Math 225A Notes

Sarah Mantell

October 11, 2022

1 Algebraic Number Theory

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* $\mathcal{O}_K$*.*

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)

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

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

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

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

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

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

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

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*

$$T_a : L \longrightarrow L$$

$$x \longmapsto ax.$$

Define the trace and norm for a *as*

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

and

$$Nm_{L/K}(a) = det(T_a) \in K.$$

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

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

given by

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

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

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

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

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

The matrix

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

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

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 $\alpha_1, \ldots, \alpha_n$ of $\mathcal{O}_K$,

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

Definition 1.0.8 *Let L/K be an extension of number fields, $\mathfrak{P} \subseteq \mathcal{O}_L$ a nonzero prime ideal, and define $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K \subseteq \mathcal{O}_K$. Write the prime factorization of $\mathfrak{p}\mathcal{O}_L$ as*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_m^{e_m}$$

where $\mathfrak{P}_1 = \mathfrak{P}$. The ramification index of $\mathfrak{P}$ over $\mathfrak{p}$, denoted by $e(\mathfrak{P}/\mathfrak{p})$, is defined to be e_1 (as given in the prime factorization). The residue class degree, or the intertia degree, of $\mathfrak{P}$ of $\mathfrak{p}$, denoted by $e(\mathfrak{P}/\mathfrak{p})$, is defined to be $[\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$.

Definition 1.0.9 *Let L/K be an extension of number fields and $\mathfrak{p} \subseteq \mathcal{O}_K$ a nonzero prime ideal. We say $\mathfrak{p}$ is ramified in L or L/K is ramified at $\mathfrak{p}$ if $e(\mathfrak{P}/\mathfrak{p}) > 1$ for some $\mathfrak{P} \subseteq \mathcal{O}_L$ satisfying $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. We say $\mathfrak{p}$ is unramified in L or L/K is unramified at $\mathfrak{p}$ if $e(\mathfrak{P}/\mathfrak{p}) = 1$ for every $\mathfrak{P} \subseteq \mathcal{O}_L$ where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$.*

Definition 1.0.10 *Let L/K be an extension of number fields and $\mathfrak{p} \subseteq \mathcal{O}_K$ a nonzero prime ideal. We say $\mathfrak{p}$ splits or splits completely in L if $e(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}) = 1$ for every $\mathfrak{P} \subseteq \mathcal{O}_L$ with $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$.*

Definition 1.0.11 *Let L/K be an extension of number fields and $\mathfrak{p} \subseteq \mathcal{O}_K$ a nonzero prime ideal. We say that $\mathfrak{p}$ is inert in L if $\mathfrak{p}\mathcal{O}_L$ is a prime ideal of $\mathcal{O}_L$.*

From these definitions, one can derive the following identity: if $\mathfrak{p}\mathcal{O}_L = \wp_1^{e_1} \cdots \wp_m^{e_m}$ then

$$[L : K] = \sum_{j=1}^{m} e(\wp_j/\mathfrak{p}_j) f(p_j/\mathfrak{p}_j).$$