8. Algebraic numbers: Dedekind domains

Let us recap some ring-theoretic concepts. A proper ideal J of a ring R is *maximal* if, for any other ideal J' of R, $J \subset J'$ and $J \neq J'$ implies $J' = R$ (equivalently the factor ring R/J is a field), and *prime* if, for all $a, b \in R$, $ab \in J$ implies $a \in J$ or $b \in J$ (equivalently, the factor ring R/J has no zero divisors).
Let us summarise now the properties of rings of integers of algebraic number fields.

Theorem 8.27. *The ring of integers D of an algebraic number field F has the following properties:*

(a) *It is a domain and F is its field of fractions, that is every element in F is representable as a fraction $a^{-1}b$, where $a, b \in D$.*
(b) *It is noetherian.*
(c) *If $\alpha \in F$ satisfies a monic polynomial equation with coefficients in D, then $\alpha \in D$.*
(d) *Every non-zero prime ideal is maximal.*

Proof. (a) is obvious since for every $a \in F$ there exist $n \in \mathbb{Z}$ such that $na \in D$. (b) has been proved in the previous lecture (Corollary to Theorem 8.26). (c) can be proved repeating the proof of Theorem 8.10 word by word. (d) follows from Theorem 8.26. Indeed, if J is a prime ideal in D, then by Theorem 8.26 it has finite index which means that the quotient ring D/J is a finite domain. However any finite domain is a field. □

Exercise 8.13 *Prove that any finite commutative ring without zero divisors is a field.*

Any ring with properties (a) - (d) of Theorem 8.27 is called a Dedekind ring after a German mathematician Richard Dedekind.

Let D be the ring of algebraic integers in an algebraic number field F. The reason for the lack of unique factorisation in D is related to the fact that if p is a prime in D, the ideal (p) need not be a prime ideal.

The *product* of two ideals $I, J \subset D$ is the ideal $IJ = \{\sum_i \alpha_i\beta_i |\ \alpha_i \in I,\ \beta_i \in J\}$.

Exercise 8.14 *In $D = \mathbb{Z}(\sqrt{-5})$, the number 21 has two prime factorisations: $(1+2\sqrt{-5})(1-2\sqrt{-5})$ and $3 \cdot 7$. Consider the ideals $\pi_1 = (3, -1-\sqrt{-5})$, $\pi_2 = (3, -2-\sqrt{-5})$, $\pi_3 = (7, -3-\sqrt{-5})$, and $\pi_4 = (7, -4-\sqrt{-5})$. Show that $(3) = \pi_1\pi_2$, $(7) = \pi_3\pi_4$, $(1+2\sqrt{-5}) = \pi_1\pi_3$, and $(1-2\sqrt{-5}) = \pi_2\pi_4$. Further, show that π_1, π_2, π_3 and π_4 are prime ideals and that $(21) = \pi_1\pi_2\pi_3\pi_4$ is the unique prime factorisation in the ring of ideals of D.*

The moral of this example is clear. If we wish to factorise the principal ideal (x) in D, then we may get a unique factorisation $(x) = I_1 \dots I_n$, but the ideals $I_1, \dots, I_n$ may not be principal.

Theorem 8.28. *Every non-zero ideal of a Dedekind ring D can be written as a product of prime ideals, uniquely up to the order of the factors.*

Proof. We shall prove this theorem in a series of steps.

(i) Let J be a proper ideal of D. Then there exist prime ideals $\pi_1, \ldots, \pi_r$ such that $\pi_1 \cdots \pi_r \subseteq J$.

Proof. Suppose not. Since D is noetherian (Theorem 8.26) we may choose a maximal ideal I subject to non-existence of such $\pi_1, \ldots, \pi_r$. Then I is not prime (otherwise we could take $r = 1$ and $\pi_1 = I$) and there exist ideals I_1 and I_2 in D, strictly containing I, such that $I_1 I_2 \subseteq I$. By maximality of I there exist prime ideals $\pi_1, \ldots, \pi_s, \pi_{s+1}, \ldots, \pi_r$ such that

$$\pi_1 \cdots \pi_s \subseteq I_1, \qquad \pi_{s+1} \cdots \pi_r \subseteq I_2.$$

Hence

$$\pi_1 \cdots \pi_r \subseteq I_1 I_2 \subseteq I$$

contrary to the choice of I. □

(ii) If I is a non-zero ideal in D and S is any subset of F, then $IS \subseteq I$ implies $S \subseteq D$.

Proof. Follows from Proposition 8.25. □

Let I be any ideal of D. Define $I^{-1} = \{x \in F \mid xI \subseteq D\}$. Obviously $I^{-1} \supseteq D$, II^{-1} is contained in D and is an ideal of D.

(iii) Let π be a maximal ideal of D, then π^{-1} strictly contains D.

Proof. We must find a non-integer in π^{-1}. We start with any $0 \neq a \in \pi$. Using (i) we choose the smallest integer r such that $\pi_1 \cdots \pi_r \subseteq (a)$ for prime ideals $\pi_1, \ldots, \pi_r$. Since $(a) \subseteq \pi$ and π is prime (maximal implies prime) $\pi_i \subseteq \pi$ for some i. Hence $\pi_i = \pi$ since prime ideals are maximal. Without loss of generality we consider $i = 1$. By minimality of r, we have $\pi_2 \cdots \pi_r \not\subseteq (a)$ and we can find $b \in \pi_2 \cdots \pi_r \setminus (a)$. But $b\pi \subseteq (a)$, hence $ba^{-1}\pi \subseteq D$ and $ba^{-1} \in \pi^{-1}$. But $b \notin aD$ and so $ba^{-1} \notin D$, whence $\pi^{-1} \neq D$. □

(iv) Every non-zero ideal I in D is a product of prime ideals.

Proof. Suppose not, and choose an ideal maximal subject to the condition of not being a product of prime ideals. Then I is not a prime and $I \subset \pi$ for some maximal (hence prime) ideal π. Consider $J = I\pi^{-1}$. Then J is contained in D, is an ideal of D and strictly contains I due to (ii) and (iii). By the maximality of I, we conclude that $J = \pi_2 \cdots \pi_r$ for some prime ideals $\pi_2, \ldots, \pi_r$, whence $I = \pi_1 \pi_2 \cdots \pi_r$ for $\pi_1 = \pi$. □

(iv) Prime ideal factorisation is unique.

Proof. For two ideals I and J we will say that I divides J and write $I|J$ if $I \supseteq J$. Then the definition of prime ideal shows that, if π is prime and $\pi|IJ$, then $\pi|I$ or $\pi|J$. Suppose that

$$\pi_1 \cdots \pi_r = \rho_1 \cdots \rho_s$$

for prime ideals $\pi_1, \ldots, \pi_r$ and $\rho_1, \ldots, \rho_s$. Then π_i divides some ρ_i and $\pi_i = \rho_i$ by maximality of the latter. The proof finishes with an obvious induction. □