5. Ideals of rings of integers.

This section deals with properties of ideals of rings of integers of number fields. We introduce the zeta function of a number field.

Proposition 5.1. *Let F be a number field and let I, J be non-zero ideals of its ring of integers O_F. Then*

$$N(IJ) = N(I)N(J).$$

Proof. By Theorem 4.6 it suffices to prove that

$$N(I\mathfrak{p}) = N(I)N(\mathfrak{p}).$$

for a non-zero prime ideal $\mathfrak{p}$ of O_F. From the exact sequence

$$0 \longrightarrow I/I\mathfrak{p} \longrightarrow O_F/I\mathfrak{p} \longrightarrow O_F/I \longrightarrow 0$$

we deduce that all we have to show, is that $\#(I/I\mathfrak{p}) = \#(O_F/\mathfrak{p})$. The group $I/I\mathfrak{p}$ is a vector space over the field $k = O_F/\mathfrak{p}$. Theorem 4.6 implies $\mathfrak{p}I \neq I$. Therefore $I/I\mathfrak{p}$ is a non-zero vector space. Let W be a k-linear subspace of $I/I\mathfrak{p}$. The inverse image of W in O_F is an ideal J satisfying $I\mathfrak{p} \subset J \subset I$. By Theorem 4.6 we must have either $J = I\mathfrak{p}$ or $J = I$ and hence $W = 0$ or $W = I/I\mathfrak{p}$. So, apparently the vector space $I/I\mathfrak{p}$ has only trivial subspaces. It follows that its dimension is one. This proves the proposition.

We extend the norm to fractional ideals by defining a group homomorphism $N : \mathrm{Id}_F \longrightarrow \mathbf{Q}^*_{>0}$ as follows. Let I be a fractional ideal and let $\alpha \in F^*$ an element for which αI is an ideal of O_F. Then we put $N(I) = N(J)/|N(\alpha)|$. It follows from Prop. 5.1 that the norm is well defined and satisfies $N(II') = N(I)N(I)$ for any two fractional ideals I, I' of F.

The next proposition is a very useful application of the multiplicativity of the norm map.

Proposition 5.2. *Let F be a number field of degree n.*

(a) For every ideal $\mathfrak{p}$ of O_F there exists a prime number p such that $\mathfrak{p}$ divides p. The norm of $\mathfrak{p}$ is a power of p.

(b) Let $\mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_g^{e_g}$ be the prime decomposition of the ideal generated by p in O_F. Then

$$\sum_{i=1}^{g} e_i f_i = n$$

where for every i the number f_i is defined by $N(\mathfrak{p}_i) = p^{f_i}$.

(c) For every prime number p there are at most n distinct prime ideals of O_F dividing p.

(d) There are only finitely many ideals with bounded norm.

Proof. *(a)* Let $\mathfrak{p}$ be a prime ideal. By Prop. 3.9 there exists an integer $m \neq 0$ in $\mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal, it follows that $\mathfrak{p}$ contains a prime number p. This implies that $O_F/\mathfrak{p}$ is a finite field of characteristic p. Therefore $N(\mathfrak{p})$ is a power of p.

(b) This follows at once from the multiplicativity of the norm, by taking the norm of the prime decomposition of (p) in O_F.
(c) This is immediate from *(b)*.
(d) This follows from Theorem 4.6 and *(c)*.

The numbers f_i and e_i are called the inertia and ramification index respectively, of the prime ideal $\mathfrak{p}_i$. If for a prime p and a number field F of degree n one has that $e_i = f_i = 1$ for all g primes $\mathfrak{p}_i$ that divide p we say that p *is totally split in* F. In this case there are n different prime ideals dividing p. They all have norm p. If $g = 1$, there is only one prime ideal $\mathfrak{p}_1$ dividing p. If, in this case $f_1 = 1$, we say that p is *totally ramified* in F over $\mathbf{Q}$. If, on the other hand, $e_1 = 1$, the prime p is *inert*. That means that it "remains" prime, in the sense that (p) is also a prime ideal in O_F.

Example 5.3. Let $F = \mathbf{Q}(\sqrt{-5})$. By Prop. 3.3 the ring of integers of F is equal to $\mathbf{Z}[\sqrt{-5}]$. We factor some small prime numbers into prime ideals. The prime ideals $\mathfrak{p}$ of O_F that divide a prime p are precisely the ones that contain p. They are in one to one correspondence with the prime ideals of the quotient ring $O_F/(p)$. Indeed, the map that sends $\mathfrak{p}$ to its image in $O_F/(p)$ is a bijection.

