Algebraic number theory **LTCC 2008**

Lecture notes, Part 3

7. The Riemann zeta function

We write $\mathrm{Re}(z)$ for the real part of a complex number $z \in \mathbb{C}$. If a is a positive real number and $z \in \mathbb{C}$ then a^z is defined by $a^z = \exp(z \cdot \log(a))$. Note that

$$|a^z| = |\exp(z \cdot \log(a))| = \exp\big(\mathrm{Re}(z \cdot \log(a))\big) = a^{\mathrm{Re}(z)}.$$

Definition 7.1. The Riemann zeta function $\zeta(z)$ is the function defined by

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}$$

for $z \in \mathbb{C}$ with $\mathrm{Re}(z) > 1$.

The absolute convergence of the series in the definition of $\zeta(z)$ follows easily by comparison to an integral, more precisely

$$\sum_{n=1}^{\infty} \left|n^{-z}\right| = \sum_{n=1}^{\infty} n^{-\mathrm{Re}(z)} = 1 + \sum_{n=2}^{\infty} n^{-\mathrm{Re}(z)}$$
$$< 1 + \int_1^{\infty} x^{-\mathrm{Re}(z)} dx = 1 + \frac{1}{\mathrm{Re}(z) - 1}.$$

The following theorem summarises some well-known facts about the Riemann zeta function.

Theorem 7.2. (1) *The series* $\sum_{n=1}^{\infty} n^{-z}$ *converges uniformly on sets of the form* $\{z \in \mathbb{C} : \mathrm{Re}(z) \geq 1 + \delta\}$ *with* $\delta > 0$. *Therefore the function* $\zeta(z)$ *is holomorphic on the set* $\{z \in \mathbb{C} : \mathrm{Re}(z) > 1\}$.

(2) *(Euler product) For all* $z \in \mathbb{C}$ *with* $\mathrm{Re}(z) > 1$ *we have*

$$\zeta(z) = \prod_p \frac{1}{1 - p^{-z}}$$

where the product runs over all prime numbers p.

(3) *(Analytic continuation) The function* $\zeta(z)$ *can be extended to a meromorphic function on the whole complex plane.*

(4) *(Functional equation) Let*

$$Z(z) = \pi^{-z/2}\Gamma(z/2)\zeta(z)$$

where Γ *is the Gamma function. Then the function* $Z(z)$ *satisfies the functional equation* $Z(z) = Z(1 - z)$.

(5) *(Singularities) The only singularity of* $\zeta(z)$ *is a simple pole at* $z = 1$ *with residue* 1.

Proof. See for example [2, VII, §1]. □

Recall that there is a bijection between positive integers and non-zero ideals of $\mathbb{Z}$ which sends $n \in \mathbb{N}$ to the principal ideal (n). Conversely, given a non-zero ideal A of $\mathbb{Z}$ we can find the unique positive integer n generating A as $n = |\mathbb{Z}/A|$. Hence the definition of the Riemann zeta function can also be written as

$$\zeta(z) = \sum_{\substack{A \subseteq \mathbb{Z} \\ A \neq \{0\}}} \frac{1}{|\mathbb{Z}/A|^z}$$

where the sum runs over all non-zero ideals A of $\mathbb{Z}$. In this form the definition can be generalised to arbitrary number fields.

8. The norm of an ideal

In this section K is an algebraic number field and R_K the ring of integers of K. If A is an ideal of R_K, then R_K/A denotes the quotient ring, i.e. R_K/A is the set of cosets $\alpha + A$ with operations $(\alpha + A) + (\beta + A) = (\alpha + \beta) + A$ and $(\alpha + A) \cdot (\beta + A) = (\alpha\beta) + A$.

