6 Extensions of Dedekind rings

6.1 Modules over Dedekind rings

6.2 Decomposition of prime ideals

6.3 Decomposition group

6.4 Inertia group

6.5 Frobenius

6.6 Relative norm

6.7 Different

6.8 Relative discriminant

To prove Proposition 6.8.2 in general use the following facts from commutative algebra:

- For any prime ideal $\mathfrak{p}$ of a ring A the set $S := A \smallsetminus \mathfrak{p}$ is multiplicative and the ring $A_{\mathfrak{p}} := S^{-1}\mathfrak{p}$ is called the *localization of A at $\mathfrak{p}$*.
- For any ideal $\mathfrak{a} \subset A$ the set $\mathfrak{a}_{\mathfrak{p}} := S^{-1}\mathfrak{a}$ is an ideal of $A_{\mathfrak{p}}$.

Now assume that A is Dedekind and that $\mathfrak{a}$ is a maximal ideal.

- Then $A_{\mathfrak{p}}$ is a principal ideal domain.
- For any nonzero ideals $\mathfrak{a}, \mathfrak{a}' \subset A$ we have $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{a}'_{\mathfrak{p}}$ if and only if the exponents of $\mathfrak{p}$ in the prime factorizations of $\mathfrak{a}$ and $\mathfrak{a}'$ coincide.

Now let B be the integral closure of A in a finite separable extension $L/\operatorname{Quot}(A)$.

- Then $B_{\mathfrak{p}} := S^{-1}B$ is a principal ideal domain.
- The formation of $\operatorname{disc}_{B/A}$ and $\operatorname{diff}_{B/A}$ and the relative ideal norm commutes with localization at $\mathfrak{p}$.

7 Zeta functions

7.1 Riemann zeta function

Definition 7.1.1: The *Riemann zeta function* is defined by the series

$$\zeta(s) \;:=\; \sum_{n=1}^{\infty} n^{-s}.$$

Proposition 7.1.2: This series converges absolutely and locally uniformly for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ and defines a holomorphic function there.

Lemma 7.1.3: For all $\mathrm{Re}(s) > 1$ we have

$$\zeta(s) \;=\; \frac{s}{s-1} - s \cdot \int_1^\infty (x - \lfloor x \rfloor) x^{-s-1}\, dx.$$

Proposition 7.1.4: The function $\zeta(s) - \frac{1}{s-1}$ extends uniquely to a holomorphic function on the region $\mathrm{Re}(s) > 0$.

Remark 7.1.5: It is known that $\zeta(s)$ extends uniquely to a meromorphic function on $\mathbb{C}$ with a single pole at $s = 1$. This extension is again denoted by $\zeta(s)$.

Throughout the following we use the branch of the logarithm with $\log 1 = 0$.

Proposition 7.1.6: An infinite product of non-zero complex numbers $\prod_{k\geqslant 1} z_k$ converges to a non-zero value if and only if $\lim\limits_{k\to\infty} z_k = 1$ and $\sum\limits_{k\geqslant 1} \log z_k$ converges.

Proposition 7.1.7: For all $\mathrm{Re}(s) > 1$ we have the *Euler product*

$$\zeta(s) \;=\; \prod_{p \text{ prime}} (1 - p^{-s})^{-1} \;\neq\; 0.$$

Proposition 7.1.8: We have

$$\sum_{p \text{ prime}} p^{-s} = \log \tfrac{1}{s-1} + O(1) \quad \text{for real } s \to 1+.$$

Definition 7.1.9: For $x \in \mathbb{R}$ we denote the number of primes $\leqslant x$ by $\pi(x)$.

Corollary 7.1.10: There is no $\varepsilon > 0$ such that for $x \to \infty$ we have

$$\pi(x) = O\Big(\frac{x}{(\log x)^{1+\varepsilon}}\Big).$$

In particular there exist infinitely many primes.

7.2 Dedekind zeta function

Fix a number field K of degree n over $\mathbb{Q}$.

