Math 225A Notes

Sarah Mantell

October 14, 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 $\mathfrak{a} \nsubseteq \mathcal{O}_K$ 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 (Ramification index, Residue class degree/Intertia degree): Let L/K be an extension of number fields, $\wp \subseteq \mathcal{O}_L$ a nonzero prime ideal, and define $\mathfrak{p} = \wp \cap \mathcal{O}_K \subseteq \mathcal{O}_K$. Write the prime factorization of $\mathfrak{p}\mathcal{O}_L$ as

$$\mathfrak{p}\mathcal{O}_L = \wp_1^{e_1} \cdots \wp_m^{e_m}$$

where $\wp_1 = \wp$. The ramification index of $\wp$ over $\mathfrak{p}$, denoted by $e(\wp/\mathfrak{p})$, is defined to be e_1 (as given in the prime factorization). The residue class degree, or the intertia degree, of $\wp$ of $\mathfrak{p}$, denoted by $e(\wp/\mathfrak{p})$, is defined to be $[\mathcal{O}_L/\wp : \mathcal{O}_K/\mathfrak{p}]$.

Definition 1.1.9 (Ramified): 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 $e(\wp/\mathfrak{p}) > 1$ for some $\wp \subseteq \mathcal{O}_L$ satisfying $\mathfrak{p} = \wp \cap \mathcal{O}_K$. We say $\mathfrak{p}$ is unramified in L or L/K is unramified at $\mathfrak{p}$ if $e(\wp/\mathfrak{p}) = 1$ for every $\wp \subseteq \mathcal{O}_L$ where $\mathfrak{p} = \wp \cap \mathcal{O}_K$.

Definition 1.1.10 (Splits, Splits completely): 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 $e(\wp/\mathfrak{p}) = f(\wp/\mathfrak{p}) = 1$ for every $\wp \subseteq \mathcal{O}_L$ with $\wp \cap \mathcal{O}_K = \mathfrak{p}$.

Definition 1.1.11 (Inert): 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

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

Theorem 1.1.12: The extension L/K is unramified at $\mathfrak{p} \subseteq \mathcal{O}_K$ if and only if $\mathfrak{p}$ does not divide $D_{L/K}$. That is, $D_{L/K} \nsubseteq \mathfrak{p}$ if and only if $\mathfrak{p}$ and $D_{L/K}$ are coprime ($\mathfrak{p} + D_{L/K} = \mathcal{O}_K$).

Theorem 1.1.13 (Minkowski): $\mathbb{Q}$ has non nontrivial extension that is unramified at all primes. Equivalently, every $D_{K/\mathbb{Q}} \neq \pm 1$.

Note that Theorem **??** is not true for a general number field K:

Example 1: Let $K = \mathbb{Q}(\sqrt{-5})$ and $L = K(\sqrt{-1})$ so that L/K is an extension of number fields. Then, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ and $L = K(\sqrt{5})$. To see that L/K is unramified at all primes, we apply Theorem **??** and show that $D_{L/K} = \mathcal{O}_K$.

The remainder of this example is just some computations regarding the discriminant and two diferent K-bases of L.

Definition 1.1.14 (Fractional ideal): A fractional ideal of K is a nonzero finitely generated $\mathcal{O}_K$-submodule of K.

One can define a multiplication on the collection of fractional ideals of K: if $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are all fractional ideals of K, then the product is the $\mathcal{O}_K$-submodule of K generated by $\{a_1 \cdots a_n | a_j \in \mathfrak{a}_j\}$.

Proposition 1.1.15: The collection of fractional ideals of K forms an abelian group under the multiplication of fractional ideals. With this structure, the identity is $\mathcal{O}_K$ and the inverse of $\mathfrak{a}$ is $\mathfrak{a}^{-1} = \{x \in K | x\mathfrak{a} \subseteq \mathcal{O}_K\}$.

Proposition 1.1.16: 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 1.1.17 (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 1.1.18: For any number field K, the class group $\mathrm{Cl}(K)$ is finite.

Definition 1.1.19 (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 1.1.20 (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 1.1.21 (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 1.1.22 (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 $\mathbb{Q}$

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

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 satisfies 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.

Definition 1.2.4 (p-adic integers): Define the ring of p-adic integers to be the subset of $\mathbb{Q}_p$ given by

$$\mathbb{Z}_p = \left\{ a \in \mathbb{Q}_p : |a|_p \leq 1 \right\}.$$

One can easily see that the set of units is $\mathbb{Z}_p^\times = \{a \in \mathbb{Q}_p : |a|_p = 1\}$.

Example 2: The polynomial $x^{p-1} - 1$ is solvable of $\mathbb{Q}_p$.

