3.1. Norms of ideals

Recall: integer $n \in \mathbb{Z}$ $\rightsquigarrow$ ideal in $\mathcal{O}_K$

rat. number $\rightsquigarrow$ fract. ideal

$|n| \in \mathbb{Z}$ abs. val. $\rightsquigarrow$ norm of fract. ideals

$K/\mathbb{Q}$ number field, $\mathcal{O}_K \subseteq K$ r. o. i.

Def: $0 \neq I \subseteq \mathcal{O}_K$ some ideal.

$$N(I) := \#(\mathcal{O}_K/I) = [\mathcal{O}_K : I]$$

Prop.: 1) If $I = (x)$, $x \in \mathcal{O}_K \setminus \{0\}$.

$$\Rightarrow N(I) = |N_{K/\mathbb{Q}}(x)|$$

2) $N(I) \cdot N(J) = N(I \cdot J)$

3) $n \in \mathbb{Z}$, then $\{I \subseteq \mathcal{O}_K \mid N(I) = n\}$ is finite

Pf: 1) $\#\mathrm{Coker}(\mathcal{O}_K \xrightarrow{x} \mathcal{O}_K) = |\det(\mathrm{Mat}(x))|$

$\#(\mathcal{O}_K/(x)) = |N_{K/\mathbb{Q}}(x)|$

Used: $f: M \to M$ inj. endo. of finite free $\mathbb{Z}$-modules

$\Rightarrow \#\mathrm{Coker}(M f) = |\det(f)|$

2) Sufficient to see

$$N(\mathfrak{p} \cdot I) = N(\mathfrak{p}) \cdot N(I)$$

Have $I/\mathfrak{p}\cdot I \xrightarrow{\cdot \mathfrak{p}^{-1}} \mathcal{O}_K/\mathfrak{p}$ $(I^{-1} \cdot I = \mathcal{O}_K)$

multiply with I^{-1} tensor

$\Rightarrow$ $I^{-1} \cdot J \simeq I^{-1} \otimes J$

$I^{-1} = \mathrm{Hom}_A(I, A)$

$$\frac{N(I\cdot\mathfrak{p})}{N(I)} = \frac{[\mathcal{O}_K : \mathfrak{p}\cdot I]}{[\mathcal{O}_K : I]} = [I : \mathfrak{p}I]$$

$\#$

$= [\mathcal{O}_K : \mathfrak{p}] = N(\mathfrak{p})$

3) If $N(I) = n$, then

$(n) \subseteq I$ (as $n \cdot \mathcal{O}_K/I = \{0\}$)

But $\mathcal{O}_K/n$ is a finite ring $\square$

Let $I = \alpha \cdot \mathfrak{d}^{-1}$ with $\alpha, \mathfrak{d} \subseteq \mathcal{O}_K$

Set $N(I) := \dfrac{N(\alpha)}{N(\mathfrak{d})} \in \mathbb{Q}_+^*$

(ind. of $\alpha, \mathfrak{d}$ by prev. prop. 2)

Def: 1) The inverse different is $\delta_K^{-1} := \{x \in K \mid Tr_{K/\mathbb{Q}}(x \cdot y) \in \mathbb{Z}, \forall y \in \mathcal{O}_K\}$

$= \mathcal{O}_K^\vee \supseteq \mathcal{O}_K$

2) $\delta_K := (\delta_K^{-1})^{-1} \subseteq \mathcal{O}_K$ the absolute different of K

Prop: $N(\delta_K) = |\Delta_K|$

Proof: Write $\langle \alpha_1, \dots, \alpha_n \rangle_{\mathbb{Z}} = \mathcal{O}_K$

$\Rightarrow \delta_K^{-1} = \langle \alpha_1^\vee, \dots, \alpha_n^\vee \rangle_{\mathbb{Z}}$

and $\mathcal{O}_K \xrightarrow{\cdot \alpha} \delta_K^{-1}$

repr. by matrix $(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j))$

$\Rightarrow \#\mathrm{Coker}(\alpha) = |\det(\alpha)| = |\Delta_K|$

$N(\delta_K) \quad \| \quad \#\mathrm{Coker}(\delta_K \hookrightarrow \mathcal{O}_K)$

Definition: An order $\mathcal{O} \subseteq K$ is a subring $\mathcal{O}$, s.t.

1) $\mathcal{O}$ is fin. gen. over $\mathbb{Z}$ ($\rightsquigarrow \mathcal{O} \subseteq \mathcal{O}_K$)
2) $\mathbb{Q} \underset{\mathbb{Z}}{\otimes} \mathcal{O} = K$ ($\Leftrightarrow \mathrm{rk}_{\mathbb{Z}} \mathcal{O} = [K:\mathbb{Q}]$)

Ex: * $\mathcal{O} = \mathcal{O}_K$ the maximal order

* $n \geq 1$, $\mathcal{O}_n := \mathbb{Z}[n \cdot \sqrt{D}] \subset K = \mathbb{Q}(\sqrt{D})$

$D \in \mathbb{Z}$ squarefree

Def: Let $\mathcal{O}$ order in K.