First we study the prime 2. We have

$$O_F/(2) = \mathbf{Z}[\sqrt{-5}]/(2) = \mathbf{Z}[T]/(2, T^2 + 5) \cong \mathbf{F}_2[T]/(T^2 + 1).$$

The prime ideals of the ring $\mathbf{F}_2[T]/(T^2 + 1)$ are in one to one correspoendence with the monic irreducible divisors of $T^2 + 1$ in the principal ideal domain $\mathbf{F}_2[T]$. Since we have $T^2 + 1 = (T + 1)^2$ in $\mathbf{F}_2[T]$, there is only one irreducible divisor and hence only one prime ideal. The divisor is $T + 1$ and the corresponding prime ideal in O_F is computed by unraveling the various ring isomorphisms. Since the variable T is mapped to $\sqrt{-5} \in O_F$, the prime ideal is $\mathfrak{p}_2 = (2, \sqrt{-5})$. The equality $\mathfrak{p}_2^2 = (2)$ is easily checked. This is the decomposition of (2). The prime number 2 is ramified in F.

Next consider the ideal (3) in O_F. We have

$$O_F/(3) = \mathbf{Z}[\sqrt{-5}]/(3) = \mathbf{Z}[T]/(3, T^2 + 5) \cong \mathbf{F}_3[T]/(T^2 - 1).$$

Since the polynomial $T^2 - 1$ factors as $(T_1)(T + 1)$ in $\mathbf{F}_3[T]$, there are precisely two *distinct* irreducible divisors of $T^2 - 1$. The divisors are $T + 1$ and $T - 1$. The corresponding prime ideals in O_F are $\mathfrak{p}_3 = (3, \sqrt{-5} + 1)$ and $\mathfrak{p}_3' = (3, \sqrt{-5} - 1)$. The equality $\mathfrak{p}_3\mathfrak{p}_3' = (3)$ is easily checked. This is the decomposition of (3). The prime number 3 splits in F.

One checks that 7 decomposes in a way similar to 3. The prime number 11 remains prime since $O_F/(11) \cong \mathbf{F}_{11}[T]/(T^2 + 5)$ is a field of 11^2 elements. The decomposition of the prime numbers ≤ 11 is given in the following table:

Table 5.4.

p	(p)	
2	$\mathfrak{p}_2^2$	$\mathfrak{p}_2 = (2, 1 + \sqrt{-5})$
3	$\mathfrak{p}_3\mathfrak{p}_3'$	$\mathfrak{p}_3 = (3, 1 + \sqrt{-5})$ and $\mathfrak{p}_3' = (3, 1 - \sqrt{-5})$
5	$\mathfrak{p}_5^2$	$\mathfrak{p}_5 = (\sqrt{-5})$
7	$\mathfrak{p}_7\mathfrak{p}_7'$	$\mathfrak{p}_7 = (7, 3 + \sqrt{-5})$ and $\mathfrak{p}_7' = (7, -3 + \sqrt{-5})$
11	(11)	11 is inert.

The number 6 has in the ring $\mathbf{Z}[\sqrt{-5}]$ two distinct factorizations into irreducible elements:

$$\begin{aligned} 6 &= 2 \cdot 3, \\ &= (1+\sqrt{-5})(1-\sqrt{-5}). \end{aligned}$$

The factors 2, 3 and $1 \pm \sqrt{-5}$ are all irreducible. Indeed, have norms 4, 9 or 6 respectively. Proper divisors $a + b\sqrt{-5}$ with $a, b \in \mathbf{Z}$ would necessarily have norms 2 or 3. But this is impossible because the Diophantine equations $a^2 + 5b^2 = 2$ and $a^2 + 5b^2 = 3$ clearly do not have any solutions $a, b \in \mathbf{Z}$. There exists, however, a unique factorization of the ideal (6) into a product of *prime ideals*. These prime factors are non-principal ideals. The factorization refines the two factorizations above:

$$(6) = \mathfrak{p}^2 \mathfrak{p}_3 \mathfrak{p}_3'.$$

Indeed, one has that $\mathfrak{p}_2\mathfrak{p}_3 = (1+\sqrt{-5})$ and $\mathfrak{p}_2\mathfrak{p}_3' = (1-\sqrt{-5})$.

