Given integral basis $\alpha_1, \dots, \alpha_n$ for B : integral closure of A (a P.I.D.) in L/K

then $\mathrm{disc}(B) := d(\alpha_1, \dots, \alpha_n) = \det(\mathrm{Tr}(\alpha_i \alpha_j))$

If $L = K(\theta)$ separable with $\theta \in B$, then $d(1, \theta, \dots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2$

where $\theta_i := \sigma_i(\theta)$

= usual def'n of discriminant of min poly. of θ as squares of diff's of roots.

call it p_θ

But might not be true that $\mathrm{disc}(B) = \mathrm{disc}(p_\theta)$.

Why? Because $1, \theta, \dots, \theta^{n-1}$ might not be integral basis. Saw this already for $d \equiv 1 \ (4)$ and $\mathbb{Q}(\sqrt{d})$.

There $\mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$.

We do know $\mathbb{Z}[\theta]$ is submodule of B, since θ integral (even subring)

and both free modules of rank $[L:K]$, so using classification of modules over P.I.D.s $B/\mathbb{Z}[\theta]$ is finite gp (true for any quotient of B by subring with integral basis of size n)

"orders of B"

Sometimes refer to $\mathcal{O}_K$ as the "maximal order"

How to calculate the integral basis?

idea (See Ch. 6 of Cohen's "A Course in Computational Algebraic Number Theory")

enlarge $\mathbb{Z}[\theta]$ for each prime p in $[B : \mathbb{Z}[\theta]]$

In fact we know more:

$$\underbrace{d(1, \theta, \dots, \theta^{n-1})}_{\mathrm{disc}(p_\theta)} \cdot B \subseteq \underbrace{\mathbb{Z} + \mathbb{Z}\theta + \dots + \mathbb{Z}\theta^{n-1}}_{\mathbb{Z}[\theta]}$$

p_θ : minimal poly. of θ

So can look for primes dividing $\mathrm{disc}(p_\theta)$ to order ≥ 2, and enlarge $\mathbb{Z}[\theta]$ at each such p.

And if $[B : \mathbb{Z}[\theta]] = f$ then $\underbrace{\mathrm{disc}(p_\theta)}_{\text{computable using resultants.}} = \mathrm{disc}(\mathcal{O}_K) \cdot f^2$

$\mathcal{O}_K = B$

Studying $\mathcal{O}_K$: ring of integers of $K/\mathbb{Q}$, have $N_{K/\mathbb{Q}}$, $Tr_{K/\mathbb{Q}}$, $d(\mathcal{O}_K)$, integral basis as $\mathbb{Z}$-module.

want to understand how (rational) primes decompose in $\mathcal{O}_K$, but we <u>don't</u> have unique factorization into irreducible eleme<u>nts</u>.

We <u>do</u> have factorizations of any elt. into irreducibles. (follows from existence of norm function)

$$\text{if} \quad b = b_1 b_2 \quad \text{then} \quad N(b) = N(b_1)N(b_2)$$

with $N(b_1), N(b_2) < N(b)$ (since b_1, b_2 non-units)

But, for example in $\mathbb{Q}(\sqrt{-5})$, we have $\mathcal{O}_K = \mathbb{Z}(\sqrt{-5})$ since $-5 \equiv 3\ (4)$

$$6 = \underset{\substack{\uparrow \\ 4}}{2} \cdot \underset{\substack{\uparrow \\ 9}}{3} = (\underset{\substack{\uparrow \\ 6}}{1+\sqrt{-5}})(\underset{\substack{\uparrow \\ 6}}{1-\sqrt{-5}})$$

<u>norms</u> : 4 9 6 6

Are $1+\sqrt{-5}$, $1-\sqrt{-5}$ irreducible? in $\mathcal{O}_K$

If not, need to find $a+b\sqrt{-5}$ with $N(a+b\sqrt{-5}) = a^2+5b^2$ a proper divisor of 6.

No solutions.

As Neukirch nicely explains, one could hope to work in enlarged domain containing $\mathcal{O}_K$ where some further divisibility held:

Want some factorization

$$\underset{\substack{\uparrow \\ \mathfrak{p}_1\mathfrak{p}_2}}{2} \cdot \underset{\substack{\uparrow \\ \mathfrak{p}_3\mathfrak{p}_4}}{3} = (\underset{\substack{\uparrow \\ \mathfrak{p}_1\mathfrak{p}_3}}{1+\sqrt{-5}})(\underset{\substack{\uparrow \\ \mathfrak{p}_2\mathfrak{p}_4}}{1-\sqrt{-5}})$$

with properties that if $\mathfrak{p} \mid a$, $\mathfrak{p} \mid b$, $a, b \in \mathcal{O}_K$ then $\mathfrak{p} \mid a \pm b$

similarly if $\mathfrak{p} \mid a$, $a \in \mathcal{O}_K$ then $\mathfrak{p} \mid ma$ for any $m \in \mathcal{O}_K$.