Definition 1.2.5 (p-adic valuation): The p-adic valuation of $\mathbb{Q}$ is given by

$$v_p : \mathbb{Q} \longrightarrow \mathbb{R} \cup \{\infty\}$$

where $v_p(p^m \frac{a}{b}) = m$ and both a and b are coprime to p. The p-adic valuation can be extended to $\mathbb{Q}_p$ by letting $v_p(p^m a) = m$ where $a \in \mathbb{Z}_p^\times$.

Proposition 1.2.6: The p-adic valuation satisfies the following:

1. $v_p(a) = \infty$ if and only if $a = 0$
2. $v_p(ab) = v_p(a) + v_p(b)$
3. $v_p(a+b) = \min\{v_p(a), v_p(b)\}$

Furthermore, the p-adic valuation and p-adic absolute value have the following relation:

$$|a|_p = p^{-v_p(a)} \quad v_p(a) = -\log_p |a|_p.$$

Definition 1.2.7 (Absolute value, Nonarchimedean): An absolute value, or multiplicative valuation, of a field K is a function $|\cdot| : K \longrightarrow \mathbb{R}_{\geq 0}$ such that

(1) $|x| = 0$ if and only if $x = 0$
(2) $|xy| = |x| \cdot |y|$
(3) $|x+y| \leq |x| + |y|$

If instead of **??**, the stronger condition

$$|x+y| \leq \max\{|x|, |y|\}$$

holds, then $|\cdot|$ is a nonarchimedean absolute value.

Definition 1.2.8 (Equivalent): Two absolute values are equivalent if they induce the same topology.

Using topological properties, one can show that two norms $|\cdot|_1, |\cdot|_2$ on K are equivalent if and only if there exists $s \in \mathbb{R}_{>0}$ such that $|x|_1 = |x|_2^s$ for all $x \in K$. In particular, if there exists $x \in K$ where $|x|_1 \geq 1$ and $|x|_2 < 1$ the two norms are *not* equivalent.

Definition 1.2.9 (Additive valuation, Valuation): An additive valuation on a field K is a function $v : K \longrightarrow \mathbb{R} \cup \{\infty\}$ such that

(1) $v(x) = \infty$ if and only if $x = 0$
(2) $v(xy) = v(x) + v(y)$
(3) $v(x+y) \geq \min\{v(x), v(y)\}$.

With these definitions, the collection of valuations and collection of nonarchimedean absolute values are related by the exponential and logarithmic functions. With this relationships, we can define the following:

Definition 1.2.10 (Equivalent valuations): Two valuations are equivalent if their corresponding absolute values are equivalent (see Definition **??**).

Proposition 1.2.11: Every absolute value of $\mathbb{Q}$ is either the usual Euclidean absolute value or is equivalent to $|\cdot|_p$ for some prime p.

From hereafter, $|\cdot|_\infty$ is used to denote the Euclidean absolute value.

Definition 1.2.12 (Residue class field, Valuation ring): Let K be a field with valuation v. The local ring [1]

$$\mathcal{O} = \{x \in K : v(x) \geq 0\}$$

is the valuation ring for K. The unique maximal ideal of $\mathcal{O}$ is

$$\mathfrak{p}\,\{x \in K : v(x) > 0\}$$

the units are

$$\mathcal{O}^\times = \{x \in K : v(x) = 0\}$$

The field $\mathcal{O}/\mathfrak{p}$ is the residue class field of $\mathcal{O}$.

Definition 1.2.13 (Discrete valuation): A valuation v on K is called discrete if $v(K^\times) = s\mathbb{Z}$ for some $s \in \mathbb{R}_{>0}$.

Definition 1.2.14 (Uniformizer): Assume that v is a discrete valuation with $v(K^\times) = s\mathbb{Z}$. An element $\varpi \in K$ is a uniformizer if $v(\varpi) = s$.

Alternatively, we can think of the uniformizer as follows: ϖ is a uniformizer if and only if ϖ generates the unique maximal ideal of the valuation ring.

If v is a discrete valuation, then it can be normalized to a valuation $v'(x) = s^{-1}v(x)$. From this definition, v and v' are equivalent and $v'(K^\times) = \mathbb{Z}$. Once normalized, an element ϖ is a uniformizer if and only if $v'(\varpi) = 1$.

Proposition 1.2.15: Let K be a field with a discrete valuation. Then, the corresponding valuation ring is a discrete valuation ring [2].

Completions

Now that a field K can be equipped with a norm, we can construct a completion of K with respect to any p-adic norm. The definition of completeness is the usual:

Definition 1.2.16 (Complete): The pair $(K, |\cdot|)$ is complete if every Cauchy sequence converges in K (with respect to the $|\cdot|$ norm.)

Given any $(K, |\cdot|)$, we can always find a completion $\hat{K}$ and naturally extend $|\cdot|$ to $\hat{K}$. »»»> 2a2dbcd (More notes.)