Introduction to Algebraic Number Theory
Lecture 4

Andrei Jorza

2014-01-22

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

3 Trace and Norm (continued)

(3.3)

Proposition 1. *If $M/L/K$ are number fields then $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L}$ and $N_{M/K} = N_{L/K} \circ N_{M/L}$.*

Proof. Done in class. See textbook Corollary 2.4.4. □

(3.4) The trace pairing. Define $(\cdot,\cdot)_{L/K} : L \times L \to K$ by $(x,y)_{L/K} = \mathrm{Tr}_{L/K}(xy)$. It is a K-bilinear form.

Proposition 2. *The trace pairing is nondegenerate, i.e., if $(x,y) = 0$ for all y then $x = 0$.*

Proof. Too short to give reference. If $x \neq 0$ then $(x, x^{-1})_{L/K} = \mathrm{Tr}_{L/K}(1) = [L:K] \neq 0$ as number fields have characteristic 0. □

(3.5) Discriminants.

Definition 3. Suppose L/K is a finite extension of fields. If $\alpha_1, \ldots, \alpha_n \in L$ define

$$\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) = \det((\alpha_i, \alpha_j)_{L/K})_{i,j} \in K$$

Proposition 4. *Suppose $[L:K] = n$. Then*

1. $\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) = \det(\sigma_i(\alpha_j))_{i,j}^2$ *where $\sigma_1, \ldots, \sigma_n$ are the embeddings $L \to \overline{K}$ fixing K.*
2. $\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) \neq 0$ *if and only if $\alpha_1, \ldots, \alpha_n$ form a basis of L/K.*
3. *If $\alpha_i \in \mathcal{O}_L$ then $\mathrm{disc}_{L/K}(\alpha_1, \ldots, \alpha_n) \in \mathcal{O}_K$.*

Proof. Done in class. For part (i) see textbook the first paragraph of §6.2. Part (ii) follows from the fact that the trace pairing is nondegenerate, again at the beginning of §6.2 in the textbook. Finally, if $\alpha_i \in \mathcal{O}_L$ then $(\alpha_i, \alpha_j)_{L/K} \in \mathcal{O}_K$ and so the discriminant is in $\mathcal{O}_K$ since it is the determinant of a matrix with coefficients in $\mathcal{O}_K$. □

(3.6) Integral bases. First, recollections on finitely generated abelian groups. If A is a finitely generated abelian group then

$$A \cong \mathbb{Z}^d \oplus \bigoplus \mathbb{Z}/n_i\mathbb{Z}$$

and $d = \mathrm{rank}(A)$ is the rank of A. If B is a finitely generated abelian group and $A \subset B$ is a subgroup then A is also finitely generated and $\mathrm{rank}(A) \leq \mathrm{rank}(B)$.

Theorem 5. *Let K be a number field. The following statements are all equivalent and true:*

1. *$\mathcal{O}_K$ is a finite $\mathbb{Z}$-module of rank $[K:\mathbb{Q}]$.*
2. *$\mathcal{O}_K \subset K$ is a full lattice.*
3. *$\mathcal{O}_K = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$ where $n = [K:\mathbb{Q}]$. In that case $\alpha_1, \ldots, \alpha_n$ is said to be an* **integral basis**.

Proof. Part (ii) is by definition the same as part (i) while part (iii) is part (i) by the theory of finitely generated abelian groups. We will prove part (i).

Pick any basis $\beta_1, \ldots, \beta_n$ of $K/\mathbb{Q}$. Since for any $x \in K$ there exists $m \in \mathbb{Z}$ such that $xn \in \mathcal{O}_K$ (if $d_k x^k + d_{k-1}x^{k-1} + \cdots = 0$ then $(d_k x)^k + d_{k-1}(d_k x)^{k-1} + d_{k-2}d_k(d_k x)^{k-2} + \cdots = 0$ and so $d_k x \in \mathcal{O}_K$) we may rescale the β_i such that $\beta_i \in \mathcal{O}_K$.

Suppose $\alpha = \sum r_i\beta_i$ with $r_i \in \mathbb{Q}$. Then $(\alpha, \beta_j)_{K/\mathbb{Q}} = \sum r_i(\beta_i, \beta_j)_{K/\mathbb{Q}}$ which can be rewritten as a matrix multiplication $((\beta_i, \beta_j)_{K/\mathbb{Q}})_{i,j}(r_i) = ((\alpha, \beta_i)_{K/\mathbb{Q}})$. Solving using Cramer's rule shows that r_i is a ratio of a determinant of a matrix with coefficients in $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$ by $\det((\beta_i, \beta_j)_{K/\mathbb{Q}})_{i,j} = D = \operatorname{disc}_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)$. Thus $r_i \in \frac{1}{D}\mathbb{Z}$ which implies that

$$\mathcal{O}_K \subset \sum \frac{\beta_i}{D}\mathbb{Z}$$

and so $\mathcal{O}_K$ is a finitely generated abelian group with $\operatorname{rank}(\mathcal{O}_K) \leq [K:\mathbb{Q}]$. But at the same time

$$\sum \mathbb{Z}\beta_i \subset \mathcal{O}_K$$

and so $n \leq \operatorname{rank}(\mathcal{O}_K)$ and the theorem follows. □

(3.7) Discriminant of a number field.

Definition 6. Suppose K is a number field and $\alpha_1, \ldots, \alpha_n$ is an integral basis of $\mathcal{O}_K/\mathbb{Z}$. Define

$$\operatorname{disc}(K) = \operatorname{disc}(\mathcal{O}_K) = \operatorname{disc}_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)$$

Note that if $\beta_1, \ldots, \beta_n$ is another integral basis then there exists a matrix $B \in \mathrm{GL}(n, \mathbb{Z})$ such that $(\beta_i) = B(\alpha_i)$ and so

$$\operatorname{disc}(\beta_i) = \det(B)^2 \operatorname{disc}(\alpha_i)$$

Since $\det B = \pm 1 \in \mathbb{Z}^\times$ it follows that the above definition is independent of the chosen integral basis.

Example 7.
1. The discriminant of $\mathbb{Q}(\sqrt[m]{})$ is $4m$ if $m \equiv 2, 3 \pmod 4$ and m if $m \equiv 1 \pmod 4$.
2. If $m \equiv 1 \pmod 9$ then the discriminant of $\mathbb{Q}(\sqrt[3]{m})$ (see the first problem set for the ring of integers) is $-3m^2$. Also, see the Sage page on the website for Sage code proving this fact.