Definition 7.2.1: The *Dedekind zeta function of* K is defined by the series

$$\zeta_K(s) \ := \ \sum_{\mathfrak{a}} \mathrm{Nm}(\mathfrak{a})^{-s},$$

where the sum extends over all non-zero ideals $\mathfrak{a} \subset \mathcal{O}_K$.

Proposition 7.2.2: This series converges absolutely and locally uniformly for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ and defines a holomorphic function there, and we have the *Euler product*

$$\zeta_K(s) \ = \ \prod_{\mathfrak{p}} \big(1 - \mathrm{Nm}(\mathfrak{p})^{-s}\big)^{-1} \ \neq \ 0,$$

extended over all maximal ideals $\mathfrak{p} \subset \mathcal{O}_K$.

Proposition 7.2.3: We have

$$\log \zeta_K(s) \;=\; \sum_{\mathfrak{p}} \mathrm{Nm}(\mathfrak{p})^{-s} + \big(\text{holomorphic for } \operatorname{Re}(s) > \tfrac{1}{2}\big).$$

Theorem 7.2.4: The function $\zeta_K(s)$ extends uniquely to a meromorphic function on the region $\mathrm{Re}(s) > 1 - \frac{1}{n}$ which is holomorphic except for a pole of order 1 at $s = 1$.

Proposition 7.2.5: We have

$$\sum_{\mathfrak{p}} \mathrm{Nm}(\mathfrak{p})^{-s} \;=\; \log \tfrac{1}{s-1} + O(1) \quad \text{for real } s \to 1+.$$

Corollary 7.2.6: There exist infinitely many rational primes that split totally in $\mathcal{O}_K$.

7.3 Analytic class number formula

As before we set $\Sigma := \mathrm{Hom}(K,\mathbb{C})$ and let r be the number of embeddings $K \hookrightarrow \mathbb{R}$ and s the number of pairs of complex conjugate non-real embeddings $K \hookrightarrow \mathbb{C}$. With $K_\mathbb{C} := \mathbb{C}^\Sigma$ and

$$K_\mathbb{R} \;:=\; \big\{(z_\sigma)_\sigma \in K_\mathbb{C} \;\big|\; \forall\sigma\in\Sigma\colon z_{\bar\sigma} = \bar z_\sigma\big\}$$

as in §3.4 we then have

$$K_\mathbb{R}\cap\mathbb{R}^\Sigma \;=\; \big\{(t_\sigma)_\sigma \in \mathbb{R}^\Sigma \;\big|\; \forall\sigma\in\Sigma\colon t_{\bar\sigma} = t_\sigma\big\}.$$

The $\mathbb{R}$-subspace

$$H := \ker\big(\mathrm{Tr}\colon K_\mathbb{R}\cap\mathbb{R}^\Sigma \to \mathbb{R}\big)$$

from §5.2 therefore becomes a euclidean vector space by its embedding $H \subset K_\mathbb{R} \subset K_\mathbb{C}$ and the scalar product from §4.1. By §2.2 it is thus endowed with a canonical translation invariant measure $d\,\mathrm{vol}$. Recall from Theorem 5.3.1 that $\Gamma := \ell(j(\mathcal{O}_K^\times))$ is a complete lattice in H.

Definition 7.3.1: The *regulator of* K is the real number

$$R \;:=\; \mathrm{vol}(H/\Gamma) \;>\; 0.$$

Let $w := |\mu(K)|$ denote the number of roots of unity in K and let $h := |\,\mathrm{Cl}(\mathcal{O}_K)|$ the class number.

Theorem 7.2.7: *Analytic class number formula:* The residue of $\zeta_K(s)$ at $s = 1$ is

$$\operatorname{Res}_{s=1} \zeta_K(s) \;=\; \frac{2^r (2\pi)^s Rh}{w\sqrt{|d_K|}} \;>\; 0.$$

7.4 Dirichlet density

Consider a number field K and a subset A of the set P of maximal ideals of $\mathcal{O}_K$.

