Math 225A Notes

Sarah Mantell

October 12, 2022

1 Algebraic Number Theory

Definition 1.0.1 (Number field): A number field is a finite field extension over $\mathbb{Q}$.

Definition 1.0.2 (Algebraic integer): 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 $K = \mathrm{Frac}(\mathcal{O}_K)$.

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 $\mathfrak{a} \subsetneq \mathcal{O}_K$ 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 1.0.5 is actually true for any Dedekind domain, but we just focus on this specific case here.

Definition 1.0.6 (Trace, Norm): 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

$$T_a : L \to L$$

$$x \mapsto ax.$$

Define the trace and norm for a as

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

and

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

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

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

given by

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

Definition 1.0.7 (Discriminant): 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 $\mathcal{O}_K$,

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