Lecture 2-19: Rings of integers in number fields

February 19, 2025

As promised last time, I now give an account of the ring analogues of number fields (finite extensions of $\mathbb{Q}$). Such rings are not necessarily PIDs, but both their structure and module theories are very close to the corresponding theories for PIDs. Rather than Dummit and Foote, I will be following the treatment in a pdf "Number Fields" based on lectures at Cambridge; I will send an electronic copy to all of you. All page references will be to this pdf, except those labelled DF.

Let K be a number field, that is, a finite extension of $\mathbb{Q}$.

Definition 1.2, p. 2

The *ring of integers of K*, denoted $\mathcal{O}_K$, consists of the algebraic integers in K (roots of monic polynomials with integer coefficients).

We have already seen that $\mathcal{O}_K$ is indeed a ring and that $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$. We have also seen that $\mathcal{O}_K$ is integrally closed in the sense that the only elements of K that are roots of monic polynomials with coefficients in $\mathcal{O}_K$ lie in $\mathcal{O}_K$, since such elements generate rings that are finitely generated as $\mathbb{Z}$-modules and so are algebraic integers. Moreover, if $\alpha \in K$, so that $\alpha^n + \sum_{i=0}^{n-1} q_i \alpha^i = 0$ for some $q_i \in \mathbb{Q}$, then for any $z \in \mathbb{Z}$ we have $(z\alpha)^n + \sum_{i=0}^{n-1} z^{n-i} q_i (z\alpha)^i = 0$; choosing z so as to clear all the denominators of the q_i, we see that $z\alpha \in \mathcal{O}_K$ for some nonzero $z \in \mathbb{Z}$ (Lemma 1.7, p. 3).

Setting $n = [K : \mathbb{Q}]$, it follows from the above that there is a $\mathbb{Q}$-basis $\alpha_1, \ldots, \alpha_n$ of K with $\alpha_i \in \mathcal{O}_K$ for all i. I will show below that $\mathbb{O}_K$ is a finitely generated $\mathbb{Z}$-module; from the classification of such modules, it follows that $\mathcal{O}_K$ admits a free $\mathbb{Z}$-basis that is also a $\mathbb{Q}$-basis of K. For the finite generation we need

Definition 2.3,p. 4

For $\alpha \in K$ the *trace* $T(\alpha)$ is the trace of multiplication m_α by α, regarded as a $\mathbb{Q}-$linear transformation from K to itself. The *norm* $N(\alpha)$ is the determinant of m_α.

Then we have

Corollary 2.6, p. 5

We have $T(\alpha)N,(\alpha) \in \mathbb{Z}$ if $\alpha \in \mathcal{O}_K$.

Indeed, by Gauss's Lemma, the minimal polynomial of α over $\mathbb{Q}$, which is the same as that of m_α, lies in $\mathbb{Z}[x]$. By the rational canonical form, the matrix of m_α is similar to one with integer entries, whence its trace and determinant lie in $\mathbb{Z}$. Clearly $T(\alpha+\beta) = T(\alpha) + T(\beta), N(\alpha\beta) = N(\alpha)N(\beta)$.

Proposition 3.8, p. 7

$\mathcal{O}_K$ is finitely generated over $\mathbb{Z}$.

Proof.

Let $\alpha_1, \ldots, \alpha_n$ be a basis of K with the $\alpha_i \in \mathcal{O}_K$. If $\alpha \in O_K$, then $T(\alpha\alpha_i) \in \mathbb{Z}$ for all i, since $\alpha\alpha_i \in \mathcal{O}_K$. Now the map sending $x, y \in K$ to $(x, y) = T(xy)$ is a nondegenerate bilinear form; that is, it is $\mathbb{Q}$-linear in each coordinate and the only $y \in K$ with $(x, y) = 0$ is $x = 0$ (in fact $(y^{-1}, y) = T(1) = n$ if $y \neq 0$). In particular the map $m : K \to \mathbb{Q}^n$ with $m(y) = ((\alpha_1, y), \ldots, (\alpha_n, y))$ has trivial kernel and range all of $\mathbb{Q}^n$, so that there is a “dual basis” $\beta_1, \ldots, \beta_n$ of K with $(\alpha_i, \beta_j) = \delta_{ij}$. But then the $\mathbb{Z}$-submodule of K consisting of all β with $\alpha_i\beta) \in \mathbb{Z}$ for all i is free on the β_i; since this submodule contains $A = \mathcal{O}_K$, A is a submodule of a finitely generated $\mathbb{Z}$-module and so is finitely generated. (The same argument shows that any ideal I of $\mathcal{O}_K$ is free and finitely generated over $\mathbb{Z}$.) □

