Math 210B Lecture 22 Notes

Daniel Raban

March 4, 2019

1 Norm, Trace, Characters, and Hilbert's Theorem 90

1.1 Norm and trace

Definition 1.1. Let E/F be a finite extension. For $\alpha \in E$, let $m_\alpha : E \to E$ be $x \mapsto x_\alpha$. The **trace** $\mathrm{tr}_{E/F} : E \to F$ and **norm** $N_{E/F} : E \to F$ send $\alpha \mapsto \mathrm{tr}(m_\alpha)$ and $\alpha \mapsto \det(m_\alpha)$, where we view $m_\alpha \in \mathrm{End}_F(E)$ as a matrix.

Remark 1.1. $m_{\alpha+\lambda\beta} = m_\alpha + \lambda m_\beta$, so the trace is a linear map. The norm is multiplicative because $m_{\alpha\beta} = m_\alpha \circ m_\beta$.

Proposition 1.1. *Let E/F be finite with $x \in E$. Then*

$$N_{E/F}(x) = \prod_{\sigma \in \mathrm{Emb}_F(F(x))} \sigma(x)^N = \prod_{\sigma \in \mathrm{Emb}_F(E)} \sigma(x)^{[E:F]_i},$$

$$\mathrm{tr}_{E/F}(x) = N \sum_{\sigma \in \mathrm{Emb}_F(F(x))} \sigma(x) = \left(\sum_{\sigma \in \mathrm{Emb}_F(E)} \sigma(x) \right) [E:F]_i,$$

where $N = [F(x):F]_i[E:F(x)] = [F(x):F]_i[E:F(x)]_i[E:F(x)]_s$

Proof. In each case, the second equality follows from

$$\begin{aligned} N &= [F(x):F]_i[E:F(x)] \\ &= [F(x):F]_i[E:F(x)]_i[E:F(x)]_s \\ &= [E:F]_i[E:F(x)]_s. \end{aligned}$$

Case 1: $E = F(x)$: Let $n = [F(x):F]$, let $f_x(t) = \sum_{i=0}^n a - it^i$ be the minimal polynomial of x over F. We can write $f_x(t) = \prod_{\sigma \in \mathrm{Emb}_F(F(x))} (t - \sigma(x))^{[F(x):F]_i}$. Let β

be the basis $\{1, x, \ldots, x^{n-1}$ of $F(x)$. We want to show that $f_x(t)$ is the characteristic polynomial of m_x. The matrix of m_x is

$$[m_x]_\beta = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & & & & -a_1 \\ & 1 & & & \vdots \\ & & \ddots & & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{bmatrix}.$$

Then the characteristic polynomial of m_x is $\sum_{i=0}^{n} a_i t^i$. So

$$\mathrm{tr}(_{E/F}(x) = \mathrm{tr}(m_x) = -a_{n-1} = [F(x) : F]_i \sum \sigma_{\sigma \in \mathrm{Emb}_F(F(x))}(x)$$

$$N_{E/F}(x) = \det(m_x) = (-1)^n a_0 = \prod_{\sigma \in in\, \mathrm{Emb}_F(F(x))} \sigma(x)^{[F(x),F]_i}$$

For the general case, let $\{y-1, \ldots, y_k\}$ be an $F(x)$-basis for E. Then $E = \bigoplus_{i=1}^{k} F(x) y_i$. is a decomposition into m_x-invariant subspaces ($k = [E : F(x)]$). So $\beta = \{x^i y_j\}$ is a basis for E/F, and

$$[m_x]_\beta = \begin{bmatrix} m_x & & & \\ & m_x & & \\ & & \ddots & \\ & & & m_x \end{bmatrix}$$

is block diagonal with blocks of the type of the previous case. So

$$\mathrm{tr}(m_x) = [E : F(x)][F(x) : F]_i \sum \sigma_{\sigma \in \mathrm{Emb}_F(F(x))}(x)$$

$$\det(m_x) = \prod_{\sigma \in \mathrm{Emb}_F(F(x))} \sigma(x)^{[E:F(x)][F(x):F]_i}. \qquad \square$$

Corollary 1.1. *Let $E/K/F$ be finite. Then*

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

$$\mathrm{tr}_{K/F} = \mathrm{tr}_{E/F} \circ \mathrm{tr}_{K/E}.$$

Proof. Let $x \in K$. Then

$$N_{E/F}(N_{K/E}) = \prod_{\sigma \in \mathrm{Emb}_F(E)} \sigma \left(\prod_{\tau \in \mathrm{Emb}_E(K)} \tau(x) \right)$$

