Example: $\mathbb{Z}[i] \supseteq \mathbb{Z}$ $\quad p$ prime in $\mathbb{Z}$

$\rightsquigarrow$ how does p factor in $\mathbb{Z}[i]$?

If $p \equiv 1 \bmod 4$ then $p = \pi\overline{\pi}$ or $\pi, \overline{\pi}$ don't differ by a unit.

"p splits" $\longrightarrow$ $\pi = a+bi$ $\quad \overline{\pi} = a-bi$

$\hat{?}$

$p = a^2 + b^2$.

If $p \equiv 3 \bmod 4$ then p remains prime

"p inert"

If $p = 2 \rightsquigarrow$ $2 = (1+i)(1-i)$

"p ramifies" $\quad = (-i)(1+i)^2$

$(2) = (1+i)^2$.

Q: If A is a Dedekind domain w/fraction field K,
L/K is a finite separable extension of K
B is the integral closure of A in L.
If $\mathfrak{p}$ is a non-zero prime ideal in A,
how does $\mathfrak{p}B$ factor into prime ideals of B?

Example: $\mathbb{Z}[\sqrt{3}] / \mathbb{Z}$ $\quad$ ($\mathbb{Z}[\sqrt{3}]$ ring of integer in $\mathbb{Q}(\sqrt{3})$)

(B over A)

$p = 3$ $\quad (3) = (\sqrt{3})^2$ $\quad$ (ramifies)

$p = 2$ $\quad (2) = (1+\sqrt{3})(1-\sqrt{3})$

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

$= 1 - \sqrt{3}$

$\uparrow$ unit because norm is 1

$(2) = (1+\sqrt{3})^2$.

$(p) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots$

$\mathbb{Z}[\sqrt{3}]/(p) \cong \mathbb{Z}[x]/x^2-3/(p)$

$\cong \mathbb{F}_p[x]/x^2-3$.

$\mathbb{Z}[\sqrt{3}]/\mathfrak{p}_1^{e_1} \times \mathbb{Z}[\sqrt{3}]/\mathfrak{p}_2^{e_2} \times \cdots$

If x^2-3 is irreducible then this is a field.

(p) is prime and thus inert.

If x^2-3 factors in $\mathbb{F}_p$

double root $(x-a)^2$ only if $p=2$ or 3

$\downarrow$

$(p) = (p, \sqrt{3}-a)^2$

e.g. when $p=2$

$(2, \sqrt{3}-1) = (\sqrt{3}-1)$.

$(x-a)(x-b)$ for a, b distinct.

$\mathbb{F}_p[x]/x^2-3 \cong \mathbb{F}_p[x]/(x-a) \times \mathbb{F}_p[x]/(x-b)$.

$(p) = \mathfrak{p}_1\mathfrak{p}_2$.

$(p) = (p, \sqrt{3}-a)(p, \sqrt{3}-b)$.

Observation: For $\mathbb{Z}[i]$ the way p factors depends only on p mod 4.

For $\mathbb{Z}[\sqrt{3}]$ — — only on n mod 12.

Example: $B = \mathbb{R}[x,y]/(y^2-x)$ $\xrightarrow{\text{Frac}}$ $\mathbb{R}(x)[y]/(y^2-x)$

$A = \mathbb{R}[x]$ $\xrightarrow{\text{Frac}}$ $\mathbb{R}(x)$.

Nonzero primes $\leftrightarrow$ irreducible polynomials

$(x-a)$ for $a \in \mathbb{R}$ $\qquad$ $(x-z)(x-\bar{z})$ for $z \in \mathbb{C}\setminus\mathbb{R}$

$\|$

x^2+ax+b s.t. $b^2-4ac<0$.

$B/(x-a) = \mathbb{R}[x,y]/(y^2-x, x-a)$

$= \mathbb{R}[x,y]/(x-a)/(y^2-x)$

$= \mathbb{R}[y]/y^2-a$

always split

$\mathbb{R}[x,y]/(y^2-x, x^2+ax+b)$

$\|$

$\mathbb{C}[y]/y^2-z$

$\|$

$\mathbb{C}[y]/(y-\sqrt{z})(y+\sqrt{z})$.

if $a \in \mathbb{R}_{>0}$

$= \mathbb{R}[y]/(y-\sqrt{a})(y+\sqrt{a})$

$(x-a)\,\mathbb{R}[x,y]/y^2-x$

$\|$

$(x-a, y-\sqrt{a})(x-a, y+\sqrt{a})$.

