3 Algebraic integers

3.1 Number fields

Definition 3.1.1: (a) A finite field extension $K/\mathbb{Q}$ is called an *(algebraic) number field.*

(b) A number field of degree $2, 3, 4, 5, \ldots$ is called *quadratic, cubic, quartic, quintic,...*

(c) The integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in K is called the ring of *algebraic integers in K.*

In the rest of this chapter we fix such K and $\mathcal{O}_K$ and abbreviate $n := [\cancel{K:\mathbb{Q}}]$. $[K/\mathbb{Q}]$.

Proposition 3.1.2: (a) The ring $\mathcal{O}_K$ is Dedekind. ← 1.9.5

(c) $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n. ← 1.7.6

(b) Any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.

$$\exists\, a, b \in \mathcal{O}_K : \underbrace{a\mathcal{O}_K}_{} < \mathfrak{a} < \underbrace{\tfrac{1}{b}\mathcal{O}_K}_{}$$

free $\mathbb{Z}$-modules of rank n.

3.2 Absolute discriminant

Proposition 3.2.1: (a) For any $\mathbb{Z}$-submodule $\Gamma \subset K$ of rank n with an ordered $\mathbb{Z}$-basis $(x_1, \ldots, x_n)$ the following value depends only on Γ:

$$\operatorname{disc}(\Gamma) := \operatorname{disc}(x_1, \ldots, x_n) \in \mathbb{Z} \setminus \{0\}.$$

(b) For any two $\mathbb{Z}$-submodules $\Gamma \subset \Gamma' \subset K$ of rank n the index $[\Gamma' : \Gamma]$ is finite and we have

$$\operatorname{disc}(\Gamma) = [\Gamma' : \Gamma]^2 \cdot \operatorname{disc}(\Gamma').$$

Proof: (a) $x_1', \ldots, x_n'$ another basis of Γ $\Rightarrow$ $x_i = \sum_j a_{ij} x_j'$; $A := (a_{ij})_{i,j} \in GL_n(\mathbb{Z})$

$\Rightarrow \det(A) = \pm 1$;

$(\operatorname{tr}(x_i \cdot x_j))_{i,j} = A \cdot (\operatorname{tr}(x_i' \cdot x_j'))_{i,j} \cdot A^T$

$\Rightarrow \operatorname{disc}(x_1, \ldots, x_n) = \det(A)^2 \cdot \operatorname{disc}(x_1', \ldots, x_n')$.

(b) $x_1', \ldots, x_n'$ basis of Γ' $\Rightarrow$ $\operatorname{disc}(\Gamma) = \operatorname{disc}(x_1, \ldots, x_n) = \det(A)^2 \cdot \operatorname{disc}(\Gamma')$.

Elementary divisor thm: $\exists\, U, V \in GL_n(\mathbb{Z})$: $UAV = \begin{pmatrix} e_1 & & 0 \\ & \ddots & \\ 0 & & e_n \end{pmatrix}$ with $e_i \in \mathbb{Z}$, $e_i > 0$

$\Rightarrow \det(A) = \pm \prod_{i=1}^n e_i = \pm [\Gamma' : \Gamma]$. $\quad \Rightarrow \Gamma'/\Gamma \cong \mathbb{Z}^n / A\mathbb{Z}^n \cong \bigoplus \mathbb{Z}/e_i\mathbb{Z}$.

Definition 3.2.2: The number

$$d_K \;:=\; \mathrm{disc}(\mathcal{O}_K) \;\in\; \mathbb{Z} \setminus \{0\}$$

is called the *discriminant of $\mathcal{O}_K$ or of K.*

Corollary 3.2.3: If there exist $a_1, \ldots, a_n \in \mathcal{O}_K$ such that $\mathrm{disc}(a_1, \ldots, a_n)$ is squarefree, then

$$\mathcal{O}_K = \mathbb{Z}a_1 \oplus \ldots \oplus \mathbb{Z}a_n.$$

Proof: Let $\Gamma := \mathbb{Z}a_1 \oplus \ldots \oplus \mathbb{Z}a_n$

$$\Rightarrow \quad \underbrace{\mathrm{disc}(\Gamma)}_{\text{squarefree}} = \underbrace{[\mathcal{O}_K : \Gamma]}_{\substack{= \\ 1.}}^2 \cdot \mathrm{disc}(\mathcal{O}_K).$$

squarefree $\Rightarrow$ $\shortparallel$ $1.$

qed.

