$$\mathcal{O}_K/p\cdot\mathcal{O}_K \simeq \mathcal{O}_K \underset{\mathbb{Z}}{\otimes} \mathbb{Z}/p \simeq \mathcal{O}_K \underset{\mathbb{Z}}{\otimes} \mathbb{F}_p$$

$$\simeq \mathbb{Z}^n \underset{\mathbb{Z}}{\otimes} \mathbb{F}_p \simeq \mathbb{F}_p^n$$

as $\mathbb{Z}$-module, $n = [K : \mathbb{Q}_p]$

$\mathcal{O}_K$ noetherian?

$\mathcal{O}_K$ finite free$/\mathbb{Z}$

$\operatorname{Spec} A = \{ p \subseteq A \text{ prime} \}$

~~If~~ $f : A \to B$ ring hom.

$\Rightarrow \tilde{f} : \operatorname{Spec} B \to \operatorname{Spec} A$

$p \subseteq A$ prime, $k(p) := \operatorname{Frac}(A/p)$

$$\tilde{f}^{-1}(p) \overset{1:1}{\longleftrightarrow} \operatorname{Spec}(\underbrace{B \otimes_A k(p)})$$

localisation of $B/_{p\cdot B}$ $\quad p\cdot B = \langle \overset{a\cdot b}{f(a)\cdot b} \mid a \in p \rangle$

Apply this to $\mathbb{Z} \to \mathcal{O}_K$

$$\operatorname{Spec} \mathcal{O}_K \xrightarrow{\tilde{f}} \operatorname{Spec} \mathbb{Z} = \{(0), (2), (3), (5), \dots\}$$

$$\tilde{f}^{-1}((0)) \cong \operatorname{Spec}(\underbrace{\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Q}}_{K}) = \{(0)\}$$

p prime in $\mathbb{Z}$

$\mathrm{Spec}(\underbrace{\mathcal{O}_K \otimes_{\mathbb{Z}}} \mathbb{F}_p) = \tilde{f}^{-1}((p))$

suffices

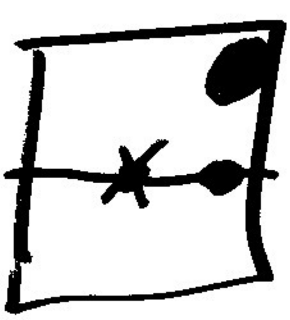
$\dim_{\mathbb{F}_p} \mathcal{O}_K/p\mathcal{O}_K < \infty$

$\mathcal{O}_K/p\mathcal{O}_K$ ← finite ring.
in part. Artinian

CRS $\Rightarrow$ each prime ideal in

$\mathcal{O}_K/p\mathcal{O}_K$ is maximal

$\Rightarrow$ max in $\mathcal{O}_K$



$k[x,y] \supsetneq (x)$

$\cup\!\!|$ $\quad$ $\rotatebox{90}{$\subsetneq$}$

(x,y)

