Lecture 25 : Norm, Trace and Hilbert's Theorem 90

Objectives

(1) The norm and the trace function.
(2) Multiplicative form of Hilbert's Theorem 90.
(3) Cyclic extensions of degree n.
(4) Additive version of Hilbert's 90.
(5) Cyclic extensions of prime degree: Artin-Schreier Theorem.

Keywords and phrases: Norm, trace, Hilbert's theorem 90, cyclic extensions, Artin-Schreier Theorem.

Definition 25.1. *Let E/F be a finite separable extension of degree n. Let $\sigma_1, \ldots, \sigma_n$ be the F-embeddings : $E \to F^a$. For any $a \in E$, define the norm and trace of a by,*

$$\begin{aligned} N_{E/K}(a) &= \sigma_1(a)\sigma_2(a)\cdots\sigma_n(a) \\ Tr_{E/K}(a) &= \sigma_1(a) + \cdots + \sigma_n(a). \end{aligned}$$

Example 25.2. Let m be a square free integer. Consider the quadratic extension $E = \mathbb{Q}(\sqrt{m})$ of $\mathbb{Q}$. The Galois group $G = G(E/\mathbb{Q})$ consists of identity map and the automorphism $\sigma(a + \sqrt{m}) = a - b\sqrt{m}$. Therefore $Tr(a + b\sqrt{m}) = 2a$ and $N(a + b\sqrt{m}) = a^2 - mb^2$.

Proposition 25.3. (1) *$N_{E/K} : E^\times \to F^\times$ is a group homomorphism.*
(2) *Let $E \supset K \supset F$ be a tower of finite separable extensions. Then*

$$N_{E/F} = N_{K/F} \circ N_{E/K}, \quad Tr_{E/F} = Tr_{K/F} \circ Tr_{E/K}$$

(3) *If $E = F(a)$ and $irr\,(a, F) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ then*

$$N_{E/F}(a) = (-1)^n a_0, \text{ and } Tr_{E/F}(a) = -a_{n-1}.$$

(4) *$Tr : E \to F$ is a surjective F-linear map.*

Proof. (1) $N_{E/F}(ab) = N_{E/F}(a)N_{E/F}(b)$ for all $a, b \in E$ is clear.

Let $L = \sigma_1(F)\ldots\sigma_n(F)$. Then L/F is a Galois extension. Let $a \in E^\times$. Then $N_{E/F}(a)$ is fixed under all $\sigma \in G(L/F)$, thus it is in $F^\times$.
(2) Let $\{\tau_j\}$ be the family of F-embeddings : $K \to F^a$ and $\{\sigma_i\}$ be the

family of all K-embeddings : $E \to F^a$. Each τ_j can be extended to an automorphism of F^a. Let this extension be denoted by τ_j. Then $\{\tau_j\sigma_i\}$ is the family of all F-embeddings of $E \to F^a$. For any $x \in E$,

$$N_{K/F} \circ N_{E/K}(x) = N_{K/F}\left(\prod_{i=1}^{n} \sigma_i(x)\right) = \prod_{j=1}^{m}\prod_{i=1}^{n} \tau_j\sigma_i(x) = N_{E/F}(x).$$

For any $x \in E$ we have

$$Tr_{K/F} \circ Tr_{E/K}(x) = Tr_{K/F}\left(\sum_{i=1}^{n} \sigma_i(x)\right) = \sum_{j=1}^{m}\sum_{i=1}^{n} \tau_j\sigma_i(x) = Tr_{E/F}(x).$$

(3) Suppose $E = F(a)$ and $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_n = $ irr (a, F) and $f(x) = (x - a_1)(x - a_2)\cdots(x - a_n)$ where $a_1, \ldots, a_n$ are all the roots in F^a of $f(x)$. Each $a_i = \sigma(a_1)$ for some F-embedding $\sigma : E \to F^a$. Thus $N_{E/F}(a) = (-1)^n a_n$ and $Tr_{E/F}(a) = -a_{n-1}$.
(4) $Tr_{E/k}(a) = \sigma_1(a) + \cdots + \sigma_n(a)$. By Dedekind's theorem on characters, $\sigma_1 + \cdots + \sigma_n$ is not a zero map. Since $Tr_{E/F}$ is a linear map of F-vector spaces, it is surjective. □