3.3 Absolute norm

Definition 3.3.1: The *absolute norm* of a non-zero ideal $\mathfrak{a} \subset \mathcal{O}_K$ is the index

$$\mathrm{Nm}(\mathfrak{a}) := [\mathcal{O}_K : \mathfrak{a}] \in \mathbb{Z}^{\geqslant 1}.$$

Proposition 3.3.2: For any $a \in \mathcal{O}_K \setminus \{0\}$ we have $\mathrm{Nm}((a)) = |\,\mathrm{Nm}_{K/\mathbb{Q}}(a)|$.

Proof: Let $T_a : K \to K,\ x \mapsto ax$

Take an ordered basis B of $\mathcal{O}_K$ over $\mathbb{Z}$

$\Rightarrow \mathrm{Nm}_{K/\mathbb{Q}}(a) = \det(T_a) = \det(M)$ for $M := {}_B[T_a]_B$. $\quad M \in \mathrm{Mat}_{n\times n}(\mathbb{Z})$

Elementary divisors thm $\Rightarrow \exists\, U, V \in GL_n(\mathbb{Z})$: $UMV = \begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_n \end{pmatrix}$ with $e_i > 0$.

$\Rightarrow |\mathrm{Nm}_{K/\mathbb{Q}}(a)| = |\det(M)| = e_1 \cdots e_n = [\mathbb{Z}^n : UMV \cdot \mathbb{Z}^n]$

$= [\mathcal{O}_K : T_a(\mathcal{O}_K)] = [\mathcal{O}_K : (a)]$.

qed.

Proposition 3.3.3: For any integer $N \geqslant 1$ there exist only finitely many non-zero ideals $\mathfrak{a} \subset \mathcal{O}_K$ with $\mathrm{Nm}(\mathfrak{a}) \leqslant N$.

Proof: If $[\mathcal{O}_K : \mathfrak{a}] \leq N \Rightarrow N! \cdot \mathcal{O}_K \subset \mathfrak{a} \subset \mathcal{O}_K$.
with $\mathcal{O}_K / N! \mathcal{O}_K$ finite. qed.

Proposition 3.3.4: For any two non-zero ideals $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ we have

$$\mathrm{Nm}(\mathfrak{a}\mathfrak{b}) = \mathrm{Nm}(\mathfrak{a}) \cdot \mathrm{Nm}(\mathfrak{b}).$$

Proof: $\mathrm{Nm}(\mathfrak{a}\mathfrak{b}) = [\mathcal{O}_K : \mathfrak{a}\mathfrak{b}] = [\mathcal{O}_K : \mathfrak{a}] \cdot [\mathfrak{a} : \mathfrak{a}\mathfrak{b}]$

1.11.9: $\mathcal{O}_K/\mathfrak{b} \xrightarrow{\sim} \mathfrak{a}/\mathfrak{a}\mathfrak{b}$. $\Rightarrow [\mathcal{O}_K : \mathfrak{a}] \cdot [\mathcal{O}_K : \mathfrak{b}] = \mathrm{Nm}(\mathfrak{a}) \cdot \mathrm{Nm}(\mathfrak{b})$

qed.

Let J_K denote the group of fractional ideals of $\mathcal{O}_K$.

Corollary 3.3.5: The absolute norm extends to a unique homomorphism

$$\mathrm{Nm}\colon J_K \longrightarrow (\mathbb{Q}^{>0}, \cdot).$$

Proof: For any $\mathfrak{a} \in J_K$ take $b \in \mathcal{O}_K \setminus \{0\}$: $\mathfrak{a} \subset (\frac{1}{b}) \Rightarrow b \cdot \mathfrak{a} \subset \mathcal{O}_K$.

Set $\mathrm{Nm}(\mathfrak{a}) := \dfrac{\mathrm{Nm}(b \cdot \mathfrak{a})}{\mathrm{Nm}((b))}$. This is independent of b (and multiplicative) by 3.3.4

If $c \cdot \mathfrak{a} \subset \mathcal{O}_K$ for $c \in \mathcal{O}_K \setminus \{0\}$

$\Rightarrow \mathrm{Nm}(b\mathfrak{a}) \cdot \mathrm{Nm}((c)) = \mathrm{Nm}(bc\mathfrak{a}) = \mathrm{Nm}(c\mathfrak{a}) \cdot \mathrm{Nm}((b))$.

qed.

