Algebraic Number Theory

Lecture 7, 19th November 2021

Last lecture: $\alpha_1, \dots, \alpha_n$ basis of L/K

$\sigma_i : L \to \overline{K}$ $\quad i = 1, \dots, n$

embeddings of L in $\overline{K}$.

- <u>discriminant:</u> $d(\alpha_1, \dots, \alpha_n) := \det(\sigma_i(\alpha_j))^2_{1 \le i,j \le n}$

$$\| $$

$$\det(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)) \in K$$

finite extension

$$\begin{array}{ccccl} \mathrm{Frac}(A) =: K & \subset & L & & \text{(e.g number field)} \\ \text{(e.g } \mathbb{Q}) \quad \cup & & \cup & & \\ A & \subset & B = \overline{A} & & \text{integral closure of } A \text{ in } L \\ & & & & \text{(e.g. } \mathcal{O}_L) \end{array}$$

integrally closed ring (e.g. $\mathbb{Z}$)

- $\omega_1, \dots, \omega_n \in B$ <u>integral basis</u> of B over A:

$$b = a_1 \omega_1 + \dots + a_n \omega_n$$

$\forall b \in B \; \exists! \; a_1, \dots, a_n \in A$

Prop 3.15: fin. gen. B-submodule $M \neq 0$ of L has integral basis over A and $n = [L:K]$

Corollary: K number field: Every fin. gen. $\mathcal{O}_K$-module $\mathfrak{a}$ has $\mathbb{Z}$-basis.

$$\mathfrak{a} = \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n$$

$$d(\mathfrak{a}) = d(\omega_1, \dots, \omega_n), \qquad d_K = d(\mathcal{O}_K).$$

$\mathbb{Z}$

discriminant of K

Proposition 3.19 If $\mathfrak{a} \subset \mathfrak{a}'$ are two nonzero fin. gen. $\mathcal{O}_K$-submodules of K, then the index $[\mathfrak{a}' : \mathfrak{a}]$ is finite and satisfies

$$d(\mathfrak{a}) = [\mathfrak{a}' : \mathfrak{a}]\, d(\mathfrak{a}').$$

Proof: Use Structure theorem for fin. gen. modules over PID

§ 4 Dedekind domains

Proposition 4.1 K: alg. Number field

In $\mathcal{O}_K$ every non-unit $\alpha \neq 0$ can be factored into a product of irreducible elements.

Proof:

Since if α is not irreducible we can write

$\alpha = \beta\gamma$ with non-units $\beta, \gamma \in \mathcal{O}_K$.

Then we have

$$\mathbb{Z} \ni N_{K/\mathbb{Q}}(\alpha) = \underbrace{N_{K/\mathbb{Q}}(\beta)}_{\in \mathbb{Z}} \cdot \underbrace{N_{K/\mathbb{Q}}(\gamma)}_{\in \mathbb{Z}}.$$

Since $N_{K/\mathbb{Q}}(\beta), N_{K/\mathbb{Q}}(\gamma) \notin \{\pm 1\}$ we get

$$1 < |N_{K/\mathbb{Q}}(\beta)|, \ |N_{K/\mathbb{Q}}(\gamma)| < |N_{K/\mathbb{Q}}(\alpha)|.$$

The statement then follows inductively. $\square$

As we have seen this decomposition is not unique. But we will see that the decomposition into prime ideals is unique for $\mathcal{O}_K$ and more generally Dedekind domains.

Definition 4.2 A domain R is called a <u>Dedekind domain</u> if

In alg. geometry

i) it is noetherian, ~ coordinate ring affine variety

ii) it is integrally closed, ~ nonsingular

iii) every non-zero prime ideal in R is maximal. (Krull dimension 1) ~ curve

Coordinate rings of nonsingular curves are Dedekind domains

Proposition 4.3 The ring of integers $\mathcal{O}_K$ of an alg. number field K is a Dedekind domain.

Proof: i) $\mathcal{O}_K$ is noetherian since it is a finitely generated $\mathbb{Z}$-module.
($\mathbb{Z}$ noetherian $\overset{\text{HW2 Ex6}}{\Longrightarrow}$ $\mathcal{O}_K$ noetherian)

ii) $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K, i.e. integrally closed by Corollary 2.8.

iii) Let $\mathfrak{p} \neq (0)$ be a prime ideal in $\mathcal{O}_K$.
Then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$.
This ideal is non-zero, since for a non-zero $y \in \mathfrak{p}$ consider

$$y^n + a_{n-1} y^{n-1} + \dots + a_0 = 0 \qquad a_j \in \mathbb{Z}$$

of minimal degree. We see $a_0 \neq 0$ (otherwise this n would not be minimal) and $a_0 \in \mathbb{Z} \cap \mathfrak{p} \Rightarrow \mathfrak{p} \cap \mathbb{Z} \neq (0)$.

