Introduction to Algebraic Number Theory
Lecture 3

Andrei Jorza

2014-01-20

Today: more number rings; traces and norms. Textbook here is `http://wstein.org/books/ant/ant.pdf`

2 Number Rings (continued)

(2.1) We have shown that for a number field K the algebraic integers $\mathcal{O}_K$ form a ring.

Definition 1. An order is a subring $\mathcal{O} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{O}$ is finite. The ring of integers is said to be the maximal order.

Some examples later.

(2.2) Having shown that for a number field K the algebraic integers $\mathcal{O}_K$ form a ring we should answer some natural questions:

1. Is $\mathcal{O}_K$ torsion-free? Of course, since K is.
2. Is $\mathcal{O}_K$ a finite $\mathbb{Z}$-module? We know that every $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$ is finite over $\mathbb{Z}$ and the question is whether $\mathcal{O}_K$ is generated by finitely many algebraic integers.
3. A finite $\mathbb{Z}$-module is just a finitely generated abelian group and once we show that $\mathcal{O}_K$ is finite over $\mathbb{Z}$ and torsion-free we deduce that $\mathcal{O}_K \cong \mathbb{Z}^d$ for $d = \mathrm{rank}(\mathcal{O}_K)$. What is this rank?
4. Can we find generators for $\mathcal{O}_K$ as a $\mathbb{Z}$-module?

(2.3)

Example 2. If m is a square-free integer not equal to 1 then the ring of integers of $\mathbb{Q}(\sqrt{m})$ is $\mathbb{Z}[\sqrt{m}]$ when $m \equiv 2, 3 \pmod 4$ and $\mathbb{Z}[\frac{1+\sqrt{m}}{2}]$ when $m \equiv 1 \pmod 4$.

Proof. If $a + b\sqrt{m} \in \mathcal{O}_K$ then the minimal polynomial $X^2 - 2aX + a^2 - b^2 m \in \mathbb{Z}[X]$ and so $2a = p \in \mathbb{Z}$. Therefore $p^2 - (2b)^2 m \in 4\mathbb{Z}$ and so $(2b)^2 m$ is an integer. If $2b$ has a denominator, its square would divide the square-free m and so it would have to be 1. Thus $2b = q \in \mathbb{Z}$.

We have $p^2 \equiv q^2 m \pmod 4$. If $m \equiv 2, 3 \pmod 4$ then the only possibility is that p and q are both even as the squares mod 4 are only 0 and 1. This implies that $a, b \in \mathbb{Z}$ and so $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$.

If $m \equiv 1 \pmod 4$ then $p^2 \equiv q^2 \pmod 4$ and so p and q have the same parity is the only relevant condition. Noting that $\frac{1+\sqrt{m}}{2}$ has minimal polynomial $X^2 - X + \frac{1-m}{4} \in \mathbb{Z}[X]$ we deduce that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{m}}{2}]$. $\square$

(2.4)

Example 3. We have seen above that the ring of integers in $\mathbb{Q}(\sqrt{5})$ is $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ which contains the ring $\mathbb{Z}[\sqrt{5}]$. The quotient has order 2 since any integral element times 2 will be in $\mathbb{Z}[\sqrt{5}]$ and so $\mathbb{Z}[\sqrt{5}]$ is an order in the ring of integers.

(2.5) This example leads to a brief exploration of the general setup. If $A \subset B$ are integral domains then $\alpha \in B$ is said to be integral over A if it is the root of a monic polynomial in $A[X]$. The **integral closure** of A in B is the ring (!) of elements of B which are integral over A. (In this language $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K.) The ring A is said to be integrally closed in B (or simply integrally closed when B is taken to be $\operatorname{Frac} A$) if it is equal to its integral closure in B.

I gave examples in class in Sage (see the session outputs). For example we saw that $\mathbb{Z}[\sqrt{5}]$ was not integrally closed in $\mathbb{Q}(\sqrt{5})$ which we knew since the ring of integers is larger. Sage also gave us the integral closure of $\mathbb{Z}[\sqrt{5}]$ (implicitly in its fraction field $\mathbb{Q}(\sqrt{5})$ is the whole ring of integers.

That said, there is a geometric perspective on integral elements. Roughly speaking integrally closed rings have few singularities (in codimension 2) and the farther you are from being integrally closed the more singularities you introduce. Here is an explicitly geometric example: The ring $B = \mathbb{C}[t]$ is integrally closed in its fraction field (true of all polynomial rings over fields) and geometrically this ring represents a line. However, the ring $A = \mathbb{C}[t^2, t^3] \subset B = \mathbb{C}[t]$ is not integrally closed because the element $\alpha = t$ is the root of the minimal polynomial $X^2 - t^2 \in A[X]$ but $t \notin A$ as t cannot equal a polynomial of higher degree. What does A represent geometrically? Writing $x = t^2$ and $y = t^3$ produces the equation $y^2 = x^3$ and indeed A represents this cuspidal cubic curve which has a singularity at the origin.

3 Trace and Norm

(3.1)

Definition 4. If L/K is a finite extension and σ_i are the embeddings of L into $\overline{K}$ fixing K write

$$\operatorname{Tr}_{L/K}(x) = \sum \sigma_i(x)$$

and

$$N_{L/K}(x) = \prod \sigma_i(x)$$

Fact 5. The maps $\operatorname{Tr}_{L/K}, N_{L/K}$ have image in K. The trace map $\operatorname{Tr}_{L/K} : L \to K$ has the properties that $\operatorname{Tr}_{L/K}(x + y) = \operatorname{Tr}_{L/K}(x) + \operatorname{Tr}_{L/K}(y)$; if $c \in K$ then $\operatorname{Tr}_{L/K}(cx) = c \operatorname{Tr}_{L/K}(x)$; $\operatorname{Tr}_{L/K}(1) = [L : K]$. The norm map $N_{L/K} : L \to K$ has the property that $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$.

See textbook §2.4.

Example 6. If $K = \mathbb{Q}(\sqrt{m})$ then there are exactly two embeddings of K into $\overline{\mathbb{Q}}$ fixing $\mathbb{Q}$, namely $a+b\sqrt{m} \mapsto a \pm b\sqrt{m}$. Thus $\operatorname{Tr}_{K/\mathbb{Q}}(a + b\sqrt{m}) = 2a$ and $N_{K/\mathbb{Q}}(a + b\sqrt{m}) = a^2 - b^2 m$.

(3.2)

Proposition 7. *If L/K are number fields then* $\operatorname{Tr}_{L/K}, N_{L/K} : \mathcal{O}_L \to \mathcal{O}_K$.

Proof. If α is the root of the monic polynomial $P \in \mathbb{Z}[X]$ and σ is an embedding of L into $\overline{K}$ fixing $K \supset \mathbb{Z}$ it follows that $P(\sigma(\alpha)) = \sigma(P(\alpha)) = \sigma(0) = 0$ and so $\sigma(\alpha)$ is also an algebraic integer. Thus $\operatorname{Tr}_{L/K}(\alpha)$ and $N_{L/K}(\alpha)$ are algebraic integers in K and thus are elements of $\mathcal{O}_K$. $\square$