Introduction to Algebraic Number Theory
Lecture 5

Andrei Jorza

2014-01-24

Today: traces and norms, discriminants and integral bases. Textbook here is `http://wstein.org/books/ant/ant.pdf`

3 Trace and Norm (continued)

(3.8)

Proposition 1. *Let $p > 2$ be prime. Then the ring of integers of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}[\zeta_p]$. In fact for any positive integer n the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$.*

Proof. Only did in class the case of p prime. First, note that $\mathbb{Z}[\zeta_p] = \mathbb{Z}[1-\zeta_p]$ as a basis of the LHS over $\mathbb{Z}$ is $1, \zeta_p, \dots, \zeta_{p-2}$ while of the RHS is $1, 1-\zeta_p, (1-\zeta_p)^2, \dots, (1-\zeta_p)^{p-2}$ and it's clear one can go from the LHS basis to the RHS basis using a lower-triangular matrix with 1-s on the diagonal. This matrix is then invertible in $\mathrm{GL}(p-1, \mathbb{Z})$ and so the two bases are equivalent.

From one of the problems on problem set 1 you computed that ($K = \mathbb{Q}(\zeta_p)$)

$$\mathrm{disc}_{K/\mathbb{Q}}(1, \zeta_p, \dots, \zeta_p^{p-2}) = (-1)^{(p-1)/2} p^{p-2}$$

But this discriminant (as shown in class) is independent of a $\mathbb{Z}$-basis and so it is also equal to $D = \mathrm{disc}_{K/\mathbb{Q}}(1, 1-\zeta_p, (1-\zeta_p)^2, \dots, (1-\zeta_p)^{p-2})$.

We have show in class that if $\alpha = a_0 + a_1(1-\zeta_p) + \cdots + a_{p-2}(1-\zeta_p)^{p-2} \in \mathcal{O}_K$ then $Da_i \in \mathbb{Z}$ and so we may write

$$\alpha = \frac{m_0 + m_1(1-\zeta_p) + \cdots + m_{p-2}(1-\zeta_p)^{p-2}}{p^{p-2}} \in \mathcal{O}_K$$

If $\alpha \notin \mathbb{Z}[\zeta_p] = \mathbb{Z}[1-\zeta_p]$ then the coefficients m_i are not all divisible by p^{p-2}. In fact we may cancel out any common factor of p among the m_i and write

$$\alpha = \frac{m_0 + m_1(1-\zeta_p) + \cdots + m_{p-2}(1-\zeta_p)^{p-2}}{p^k}$$

where not all m_0 are divisible by p and $k \le p-2$. Let i be the smallest index such that $p \nmid m_i$. Then

$$\beta = p^{a-1}\alpha - \frac{m_0 + m_1(1-\zeta_p) + \cdots + m_{i-1}(1-\zeta_p)^{i-1}}{p} = \frac{m_i(1-\zeta_p)^i + \cdots + m_{p-2}(1-\zeta_p)^{p-2}}{p}$$

is also in $\mathcal{O}_K$ since $\mathbb{Z}[\zeta_p] \subset \mathcal{O}_K$.

Note that $N_{K/\mathbb{Q}}(1-\zeta_p) = (1-\zeta_p)(1-\zeta_p^2)\cdots(1-\zeta_p^{p-1}) = 1^{p-1} + 1^{p-2} + \cdots + 1 + 1 = p$. Since $1-\zeta_p \mid 1-\zeta_p^i$ (here $a \mid b$ means $b/a \in \mathcal{O}_K$) it follows that $(1-\zeta_p)^{p-1} \mid p$. Now

