Norm / Trace
Discriminant

$$\begin{array}{ccc} L & \supset & B \\ | & & | \\ K & \supset & A \end{array}$$

B = free A-module

basis $\beta_1, \dots, \beta_n$.

$Tr_{B/A} : B \to A$

$Disc(B/A) = \det\left(Tr(\beta_i \beta_j)\right)$

get ideal in A

Discriminant ideal:

e.g. $A = \mathbb{Z}$, $B = \mathcal{O}_L$

get well defined integer

discriminant of $\mathcal{O}_L$, L.

e.g. $f = X^3 + X^2 - 1$ nonreal cubic

get $D = -23$.

we took the order

$\mathcal{O} = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2 \subset L$

θ = root of f in L.

$\Rightarrow \mathcal{O} = \mathcal{O}_L$

L/K finite, separable

$\sigma_1, \dots, \sigma_n$ distinct K-embds of L.

$\beta_1, \dots, \beta_n$ K-basis of L

$D(\beta_1, \dots, \beta_n) = \det(\sigma_i \beta_j)^2$

$\Rightarrow D \neq 0$.

$$\begin{array}{ccc} L & \supset & B \\ n \,| & & | \\ K & \supset & A \end{array}$$

int domain, int closed

$\exists$ free A-submods M, M'
rank $= n$
and

$$M \subset B \subset M'$$

Cor A Noetherian $\Rightarrow B$ fin gen.
A PID $\Rightarrow B$ free.

Cor $A = \mathbb{Z}$, $B = \mathcal{O}_L$
$\Rightarrow B$ free $\mathbb{Z}$ module of finite rank.

Prop $L = K(\beta)$ deg n.
f = min poly of β / K.
Ω gal closure of L
$f = \prod (x - \beta_i)$ in $\Omega[x]$

Then

$$D(1, \beta, \beta^2, \dots, \beta^{n-1}) = \prod_{i<j} (\beta_i - \beta_j)^2 = (-1)^{n(n-1)/2} N_{L/K}(f'(\beta))$$

Pf

$$D = \det(\sigma_i \beta_j)^2 = \det(\beta_i^j)^2 = \det \begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \cdots \\ 1 & \beta_2 & \beta_2^2 & \cdots \\ \vdots & & & \\ 1 & \beta_n & \beta_n^2 & \cdots \end{pmatrix}^2$$

Vandermonde det.

$$= \prod_{i<j} (\beta_i - \beta_j)^2$$

// classical fmla.

$$= (-1)^{n(n-1)/2} \prod_{i} \prod_{i \neq j} (\beta_i - \beta_j)$$

$$= (-1)^{*} \prod_{i} f'(\beta_i)$$

$$= (-1)^{*} N_{L/k} f'(\beta)$$

e.g. $f = x^3 + ax + b$

$$\Rightarrow -27b^2 - 4a^3$$

Rmk If f is irred / $\mathbb{Q}$
Then get 2 discriminants attached to it:

① n.f. discriminant
= disc of ring of ints of $\mathbb{Q}[x]/(f)$

② poly disc of f
comes from the coeffs
or $\prod_{i<j} (\alpha_i - \alpha_j)^2$ ← roots.

Not the same.

2 Classical results $D = \operatorname{disc} L \in \mathbb{Z}$.

Thm (Brill's Thm)

$\operatorname{sign} D = (-1)^s$, where
$L \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^r \times \mathbb{C}^s$

e.g. $x^3 + x^2 - 1$ $(r,s) = \{(3,0), (1,1)\}$

$r + 2s = n$ deg.

$D = -23$

Pf $\prod_{i<j} (\beta_i - \beta_j)^2$

$L = \mathbb{Q}(\beta)$ $\beta_1, \ldots, \beta_n$ roots of min poly.

real roots don't affect sign.

sim real + complex don't affect sign.

α β

complex − complex can only affect sign when $\alpha = \bar{\beta}$ and you get a -1

$\Rightarrow (-1)^s$

Thm (Stickelberger's criterion) L/Q.

$D_L \equiv 0, 1 \bmod 4$.

Pf. $D_L = \det(\sigma_i \beta_j)^2$

P = sum of terms for even perms

N = sum of terms for odd perms

$\Rightarrow \det = P - N$

$D_L = (P-N)^2 =$

$(P+N)^2 - 4PN$

$L \subset \Omega$ Gal closure.

Take $\tau \in G(\Omega/\mathbb{Q})$

Claim: either

(1) $\tau P = P$, $\tau N = N$ or

(2) $\tau P = N$, $\tau N = P$

$\Rightarrow$ $P+N$, PN invariant.

$\Rightarrow$ $\in \mathbb{Q}$

$\Rightarrow$ $\in \mathbb{Z}$ (cause β_i integral)

$\Rightarrow$ D_L is square mod 4

$\Rightarrow$ $0, 1 \bmod 4$.

e.g. $D = -23 \equiv 1 \ (4)$

e.g. $\mathbb{Q}(\sqrt{2}) = L$

$\mathcal{O}_L = \mathbb{Z}[\sqrt{2}]$.

$D_L = 8 = 4 \cdot 2$

Rem

(1) not every integer is a discriminant.

degree is large $\Leftrightarrow$ gaps are large.

(2) D_L is an invariant, but doesn't uniquely determine L.

class group

next big invariant

attaches to each $L/\mathbb{Q}$ a finite abelian group. $Cl(L)$ or $Cl(\mathcal{O}_L)$

order is called the class number

h_K

$Cl(L)$ measures how far $\mathcal{O}_L$ is from being a P.I.D.

To define it, first need to discuss Dedekind domains

Def A Dedekind domain is an integral domain satisfying the following:

(a) Noetherian
(b) Integrally closed
(c) every nonzero prime ideal is maximal.

Thm Let A be a Dedekind Domain.

Then every nonzero proper ideal $\mathfrak{a}$ admits a factorization into prime ideals

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_k^{r_k}$$

$\mathfrak{p}_i$ prime ideals

$r_i > 0$

Factorization is unique (up to order)

Thm $\mathcal{O}_L$ is a Dedekind domain.

$L = \mathbb{Q}(\sqrt{-5})$

$\mathcal{O}_L = \mathbb{Z}[\sqrt{-5}]$ (**)

$21 = 3 \cdot 7 = (1+2\sqrt{-5})(1-2\sqrt{-5})$

2 prime factorizations

Kummer:

$210 = 10 \cdot 21 = 6 \cdot 35$ (*)

(actually 4 primes $2, 3, 5, 7$)

$(2 \cdot 5) \cdot (3 \cdot 7) = (2 \cdot 3)(5 \cdot 7)$

we're seeing "groupings" in (*)

sim in (**), there are 4 "primes" being grouped

p_1, p_2, p_3, p_4

$3 = p_1 p_2$, $7 = p_3 p_4$

$1 - 2\sqrt{-5} = p_1 p_4$

$1 + 2\sqrt{-5} = p_2 p_3$

in $\mathbb{Z}$: $a \mid b \iff (a) \supseteq (b)$

so $p_1 \mid (3)$, $p_1 \mid (1-2\sqrt{-5})$

$\Rightarrow$ $\mathfrak{p}_1$ should contain these ideals

(3) , $(1-2\sqrt{-5})$ ⓐ

$\Rightarrow$ we set $\mathfrak{p}_1$ to be the ideal

$(3, 1-2\sqrt{-5}) \subseteq \mathcal{O}_L$

should be analogue of GCD

does give a prime ideal dividing ⓐ (in the sense of containment)