Finally we will apply Theorem 4.6 and Proposition 5.1 to the ζ-function $\zeta_F(s)$ of a number field F. First we consider the ζ-function of Riemann:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad \text{for } s \in \mathbf{C},\ \mathrm{Re}(s) > 1.$$

This series is absolutely convergent. L. Euler (Swiss mathematician who lived and worked in Berlin and St. Petersburg 1707–1783) found an expression for $\zeta(s)$ in terms of an infinite product:

$$\zeta(s) = \prod_{p \text{ prime}} (1 - \frac{1}{p^s})^{-1} \qquad \text{for } s \in \mathbf{C},\ \mathrm{Re}(s) > 1\ .$$

This implies at once that $\zeta(s)$ does not have any zeroes in $\mathbf{C}$ with real part larger than 1. The proof of Euler's formula is as follows: let $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$. We have the following converging geometric series.

$$(1 - \frac{1}{p^s})^{-1} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \dots$$

Since every positive integer can be written as a product of primes *in a unique way*, we find that for every $X \in \mathbf{R}_{>0}$

$$\prod_{p \le X} (1 - \frac{1}{p^s})^{-1} = \sum_{n} \frac{1}{n^s}$$

where n runs over the positive integers that have only prime factors less than X. Therefore we have

$$|\sum_{n=1}^{\infty} \frac{1}{n^s} - \prod_{p \le X} (1 - \frac{1}{p^s})^{-1}| \le \sum_{n > X} \frac{1}{n^{\mathrm{Re}(s)}}.$$

Since the series $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converges absolutely, the right hand side tends to 0 as $X \to \infty$. The shows that the Riemann zeta function admits a so-called *Euler product*.

Definition 5.5. *Let F be a number field. The Dedekind ζ-function $\zeta_F(s)$ is given by*

$$\zeta_F(s) = \sum_{I \neq 0} \frac{1}{N(I)^s}$$

where I runs over the non-zero ideals of O_F.

The definition makes sense, because there are only finitely many ideals I of a given norm. For $F = \mathbf{Q}$ the Dedekind ζ-function $\zeta_{\mathbf{Q}}(s)$ is just Riemann's ζ-function. In the next proposition we show that $\zeta_F(s)$, like the Riemann zeta function, admits an Euler product. We use it to prove convergence of the series $\sum_{I \neq 0} \frac{1}{N(I)^s}$ for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$.

Proposition 5.6. *Let F be a number field. Then we have*

$$\zeta_F(s) = \sum_{I \neq 0} \frac{1}{N(I)^s} = \prod_{\mathfrak{p}} (1 - \frac{1}{N(\mathfrak{p})^s})^{-1}$$

where I runs over the non-zero ideals of O_F and $\mathfrak{p}$ over the prime ideals of O_F. The sum and the product converge absolutely for $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$.

Proof. Let m be the degree of F and let $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$. By Prop. 5.2*(c)* there are at most m prime ideals dividing a fixed prime number p. Therefore

$$\sum_{N(\mathfrak{p}) \leq X} |\frac{1}{N(\mathfrak{p})^s}| \leq m \sum_{p \leq X} \frac{1}{p^{\mathrm{Re}(s)}} \leq m \sum_{n \leq X} \frac{1}{n^{\mathrm{Re}(s)}}$$

where $\mathfrak{p}$ runs over the primes of O_F of norm at most X, where p runs over the prime numbers at most X and where n runs over the integers $\leq X$. Since the rightmost sum converges absolutely, so does the leftmost one. Hence, by Exercise 5.1 the product

$$\prod_{\mathfrak{p}} (1 - \frac{1}{N(\mathfrak{p})^s})^{-1}$$

converges absolutely. By Theorem 4.6 the ideals I admit a unique factorization as a product of prime ideals. By Proposition 5.1 the norm is multiplicative. For $\sigma \in \mathbf{R}_{>1}$ this implies the inequality

$$\sum_{N(I) \leq X} \frac{1}{N(I)^\sigma} \leq \prod_{\mathfrak{p}} (1 - \frac{1}{N(\mathfrak{p})^\sigma})^{-1}.$$

Since the terms $\frac{1}{N(I)^\sigma}$ are positive, the sum converges. In particular $\sum_{N(I) > X} \frac{1}{N(I)^\sigma}$ tends to zero as $X \to \infty$.

For $s \in \mathbf{C}$ with $\mathrm{Re}(s) > 1$ we have

$$|\sum_{I \neq 0} \frac{1}{N(I)^s} - \prod_{N(\mathfrak{p}) \leq X} (1 - \frac{1}{N(\mathfrak{p})^s})^{-1}| = |\sum_{\substack{I \text{ prime to } \mathfrak{p} \\ \text{if } N(\mathfrak{p}) \leq X}} \frac{1}{N(I)^s}| \leq \sum_{N(I) > X} \frac{1}{N(I)^{\mathrm{Re}(s)}},$$

which we just saw, tends to zero as $X \to \infty$. This concludes the proof.

