

Math 225A Notes

Sarah Mantell

October 7, 2022

Algebraic Number Theory

1

Definition 1.0.1 A number field is a finite field extension over \mathbb{Q} .

Definition 1.0.2 Let K be a number field. An algebraic number $a \in K$ is called integral or an algebraic integer of K if $f(a) = 0$ for some monic polynomial f with coefficients in \mathbb{Z} . Denote the set of algebraic integers in K by \mathbb{O}_K .

Proposition 1.0.3 Let K be a number field. Then \mathbb{O}_K is a ring and $K = \text{Frac}(\mathbb{O}_K)$.

Proposition 1.0.4 The ring \mathbb{O}_K is Noetherian, integrally closed, and every nonzero prime ideal of \mathbb{O}_K is maximal.

Notice that the results presented in the proposition above imply that \mathbb{O}_K is a Dedekind domain, using one of the many equivalent definitions of a Dedekind domain.

Theorem 1.0.5 (Unique Factorization of Ideals) Every nonzero ideal $\mathfrak{a} \not\subseteq \mathbb{O}_K$ can be uniquely written as

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}$$

where $m \geq 1$, $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ are distinct nonzero prime ideals of \mathbb{O}_K , and $r_1, \dots, r_m \in \mathbb{N}$.

Definition 1.0.6 Suppose that $\mathbb{Q} \subseteq K \subseteq L$ is an extension of fields. Let $a \in L$ and view L as a K -vector space to consider the linear transformation

$$T_a : L \rightarrow$$

$$x \mapsto ax.$$

Define the trace and norm for a as

$$\text{Tr}_{L/K}(a) = \text{Tr}(T_a) \in K$$

and

$$\text{Nm}_{L/K}(a) = \det(T_a) \in K.$$

The notes here about algebraic number theory are very brief – the recommended texts for a more in depth reading are:

- Algebraic Number Theory Chapters I, II (Neukirch)
- Algebraic Number Theory Notes (Milne)

Theorem 1.0.5 is actually true for any Dedekind domain, but we just focus on this specific case here.

With trace and norm defined as in Definition 1.0.6, we obtain a bi- K -linear pairing:

$$\langle, \rangle_{L/K} : L \times K \rightarrow K$$

given by

$$\langle a, \rangle_{L/K} = \text{Tr}_{L/K}(ab).$$

Definition 1.0.7 Let $\alpha_1, \dots, \alpha_n$ be a basis of L over K . The discriminant of $\alpha_1, \dots, \alpha_n$ is defined as

$$D(\alpha_1, \dots, \alpha_n) = \det \left(\left(\langle \alpha_i, \alpha_j \rangle \right)_{1 \leq i, j \leq n} \right).$$

The discriminant of L/K is denoted by $D_{L/K}$ and is the ideal of \mathcal{O}_K generated by

$$\{D(\alpha_1, \dots, \alpha_n) : \alpha_1, \dots, \alpha_n \text{ is a basis of } L/K \text{ contained in } \mathcal{O}_L\}.$$

For K/\mathbb{Q} , $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ and therefore is a PID. So, \mathcal{O}_K is a free \mathbb{Z} -module of rank $n = [K : \mathbb{Q}]$. For any \mathbb{Z} -basis $\alpha_1, \dots, \alpha_n$ of \mathcal{O}_K ,

$$D_{K/\mathbb{Q}} = (D(\alpha_1, \dots, \alpha_n)).$$

The matrix

$$\left(\langle \alpha_i, \alpha_j \rangle \right)_{1 \leq i, j \leq n}$$

is an $n \times n$ matrix, with entries in K .