BASICS OF NUMBER FIELDS

PÉTER P. VARJÚ

Disclaimer, acknowledgement, etc

These notes provide a short summary of definitions and facts about number fields used in my course in Diophantine analysis. No proofs or explanations are given. I recommend the books of Baker [1, Chapters 10–12] and Marcus [2] for proper introductions to the subject. My lecture notes for the Part II Number Fields course may also be available on my webpage.

Please send comments to: pv270@dpmms.cam.ac.uk.

1. Number fields, rings of integers

A **number field** K is a finite degree extension of the field of rational numbers $\mathbf{Q}$.

Given an algebraic number α its **monic minimal polynomial** is the lowest degree monic polynomial $P(X) \in \mathbf{Q}[X]$ with $P(\alpha) = 0$. The **minimal polynomial** of α **in** $\mathbf{Z}[X]$ is an integer multiple of the monic minimal polynomial whose coefficients are coprime integers.

An algebraic number α is an **algebraic integer** if and only if one of the following equivalent conditions hold.

- The monic minimal polynomial has integer coefficients.
- The minimal polynomial in $\mathbf{Z}[X]$ is monic.
- The two kinds of minimal polynomials are equal.
- α is a zero of a monic polynomial with algebraic integer coefficients.

The set of algebraic integers is denoted by $\mathcal{O}$ and it forms a ring with addition and multiplication. The set of algebraic integers in a number field K is denoted by $\mathcal{O}_K$ and called the **ring of integers** of K.

The ring of integers of a number field is a free $\mathbf{Z}$-module of rank $d = \deg K$. A free $\mathbf{Z}$-module basis, that is, elements $\alpha_1, \ldots, \alpha_d \in \mathcal{O}_K$ such that each element of $\mathcal{O}_K$ can be written uniquely in the form $x_1\alpha_1 + \ldots + x_d\alpha_d$ for $x_1, \ldots, x_n \in \mathbf{Z}$ is called an **integral basis**.

2. Ideals

Let K be an number field. An **ideal** in $\mathcal{O}_K$ is a non-empty subset I that is closed under addition and $\alpha I \subset I$ for all $\alpha \in \mathcal{O}_K$. A proper ideal $I \subsetneq \mathcal{O}_K$ is **maximal** if there is no proper ideal $J \subsetneq \mathcal{O}_K$ with

$I \subsetneq J$. A proper ideal $I \subsetneq \mathcal{O}_K$ is a **prime ideal** if $\alpha \cdot \beta \in I$ implies $\alpha \in I$ or $\beta \in I$ for all $\alpha, \beta \in \mathcal{O}_K$. An ideal is maximal if and only if the quotient $\mathcal{O}_K/I$ is a field and it is a prime ideal if and only if $\mathcal{O}_K/I$ is an integral domain. In a number field, all non-zero prime ideals are maximal.

Given two ideals $I, J \subset \mathcal{O}_K$, their product is defined as

$$IJ = \{\alpha_1\beta_1 + \ldots + \alpha_k\beta_k : \alpha_1, \ldots, \alpha_k \in I, \beta_1, \ldots, \beta_k \in J, k \in \mathbf{Z}_{\geq 1}\},$$

that is the smallest ideal that contains all products of an element from I with an element from J. The set of ideals in $\mathcal{O}_K$ form a semigroup with respect to this multiplication.

The **norm of an ideal** $I \subset \mathcal{O}_K$ is defined as $\mathrm{N}(I) = |\mathcal{O}_K/I|$. This is a multiplicative function, that is $\mathrm{N}(IJ) = \mathrm{N}(I)\,\mathrm{N}(J)$. For principal ideals, we have $\mathrm{N}(\alpha\mathcal{O}_K) = |\,\mathrm{N}_{K|\mathbf{Q}}(\alpha)|$.

All ideals $I \subset \mathcal{O}_K$ can be written as a product of non-zero prime ideals, and this decomposition is unique up to the order of the factors. We call the non-zero prime ideals in $\mathcal{O}_K$ the **primes** of $\mathcal{O}_K$ or K.

For ideals $I, J \subset \mathcal{O}_K$ the following are equivalent.

- $I \subset J$.
- $J|I$, that is, there is some ideal $\widetilde{J} \subset \mathcal{O}_K$ with $J\widetilde{J} = I$.

3. Field extensions

Let K be a number field. Given a prime $P \subset \mathcal{O}_K$, there is a unique rational prime p with $p \in P$, which is equivalent to $P|p\mathcal{O}_K$. We call p the rational prime **lying under or below** P. Conversely, for each rational prime p, there is at least one prime $P \in \mathcal{O}_K$ with $p \in P$. We say that such primes P **lie over or above** p. We denote this by $P|p$.

