Math 225A Notes

Sarah Mantell

October 13, 2022

Algebraic Number Theory 1

1.1 General Definitions

Definition 1.1.1 (Number field): A number field is a finite field extension over $\mathbb{Q}$.

Definition 1.1.2 (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 1.1.3: Let K be a number field. Then $\mathcal{O}_K$ is a ring and $K = \mathrm{Frac}(\mathcal{O}_K)$.

Proposition 1.1.4: 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 1.1.5 (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 1.1.6 (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

$$T_a : L \longrightarrow L$$

$$x \mapsto ax.$$

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 **??**, we obtain a bi-K-linear pairing:

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

given by

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

Definition 1.1.7: Let $\alpha_1, \ldots, \alpha_n$ be a basis of L over K. The discriminant of $\alpha_1, \ldots, \alpha_n$ is defined as

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

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

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

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 1.1.8: 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 1.1.9: 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 1.1.10: 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 1.1.11: 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 $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_m^{e_m}$ then

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

Proposition 1.1.12: Let K be a number field. Every fractional ideal $\mathfrak{a}$ of K can be written uniquely in the form

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{r_{\mathfrak{p}}}$$

where the product is taken over all the nonzero prime ideals of $\mathcal{O}_K$, each $r_{\mathfrak{p}} \in \mathbb{Z}$, and almost every $r_{\mathfrak{p}}$ is zero.

Remark 1 With these definitions, I_K is the free abelian group on the set of nonzero prime ideals of $\mathcal{O}_K$.

Define a subgroup of I_K by

$$P_K = \left\{(a) = a\mathcal{O}_K : a \in K^{\times}\right\}.$$

Definition 1.1.13 (Ideal class group, Class group): The ideal class group or class group of K is defined as

$$\mathrm{Cl}(K) = I_K / P_K.$$

Theorem 1.1.14: For any number field K, the class group $\mathrm{Cl}(K)$ is finite.

Definition 1.1.15 (Class number): The class number of a number field K is the order of the class group $\mathrm{Cl}(K)$.

The proof that the class number of a given number field is indeed finite uses Minkowski Theory.

For a number field K, let r_k denote the number of real embeddings of K into $\mathbb{R}$ and s_k denote the number of pairs of complex embeddings of K into $\mathbb{C}$. Here we are assuming that s_k is counting the pairs of embeddings that are not strictly contained in $\mathbb{R}$. Note that the complex embeddings occur in pairs through complex conjugation.

Theorem 1.1.16 (Dirichlet's Unit Theorem): Suppose that K is a number field and $\mu(K)$ is the finite group of roots of unity that are contained in K. Then,

$$\mathcal{O}_K^\times \cong \mathbb{Z}^{r_k + s_k - 1} \times \mu(K).$$

Definition 1.1.17 (Decomposition group): Suppose that L/K is a Galois extension of number fields, $\wp \subseteq L$ is a prime ideal, and $\mathfrak{p} = \wp \cap \mathcal{O}_K$. The decomposition group of $\wp$ is the set

$$G_\wp = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\wp) = \wp\}.$$

Need to check the assumptions here – where is $\wp$ living? Nonzero?

Definition 1.1.18 (Inertia group): Let $\kappa = \mathcal{O}_K/\mathfrak{p}$ and $\lambda = \mathcal{O}_L/\wp$. The kernel of the map

$$G_\wp \longrightarrow \mathrm{Aut}(\lambda/\kappa)$$

is the inertia group of $\wp$ and is denoted by $I_\wp$.

1.2 Valuations and Absolute Values

In general, assume hereafter that p denotes some prime number.

Definition 1.2.1 (p-adic absolute value, p-adic norm): The p-adic absolute value or norm of $\mathbb{Q}$

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R}$$

is defined by

$$\left|p^m \frac{a}{b}\right|_p = p^{-m}$$

where both a and b are coprime to p. Set $|0|_p = 0$.

Proposition 1.2.2: The p-adic norm is indeed a norm. That is:

1. $|a|_p > 0$ for all $a \in \mathbb{Q}^\times$
2. $|ab|_p = |a|_p|b|_p$
3. $|a+b|_p \leq |a|_p + |b|_p$

The p-adic norm actually satsifies a stronger version of the triangle inequality: $|a+b|_p \leq \max\{|a|_p, |b|_p\}$. Since we have now equipped $\mathbb{Q}$ with a norm, it can be viewed as a topological space and thus there is a notion of convergence and Cauchy sequences. In particular, we are interested in studying the completion of $\mathbb{Q}$ with respect to a given p-adic norm.

Definition 1.2.3 (p-adic numbers): Let $\mathbb{Q}_p$ be the completion of $\mathbb{Q}$ with respect to the p-adic norm. The elements of $\mathbb{Q}_p$ are called the p-adic numbers.

Using properties of limits and the fact that every element of $\mathbb{Q}_p$ can be represented as the limit of a sequence of points in $\mathbb{Q}$, the addition and multiplication of $\mathbb{Q}$ can be naturally extended to $\mathbb{Q}_p$. Likewise, the norm $|\cdot|_p$ can be extended to a norm on $\mathbb{Q}_p$. With these operations, $\mathbb{Q}_p$ is a field that contains $\mathbb{Q}$ as a subfield.