Algebraic Number Theory

Lecture 6, 12th November 2021

Last lecture: Let L/K be a field extension with $[L:K]=n$.

For an $x \in L$ define the K-linear map

$$T_x : L \longrightarrow L$$
$$\alpha \longmapsto x\alpha .$$

Then we define the <u>trace</u> and <u>norm</u> of x by

$$Tr_{L/K}(x) = Tr(T_x) \qquad N_{L/K}(x) = \det(T_x).$$

$$f_x(\lambda) = \det(\lambda\, id - T_x) = \lambda^n - a_1\lambda^{n-1} + \dots + (-1)^n a_n \in K[\lambda]$$

$$a_1 = Tr_{L/K}(x), \quad a_n = N_{L/K}(x).$$

<u>Example 3.5</u> $K=\mathbb{Q}$, $L=\mathbb{Q}(i)$ $n=2$

$B=\{1,i\}$ basis of L

$x=a+bi$ $\quad [T_x]_B = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ matrix of T_x with respect to B

$N_{L/K}(x) = \det[T_x]_B = a^2+b^2$

$Tr_{L/K}(x) = Tr(T_x) = 2a$

Proposition 3.6 Let L/K be a finite field extension with $\mathrm{char}(K)=0$ or $|K|<\infty$ and $[L:K]=n$.

If $\sigma_i : L \to \overline{K}$ for $i=1,\dots,n$ denote the n embeddings of L in $\overline{K}$, then

$$f_x(\lambda) = \prod_{i=1}^{n} \left(\lambda - \sigma_i(x)\right),$$

$$\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x),$$

$$N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x).$$

$x_i \in \overline{K}$

$$\prod_{i=1}^{m} (t - x_i)$$

Proof: Let $p_x(t) = t^m + c_1 t^{m-1} + \dots + c_m \in K[t]$ the minimal polynomial of x, i.e $[K(x):K]=m$.

Then $1, x, \dots, x^{m-1}$ is a basis of $K(x)/K$ and if $\alpha_1, \dots, \alpha_d$ is a basis of $L/K(x)$, then

$$B = \{\alpha_1, \alpha_1 x, \dots, \alpha_1 x^{m-1}, \dots, \alpha_d, \alpha_d x, \dots, \alpha_d x^{m-1}\}$$

is a basis of L/K.

Then the matrix of T_x with respect to this basis is

$$[T_x]_B = \begin{array}{c} \\ n \\ \\ \end{array}\begin{pmatrix} M & & \\ & \boxed{M} & \\ & & \ddots \\ & & & \boxed{M} \end{pmatrix} \qquad n = d \cdot m$$

$$\text{—} n \text{—}$$

where

$$M = \begin{pmatrix} 0 & & 0 & -c_m \\ 1 & \ddots & & -c_{m-1} \\ & 1 & \ddots & \vdots \\ 0 & & \ddots \; 0 & -c_1 \end{pmatrix}.$$

Since $\det(tE - M) = p_x(t)$ we get

$$f_x(t) = \det([T_x]_B - tE) = p_x(t)^d.$$

We have n embeddings $\sigma \in \mathrm{Hom}_K(L, \overline{K})$, which can be divided into m classes of size d by the equivalence relation $\sigma \sim \tau \iff \sigma(x) = \tau(x)$.

Let $\tau_1, \dots, \tau_m$ be a system of representatives, then

$$p_x(t) = \prod_{j=1}^{m} (t - \tau_j(x))$$

and

$$f_x(t) = p_x(t)^d = \prod_{j=1}^{m} (t - \tau_j(x))^d$$

$$= \prod_{j=1}^{m} \prod_{\sigma \sim \tau_j} (t - \tau_j(x)) = \prod_{i=1}^{n} (t - \sigma_i(x)) \qquad \square$$

Corollary 3.7 If we have finite field extensions $K \subset L \subset M$ with $\mathrm{char}(K)=0$ or $|K|<\infty$ then

$$\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$$

$$N_{L/K} \circ N_{M/L} = N_{M/K}$$

Proof: Homework 3.

Definition 3.8 Let $\mathrm{char}(K)=0$ or $|K|<\infty$ and let L/K be a finite extension with K-embeddings $\sigma_i : L \to \overline{K}$, $i=1,\dots,n$, $n=[L:K]$.