$\Rightarrow$ There exist a prime number p with $\mathfrak{p} \cap \mathbb{Z} = (p)$.

Want to show: $\underbrace{\mathcal{O}_K/\mathfrak{p}}_{\bar{\mathcal{O}}:=}$ is a field.

$\overline{\mathcal{O}}$ has $\overline{K} = \mathbb{Z}/p\mathbb{Z}$ as a subring and all $x \in \overline{\mathcal{O}} \setminus \{0\}$ are algebraic over $\overline{K}$, i.e.

$$x^n + \beta_{n-1} x^{n-1} + \dots + \beta_0 = 0$$

for some $\beta_j \in \overline{K}$. Assuming n is minimal we get $\beta_0 \neq 0$ and therefore

$$x \cdot \underbrace{\left((-\beta_0)^{-1} (x^{n-1} + \dots + \beta_1) \right)}_{x^{-1}} = 1$$

$\Rightarrow$ x has an inverse $\Rightarrow$ $\overline{\mathcal{O}}$ is a field

$\Rightarrow$ $\mathfrak{p}$ is maximal. $\square$

Theorem 4.4 Every ideal $\mathfrak{a} \neq (1)$, $\neq (0)$ of a Dedekind domain $\mathcal{O}$ admits a factorization

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

into nonzero prime ideals $\mathfrak{p}_i$ of $\mathcal{O}$, which is unique up to the order of the factors.

To prove this we will need two Lemmas.

Let $\mathcal{O}$ be a Dedekind domain.

<u>Lemma 4.5</u> For every ideal $\mathfrak{a} \neq 0$ of $\mathcal{O}$ there exist nonzero prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ with

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a} . \quad (\star)$$

Proof: Let $\mathcal{M}$ be the set of ideals $\mathfrak{a} \neq 0$ of $\mathcal{O}$ for which there exist no $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ with $(\star)$.

$\mathcal{O}$ is noetherian and if $\mathcal{M} \neq \emptyset$ then there exist a maximal element $\mathfrak{a}$ in $\mathcal{M}$ with respect to the inclusion. This $\mathfrak{a}$ can not be a prime ideal (otherwise $(\star)$ would hold), i.e. there are $b_1, b_2 \in \mathcal{O}$ with $b_1 b_2 \in \mathfrak{a}$ but $b_1 \notin \mathfrak{a}$ and $b_2 \notin \mathfrak{a}$.

Setting $\mathfrak{a}_1 = (b_1) + \mathfrak{a}$, $\mathfrak{a}_2 = (b_2) + \mathfrak{a}$ we have

$$\mathfrak{a} \subsetneq \mathfrak{a}_1 \qquad \mathfrak{a}_1 \mathfrak{a}_2 \subseteq \mathfrak{a} .$$
$$\mathfrak{a} \subsetneq \mathfrak{a}_2$$

Since $\mathfrak{a}$ is an maximal element in $\mathcal{M}$ we get $\mathfrak{a}_1, \mathfrak{a}_2 \notin \mathcal{M}$

$\Rightarrow$ $\exists$ prime ideals $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}_1$
$\mathfrak{p}_1' \cdots \mathfrak{p}_{r'}' \subseteq \mathfrak{a}_2$

$$\Rightarrow \quad \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{p}_1' \cdots \mathfrak{p}_{r'}' \subseteq \mathfrak{a}_1 \mathfrak{a}_1 \subseteq \mathfrak{a}. \quad ↯$$

$$\Rightarrow \quad \mathcal{M} = \emptyset. \qquad \square$$

Lemma 4.6 Let $\mathfrak{p} \subset \mathcal{O}$ be a prime ideal and set

$$(\mathcal{O} \subseteq)\ \mathfrak{p}^{-1} = \{ x \in K \mid x\mathfrak{p} \subseteq \mathcal{O} \}.$$

Then we have $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$ for any ideal $\mathfrak{a} \neq 0$.

$$\mathfrak{a}\mathfrak{p}^{-1} = \{ \textstyle\sum a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1} \}$$

<u>Proof:</u> • If $\mathfrak{p} = (0)$, then $\mathfrak{p}^{-1} = K \Rightarrow \mathfrak{a}K = K \neq \mathfrak{a}$.

• Let $\mathfrak{p} \neq (0)$ and $a \in \mathfrak{p}$ with $a \neq 0$.

Lemma 4.5

$\Longrightarrow \quad \exists \; \mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$

Choose r as small as possible.