Leads us to the concept of "ideal". Recall that "prime ideal" $\mathfrak{p}$ in ring A is ideal s.t. $A/\mathfrak{p}$ is integral domain. For example if $\mathfrak{m}$ maximal ideal, then $A/\mathfrak{m}$ field, so all maximal ideals are prime.

Dedekind realized right set of conditions required for a ring to have unique factorization into product of prime ideals.

"Dedekind domain" – integral domain that is

(i) Noetherian

(ii) integrally closed (in its field of fractions)

(iii) every non-zero prime ideal is maximal.

To show (1) $\mathcal{O}_K$ is Dedekind domain

(2) Any Dedekind domain has unique factorization of non-trivial ideal into product of prime ideals.

Proposition: $\mathcal{O}_K$ is Dedekind domain.

pf: (ii) follows by definition. For (i), we use the fact that $\mathbb{Z}$, as P.I.D., is Noetherian (as $\mathbb{Z}$-module, every increasing sequence of submodules is stationary)

and $\mathcal{O}_K$ is finitely generated over $\mathbb{Z}$, so also Noetherian

(in general $E' \subset E$ are A-modules, then E Noetherian $\Leftrightarrow$ E', E/E' Noetherian)

So left to show if $\mathfrak{p} \neq 0$ is prime ideal then $\mathfrak{p}$ maximal:

we have $\mathfrak{p} \cap \mathbb{Z}$ is prime ideal of $\mathbb{Z}$, say (p), because $\mathfrak{p} \cap \mathbb{Z}$ is kernel of $\mathbb{Z} \to \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$ so have injective hom $\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z}) \to \mathcal{O}_K/\mathfrak{p}$

so $\mathbb{Z}/(\mathfrak{p} \cap \mathbb{Z})$ is subring of integral domain.

Given $x \in \mathfrak{p} \setminus \{0\}$ with min. poly $x^n + a_1 x^{n-1} + \dots + a_n = 0$

$a_n \neq 0$ since else this wasn't min. poly, b/c we can factor out x.

Now $a_n \in \mathcal{O}_K \cdot x \cap \mathbb{Z} \subset \mathfrak{p} \cap \mathbb{Z} = (p)$ so $p \neq 0$. (which we didn't know a priori)

Now ~~[scribble]~~ $\mathcal{O}_K/\mathfrak{p}$ integral over $\mathbb{Z}/(p)$, a field, since $\mathcal{O}_K$ integral over $\mathbb{Z}$ $\Rightarrow$ $\mathcal{O}_K/\mathfrak{p}$ a field $\Rightarrow$ $\mathfrak{p}$ maximal.

Every $b \in \mathcal{O}_K/\mathfrak{p}$ satisfies integral equation with coeffs in field $\mathbb{Z}/p\mathbb{Z}$.

so $A[b] = A(b)$ i.e. b invertible. (use division algorithm for polynomial rings)

Main theorem: Every non-trivial ideal $\mathfrak{a}$ in Dedekind domain $\mathcal{O}$ has a unique factorization $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ into non-zero prime ideals.

—

Recall that product of ideals $\mathfrak{a}\mathfrak{b} = \{ \sum_i a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \}$

and similarly $\mathfrak{a} + \mathfrak{b} = \{ a+b \mid a \in \mathfrak{a}, b \in \mathfrak{b} \}$

Sometimes write $\mathfrak{a} \mid \mathfrak{b}$ for $\mathfrak{b} \subseteq \mathfrak{a}$ (just think about integers $7 \mid 14$ means $(14) \subseteq (7)$)

—

Lemma 1: For every non-zero ideal $\mathfrak{a}$ of $\mathcal{O}$, $\exists\ \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ with $\mathfrak{a} \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_r$. (Really only uses fact that $\mathcal{O}$ Noetherian)

pf: Let M: set of ideals for which desired property fails. Then order these ideals by inclusion. Since $\mathcal{O}$ Noetherian, every ascending chain stabilizes, so $\exists$ maximal elt. in M, call it $\mathfrak{m}$. (not prime, since in M)

$\overset{\text{def'n}}{\Longrightarrow}$ $\exists\ b_1, b_2 \in \mathcal{O}$ with $b_1 b_2 \in \mathfrak{m}$ but $b_1, b_2 \notin \mathfrak{m}$

Let $\mathfrak{m}_1 = (b_1) + \mathfrak{m}$
$\mathfrak{m}_2 = (b_2) + \mathfrak{m}$ so $\mathfrak{m} \subsetneq \mathfrak{m}_i$, $\mathfrak{m}_1 \mathfrak{m}_2 \subseteq \mathfrak{m}$.

But $\mathfrak{m}_i$ not in M by maximality, so are products of primes $\Rightarrow$ $\mathfrak{m}$ contains product of both $\mathfrak{m}_i$.