Lemma 8.1. *Let A be a non-zero ideal of R_K. Then $A \cap \mathbb{Z} \neq \{0\}$, i.e. A contains a non-zero rational integer.*

Proof. Let $\alpha \in A \setminus \{0\}$. Then α is integral over $\mathbb{Z}$ and therefore satisfies an equation of the form

$$\alpha^d + c_{d-1}\alpha^{d-1} + \cdots + c_1\alpha + c_0 = 0 \tag{1}$$

with $c_0, c_1, \ldots, c_{d-1} \in \mathbb{Z}$. We can assume that $c_0 \neq 0$ because otherwise we could divide equation (1) by α. Now $\alpha \in A$, $-\alpha^{d-1} - c_{d-1}\alpha^{d-2} - \cdots - c_1 \in R_K$ and A is an ideal. Hence it follows that

$$c_0 = \alpha \cdot (-\alpha^{d-1} - c_{d-1}\alpha^{d-2} - \cdots - c_1) \in A,$$

so c_0 is a non-zero element in $A \cap \mathbb{Z}$. □

Lemma 8.2. *Let $c \in \mathbb{Z} \setminus \{0\}$ and let (c) denote the principal ideal of R_K generated by c. Then $|R_K/(c)| = |c|^{[K:\mathbb{Q}]}$.*

Proof. Theorem 3.7 shows that there exists an isomorphism of abelian groups $R_K \cong \mathbb{Z}^n$ for some $n \in \mathbb{N}$. In fact one has $n = [K : \mathbb{Q}]$ because it follows easily from Lemma 3.4 that any $\mathbb{Z}$-basis of R_K is also a $\mathbb{Q}$-basis of K. Under the isomorphism $R_K \cong \mathbb{Z}^n$ the ideal (c) corresponds to the subgroup $(c\mathbb{Z})^n$ of $\mathbb{Z}^n$, therefore $R_K/(c) \cong \mathbb{Z}^n/(c\mathbb{Z})^n \cong (\mathbb{Z}/c\mathbb{Z})^n$ which is a finite group of order $|c|^n$. □

Lemma 8.3. *Let A be a non-zero ideal of R_K. Then the ring R_K/A is finite.*

Proof. By Lemma 8.1 the ideal A contains a non-zero integer $c \in \mathbb{Z}$. Then $(c) \subseteq A$ where (c) denotes the ideal of R_K generated by c. It follows that $|R_K/(c)| \geq |R_K/A|$. Now $|R_K/(c)|$ is finite by Lemma 8.2, hence $|R_K/A|$ is finite. □

Definition 8.4. Let A be a non-zero ideal of R_K. Then we define the *norm* of the ideal A to be the number of elements of R_K/A. We write $\mathbf{N}(A)$ for the norm of A.

Lemma 8.5. *The norm of ideals is multiplicative, i.e. if A and B are non-zero ideals of R_K then $\mathbf{N}(AB) = \mathbf{N}(A)\mathbf{N}(B)$.*

Proof. Since B can be written as a product of non-zero prime ideals it suffices to show $\mathbf{N}(AP) = \mathbf{N}(A)\mathbf{N}(P)$ where P is a non-zero prime ideal. Note that $AP \subseteq A \subseteq R_K$, hence

$$|R_K/AP| = |R_K/A| \cdot |A/AP|.$$

Now $\mathbf{N}(AP) = |R_K/AP|$, $\mathbf{N}(A) = |R_K/A|$ and $\mathbf{N}(P) = |R_K/P|$, so to complete the proof we only need to show that $|R_K/P| = |A/AP|$.

Unique factorisation into prime ideals implies that $A \neq AP$, so there exists an $\alpha \in A \setminus AP$. Define a map $f : R_K \to A/AP$ by $f(x) = x\alpha + AP$. It is not difficult to check that f is a homomorphism of R_K-modules. Using the fact that the ideal P is maximal, it then easily follows that f is surjective and has kernel P. Therefore $R_K/P \cong A/AP$ and thus $|R_K/P| = |A/AP|$. □

Theorem 8.6.