Then for one j we have $\mathfrak{p}_j \subseteq \mathfrak{p}$

(otherwise $\exists \; a_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ for all $i = 1, \dots, r$

$\Longrightarrow \quad a_1 \cdot \ldots \cdot a_r \in \mathfrak{p}$ $\lightning$)

Assume $\mathfrak{p}_1 \subseteq \mathfrak{p}$ then we get $\mathfrak{p} = \mathfrak{p}_1$

since $\mathfrak{p}_1$ is maximal.

Since r is minimal we have $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (a)$

choose $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (a)$

$\Longrightarrow \quad a^{-1} b \notin \mathcal{O}.$

On the other hand $b\mathfrak{p} \subseteq (a)$

$\Longrightarrow \quad a^{-1} b \mathfrak{p} \subseteq \mathcal{O} \Rightarrow a^{-1} b \in \mathfrak{p}^{-1}.$

$\mathcal{O} \neq \mathfrak{p}^{-1}.$

- Now let $\mathfrak{a} \subset \mathcal{O}$ be an ideal.

$\mathcal{O}$ noetherian $\Rightarrow$ $\mathfrak{a}$ fin. gen.

Let $\{\alpha_1, \dots, \alpha_n\}$ be generators of $\mathfrak{a}$.

Suppose that $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Then for all $x \in \mathfrak{p}^{-1}$ we have

$$x\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j \qquad a_{ij} \in \mathcal{O}$$

i.e $A\begin{pmatrix}\alpha_1 \\ \vdots \\ \alpha_n\end{pmatrix} = 0$ with $A = xE - (a_{ij})$

$\Rightarrow \det(A) = 0 \Rightarrow x$ integral over $\mathcal{O}$.

$\Rightarrow x \in \mathcal{O} \Rightarrow \mathfrak{p}^{-1} = \mathcal{O}$ ↯

$\Rightarrow \mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$. $\square$

Proof of Theorem 4.4:

Existence: $\mathcal{M}$ = set of ideals $\neq (0), (1)$ which do not admit a prime ideal decomposition.

If $\mathcal{M} \neq \emptyset$ then $\mathcal{M}$ has a maximal element $\mathfrak{a} \subset \mathcal{M}$. (since $\mathcal{O}$ is noetherian)

Since $\mathfrak{a}$ is not prime there exist a maximal ideal $\mathfrak{p}$ with $\mathfrak{a} \subsetneq \mathfrak{p}$.

Lemma 4.6 $\Rightarrow$ $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1}$, $\mathfrak{p} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$

Since $\mathfrak{p}$ is maximal we get $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$ and with $\mathcal{O} \subseteq \mathfrak{p}^{-1}$ we get

$$\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}.$$

We have $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathcal{O}$, otherwise $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$.

Since $\mathfrak{a}$ is maximal in $\mathcal{M}$ with respect to the inclusion we see that $\mathfrak{a}\mathfrak{p}^{-1} \notin M$, i.e

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

$$\Rightarrow \quad \mathfrak{a} = \mathfrak{a}\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{p} \Rightarrow \mathcal{M} = \emptyset.$$

Uniqueness:

Let $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s$

two factorizations of $\mathfrak{a}$ into prime ideals.

For $\mathfrak{p}$ prime we have: $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$

Notation $\Updownarrow$

$$\mathfrak{p} \mid \mathfrak{a}\mathfrak{b} \Rightarrow \mathfrak{p} \mid \mathfrak{a} \text{ or } \mathfrak{p} \mid \mathfrak{b}$$

Now we get that $\mathfrak{p}_1$ divides one of the $\mathfrak{q}_j$, say $\mathfrak{p}_1 \mid \mathfrak{q}_1$, i.e. $\mathfrak{q}_1 \subseteq \mathfrak{p}_1$. Since $\mathfrak{q}_1$ is maximal we get $\mathfrak{q}_1 = \mathfrak{p}_1$.

Multiplying with $\mathfrak{p}_1^{-1}$ gives $(\mathfrak{p}_1\mathfrak{p}_1^{-1} = \mathcal{O})$

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s .$$

Continuing this shows $r = s$ and $\mathfrak{p}_i = \mathfrak{q}_i$ after possible renumbering. $\square$

Therefore any ideal $\mathfrak{a} \neq (0)$ of $\mathcal{O}$ can be (uniquely up to reordering) written as

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdots \mathfrak{p}_r^{\nu_r}$$

with $r_1, \dots, r_r \geq 1$ and pairwise distinct prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$.

$\mathcal{O}$: Dedekind domain, $K = \mathrm{Frac}(\mathcal{O})$

Definition 4.7 A <u>fractional ideal</u> of K is a finitely generated $\mathcal{O}$-submodule $\mathfrak{a} \neq 0$ of K.