Proposition 25.4. *Let E/F be a finite separable extension of degree n and $a \in E$. Let $m_a : E \to E$ be the F-linear map defined as $m_a(x) = ax$ for all $x \in E$. Then*

$$N_{E/F}(a) = \det(m_a) \ \text{ and } \ Tr_{E/F}(a) = Tr(m_a).$$

Proof. Let $K = F(a)$ and $f(x) = $ irr $(a, F) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$. Then $1, a, a^2, \ldots, a^{d-1}$ is an F-basis for K. Let $v_1, v_2, \ldots, v_e$ be a K-basis of E. Then $\{v_i a^j \mid i = 1, 2, \ldots, e; j = 0, 1, \ldots, d-1\}$ is an F-basis of E. We order this basis as :

$$B = \{v_1, av_1, a^2v_1, \ldots, a^{d-1}v_1; \ldots;, v_e, av_e, a^2v_e, \ldots, a^{d-1}v_e\}.$$

Consider the matrix

$$A = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & -a_{d-1} \end{bmatrix}.$$

Then the characteristic polynomial of A is $f(x)$. The matrix of m_a with respect to B is the $n \times n$ matrix:

$$\begin{bmatrix} A & 0 & 0 & \dots & 0 \\ 0 & A & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & A \end{bmatrix}.$$

Therefore $\det m_a = (\det A)^e$ and $\operatorname{Tr} m_a = e \operatorname{Tr} A$. Therefore

$$N_{E/F}(a) = N_{K/F} \circ N_{E/K}(a) = N_{K/F}(a^e) = (\det A)^e = \det m_a,$$

$$\operatorname{Tr}_{E/F}(a) = \operatorname{Tr}_{K/F} \circ \operatorname{Tr}_{E/K}(a) = \operatorname{Tr}_{K/F}(ea) = e \operatorname{Tr} A = \operatorname{Tr} m_a.$$

□

Proposition 25.5. *Let E/F be a finite separable extension. Then*
(1) *the map $\varphi : E \times E \to F$ given by $\varphi(x, y) = Tr(xy)$ is bilinear.*
(2) *The map $T_x : E \to F$ given by $T_x(y) = Tr(xy)$ is an F-linear map.*
(3) *The map $\psi : E \to \operatorname{Hom}(E, F)$ given by $\psi(x) = Tr_x$ is an isomorphism.*

Proof. It is easy to see (1) and (2). For (3), if $\psi(x) = Tr_x = 0$ then $Tr_x(y) = Tr(xy) = 0$ for all $y \in E$. Hence for any $e \in E$, $Tr_x(x^{-1}e) = Tr(e) = 0$. Thus Tr is the zero functional. This is a contradiction. Hence ψ is an injective linear map. Since $\dim E = \dim \operatorname{Hom}(E, F)$, we conclude that ψ is an isomorphism.

□

Theorem 25.6 (**Hilbert's Theorem 90 (multiplicative form)**). *Let E/F be a cyclic extension. Let $G(E/F) = (\sigma)$. Then for $\beta \in E$,*

$$N_{E/F}(\beta) = 1 \quad \textit{if and only if } \beta = \frac{\alpha}{\sigma(\alpha)} \textit{ for some } \alpha \in E^\times.$$

Proof. Let $[E : F] = n$. If $\beta = \frac{\alpha}{\sigma(\alpha)}$, then

$$N_{E/F}(\beta) = \beta\sigma(\beta) \cdots \sigma^{n-1}(\beta) = \frac{\alpha\sigma(\alpha)}{\sigma(\alpha)\sigma^2(\alpha)} \cdots \frac{\sigma^{n-1}(\alpha)}{\alpha} = 1.$$

Conversely, suppose $N_{E/k}(\beta) = 1$. Consider

$$id + \beta\sigma + \beta\sigma(\beta)\sigma^2 + \beta\sigma(\beta)\sigma^2(\beta)\sigma^3 + \cdots + \beta\sigma(\beta) \cdots \sigma^{n-2}(\beta)\sigma^{n-1}$$

is a nonzero map from $E \to F$ due to Dedekind's independence theorem. Let $\theta \in K$ be such that

$$\alpha = \theta + \beta\sigma(\theta) + \beta\sigma(\beta)\sigma^2(\theta) + \cdots + \beta\sigma(\beta)\cdots\sigma^{n-2}(\beta)\sigma^{n-1}(\theta) \neq 0.$$

Then

$$\beta\sigma(\alpha) = \beta\sigma(\theta) + \beta\sigma(\beta)\sigma^2(\theta) + \cdots + \beta\sigma(\beta)\sigma^2(\beta)\cdots\sigma^{n-1}(\beta)\theta = \alpha.$$

Therefore $\beta = \frac{\alpha}{\sigma(\alpha)}$.