$B := k[x,y]/(y^2 - x^3 + x = F(x,y)) \leftarrow k[x] =: A$

char $k \neq 2$

$F'_x(x,y),\ F'_y(x,y)$

$F(x,y)$

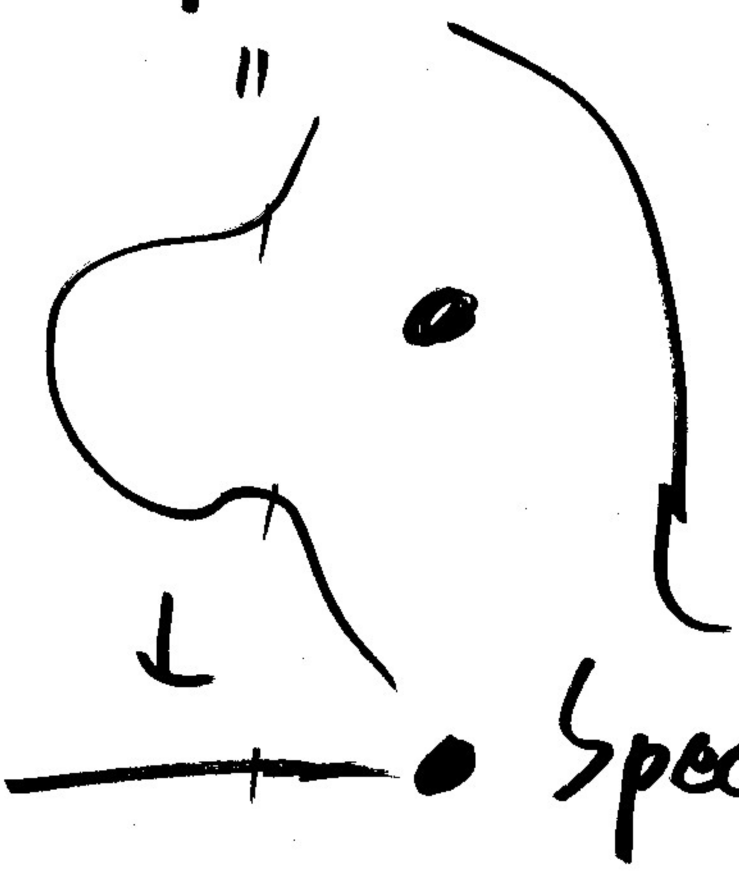
don't have a common zero

$\operatorname{Spec} B \to \operatorname{Spec} A$

Int. dom.

$\operatorname{Spec} A = \{(0)\} \leftarrow$ gen. pt.

$\overline{\{(0)\}} = \operatorname{Spec} A$



Spec A

For which result was it important that K is a numberfield?

Used: – $\mathbb{Z}$ PID $\Rightarrow \langle \alpha_1, \dots, \alpha_n \rangle_{\mathbb{Z}} \subseteq \mathcal{O}_K \subseteq \langle \alpha_1^\vee, \dots, \alpha_n^\vee \rangle_{\mathbb{Z}}$

$\Rightarrow \mathcal{O}_K$ fin. free of rk n over $\mathbb{Z}$

– $\mathbb{Z} = \{\pm 1\} \Rightarrow \Delta_K = \mathrm{Disc}(\alpha_1, \dots, \alpha_n)$

$= \mathrm{Disc}(\beta_1, \dots, \beta_n) \cdot \det(C)^2$

welldefined

Can generalize to following setup

A Ded. ring, $K = \mathrm{Frac}\, A$, L/K fin. sep.

(e.g. $\mathbb{Z}$)

⚠ $\mathrm{Tr}_{L/K}$ non-deg.

B = int. cl. of A in L

Then: B is fin. gen., torsionfree
over A ($\Rightarrow$ B fin. projective/A)

$$\Big(\underbrace{\langle \alpha_1, \dots, \alpha_n \rangle}_{\text{Basis of } L/K}{}_{\mathbb{Z}} \subseteq B \subseteq \langle \alpha_1^\vee, \dots, \alpha_n^\vee \rangle_{\mathbb{Z}} \Big)$$

M over R torsionfree $\Leftrightarrow$ $M \hookrightarrow M \otimes_R \mathrm{Frac}(R)$

Int. dom.

$\Leftrightarrow$ (if $r \cdot m = 0$, $r \neq 0$ $\Rightarrow$ $m = 0$)

M free, proj. $\Rightarrow$ M torsionfree

M fin proj. $\Leftarrow$ R Ded, M fin. gen.

$R = \mathbb{Z}[T] \supseteq M := (p, T)$ torsionfree

M not free (e.g. calculate $\mathrm{Tor}_i^R(M, \mathbb{Z}[T]/(p,T))$ using Koszul)

$R = \mathbb{Z}$, $M = \mathbb{Q}$ torsionfree,
but not free (as it is divisible)

B fin. gen. over A can fail
for L/K inseparable (subtle)

A int. cld $\Rightarrow \mathrm{Tr}_{L/K}(B) \subseteq A$

Set $B^\vee = \mathrm{Hom}_A(B, A)$ (a fin. proj.)

$\Rightarrow B \hookrightarrow B^\vee$

$x \mapsto (y \mapsto \mathrm{Tr}_{L/K}(x \cdot y))$

Define

$\Delta_{B/A} := \mathrm{Ann}_A(B^\vee/B)$ $(\mathcal{O}_K \hookrightarrow \mathcal{O}_K^\vee)$ $(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j))$

$\subseteq A$ ideal in A

(if $A = \mathbb{Z}$, $B = \mathcal{O}_K$

$\Rightarrow \Delta_{B/A} = (\Delta_K)$

⚠ $K/\mathbb{Q}$ numberfield

$\Rightarrow$ $\forall \mathfrak{p} \subseteq \mathcal{O}_K$ maximal,

$k(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p}$ is finite!

$$\begin{array}{c} k(\mathfrak{p}) \\ \cong \\ \mathbb{F}_q \end{array}$$

(e.g. $Gal(\overline{k(\mathfrak{p})}/k(\mathfrak{p})) \underset{\text{can}}{\cong} \mathrm{Frob}_q^{\hat{\mathbb{Z}}}$)

(also satisfied if
$A = \mathbb{F}_p[T] \subseteq B$ = int. closure of A in a finite, sep. ext. $L/\mathbb{F}_p(T)$)