$$p\beta = m_i(1-\zeta_p)^i + \cdots + m_{p-2}(1-\zeta_p)^{p-2}$$

in $\mathcal{O}_K$. If $i < p-2$ then note that $(1-\zeta_p)^{i+1} \mid (1-\zeta_p)^{p-2} \mid p$ and so we deduce that $1-\zeta_p \mid m_i$. But $1-\zeta_p \mid p$ and since $p \nmid m_i$ it follows that we can find $u, v \in \mathbb{Z}$ such that $m_i a + pb = 1$ which would imply that $1-\zeta_p \mid 1$. But then $1/(1-\zeta_p) \in \mathcal{O}_K$ which is impossible because then $N_{K/\mathbb{Q}}(1/(1-\zeta_p)) = 1/p$ would be an integer. Thus we get a contradiction. If $i = p-2$ then $p\beta = m_{p-2}(1-\zeta_p)^{p-2}$ which would imply that $1-\zeta_p \mid m_{p-2}$ yielding a contradiction as before.

The conclusion is that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ as desired. □

4 Unique factorizations in Dedekind domains

(4.1)

Definition 2. A ring R is said to be noetherian if every increasing chain of ideals $I_1 \subset I_2 \subset \dots$ stabilizes, i.e., $I_n = I_{n+1} = \cdots$ for $n >> 0$. A module M/R is noetherian if every chain of R-submodules $M_1 \subset M_2 \subset \dots$ stabilizes.

Example 3. $\mathbb{Z}$, $F[X]$ are noetherian because ideals are principal. The ring $\overline{\mathbb{Z}}$ is not noetherian because $(2) \subset (2^{1/2}) \subset (2^{1/4}) \subset \dots$ doesn't stabilize.

Fact 4.

1. Quotients of noetherian rings are noetherian.
2. (Hilbert basis theorem) If R is noetherian then $R[X_1, \dots, X_n]$ is noetherian.
3. The noetherian modules over a noetherian ring are precisely the finitely generated ones.

Remark 1. The main use of the noetherian condition is the following. Suppose $\mathcal{P}$ is a set of ideals (defined, say, by having a certain property). If R is noetherian then every ideal in $\mathcal{P}$ is contained in an ideal in $\mathcal{P}$ which is maximal in $\mathcal{P}$, i.e., it is not contained in any bigger ideal in $\mathcal{P}$. Indeed, if $I_1 \subset I_2 \subset \dots$ is a chain of ideals in $\mathcal{P}$ then it stabilizes and the "limit" is necessarily in $\mathcal{P}$. Thus Zorn's lemma implies that every ideal is contained in an ideal of $\mathcal{P}$ which is maximal. We will use this many times.

(4.2)

Definition 5. If R is an integral domain and K is its fraction field, a **fractional ideal** of R is a finitely generated R-submodule of K.

Note that finite generation implies that if I is a fractional ideal then there exists $\alpha \in R$ such that $\alpha I \subset R$, i.e., is an ideal of R.

Example 6. $\frac{m}{n}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$. Similarly $\frac{P(X)}{Q(X)}F[X]$ is a fractional ideal of $F[X]$ where F is any field.

Definition 7. We define a multiplication law on fractional ideals given by $IJ = \{\sum x_i y_i | x_i \in I, y_i \in J\}$. Note that $IR = I$ for every fractional ideal I of R. With respect to this multiplication and unit a fractional ideal I is invertible if there exists a fractional ideal I^{-1} such that $II^{-1} = R$.

For example $(\frac{m}{n}\mathbb{Z})^{-1} = \frac{n}{m}\mathbb{Z}$.

(4.3)

Definition 8. An integral domain R is said to be a Dedekind domain if

1. R is noetherian
2. R is integrally closed (i.e., in its fraction field K)
3. Every prime ideal of R is maximal.

Example 9. $\mathbb{Z}$ and $\mathbb{F}_p[X]$ are Dedekind domains. The algebraic integers $\overline{\mathbb{Z}}$ is not because it is not noetherian. The ring $\mathbb{Z}[\sqrt{5}]$ is not because it is not integrally closed. The ring $\mathbb{Z}[X]$ is noetherian and integrally closed but the prime ideal (X) is not maximal because $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ is an integral domain which is not a field. Thus $\mathbb{Z}[X]$ is not a Dedekind domain.