Definition 7.4.1: (a) The value

$$\overline{\mu}(A) \;:=\; \limsup_{s\to 1+} \frac{\sum_{\mathfrak{p}\in A} \mathrm{Nm}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in P} \mathrm{Nm}(\mathfrak{p})^{-s}}$$

is called the *upper Dirichlet density of A.*

(b) The value

$$\underline{\mu}(A) \;:=\; \liminf_{s\to 1+} \frac{\sum_{\mathfrak{p}\in A} \mathrm{Nm}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in P} \mathrm{Nm}(\mathfrak{p})^{-s}}$$

is called the *lower Dirichlet density of A.*

(c) If these coincide, their common value

$$\mu(A) \;:=\; \lim_{s\to 1+} \frac{\sum_{\mathfrak{p}\in A} \mathrm{Nm}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in P} \mathrm{Nm}(\mathfrak{p})^{-s}}$$

is called the *Dirichlet density of A.*

Proposition 7.4.2: (a) We have $0 \leqslant \underline{\mu}(A) \leqslant \overline{\mu}(A) \leqslant 1$.

(b) For any subset $B \subset A$ we have $\overline{\mu}(B) \leqslant \overline{\mu}(A)$ and $\underline{\mu}(B) \leqslant \underline{\mu}(A)$, and also $\mu(B) \leqslant \mu(A)$ if these exist.

(c) We have $\mu(A) = 0$ if A is finite.

(d) We have $\mu(A) = 1$ if $P \smallsetminus A$ is finite.

(e) For any disjoint subsets $A, B \subset P$, if two of $\mu(A)$, $\mu(B)$, $\mu(A \cup B)$ exist, then so does the third and we have $\mu(A) + \mu(B) = \mu(A \cup B)$.

Proposition-Definition 7.4.3: If the *natural density of A*

$$\gamma(A) \ := \ \lim_{x \to \infty} \frac{\left|\{\mathfrak{p} \in A \mid \mathrm{Nm}(\mathfrak{p}) \leqslant x\}\right|}{\left|\{\mathfrak{p} \in P \mid \mathrm{Nm}(\mathfrak{p}) \leqslant x\}\right|}$$

exists, so does the Dirichlet density $\mu(A)$ and they are equal.

7.5 Primes of absolute degree 1

Definition 7.5.1: The *absolute degree* of a prime $\mathfrak{p}$ of $\mathcal{O}_K$ is the degree of $k(\mathfrak{p})$ over its prime field.

Proposition 7.5.2: The set of primes of absolute degree 1 has Dirichlet density 1.

Proposition 7.5.3: A subset $A \subset P$ has a Dirichlet density if and only if the set of all $\mathfrak{p} \in A$ of absolute degree 1 has a Dirichlet density, and then they are equal.

For any finite galois extension of number fields L/K we let $\mathrm{Split}_{L/K}$ denote the set of primes $\mathfrak{p} \subset \mathcal{O}_K$ that are totally split in $\mathcal{O}_L$.

Proposition 7.5.4: $\mathrm{Split}_{L/K}$ has Dirichlet density $\frac{1}{[L/K]}$. In particular it is infinite.

Now consider two finite galois extensions of number fields $L, L'/K$.

Proposition 7.5.5: Then $\mathrm{Split}_{LL'/K} = \mathrm{Split}_{L/K} \cap \mathrm{Split}_{L'/K}$.

Proposition 7.5.6: The following are equivalent:

(a) $L \subset L'$.

(b) $\mathrm{Split}_{L'/K} \subset \mathrm{Split}_{L/K}$.

(c) $\mu(\mathrm{Split}_{L'/K} \setminus \mathrm{Split}_{L/K}) < \frac{1}{2[L/K]}$.

Proposition 7.5.7: The following are equivalent:

(a) $L = L'$.

(b) $\mathrm{Split}_{L'/K}$ and $\mathrm{Split}_{L/K}$ differ only by a set of Dirichlet density 0.

In particular, a number field K that is galois over $\mathbb{Q}$ is uniquely determined by the set of rational primes p that split totally in K.

7.6 Dirichlet L-series

Definition 7.6.1: (a) A homomorphism $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ is called a *Dirichlet character of modulus* $N \geqslant 1$.