1. *Let P be a non-zero prime ideal of R_K. Then P contains precisely one prime number p. We have $\mathbf{N}(P) = p^f$ where $1 \leq f \leq [K : \mathbb{Q}]$.*
2. *Every prime number p is contained in at most $[K : \mathbb{Q}]$ prime ideals of R_K.*

Proof. Let P be a non-zero prime ideal of R_K. It is easy to check that $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. Furthermore $P \cap \mathbb{Z} \neq \{0\}$ by Lemma 8.1. Hence Lemma 4.5 shows that $P \cap \mathbb{Z}$ is a principal ideal of $\mathbb{Z}$ generated by a prime number p, so in particular $p \in P$. Now suppose that p and q are distinct prime numbers contained in P. Since p and q are coprime, there exist $x, y \in \mathbb{Z}$ such that $px + qy = 1$. But $p, q \in P$ implies that $1 = px + qy \in P$, hence $P = R_K$ contradicting the definition of a prime ideal. This completes the proof that a non-zero prime ideal P contains precisely one prime number p.

Now let p be a prime number and consider the principal ideal (p) of R_K. By Theorem 4.7 we can write

$$(p) = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r} \tag{2}$$

where $P_1, P_2, \ldots, P_r$ are distinct prime ideals of R_K and $e_1, e_2, \ldots, e_r \in \mathbb{N}$. Clearly $p \in P_i$ for $i = 1, \ldots, r$. Conversely assume that $p \in P$ for some prime ideal P of R_K. Then $P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r} \subseteq P$ and since P is a prime ideal this implies $P_i \subseteq P$ for some $i = 1, \ldots, r$. It follows that $P_i = P$ since P_i is maximal. This shows that a prime ideal P contains the prime number p if and only if $P = P_i$ for some $i = 1, \ldots, r$. So the prime number p is contained in precisely r prime ideals of R_K.

Taking the norm of (2) and using Lemma 8.5 gives

$$\mathbf{N}((p)) = \mathbf{N}(P_1)^{e_1} \mathbf{N}(P_2)^{e_2} \cdots \mathbf{N}(P_r)^{e_r}. \tag{3}$$

By Lemma 8.2 we have $\mathbf{N}((p)) = |R_K/(p)| = p^{[K:\mathbb{Q}]}$. It therefore follows from (3) that $\mathbf{N}(P_i) = p^{f_i}$ for some $f_i \in \mathbb{N}$, and that $p^{[K:\mathbb{Q}]} = (p^{f_1})^{e_1} \cdots (p^{f_r})^{e_r} = p^{e_1 f_1 + \cdots + e_r f_r}$, hence

$$[K : \mathbb{Q}] = e_1 f_1 + \cdots + e_r f_r.$$

This equation implies $f_i \leq [K : \mathbb{Q}]$ which completes the proof of part (1). Furthermore this equation also implies that $r \leq [K : \mathbb{Q}]$ which proves part (2). □

Remark 8.7. Let P be a non-zero prime ideal of R_K and let p be the unique prime number contained in P. Since P is a maximal ideal of R_K, the quotient ring R_K/P is a field. The ring homomorphism $\mathbb{Z} \to R_K/P$ has kernel $P \cap \mathbb{Z} = (p)$ where now (p) denotes the principal ideal of $\mathbb{Z}$ generated by p, hence there exists an injective ring homomorphism $\mathbb{Z}/(p) \to R_K/P$. This shows that R_K/P can be considered as a field extension of the field $\mathbb{Z}/(p)$.

We claim that $[R_K/P : \mathbb{Z}/(p)] = f$ where f is given by $\mathbf{N}(P) = p^f$. Indeed, since R_K/P is a vector space of dimension $[R_K/P : \mathbb{Z}/(p)]$ over the field $\mathbb{Z}/(p)$, it follows that $|R_K/P| = |\mathbb{Z}/(p)|^{[R_K/P:\mathbb{Z}/(p)]}$. From this the claim follows because $|R_K/P| = \mathbf{N}(P)$ and $|\mathbb{Z}/(p)| = p$.