Example

As a simple but surprisingly rich example, consider a quadratic extension $K = \mathbb{Q}[\sqrt{d}]$, where d is a square-free integer (having no nontrivial factor that is a square). The Galois group of K is cyclic of order 2; its nontrivial element is the conjugation map sending $a + b\sqrt{d}$ to $a - b\sqrt{d}$. Let's compute $R = \mathcal{O}_K$. To begin with, clearly $1, \sqrt{d} \in R$, whence $a + b\sqrt{d} \in \mathcal{R}$ if $a, b \in \mathbb{Z}$. Next, if $x = a + b\sqrt{d} \in R$, then $T(x) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a \in \mathbb{Z}$, so we must have $a \in \mathbb{Z}$ or $a \in \mathbb{Z} + \frac{1}{2}$. If $a \in \mathbb{Z}, x \in R$, then $x - a = b\sqrt{d} \in R$, whence $N(b\sqrt{d}) = b^2 d \in \mathbb{Z}, b \in \mathbb{Q}$. Since d is square-free, this forces $b \in \mathbb{Z}$. We are reduced to considering elements $x = a + b\sqrt{d}$ with $a = \frac{m}{2}, b = \frac{n}{2}$ and m, n odd, whence $m^2 \equiv n^2 \equiv 1 \bmod 4$. Then $N(x) = \frac{a^2 - db^2}{4} \in \mathbb{Z}$, forcing $d \equiv 1$ modulo 4. Conversely, if $d \equiv 1 \bmod 4$, then $T(x)$ and $N(x)$ are both integral and x is a root of a monic quadratic polynomial over $\mathbb{Z}$. The upshot is that $R = \mathcal{O}_K = \mathbb{Z}[\omega]$, where $\omega = \sqrt{d}$ if $d \not\equiv 1 \bmod 4$, while $\omega = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \bmod 4$. See Proposition 2.7 on p. 5.

Returning now to general rings $\mathcal{O}_K$, recall first that a proper ideal I of an arbitrary commutative ring R is called prime if $xy \in I$ if and only if $x \in I$ or $y \in I$, or equivalently the quotient ring R/I is an integral domain (DF, p. 255). The ideal I is maximal if it is not contained in any other proper ideal, or equivalently if and only if R/I is a field (DF, p. 254). Thus all maximal ideals are prime. In the case $R = \mathcal{O}_K$, any nonzero ideal I contains a nonzero element x, whence it also contains the nonzero integer $n = N(x)$, since this is up to sign the constant term of the characteristic polynomial of multiplication m_x by x, which lies in $\mathbb{Z}[x]$. Since R is finitely generated over $\mathbb{Z}$, it follows that both nR and I have finite index in R, whence R/I is finite. We define the norm $N(I)$ of I to be the index $[R : I]$ of I in R as an additive subgroup (Definition 3.14, p. 9).

An elementary fact from commutative ring theory is that a finite integral domain D is a field (DF, p, 228); this is clear, since if $a_1, \ldots, a_n$ are the elements of D and $b \in D, b \neq 0$, then the products ba_i are distinct and one of them must equal 1. If $R = \mathcal{O}_K$, then we know that any quotient R/I of R is finite. Thus if I is prime and nonzero, then it is maximal.

We have the following

Definition, DF p. 764

A *Dedekind domain* is an integrally closed integral domain such that every ideal is finitely generated and every nonzero prime ideal is maximal.

Proposition 14, DF p. 764

The ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind domain.

Proof.

Since $\mathcal{O}_K$ is a subring of a field and so an integral domain, it only remains to show that every ideal I of it is finitely generated; but this is clear since in fact I is finitely generated as a $\mathbb{Z}$-module (as noted above). □

I now turn to factorization of ideals in $R = \mathcal{O}_K$; this turns out to be substantially better behaved than factorization of elements in this ring. In fact factorization of ideals in R is completely parallel to factorization of elements in a PID, but without the complication of multiplicative units.

My goal is to show that any ideal in R is a product of prime ideals. I first prove a weak version of this.

Lemma 4.4, p. 11

Any nonzero ideal of R contains a product of nonzero prime ideals.

Suppose not and let I be a counterexample with $N(I)$ minimal; this is possible since $N(I)$ takes values in the positive integers. Then clearly I cannot be prime itself, nor can we have $I = R$, since R contains maximal prime ideals. Choose $a, b \in R, a, b \notin I$ with $ab \in I$. The ideals $I + (a), I + (b)$, being strictly larger than I and thus having smaller norm, must each contain a product of prime ideals, whence $(I + (a))(I + (b)) \subset I$ contains the product of these products, another product of prime ideals. This is a contradiction.

Now we bring in elements in elements of the field K but not in $\mathcal{O}_K$.

Lemma 4.5, p. 11

Let I be a nonzero ideal of R. Then there is $\gamma \in K, \gamma \notin R$, with $\gamma I \subset R$.

Proof.

Choose a nonzero $\alpha \in I$. The principal ideal (α) then contains a product $P_1 \dots P_r$ of nonzero prime ideals P_i; choose such a product with r minimal. Enlarge I to a maximal ideal P, which is prime. Then P contains the product $P_1 \dots P_r$, whence P contains one of the factors, say P_1, whence $P = P_1$. Then (α) does not contain the shorter product $P_2 \dots P_r$, whence there is $\beta \in P_2 \dots P_r, \beta \notin \alpha$. I claim that $\gamma = \beta/\alpha$ has the desired property. Indeed, if $\gamma \in R$, then $\beta = \alpha\gamma \in (\alpha)$, contradicting the choice of β, so γ lies in K but not in R. On the other hand, $\gamma I = \frac{\beta}{\alpha} I \subset \frac{1}{\alpha} P_2 \dots P_r I \subset \frac{1}{\alpha} P_1 \dots P_r \subset R$, as required. □

My aim is also to show that a suitable enlargement of the set of nonzero ideals of R is a group under multiplication. I will continue with this program next time.