□

Theorem 25.7. *Let k be a field, n a positive integer coprime with char k and assume k has a primitive n^{th} root w of 1. Let E/k be cyclic extension of degree n. Then E is splitting field of $x^n - a \in k[x]$.*

Proof. Let $G(E/k) = (\sigma)$. Then $N_{E/k}(w^{-1}) = w^{-n} = 1$. By Hilbert's theorem 90, there exists $\alpha \in E$ such that $\sigma(\alpha) = w\alpha$. Thus $\sigma^i(\alpha) = w^i\alpha$ for $i = 1, ..., n$. Hence α has n distinct conjugates in E. Since $[E : k] = n$, $E = k(\alpha)$. Since $\sigma(\alpha^n) = (w\alpha)^n = \alpha^n := a \in E^G = k$. Thus E is a splitting field of $x^n - a$.

□

We now discuss the additive form of Hilbert 90 and its application to cyclic extension of degree p, where p is prime and is equal to the characteristic of the base field.

Theorem 25.8 (**Additive form of Hilbert's Theorem 90**). *Let E/k be a cyclic extension of degree n with Galois group G. Let $G = \langle\sigma\rangle$. Then for $\beta \in E$*

$$Tr_{E/k}(\beta) = 0 \text{ if and only if } \beta = \alpha - \sigma(\alpha) \text{ for some } \alpha \in E.$$

Proof. Let $\beta = \alpha - \sigma(\alpha)$. Then $Tr(\beta) = Tr(\alpha) - Tr(\sigma(\alpha)) = 0$.

Let $Tr(\beta) = 0$. Since $Tr : E \to k$ is a nonzero map, there exits $\theta \in E$ such that $Tr(\theta) \neq 0$. For the element

$\alpha = \frac{1}{Tr(\theta)}[\beta\theta + (\beta + \sigma(\beta))\sigma(\theta) + \cdots + (\beta + \sigma(\beta) + \cdots + \sigma^{n-2}(\beta))\sigma^{n-2}(\theta)]$,

$\sigma(\alpha) = \frac{1}{Tr(\theta)}[\sigma(\beta)\sigma(\theta) + (\sigma(\beta) + \sigma^2(\beta))\sigma^2(\theta) + \cdots + (\sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^{n-1}(\beta))\sigma^{n-1}(\theta)]$

As $Tr(\beta) = 0$, $\alpha - \sigma(\alpha) = \frac{1}{Tr(\theta)}[\beta\theta + \beta\sigma(\theta) + \cdots + \beta\sigma^{n-1}(\theta)] = \beta$. □

Theorem 25.9 (**Artin-Schreier**). *Let k be a field of char $p > 0$. Let E/k be a cyclic extension of degree p. Then E is a splitting field of $x^p - x - a$ for some $a \in E$ and $E = k(\alpha)$ where $\alpha^p - \alpha = a$ for some $\alpha \in E$.*

Proof. Let E/k be cyclic of degree p. Then $Tr(-1) = 0$. Hence there exists $\alpha \in E$ such that $\alpha - \sigma(\alpha) = -1$ where $\langle\sigma\rangle = G(E/k)$. Thus $\sigma(\alpha) = \alpha + 1$. Hence $\sigma^i(\alpha) = a + i$ for $i = 1, 2, \ldots, p$. Since char $k = p$, the elements $\alpha, \alpha + 1, ..., \alpha + p - 1$ are distinct. Hence $[k(\alpha) : k] = p$ and $E = k(\alpha)$. As $\sigma(\alpha^p - \alpha) = (\sigma(\alpha))^p - \sigma(\alpha) = (\alpha+1)^p - (\alpha+1) = \alpha^p - \alpha$, $\alpha^p - \alpha \in E^{(\sigma)} = k$. Let $a = \alpha^p - \alpha \in k$. Then α satisfies $f(x) = x^p - x - a = 0$. The roots of $f(x)$ are $\alpha, \alpha + 1, \ldots, \alpha + p - 1$. Thus E is a splitting field of $f(x)$.

□

Example 25.10. (Pythagorean Triples) Let us find all Pythagorean triples (x, y, z) such that $x^2 + y^2 = z^2$ where $x, y, z \in \mathbb{N}$. Hence $x^2/z^2 + y^2/z^2 = N(x/z + iy/z) = 1$. Let us apply Hilbert's theorem 90 to the cyclic extension $\mathbb{Q}(i)/\mathbb{Q}$. The Galois group of this extension is cyclic of order 2 generated by the conjugation automorphism. Hence $N(a+ib) = a^2 + b^2$. So there exists $\alpha = c + id \in \mathbb{Q}(i)$ such that

$$x/z + iy/z = (c + id)/(c - id) = (c^2 - d^2 + 2icd)/(c^2 + d^2).$$

Thus $x/z = (c^2 - d^2)/(c^2 + d^2)$ and $y/z = 2cd/(c^2 + d^2)$. Putting $c = s/u$ and $d = t/u$ where $s, t, u \in \mathbb{N}$, we get

$$x = s^2 - t^2,\ y = 2st,\ z = s^2 + t^2.$$