The number $f = [R_K/P : \mathbb{Z}/(p)]$ is called the *residue class degree* of the prime ideal P.

9. Dedekind zeta functions

Definition 9.1. The Dedekind zeta function $\zeta_K(z)$ of the algebraic number field K is the function defined by

$$\zeta_K(z) = \sum_{\substack{A \subseteq R_K \\ A \neq \{0\}}} \frac{1}{\mathbf{N}(A)^z}$$

for $z \in \mathbb{C}$ with $\mathrm{Re}(z) > 1$. Here the sum runs over all non-zero ideals A of R_K.

We note that the Dedekind zeta function $\zeta_{\mathbb{Q}}(z)$ of the field $\mathbb{Q}$ is precisely the Riemann zeta function $\zeta(z)$.

Theorem 9.2. *The series defining $\zeta_K(z)$ converges absolutely and uniformly on sets of the form $\{z \in \mathbb{C} : \mathrm{Re}(z) \geq 1+\delta\}$ with $\delta > 1$. Therefore the function $\zeta_K(z)$ is holomorphic on the set $\{z \in \mathbb{C} : \mathrm{Re}(z) > 1\}$. Moreover for $z \in \mathbb{C}$ with $\mathrm{Re}(z) > 1$ we have the Euler product*

$$\zeta_K(z) = \prod_{\substack{P \subseteq R_K \\ P \neq \{0\}}} \frac{1}{1 - \mathbf{N}(P)^{-z}}$$

where the product runs over all non-zero prime ideals P of R_K.

Proof. We first show that

$$\sum_P \log\left(\frac{1}{1-\mathbf{N}(P)^{-(1+\delta)}}\right) \leq [K:\mathbb{Q}] \cdot \zeta(1+\delta) \tag{4}$$

where the sum runs over all non-zero prime ideals of R_K. For this we recall that

$$\log\left(\frac{1}{1-x}\right) = \sum_{n=1}^{\infty} \frac{x^n}{n}.$$

Now if P is a non-zero prime ideal containing the prime number p then $\mathbf{N}(P) \geq p$ by Theorem 8.6.(1). But by Theorem 8.6.(2) there exist at most $[K:\mathbb{Q}]$ prime ideals containing p, hence

$$\begin{aligned}
\sum_P \log\left(\frac{1}{1-\mathbf{N}(P)^{-(1+\delta)}}\right) &= \sum_P \sum_{n=1}^{\infty} \frac{1}{n\mathbf{N}(P)^{n(1+\delta)}} \\
&= \sum_p \sum_{p \in P} \sum_{n=1}^{\infty} \frac{1}{n\mathbf{N}(P)^{n(1+\delta)}} \\
&\leq \sum_p \sum_{n=1}^{\infty} \frac{[K:\mathbb{Q}]}{np^{n(1+\delta)}} \\
&\leq [K:\mathbb{Q}] \cdot \sum_p \sum_{n=1}^{\infty} \frac{1}{(p^n)^{1+\delta}} \\
&\leq [K:\mathbb{Q}] \cdot \zeta(1+\delta),
\end{aligned}$$

where the last inequality comes from

$$\sum_p \sum_{n=1}^{\infty} \frac{1}{(p^n)^{1+\delta}} = \sum_{\substack{m \text{ is a} \\ \text{prime power}}} \frac{1}{m^{1+\delta}} \leq \sum_{m \in \mathbb{N}} \frac{1}{m^{1+\delta}} = \zeta(1+\delta).$$

This proves (4).