3.4 Real and complex embeddings

Throughout the following we abbreviate $\Sigma := \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ and set

The group $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ acts on Σ. So $r = \#$ fixed points and $s = \#$ orbits of length 2. hence $|\Sigma| = r + 2s$.

$$\begin{aligned} r &:= \text{ the number of } \sigma \in \Sigma \text{ with } \sigma(K) \subset \mathbb{R}, \\ s &:= \text{ the number of } \sigma \in \Sigma \text{ with } \sigma(K) \not\subset \mathbb{R}, \text{ up to complex conjugation.} \end{aligned}$$

Proposition 3.4.1: We have $r + 2s = n$.

Proof: $n = [K/\mathbb{Q}] = |\Sigma|$ because $K/\mathbb{Q}$ is finite separable.

Proposition 3.4.2: We have ring isomorphisms

$$\begin{array}{ccc} K \otimes_{\mathbb{Q}} \mathbb{C} & \xrightarrow[\sim]{(*)} & K_{\mathbb{C}} := \prod_{\sigma\in\Sigma} \mathbb{C}, \quad = \mathbb{C}^{\Sigma} \\ \cup & & \cup \\ K \otimes_{\mathbb{Q}} \mathbb{R} & \xrightarrow[\sim]{(**)} & K_{\mathbb{R}} := \left\{ (z_\sigma)_\sigma \in K_{\mathbb{C}} \,\middle|\, \forall \sigma \in \Sigma\colon z_{\bar\sigma} = \bar z_\sigma \right\}. \\ x \otimes z & \longmapsto & (\sigma(x) z)_{\sigma\in\Sigma} \end{array}$$

The map $x \mapsto x \otimes 1$ induces an embdding $j\colon K \hookrightarrow K_{\mathbb{R}}$.

Proof: $K \times \mathbb{C} \to K_{\mathbb{C}}$, $(x, z) \mapsto (\sigma(x)\cdot z)_{\sigma\in\Sigma}$ is $\mathbb{Q}$-bilinear $\Rightarrow$ yields $(*)$

$(*)$ is $\mathbb{Q}$-linear, in fact $\mathbb{C}$-linear because this is $\mathbb{C}$-linear in z.

The $\sigma \in \Sigma$ are $\mathbb{C}$-linearly independent $\Rightarrow (*)$ is an isomorphism.

Next: if $z \in \mathbb{R}$, then $\bar\sigma(x)\cdot z = \overline{\sigma(x)\cdot z}$, so $(*)$ maps $K \otimes_{\mathbb{Q}} \mathbb{R}$ into $K_{\mathbb{R}}$.

$(**)$ is injective; $\boxed{K_{\mathbb{R}} \cong \prod_{\sigma \text{ fixed}} \mathbb{R} \times \prod_{\sigma \text{ nonfixed up to } \bar{\ }} \mathbb{C}}$ $\Rightarrow \dim_{\mathbb{R}}(K_{\mathbb{R}}) = r + 2s = n = \dim_{\mathbb{Q}}(K)$.

$\Rightarrow [**]$ is an isomorphism. qed.

Proposition 3.4.3: For every fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ the image $j(\mathfrak{a})$ is a complete lattice in $K_{\mathbb{R}}$.

Proof:
$$\begin{array}{ccccc} \mathfrak{a} \subset K & \hookrightarrow & K \otimes_{\mathbb{Q}} \mathbb{R} \\ \cong & \rightsquigarrow & \cong \\ \mathbb{Z}^n \subset \mathbb{Q}^n & \hookrightarrow & \mathbb{R}^n \end{array}$$
qed.

$\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+1}}, \ldots, \overline{\sigma_{r+s}}$

To describe this with more explicit coordinates we let $\sigma_1, \ldots, \sigma_r$ be the real embeddings and $\sigma_{r+1}, \ldots, \sigma_n$ the non-real embeddings such that $\bar{\sigma}_{r+j} = \sigma_{r+j+s}$ for all $1 \leqslant j \leqslant s$.

Proposition 3.4.4: We have an isomorphism of $\mathbb{R}$-vector spaces

$$K_{\mathbb{R}} \xrightarrow{\sim} \mathbb{R}^n, (z_\sigma)_\sigma \longmapsto \left(z_{\sigma_1}, \ldots, z_{\sigma_r}, \operatorname{Re} z_{\sigma_{r+1}}, \ldots, \operatorname{Re} z_{\sigma_{r+s}}, \operatorname{Im} z_{\sigma_{r+1}}, \ldots, \operatorname{Im} z_{\sigma_{r+s}}\right).$$

3.5 Quadratic number fields

Proposition 3.5.1: The quadratic number fields K are precisely the splitting fields of the poiynomials $X^2 - d$ for all squarefree integers $d \in \mathbb{Z} \setminus \{0, 1\}$. and this d is uniquely determined by K.

