number

$$v_p(t) = v_p(r) - v_p(s)$$

$v_p(r)$: the largest power of p dividing r.

$v_p(s)$: "

i.e. $t = p^{v_p(t)} \frac{r'}{s'}$ r' and s' are not divisible by p.

$$t = \pm 1 \cdot \prod_p p^{v_p(t)}.$$

(We can think of $\mathbb{Z}$ as being "functions" on the primes)

$n \in \mathbb{Z}$

$\updownarrow$

$p \mapsto n(p) := n \bmod p$

$\in$

$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Example: Back to $\mathbb{C}[x]$

$\mathbb{Z}[\sqrt{-5}]$ $\quad$ $\mathbb{C}[x,y]/y^2=x^3-1$

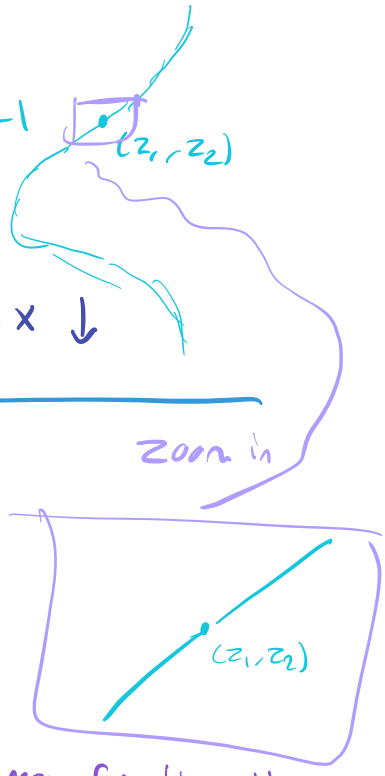
$\uparrow$ $\quad$ $\uparrow f^*$ $\quad$ $f^*\uparrow g(f(x,y))$

like $\mathbb{Z}$ $\quad$ $\mathbb{C}[x]$ $\quad$ $g(x)$

$-5 \rightsquigarrow x^3-1$.

Maximal ideals were $(x-z)$ $z\in\mathbb{C}$

Maximal ideals $(x-z_1, y-z_2)$ $(z_1,z_2) \mid z_2^2=z_1^2-1$



For each maximal ideal (z_1,z_2), I get an "order of vanishing function" $v_{(z_1,z_2)}(\cdot)$ on $\mathbb{C}[x,y]/y^2=x^3-1$.

Inverse function theorem says either x or y gives a local coordinate.

I.e. I can expand any holomorphic function as a power series in $(x-z_1)$ or $(y-z_2)$.

The order of vanishing is the # of zeroes at the start of that expansion.

Theorem: If $K/\mathbb{Q}$ is a finite extension, then

1. $\mathcal{O}_K$ is Noetherian
2. $\mathcal{O}_K$ is integrally closed
3. Every non-zero prime ideal is maximal in $\mathcal{O}_K$.

Remark: These are the same properties satisfied by

the ring of polynomial functions on a smooth curve.

Proof: ① We saw last week that $\mathcal{O}_K$ is a Noetherian $\mathbb{Z}$-module. $\Rightarrow$ Noetherian $\mathcal{O}_K$-module $\Rightarrow$ Noetherian ring.

② We saw last week.

③ Let $\mathfrak{p}$ be a non-zero prime ideal in $\mathcal{O}_K$.

Let $\alpha \in \mathfrak{p}$ $\alpha \neq 0$.

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

(α integral / $\mathbb{Z}$) $\qquad a_i \in \mathbb{Z}$.

Take minimal $\Rightarrow$ $a_0 \neq 0$.

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha = -a_0$$

so $-a_0 \in \mathfrak{p}$.

$\Rightarrow$ $\mathfrak{p} \cap \mathbb{Z} \neq (0)$.

$\mathfrak{p} \cap \mathbb{Z} = (p)$

$\mathcal{O}_K/\mathfrak{p} \hookleftarrow \mathbb{F}_p$

Integrality of $\mathcal{O}_K$ / $\mathbb{Z}$ $\Rightarrow$ every element is algebraic / $\mathbb{F}_p$.

$\Rightarrow \mathcal{O}_K/\mathfrak{p}$ is a field.