Next we show that for every positive real number B we have

$$\prod_{\mathbf{N}(P) \leq B} \frac{1}{1-\mathbf{N}(P)^{-z}} = \sum_{A \in \mathcal{M}(B)} \frac{1}{\mathbf{N}(A)^z} \tag{5}$$

where the product extends over all non-zero prime ideals P with norm at most B and $\mathcal{M}(B)$ denotes the set of all non-zero ideals A whose prime ideal factorisation contains only prime ideals with norm at most B. Indeed, if $P_1, \ldots, P_r$ is the list of prime ideals with norm at most B then

$$\begin{aligned}\prod_{\mathbf{N}(P)\le B}\frac{1}{1-\mathbf{N}(P)^{-z}} &= \prod_{i=1}^{r}\frac{1}{1-\mathbf{N}(P_i)^{-z}}\\ &= \prod_{i=1}^{r}\left(1+\frac{1}{\mathbf{N}(P_i)^{z}}+\frac{1}{\mathbf{N}(P_i)^{2z}}+\dots\right)\\ &= \sum_{\nu_1,\dots,\nu_r=0}^{\infty}\frac{1}{(\mathbf{N}(P_1)^{\nu_1}\cdots\mathbf{N}(P_r)^{\nu_r})^{z}}\\ &= \sum_{A\in\mathcal{M}(B)}\frac{1}{\mathbf{N}(A)^{z}},\end{aligned}$$

where for the last equality we used that every ideal $A \in \mathcal{M}(B)$ can be expressed uniquely as $A = P_1^{\nu_1}\cdots P_r^{\nu_r}$ with $\nu_1,\dots,\nu_r \in \mathbb{N}\cup\{0\}$.

We can now show that the series $\sum_A \frac{1}{\mathbf{N}(A)^z}$ converges absolutely and uniformly for $z \in \mathbb{C}$ with $\mathrm{Re}(z) \ge 1+\delta$. Since

$$\left|\frac{1}{\mathbf{N}(A)^{z}}\right| = \frac{1}{\mathbf{N}(A)^{\mathrm{Re}(z)}} \le \frac{1}{\mathbf{N}(A)^{1+\delta}}$$

the absolute and uniform convergence of $\sum_A \frac{1}{\mathbf{N}(A)^z}$ will follow if we show that $\sum_A \frac{1}{\mathbf{N}(A)^{1+\delta}}$ converges. The convergence of the series $\sum_A \frac{1}{\mathbf{N}(A)^{1+\delta}}$ follows from the fact that $\sum_{\mathbf{N}(A)\le B}\frac{1}{\mathbf{N}(A)^{1+\delta}}$ is monotonically increasing as $B\to\infty$ and bounded above because

$$\begin{aligned}\sum_{\mathbf{N}(A)\le B}\frac{1}{\mathbf{N}(A)^{1+\delta}} &\le \sum_{A\in\mathcal{M}(B)}\frac{1}{\mathbf{N}(A)^{1+\delta}}\\ &= \prod_{\mathbf{N}(P)\le B}\frac{1}{1-\mathbf{N}(P)^{-(1+\delta)}}\\ &= \exp\left(\sum_{\mathbf{N}(P)\le B}\log\left(\frac{1}{1-\mathbf{N}(P)^{-(1+\delta)}}\right)\right)\\ &\le \exp\left(\sum_{P}\log\left(\frac{1}{1-\mathbf{N}(P)^{-(1+\delta)}}\right)\right)\\ &\le \exp\big([K:\mathbb{Q}]\cdot\zeta(1+\delta)\big).\end{aligned}$$

The final step is to show the identity

$$\prod_{\substack{P\subseteq R_K\\ P\ne\{0\}}}\frac{1}{1-\mathbf{N}(P)^{-z}} = \sum_{\substack{A\subseteq R_K\\ A\ne\{0\}}}\frac{1}{\mathbf{N}(A)^{z}}. \tag{6}$$

The idea is to first use (4) to prove the convergence of the product and then to show (6) by letting B tend to ∞ in (5). For more details see for example [2, VII, §8]. □

Before we can state further properties of the Dedekind zeta function we must define the discriminant d_K of an algebraic number field K. Recall that if K has degree n over $\mathbb{Q}$, then R_K is a free $\mathbb{Z}$-module of rank n (because Theorem 3.7 shows that R_K is a free $\mathbb{Z}$-module and Lemma 3.4 implies that the rank of R_K over $\mathbb{Z}$ is equal to the dimension of K over $\mathbb{Q}$) and there exist precisely n distinct embeddings of K into $\mathbb{C}$ (Theorem 6.6).