Then the <u>discriminant</u> of a basis $\alpha_1,\dots,\alpha_n$ of L is defined by

$$d(\alpha_1,\dots,\alpha_n) = \det(\sigma_i \alpha_j)^2$$

Remark 3.9

i) Since $\mathrm{Tr}_{L/K}(\alpha_i \alpha_j) = \sum_{\ell=1}^{n} \sigma_\ell(\alpha_i)\sigma_\ell(\alpha_j)$ the matrix $(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j))_{1\le i,j\le n}$ is given by the product of $(\sigma_\ell(\alpha_i))^T_{1\le \ell, i\le n}$, $(\sigma_\ell(\alpha_j))_{1\le \ell, j\le n}$.

Therefore

$$d(\alpha_1,\dots,\alpha_n) = \det(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)).$$

ii) If θ is a primitive element of L/K, then $\{1,\theta,\dots,\theta^{n-1}\}$ is a basis of L/K. Setting $\theta_i := \sigma_i\theta$ we get the Vandermonde matrix

$$(\sigma_i(\theta^j)) = \begin{pmatrix} 1 & \theta_1 & \theta_1^2 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & & & \theta_2^{n-1} \\ \vdots & \vdots & & & \\ 1 & \theta_n & & & \theta_n^{n-1} \end{pmatrix}$$

and $d(1,\theta,\dots,\theta^{n-1}) = \prod_{i<j}(\theta_j-\theta_i)^2$.

In particular this is non-zero.

In general we get:

Proposition 3.10 Let $\mathrm{char}(K) = 0$ or $|K| < \infty$ and let L/K be a finite extension with basis $\alpha_1, \ldots, \alpha_n$. Then

$$d(\alpha_1, \ldots, \alpha_n) \neq 0$$

and

$$(x, y) = \mathrm{Tr}_{L/K}(x \cdot y)$$

is a nondegenerate bilinear form on the K-vector space L.

Proof: If θ is a primitive element then

$$d(1, \theta, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \neq 0.$$

With respect to this basis the matrix of $\mathrm{Tr}_{L/K}$ is given by $M = (\mathrm{Tr}_{L/K}(\theta^{i-1}\theta^{j-1}))$ and $\det(M) = d(1, \theta, \ldots, \theta^{n-1}) \neq 0$.

Therefore (x, y) is nondegenerate.

With respect to another basis $\alpha_1, \ldots, \alpha_n$ the matrix of (x, y) is given by

$M = (\mathrm{Tr}_{L/K}(\alpha_i \alpha_j))$ i.e

$$0 \neq \det(M) = \det(\alpha_1, \dots, \alpha_n) \qquad \square$$

From now on we consider:

$$\begin{array}{ccccl} & & \text{finite extension} & & \\ \mathrm{Frac}(A) =: & K & \subset & L & \text{(e.g number field)} \\ \text{(e.g } \mathbb{Q}) & \cup & & \cup & \\ & A & \subset & B = \text{Integral closure of } A \text{ in } L & \\ & & & \overline{A} & \text{(e.g. } \mathcal{O}_L) \end{array}$$

integrally closed ring (e.g. $\mathbb{Z}$)

Proposition 3.11 In the above situation we have

i) Every element $\beta \in L$ has the form

$$\beta = \frac{b}{a} \quad \text{with } b \in B,\ a \in A.$$

In particular $L = \mathrm{Frac}(B)$.

ii) $\beta \in L$ is integral over A iff $\min_K(\beta) \in A[x]$.

iii) If $b \in B$ then $T_{L/K}(b), N_{L/K}(b) \in A$.

iv) We have $b \in B^\times$ iff $N_{L/K}(b) \in A^\times$.