Then

$\Delta_{\mathcal{O}} := \mathrm{Disc}(\alpha_1, \ldots, \alpha_n)$ for

$\alpha_1, \ldots, \alpha_n \in \mathcal{O}$ $\mathbb{Z}$-basis

the "disc. of $\mathcal{O}$" (indep. of choice)

Clearly, $\Delta_{\mathcal{O}_K} = \Delta_K$, $\Delta_K \mid \Delta_{\mathcal{O}}$

Ex: * $\mathcal{O}_n \rightsquigarrow \Delta_{\mathcal{O}_n} = 4 \cdot n^2 \cdot D$

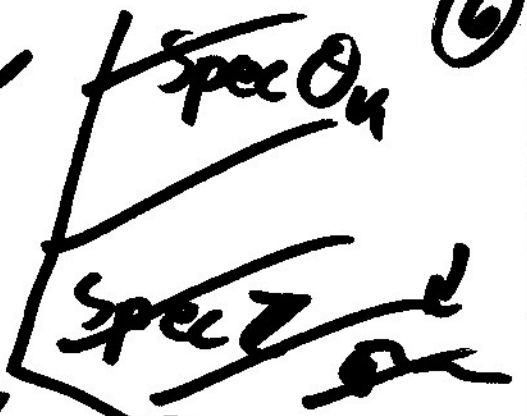
Prop: $\mathcal{O} \subseteq K$ order

$\Rightarrow \Delta_{\mathcal{O}} \cdot \mathcal{O}_K \subseteq \mathcal{O}$

Pf: $\mathcal{O} \subseteq \mathcal{O}_K \subseteq \mathcal{O}_K^\vee \subseteq \mathcal{O}^\vee$

and $[\mathcal{O}^\vee : \mathcal{O}] = |\Delta_{\mathcal{O}}|$

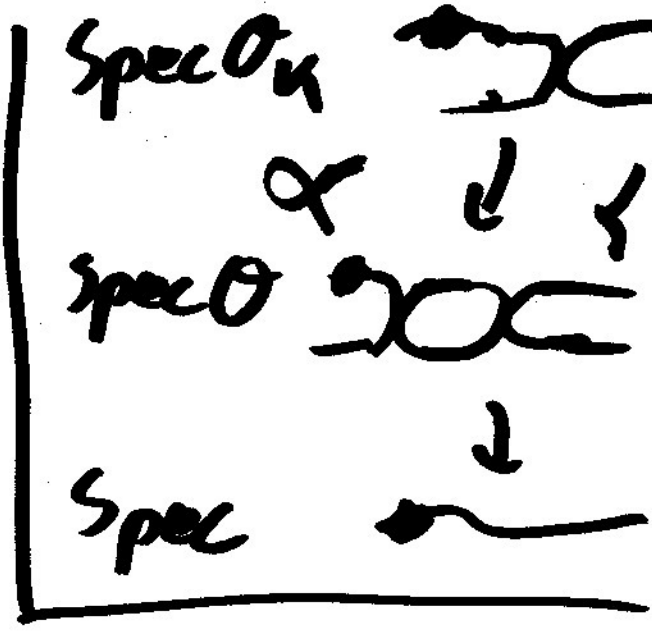
$\Rightarrow \Delta_{\mathcal{O}} \cdot \mathcal{O}_K \subseteq \Delta_{\mathcal{O}} \cdot \mathcal{O}^\vee \subseteq \mathcal{O}$.



3.2. Decomposition of primes

Δ L/K fin. ext. of number fields

(more gen:
A Ded., $K = \mathrm{Frac}(A)$,
L fin. sep. ext.)



$0 \neq \mathfrak{p} \subseteq \mathcal{O}_K$ prime

$\Rightarrow \mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdot \ldots \cdot \mathfrak{q}_g^{e_g}$ for pairwise dist. maximal primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_g \subseteq \mathcal{O}_L$

Def: 1) $e(\mathfrak{q}_i|\mathfrak{p}) = e_i = v_{\mathfrak{q}_i}(\mathfrak{p}\mathcal{O}_L)$

ramification index of $\mathfrak{q}_i$ over $\mathfrak{p}$

2) $f(\mathfrak{q}_i|\mathfrak{p}) = [k(\mathfrak{q}_i) : k(\mathfrak{p})]$

residue degree of $\mathfrak{q}_i$ over $\mathfrak{p}$

3) (Here $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{q}_i$

as $\mathfrak{p} = \mathcal{O}_K \cap \mathfrak{q}_i$)

⚠ 3) $\mathfrak{p}$ is

- unramified in L/K if

$e(\mathfrak{q}_i|\mathfrak{p}) = 1$ for all i

- split in L/K if

$e(\mathfrak{q}_i|\mathfrak{p}) = 1$ for all i

$\times$ $f(\mathfrak{q}_i|\mathfrak{p}) = 1$ for all i

- inert if $g=1$ and
  $e(\mathfrak{q}_1|\mathfrak{p})=1$ (i.e. $\mathfrak{p}\mathcal{O}_L$ is prime)
- ramified in L/K if $e(\mathfrak{q}_i|\mathfrak{p})>1$
  for some i
- totally ramified if $g=1$
  and $f(\mathfrak{q}_1|\mathfrak{p})=1$

In the general situation one
should assume
that $k(\mathfrak{q}_i]$ is sep. over $k(\mathfrak{p})$.