(b) The *conductor* of such χ is the smallest divisor $N'|N$ such that χ factors through a homomorphism $(\mathbb{Z}/N'\mathbb{Z})^\times \to \mathbb{C}^\times$.

(c) Such χ is called *primitive* if $N' = N$.

(d) Such χ is called *principal* if $N' = 1$, that is, if χ is the trivial homomorphism.

Convention 7.6.2: Often one identifies a Dirichlet character χ of modulus N with a function $\chi\colon \mathbb{Z} \to \mathbb{C}$ by setting

$$\chi(a) \;:=\; \begin{cases} \chi(a \bmod (N)) & \text{if } \gcd(a,N) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Caution 7.6.3: When the conductor N' is smaller than the modulus N, one has to be somewhat careful with the divisors of N/N'.

Example: For any prime p the Legendre symbol defines a Dirichlet character $a \mapsto \left(\frac{a}{p}\right)$ of modulus p.

Definition 7.6.4: The *Dirichlet L-function* associated to any Dirichlet character χ is

$$L(\chi, s) \;:=\; \sum_{n \geqslant 1} \chi(n) n^{-s}.$$

Proposition 7.6.5: This series converges absolutely and locally uniformly for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ and defines a holomorphic function there.

Proposition 7.6.6: For all $\mathrm{Re}(s) > 1$ we have the *Euler product*

$$L(\chi, s) \;=\; \prod_{p \nmid N} (1 - \chi(p) p^{-s})^{-1}.$$

Proposition 7.6.7: If a Dirichlet character χ of modulus N corresponds to a primitive Dirichlet character χ' of modulus N', then

$$L(\chi', s) \;=\; L(\chi, s) \cdot \prod_{p|N,\, p\nmid N'} (1 - p^{-s})^{-1}.$$

Proposition 7.6.8: (a) For the principal Dirichlet character χ of modulus 1 we have $L(\chi, s) = \zeta(s)$.

(b) For every non-principal Dirichlet character χ the function $L(\chi, s)$ extends uniquely to a holomorphic function on the region $\mathrm{Re}(s) > 0$.

Theorem 7.6.9: The zeta function $\zeta_K(s)$ of the field $K := \mathbb{Q}(\mu_N)$ is the product of the L-functions $L(\chi, s)$ for all primitive Dirichlet characters χ of conductor dividing N.

Theorem 7.6.10: For any non-principal Dirichlet character χ we have $L(\chi, 1) \neq 0$.

Proposition 7.6.11: For any non-principal Dirichlet character χ we have

$$\sum_{p \text{ prime}} \chi(p) p^{-s} \;=\; O(1) \quad \text{for real } s \to 1+.$$

7.7 Primes in arithmetic progressions

Theorem 7.7.1: For any coprime integers a and $N \geqslant 1$ the set of rational primes $p \equiv a \bmod (N)$ has Dirichlet density $\frac{1}{\varphi(N)}$. In particular it is infinite.

This can also be viewed as the special case $L = \mathbb{Q}(\mu_N)$ and $K = \mathbb{Q}$ of the following general theorem:

Theorem 7.7.2: *Cebotarev density theorem:* Let L/K be a Galois extension of number fields with Galois group Γ. For any $\gamma \in \Gamma$ consider its conjugacy class $O_\Gamma(\gamma) := \{{}^{\gamma'}\gamma \mid \gamma' \in \Gamma\}$. Then the set of primes $\mathfrak{p} \subset \mathcal{O}_K$ that are unramified in $\mathcal{O}_L$ and whose Frobenius substitution lies in $O_\Gamma(\gamma)$ has the Dirichlet density $\frac{|O_\Gamma(\gamma)|}{|\Gamma|}$.

References

- Atiyah, M. F., MacDonald, I. G.: *Introduction to Commutative Algebra*, Westview Press, 1969.
- Hungerford, T.W.: *Algebra.* Springer 1974
- Neukirch, Jürgen: *Algebraic Number Theory.* Springer 1999.