Proof: $[K/\mathbb{Q}] = 2 \Rightarrow$ Take $\xi \in K \setminus \mathbb{Q} \Rightarrow \xi^2 + a\xi + b = 0$ with $a, b \in \mathbb{Q}$.

$\Rightarrow \left(\xi + \frac{a}{2}\right)^2 = \frac{a^2}{4} - b$. Replace ξ by $\xi + \frac{a}{2} \Rightarrow \xi^2 = \frac{d}{c} e^2$ for $e, c, d \in \mathbb{Z} \setminus \{0\}$ coprime.

$\Rightarrow \left(\frac{c\xi}{e}\right)^2 = cd \in \mathbb{Z} \setminus \{0\}$. Replace ξ by $\frac{c\xi}{e} \Rightarrow \xi^2 = d \in \mathbb{Z} \setminus \{0, 1\}$ squarefree.

Conversely for any $d \in \mathbb{Z} \setminus \{0, 1\}$ squarefree we have $[\mathbb{Q}(\sqrt{d})/\mathbb{Q}] = 2$.

Finally: $\mathbb{Q}(\sqrt{d}) \ni \sqrt{d'} \iff \frac{d'}{d} \in (\mathbb{Q}^\times)^2 \iff d = d'$ if d, d' are squarefree.

qed.

Convention 3.5.2: For any positive integer d we let $\sqrt{d}$ be the positive real square root of d. For any negative integer d we uncanonically *choose* a square root $\sqrt{d}$ in $i\mathbb{R}$.

Proposition 3.5.2: For d as above and $K = \mathbb{Q}(\sqrt{d})$ we have

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2,3 \bmod (4), \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \bmod (4) \end{cases}$$

$d \equiv 0$ (4) does not occur!

and

$$d_K = \begin{cases} 4d & \text{if } d \equiv 2,3 \bmod (4), \\ d & \text{if } d \equiv 1 \bmod (4) \end{cases}$$

square free

Proof: $\sqrt{d}$ integral over $\mathbb{Z}$ as zero of $X^2 - d \in \mathbb{Z}[X]$. So $\mathbb{Z}[\sqrt{d}] \subset \mathcal{O}_K$.

$\operatorname{disc}(\mathbb{Z}[\sqrt{d}]) = \operatorname{disc}(1, \sqrt{d}) = (\text{discriminant of } X^2 - d) = (\sqrt{d} - (-\sqrt{d}))^2 = (2\sqrt{d})^2 = 4d$.

$\overset{\|}{[\mathcal{O}_K : \mathbb{Z}[\sqrt{d}]]^2 \cdot \operatorname{disc}(\mathcal{O}_K)} \Rightarrow [\mathcal{O}_K : \mathbb{Z}[\sqrt{d}]] \leq 2$. So $\mathcal{O}_K \subseteq \frac{1}{2}(\mathbb{Z} \oplus \mathbb{Z} \cdot \sqrt{d})$.

Check: $\frac{1}{2}, \frac{\sqrt{d}}{2}, \frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$?

$N_{K/\mathbb{Q}}(\frac{1}{2}) = \frac{1}{4} \notin \mathbb{Z}$

$N_{K/\mathbb{Q}}(\frac{\sqrt{d}}{2}) = \frac{\sqrt{d}}{2} \cdot \frac{-\sqrt{d}}{2} = -\frac{d}{4} \notin \mathbb{Z}$

$N_{K/\mathbb{Q}}(\frac{1+\sqrt{d}}{2}) = \frac{1+\sqrt{d}}{2} \cdot \frac{1-\sqrt{d}}{2} = \frac{1-d}{4} \in \mathbb{Z}$ iff $d \equiv 1$ (4).

$\operatorname{Tr}_{K/\mathbb{Q}}(\frac{1+\sqrt{d}}{2}) = \frac{1+\sqrt{d}}{2} + \frac{1-\sqrt{d}}{2} = 1 \in \mathbb{Z}$. $\Rightarrow \frac{1+\sqrt{d}}{2}$ is a root of $X^2 - X + \frac{1-d}{4}$.

Corollary 3.5.4: The integer d is uniquely determined by K, namely as the squarefree part of d_K.

Remark 3.5.5: The possible discriminants of quadratic number fields are sometimes called *fundamental discriminants.* As the discriminant is somewhat more canonically associated to K than the number d, some authors prefer to write $K = \mathbb{Q}(\sqrt{d_K})$.