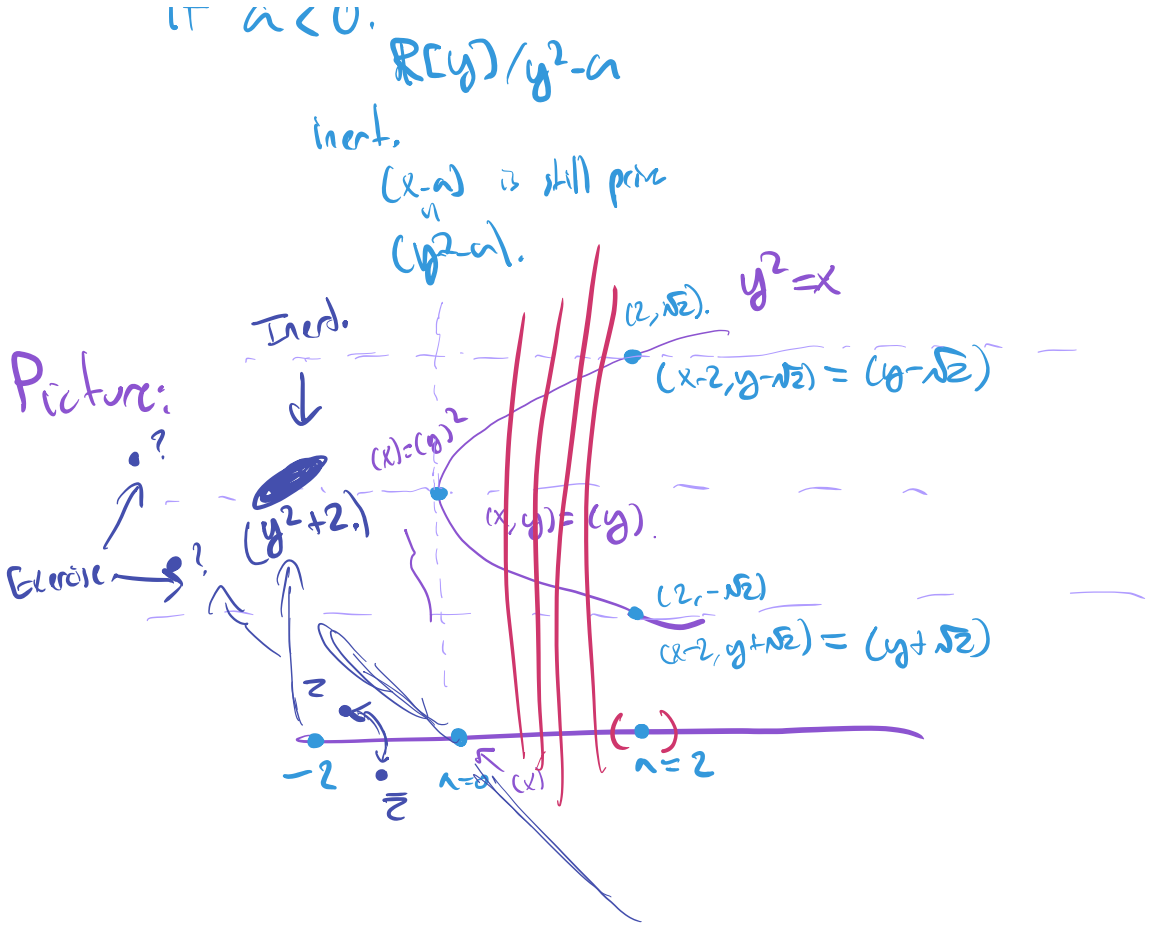
$\|$

$(y-\sqrt{a})(y+\sqrt{a})$.

if $a = 0$ $\quad \mathbb{R}[y]/y^2$.

ramified. $\quad (x) = (y)^2$.

if $a < 0$



Theorem: If A is a DD w/ fraction field K, L is a finite extension, B integral closure of A in L, and $B=A[b]$ (B is monogenic).

Then, for f the minimal polynomial of b, for $\mathfrak{p}$ prime in A

$b \mapsto x$

$B \cong A[x]/f(x)$

factorization of $\mathfrak{p}B \longleftrightarrow$ factorization of f in $A/\mathfrak{p}[x]$.

$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m} \longleftrightarrow f_1^{e_1} \cdots f_m^{e_m}$

$\mathfrak{p}_i = (\mathfrak{p}, f(b))$.

WARNING: Not even B/A is monogenic.

Example: $K = \mathbb{Q}[x]/x^3+3x+12$

$\mathcal{O}_K$ is not monogenic over $\mathbb{Z}$

i.e., not $\cong \mathbb{Z}[\alpha]$ for some α.