$\Rightarrow \mathfrak{p}$ is maximal.

Def'n: A ring satisfying the 3 properties of the theorem is called a Dedekind domain.

Theorem: If A is a Dedekind domain and $\mathfrak{p}$ is a nonzero prime ideal in A, then $A_{\mathfrak{p}}$ is a principal ideal domain with a unique irreducible element (up to associates).

$A_{\mathfrak{p}}$ is $S^{-1}A$ with $S = A \setminus \mathfrak{p}$.

Such a ring is called a discrete valuation ring.

Idea: An element that generates $\mathfrak{p}A_{\mathfrak{p}}$ ← unique nonzero prime in $A_{\mathfrak{p}}$

"is" a local coordinate at $\mathfrak{p}$.

Valuations $\mathfrak{p}A_{\mathfrak{p}} = (\pi)$ $\quad f \in A$

$v_{\mathfrak{p}}(f)$ = power of π dividing f in $A_{\mathfrak{p}}$

I an ideal of A $\quad v_{\mathfrak{p}}(I) = k$ s.t. $IA_{\mathfrak{p}} = (\pi^k)$.

$(v_{\mathfrak{p}}((f)) = v_{\mathfrak{p}}(f))$.

Proof sketch:

1. If A is a Dedekind domain, so is any localization $S^{-1}A$.
2. A local Dedekind domain is a PID

unique maximal ideal

In Milne - precise ref. on worksheet.

Theorem: In a Dedekind domain A, any nonzero ideal I has a unique factorization into nonzero prime ideals

$$I = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_n^{e_n}$$

for $\mathfrak{p}_i$ distinct prime ideals.

Example: In $\mathbb{Z}[\sqrt{-5}]$

$$(6) = (1+\sqrt{-5}, 2)^2 (1-\sqrt{-5}, 3)(1+\sqrt{-5}, 3).$$

Combine in different ways to give $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$.

Proof sketch:

Lemma: If A is Noetherian, any nonzero ideal $I \subseteq A$ contains a product of nonzero prime ideals.

Pf: Assume not, take I largest possible that does not (because A Noetherian). I can't be prime. So $\exists\ x, y$ s.t. $xy \in I$ but $x, y \notin I$.

$$((x) + I) \cdot ((y) + I) \subseteq I.$$

both bigger than I. Both contain products of prime ideals, thus so does their product.

Take I a nonzero ideal.

By lemma, $I \supseteq \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_n^{m_n}$.

Ideals of A containing $\mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_n^{m_n}$ $\longleftrightarrow$ Ideals of $A/\mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_n^{m_n}$.

$I \longleftrightarrow$? $\overset{\text{CRT}}{=}$

$$\prod_{i=1}^{n} A/\mathfrak{p}_i^{m_i}$$

$\downarrow \cong$

$$\prod_{i=1}^{n} A_{\mathfrak{p}_i}/(\mathfrak{p}A_{\mathfrak{p}})^{m_i}$$

$\|$

$$\prod_{i=1}^{n} A_{\mathfrak{p}_i}/(\pi_i^{m_i})$$ π_i generates $\mathfrak{p}A_{\mathfrak{p}_i}$.

$I \longrightarrow \prod_{i=1}^{n} (\pi_i^{v_{\mathfrak{p}}(I)})$.

$\|$ $\longleftarrow$

$$\prod_{i=1}^{n} \mathfrak{p}_i^{v_{\mathfrak{p}}(i)}$$

Corollary: Dedekind domain is a PID $\Leftrightarrow$ a UFD

Proof: Suppose A Dedekind + UFD.

I a nonzero ideal of A.

$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$

Suffices to show each prime ideal is principal.

If $\mathfrak{p}$ is a nonzero prime ideal, take

$f \in \mathfrak{p}$ $f \neq 0$.

UFD $\Rightarrow \exists$ $\pi \mid f$

π irreducible.

$f = a\pi$

either a or π is in $\mathfrak{p}$.

$\rightsquigarrow$ some irreducible π in $\mathfrak{p}$.

$\mathfrak{p} \supseteq (\pi)$

$\uparrow$ This is prime so maximal since A Dedekind

$\Rightarrow \mathfrak{p} = (\pi)$.