Any $\varphi : K \to \overline{F}$ can be written as $\hat{\sigma} \circ \tau$ for some unique $|sigma \in \mathrm{Emb}_F(E)$ and $\tau \in \mathrm{Emb}_E(K)$.

$$\begin{tikzcd}
K \arrow[r, "\varphi"] \arrow[d, dash] & \overline{F} \\
E \arrow[ur, "\sigma"] \arrow[d, dash] & \\
F \arrow[uur] &
\end{tikzcd}$$

Then $\tau = \varphi \circ \hat{\sigma}^{-1}$ fixes E. So

$$N_{E/F}(N_{K/E}) = \prod_{\sigma} \prod_{\tau} \hat{\sigma}\tau(x) = \prod_{\varphi \in \mathrm{Emb}_F(K)} \varphi(x). \qquad \square$$

1.2 Characters and Hilbert's theorem 90

Theorem 1.1 (Hilbert's theorem 90)**.** *Let E/F be finite, Galois with cyclic Galois group $G = \langle \sigma \rangle$. Then*

$$\begin{aligned}
\ker(N_{E/F}) &= \{\sigma(x)/x : x \in E^\times\}, \\
\ker(\mathrm{tr}_{E/F}) &= \{\sigma(x) - x : x \in E\}.
\end{aligned}$$

The $\supseteq$ containments require no conditions, so we need to prove the other containments. To prove this, we need a bit of character theory.

Definition 1.2. Let G be a group, and let E be a field. A **character** on G with values in E is a group homomorphism $\chi : G \to E^\times$.

The set of all characters $\mathrm{char}_F(G) \subseteq \mathrm{Fun}(G.E)$ is subset of an E-vector space.

Lemma 1.1. $\mathrm{char}_E(G)$ *is linearly independent.*

Proof. Let $\{\chi_1, \dots, \chi_m\}$ be a minimal linearly dependent set. Let $\sum_{i=1}^\infty a_i \chi_i = 0$ with all $a_i \neq 0$. Choose $h \in G$ such that $\chi_1(h) \neq \chi_m(h)$. Let $b_i = a_i(\chi_i(h) - \chi_m(h)) \in E$; then $b_1 \neq 0$ and $b_m = 0$ (by definition). Now for $g \in G$,

$$\begin{aligned}
\sum_{i=1}^{m-1} b_i \chi_i(g) &= \sum_{i=1}^{m-1} a - i\chi_i(h)\chi_i(g) - a_i \chi_m(j)\chi_i(g) \\
&= \sum_{i=1}^{m-1} a_i \chi_i(hg) - \chi_m(h) \sum_{i=1}^{m-1} a_i \chi_i(g) \\
&= -a_m \chi_m(hg) - \chi_m(h)(-a_m \chi_m(g)) \\
&= -a_m \chi_m(hg) + a - m\chi_m(hg) \\
&= 0.
\end{aligned}$$

This contradicts the minimality of $\{\chi_1, \dots, \chi_m\}$. $\square$

We can now prove Hilbert's theorem 90.

Proof. We want to show that $\ker(N_{E/F}) = \{\sigma(x)/x : x \in E^\times\}$. Take $x \in \ker(N_{E/F})$. Then

$$\chi_x = \sum_{i=0}^{n-1} \left(\prod_{j=0}^{i-1} \sigma^j(x) \right) \sigma^i$$

is a character. Then

$$\chi_x(y) = y + x\sigma(y) + x\sigma(x)\sigma^2(y) + \cdots + x\sigma(x)\sigma^2(x)\cdots\sigma^{n-2}(x)\sigma^{n-1}(y).$$

The idea is we want to find a fixed point of applying σ and multiplying by x. This is because if $y \neq 0$,

$$x = \frac{\sigma(y)}{y} \iff x = \frac{y}{\sigma(y)} \iff \sigma(y)x = y.$$

For all $y \in E$, we have that $x\sigma(\chi_x(y)) = \chi_x(y)$. If $\chi_x(y) \neq 0$, we are done because $x = \chi_x(y)/\sigma(\chi_x(y))$. So χ_x is a nonzero linear combination of distinct characters and is hence nonzero by the lemma. Thus, there exists $y \in E^\times$ such that $\chi_x(y) \neq 0$. $\square$

We will do the trace next time.