In fact if $S = \mathbb{Z}\setminus(2)$

$S^{-1}\mathcal{O}_K$ = integral closure of $S^{-1}\mathbb{Z} = \mathbb{Z}_{(2)}$

is not monogenic.

Theorem: If A is a DD, K fraction field

L/K is a fin. ext., B integral closure of A in L. (cap) $n = [L:K]$.

Then for any $\mathfrak{p}$ nonzero prime in A

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

$$f_i = [B/\mathfrak{q}_i : A/\mathfrak{p}]$$

$$\sum_{i=1}^{n} e_i f_i = n.$$

Proof: $B/\mathfrak{p}B$ is a vector space over $A/\mathfrak{p}$.

Simplifying assumption: B is free as an A-module

$\Rightarrow B \cong A^n$

$B/\mathfrak{p}B \cong A^n/\mathfrak{p}A^n = (A/\mathfrak{p})^n$

n-dim'l $A/\mathfrak{p}$ vector space.

$$B/\mathfrak{p}B \cong \prod^{n} B/\mathfrak{q}_i$$

$\prod_{i=1}^{} \mathfrak{q}_i$

need to see this is of dim $e_i f_i$ over $A/\mathfrak{p}$.

$$B/\mathfrak{q}_i^{e_i} \supseteq \mathfrak{q}_i/\mathfrak{q}_i^{e_i} \supseteq \mathfrak{q}_i^2/\mathfrak{q}_i^{e_i} \supseteq \cdots \supseteq \mathfrak{q}_i^{e_i-1}/\mathfrak{q}_i^{e_i}$$

$\wr$ quot. $\wr$ quot. $\wr$

$B/\mathfrak{q}_i$ $\quad \pi_i\,\mathfrak{q}_i/\mathfrak{q}_i^2 \quad \pi_i^2\,\mathfrak{q}_i^2/\mathfrak{q}_i^3 \quad \cdots$

$\wr\wr$ $\quad \cong \wr\wr$

$B/\mathfrak{q}_i$

Take π_i which generates $\mathfrak{q}_i\, B/\mathfrak{q}_i^{e_i}$

e_i things $\cong B/\mathfrak{q}_i \cong \dim f_i$ by definition.

To eliminate assumption, localize at $\mathfrak{p}$.

$A_{\mathfrak{p}}$ is a PID.

B torsion-free $\Rightarrow$ B is f.g. free

Corollary: If L/K is Galois

$e_i = e$ for all i

$f_i = f$ for all i

$n = mef$. $\qquad \mathfrak{p}B = \mathfrak{q}_1^e \mathfrak{q}_2^e \cdots \mathfrak{q}_m^e$

$B/\mathfrak{q}_i \cong B/\mathfrak{q}_j$.

Proof Exercise $\rightsquigarrow$ show Galois group acts transitively on the $\mathfrak{q}_i$.

Theorem: $K/\mathbb{Q}$ finite extension. p ramifies in K (i.e. $p\mathcal{O}_K = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_n^{e_n}$ w/ $e_i > 1$ for some i) if and only if $p \mid \operatorname{disc}(K/\mathbb{Q})$.

Proof: Take $a_1, \ldots, a_n$ a basis for $\mathcal{O}_K$

$\operatorname{disc} = D = \det\left(\operatorname{tr}_{K/\mathbb{Q}}(a_i a_j)\right)$.

$D \bmod p = \det\left(\operatorname{tr}_{\mathcal{O}_K/p\,/\,\mathbb{F}_p}(\bar{a}_i \bar{a}_j)\right)$.

$\bar{a}_i$ reduction mod p of a_i.

$\mathcal{O}_K/p = \mathcal{O}_K/\mathfrak{q}_1^{e_1} \times \mathcal{O}_K/\mathfrak{q}_2^{e_2} \times \cdots \times \mathcal{O}_K/\mathfrak{q}_n^{e_n}$.

Suppose $e_1 = 2$. $n = 1$. (Reg. example)

$\mathcal{O}_K/\mathfrak{q}_1 = \mathbb{F}_p$

π generates $\mathfrak{q}_1$ in $\mathcal{O}_K/\mathfrak{q}_1^2$.

$\mathbb{F}_p[\pi]/\pi^2$.

1 π basis

$\pi = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ $\quad \begin{pmatrix} \operatorname{tr} 1 & \operatorname{tr} \pi \\ \operatorname{tr} \pi & \operatorname{tr} \pi^2 \end{pmatrix}$.

$\pi^2 = 0$

$$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$$