<u>Proof:</u> i) Since L/K is finite, β is algebraic over K, i.e

$$\beta^n + \tilde{a}_{n-1}\beta^{n-1} + \ldots + \tilde{a}_1\beta + \tilde{a}_0 = 0 \qquad \tilde{a}_i \in \underset{\mathrm{Frac}(A)}{\underset{\parallel}{K}}.$$

Multiplying with the common denominator $a_n \in A$ of the $\tilde{a}_i$ we get

$$a_n\beta^n + \ldots + a_1\beta + a_0 = 0 \qquad a_i \in A.$$

Multiplying with a_n^{n-1} gives

$$(a_n\beta)^n + \ldots + a_1'(a_n\beta) + a_0' = 0 \qquad a_i' \in A,$$

i.e $a_n\beta$ is integral over $A \Rightarrow \underbrace{a_n\beta}_{=:b} \in B$

ii) – iv) Exercise. $\square$

<u>Lemma 3.12</u> Let $\alpha_1, \ldots, \alpha_n$ be a basis of L/K which is contained in B of discriminant $d = d(\alpha_1, \ldots, \alpha_n)$. Then

$$dB \subseteq A\alpha_1 + \ldots + A\alpha_n.$$

<u>Proof</u>: For $\alpha = a_1\alpha_1 + \dots + a_n \alpha_n \in B$, $a_j \in K$ we have

$$A \ni \mathrm{Tr}_{L/K}(\alpha\alpha_j) = \sum_{i=1}^{n} a_i \, \mathrm{Tr}_{L/K}(\alpha_i\alpha_j).$$

Therefore the a_i are the solution of

$$\left(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)\right)\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}(\alpha\alpha_1) \\ \vdots \\ \mathrm{Tr}(\alpha\alpha_n) \end{pmatrix} \in A^n,$$

i.e. they can be written as an element in A divided by $\det(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)) = d$

$\Rightarrow \quad d\, a_i \in A$

$\Rightarrow \quad d\alpha \in A\alpha_1 + \dots + A\alpha_n$ $\square$

Definition 3.13 An <u>integral basis</u> of B over A (A-basis of B) is a system of elements $\omega_1, \dots, \omega_n \in B$, such that each $b \in B$ can be written uniquely as a linear combination

$$b = a_1\omega_1 + \dots + a_n\omega_n \qquad a_i \in A.$$

Remark 3.14 i) An integral basis of B over A is automatically also a basis of L/K as a K-vector space, i.e $n = [L:K]$. This follows from Proposition 3.11 i).
In this case we say that L/K has an integral basis.

ii) If B as an integral basis over A then B is a free A-module of rank $[L:K]$.

In general an integral basis does not exist. But in the case that A is a PID we have:

Proposition 3.15 ⊛ Let A be a PID and $K = \mathrm{Frac}(A)$, L/K finite and let B be the integral closure of A in L. Then every fin. gen. B-submodule $M \neq 0$ of L is a free A-module of rank $[L:K]$. In particular, B admits an integral basis over A.

Proof: See Neukirch Prop 2.10

$$\begin{array}{ccc} \mathbb{Q} & \subset & K \\ \cup & & \cup \\ \mathbb{Z} & \subset & \mathcal{O}_K \end{array} \qquad [K:\mathbb{Q}]$$

Corollary 3.16 Let K be a number field. Then every fin. gen. $\mathcal{O}_K$-modul $\mathfrak{a}$ in K has a $\mathbb{Z}$-basis $\alpha_1, \dots, \alpha_n$

$$\mathfrak{a} = \mathbb{Z}\alpha_1 + \dots + \mathbb{Z}\alpha_n$$

with $n = [K:\mathbb{Q}]$.

The discriminat $d(\alpha_1, \dots, \alpha_n) = \det(\sigma_i \alpha_j)^2$ is independent of the choice of the basis.

<u>Proof</u>: The first part follows from Prop 3.15.

If $\alpha_1', \dots, \alpha_n'$ is another basis, then

$$\alpha_i' = \sum T_{ij} \alpha_j \qquad T = (T_{ij}) \in M_n(\mathbb{Z})$$

with $\det(T) \in \mathbb{Z}^\times = \{\pm 1\}$.

$$\Rightarrow \quad d(\alpha_1', \dots, \alpha_n') = (\det(T))^2 \, d(\alpha_1, \dots, \alpha_n) \qquad \square$$

Definition 3.17 (With the notation as Cor 3.16)

$d(\mathfrak{a}) = d(\alpha_1, \dots, \alpha_n)$ is the <u>discriminant of the $\mathcal{O}_K$-module $\mathfrak{a}$</u>.

In particular

$$d_K = d(\mathcal{O}_K) = d(\omega_1, \dots, \omega_n),$$

where $\omega_1, \dots, \omega_n$ is an intesral basis of $K/\mathbb{Q}$, is called the <u>discriminant</u> of the number field K.