Definition 9.3. Let K be an algebraic number field and $n = [K:\mathbb{Q}]$. Let $\beta_1,\dots,\beta_n$ be a $\mathbb{Z}$-basis of R_K, and let $\sigma_1,\dots,\sigma_n$ be the distinct embeddings of K into $\mathbb{C}$. Let

W be the $n \times n$-matrix $W = \big(\sigma_i(\beta_j)\big)_{1\le i,j\le n}$. Then the *discriminant* d_K of K is defined to be $d_K = \det(W)^2$.

It is not difficult to check that the discriminant d_K is well-defined. Since $\sigma_i(\beta_j)$ is integral over $\mathbb{Z}$ for all i and j, it follows that d_K is integral over $\mathbb{Z}$. Using Galois theory it is easy to see that d_K lies in $\mathbb{Q}$, hence $d_K \in \mathbb{Z}$.

Theorem 9.4. *Let K be an algebraic number field and $\zeta_K(z)$ the Dedekind zeta function of K.*

1. *(Analytic continuation) The function $\zeta_K(z)$ can be extended to a meromorphic function on the whole complex plane.*
2. *(Functional equation) Let*
$$Z_K(z) = \big(\pi^{-z/2}\Gamma(z/2)\big)^r \cdot \big(2(2\pi)^{-z}\Gamma(z)\big)^s \cdot \zeta_K(z)$$
where r is the number of real embeddings of K, $2s$ is the number of complex embeddings of K, and Γ is the Gamma function. Then the function $Z_K(z)$ satisfies the functional equation
$$Z_K(z) = |d_K|^{1/2-z} \cdot Z_K(1-z)$$
where d_K is the discriminant of K.
3. *(Singularities) The only singularity of $\zeta_K(z)$ is a simple pole at $z = 1$ with residue*
$$\frac{2^r(2\pi)^s h_K \mathrm{Reg}_K}{|\mu_K|\sqrt{|d_K|}}.$$
where r is the number of real embeddings of K, $2s$ is the number of complex embeddings of K, h_k is the class number of K, Reg_K is the regulator of K, $|\mu_K|$ is the number of roots of unity in K, and d_K is the discriminant of K.

Proof. See for example [2, VII, §5]. □

The formula for the residue of $\zeta_K(z)$ at $z = 1$ is often called the *analytic class number formula*. It is not too difficult to prove this formula in the form

$$\lim_{z\to 1+}(z-1)\zeta_K(z) = \frac{2^r(2\pi)^s h_K \mathrm{Reg}_K}{|\mu_K|\sqrt{|d_K|}}.$$

where $z \to 1+$ means that the limit $z \to 1$ is taken over real numbers $z > 1$ (see [1, VIII, §2]). In certain cases (e.g. for quadratic fields or cyclotomic fields) one can write the Dedekind zeta function $\zeta_K(z)$ as a product of L-functions and evaluate these L-functions at $z = 1$, which then leads to more explicit class number formulas (see for example [1, VIII, §5 and §6], [3, Chapter 4]).

References

[1] A. Fröhlich, M.J. Taylor, *Algebraic number theory*, CUP, 1991.
[2] J. Neukirch, *Algebraic number theory*, Springer, 1999.
[3] L.C. Washington, *Introduction to cyclotomic fields*, 2nd edition, Springer, 1997.