If $P \subset \mathcal{O}_K$ is a prime lying over a rational prime p, then $\mathcal{O}_K/P$ is a finite field of characteristic p, whose order is p^{f_P}, where f_P is called the **inertial degree** of P. The largest integer m such that $P^m|p\mathcal{O}_K$ is called the **ramification index**, and it is denoted by e_P. A simple calculation with norms of ideals gives

$$\sum_{P|p} e_P f_P = [K : \mathbf{Q}].$$

More generally, let $L|K$ be an extension of number fields. Given an ideal $I \subset \mathcal{O}_K$, we consider

$$I\mathcal{O}_L = \{\alpha_1\beta_1 + \ldots + \alpha_k\beta_k : \alpha_1, \ldots, \alpha_k \in I, \beta_1, \ldots, \beta_k \in \mathcal{O}_L, k \in \mathbf{Z}_{\geq 1}\},$$

the smallest ideal of $\mathcal{O}_L$ containing I. In the other direction, given an ideal $I \subset \mathcal{O}_L$, $I \cap \mathcal{O}_K$ is an ideal in $\mathcal{O}_K$. For ideals $I, J \subset \mathcal{O}_K$, we have

$$(I\mathcal{O}_L)(J\mathcal{O}_L) = IJ\mathcal{O}_L.$$

On the other hand, for $I, J \subset \mathcal{O}_L$, $(I \cap \mathcal{O}_K)(J \cap \mathcal{O}_K)$ may differ from $IJ \cap \mathcal{O}_K$. For an ideal $I \subset \mathcal{O}_K$, we have

$$\mathrm{N}(I\mathcal{O}_L) = \mathrm{N}(I)^{[L:K]}.$$

Given a prime $P \subset \mathcal{O}_K$ and a prime in $Q \subset \mathcal{O}_L$ we say that P **lies under or below** Q and Q **lies above or over** P if one of the following equivalent conditions hold.

- $P = Q \cap \mathcal{O}_K$.
- $P\mathcal{O}_K \subset Q$.
- $Q|P\mathcal{O}_K$.

When this is the case, we denote it by $Q|P$.

Given a prime $P \subset \mathcal{O}_K$, there is at least one prime that lies over P. Conversely, given a prime $Q \subset \mathcal{O}_L$, $Q \cap \mathcal{O}_K$ is the unique prime in K that lies below Q.

Let $P \subset \mathcal{O}_K$ and $Q \subset \mathcal{O}_L$ be primes such that $Q|P$. Then a subfield of $\mathcal{O}_L/Q$ can be naturally identified with $\mathcal{O}_K/P$. The degree of this extension of finite fields is called the **inertial degree** and we denote it by $f_{Q|P}$. The largest integer m such that $P^m|Q$ is called the **ramification index** and it is denoted by $e_{Q|P}$. We have

$$\sum_{Q|P} e_{Q|P} f_{Q|P} = [L : K].$$

Consider a tower of field extensions of number fields $M|L|K$, and let $P \subset \mathcal{O}_K$, $Q \subset \mathcal{O}_L$ and $R \subset \mathcal{O}_M$ be primes with $R|Q|P$. Then we have the chain rules

$$\begin{aligned} f_{R|P} &= f_{R|Q} f_{Q|P}, \\ e_{R|P} &= e_{R|Q} e_{Q|P}. \end{aligned}$$

4. Units

An algebraic integer $\alpha \in \mathcal{O}$ is a unit if and only if $\alpha^{-1} \in \mathcal{O}$. This is equivalent to the minimal polynomial of α having constant term ± 1 and $\mathrm{N}(\alpha) = \pm 1$.

We denote by $\mathcal{O}_K^\times$ the set of algebraic units in $\mathcal{O}_K$. They form a group with respect to multiplication.

The set of infinite places $M_{K,\infty}$ of K consists of the embeddings $\sigma : K \to \mathbf{R}$ together with one from each conjugate pairs of complex embeddings $\sigma : K \to \mathbf{C}$. For $\sigma \in M_{K,\infty}$, we define $d_\sigma = 1$ if $\sigma(K) \subset \mathbf{R}$ and $d_\sigma = 2$ otherwise.

We consider the so-called logarithmic embedding

$$\mathrm{Log} : K \to \mathbf{R}^{M_{K,\infty}}; \quad \mathrm{Log}(\alpha) = (d_\sigma \log |\sigma(\alpha)|)_{\sigma \in K_{K,\infty}}.$$

We note that

$$\log |\mathrm{N}(\alpha)| = \sum_{\sigma \in M_{K,\infty}} d_\sigma \log |\sigma(\alpha)|,$$

so we have $\mathrm{Log}(\mathcal{O}_K^\times) \subset V$, where

$$V = \{(x_\sigma) : \sum_\sigma d_\sigma x_\sigma = 0\}.$$

A theorem of Kronecker states that $\mathrm{Ker}(\mathrm{Log}) \cap \mathcal{O}_K$ is precisely the set of roots of unity in K.

Dirichlet's unit theorem states that $\mathrm{Log}(\mathcal{O}_K^\times)$ is a lattice in V, that is it is a free $\mathbf{Z}$ module of rank $\dim V = |M_{K,\infty}| - 1$. An alternative way to sate this is that $\mathcal{O}_K^\times$ is the direct product of a finite group, which is the roots of unity in K and a free Abelian group of rank $\dim V$.

References

[1] A. Baker, *A comprehensive course in number theory*, Cambridge University Press, Cambridge, 2012. MR2954465

[2] D. A. Marcus, *Number fields*, Universitext, Springer, Cham, 2018. Second edition of [MR0457396], With a foreword by Barry Mazur. MR3822326