Corollary 5.7. *Let F be a number field. The zeta function of F does not vanish on the right half plane $\{s \in \mathbf{C} : \mathrm{Re}(s) > 1\}$.*

Proof. Indeed, the Euler product converges.

Exercises.

5.1 Let $a_k \in \mathbf{C}$ for $k = 1, 2, \ldots$. Show that the series $\sum_k a_k$ converges absolutely if and only if the product $\prod_k (1 + a_k)$ converges absolutely.

5.2 Show that the ideal $I = (2, 2i) \subset \mathbf{Z}[2i]$ is not invertible, i.e. show $I^{-1}I \neq R$. Show also that $N(I^2) \neq N(I)^2$.

5.3 Show that $\mathbf{Q}^*_{>0}$ and the additive group of the ring $\mathbf{Z}[T]$ are isomorphic as abelian groups.

5.4 Let F be a number field of degree n. Show that for every $q \in \mathbf{Q}^*$, the fractional ideal generated by q has norm q^n.

5.5 Let F be a number field and let I be a fractional ideal of F. Show that there is a positive integer m such that mI is an ideal.

5.6 Let $F = \mathbf{Q}(\sqrt{-6})$.
- (a) Show that O_F is equal to $\mathbf{Z}[\sqrt{-6}]$.
- (b) Show that $6 = 2 \cdot 3 = -\sqrt{-6}^2$ are two factorizations of 6 into products of irreducible elements of O_F.
- (c) Show that $\mathfrak{p} = (2, \sqrt{-6})$ is a prime ideal of norm 2. Show that $\mathfrak{p}^2 = (2)$.
- (d) Show that $\mathfrak{q} = (3, \sqrt{-6})$ is a prime ideal of norm 3. Show that $\mathfrak{q}^2 = (3)$.
- (e) Factor the ideal (6) into a product of prime ideals. Show that $\sqrt{-6})$ is equal to $\mathfrak{pq}$.

5.7 Let $F = \mathbf{Q}(\sqrt{-23})$.
- (a) Show that O_F is equal to $\mathbf{Z}[\alpha]$ with $\alpha^2 - \alpha + 6 = 0$.
- (b) Show that $\mathfrak{p} = (2, \alpha)$ is a prime ideal of norm 2.
- (c) Show that $\mathfrak{p}$ is not princiapl, but $\mathfrak{p}^3$ is.

5.8 Let $F = \mathbf{Q}(\sqrt{10})$.
- (a) Show that O_F is equal to $\mathbf{Z}[\sqrt{10}]$.
- (b) Show that $\mathfrak{p} = (2, \sqrt{10})$ is a prime ideal of norm 2. Show that $\mathfrak{p}^2 = (2)$.
- (c) Show that $\mathfrak{p}$ is not principal. (Hint. there are no elements in O_F with norm ± 2)

5.9
- (a) Show that the ring of integers of $\mathbf{Q}(i)$ is $\mathbf{Z}[i]$.
- (b) Show that $\mathbf{Z}[i]$ is a Euclidean domain and hence a PID.
- (c) Factor the prime numbers p into products of prime ideal in $\mathbf{Z}[i]$ and show

$$\begin{aligned} (2) &= (1+i)^2, \\ (p) &= (p), \qquad \text{if } p \equiv 3 \pmod 4; \\ (p) &= (\pi)(\overline{\pi}), \quad \text{if } p \equiv 1 \pmod 4. \end{aligned}$$

In the case $p \equiv 1 \pmod 4$ we have $\pi = a + bi$ with $a, b \in \mathbf{Z}$ satisfying $a^2 + b^2 = p$.

(d) Show that the zeta function of $\mathbf{Q}(i)$ is given by

$$\zeta_{\mathbf{Q}(i)}(s) = \left(1 - \frac{1}{2^s}\right)^{-1} \prod_{p \equiv 1 \pmod 4} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{p \equiv 3 \pmod 4} \left(1 - \frac{1}{p^{2s}}\right)^{-1}.$$

5.10 Let F be a number field. For a non-zero ideal $I \subset O_F$ we put $\Phi(I) = \#(O_F/I)^*$.

(a) Show that $\sum_{I \subset J \subset R} \Phi(J) = N(I)$.

(b) Show that

$$\Phi(I) = N(I) \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-1}).$$

Here the product runs over the prime ideals $\mathfrak{p}$ with $I \subset \mathfrak{p} \subset R$.