

Frank Moore
Algebra 901 Notes
Professor: Tom Marley

Definition: Let E/F be a finite field extension, and let $\sigma_1, \dots, \sigma_r$ be the distinct embeddings of E into \bar{F} fixing F (so $r = [E : F]_s$). Define

$$N_F^E(\alpha) := \left(\sigma_1(\alpha) \cdots \sigma_r(\alpha) \right)^{[E:F]_i}$$

$$Tr_F^E(\alpha) := [E : F]_i \left(\sigma_1(\alpha) \cdots \sigma_r(\alpha) \right)$$

to be the **norm** and **trace** of α respectively.

Examples:

1. Let $E = \mathbb{Q}(\sqrt{2})$. Then $1 : E \rightarrow E$ and $\sigma : E \rightarrow E$, where $\sigma(\sqrt{2}) = -\sqrt{2}$ are the distinct \mathbb{Q} embeddings of E into \bar{F} . Then $N_{\mathbb{Q}}^E(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Q}$, and $Tr_{\mathbb{Q}}^E = ((a + b\sqrt{2}) + (a - b\sqrt{2})) = 2a \in \mathbb{Q}$.
2. Let $F = \mathbb{Z}_p(t)$, where t is an indeterminant and p a prime. Let $f(x) = x^p - t \in F[x]$. Let E be the splitting field for $f(x)$ over F . Let $\alpha \in E$ be a root of $f(x)$. Then $\alpha^p = t$ and $f(x) = (x - \alpha)^p$ in $E[x]$. Hence $E = F(\alpha)$ and E/F is purely inseparable. Hence $[E : F]_i = [E : F] = p$ and $[E : F]_s = 1$. As $[E : F]_s = 1$, for $\beta \in E$, $N_F^E(\beta) = \beta^p$ and $Tr_F^E = p\beta = 0$. Hence, in this case, trace is degenerate.

Remark: If E/F is inseparable, then $[E : F]_i = p^k$, and hence $Tr_F^E(\beta) = 0$, so trace id degenerate for inseparable extensions. We will see later that it is nondegenerate for separable extensions.

Theorem: Let E/F be a finite extension. Let $N = N_F^E$ and $Tr = Tr_F^E$. Then for all $\alpha \in E$, we have that $N(\alpha) \in F$ and $Tr(\alpha) \in F$.

Proof: First, suppose that E/F is separable. Let $\{\sigma_1, \dots, \sigma_r\}$ be the distinct embeddings of E into \bar{F} fixing F . Let L be the normal closure of E/F . So L/F is Galois, and since we may think of the σ_i as maps from L into \bar{F} fixing F , we know that σ_i actually take values in L . Note also that for the same reason, we have that for any $\phi \in \text{Gal}(L/F)$, we have that $\{\phi\sigma_1, \dots, \phi\sigma_r\} = \{\sigma_1, \dots, \sigma_r\}$. So, let $\alpha \in E$. Then $\phi(N(\alpha)) = \phi(\sigma_1(\alpha) \cdots \sigma_r(\alpha)) = \phi\sigma_1(\alpha) \cdots \phi\sigma_r(\alpha) = N(\alpha)$ by the previous remark. Hence $N(\alpha)$ is in the fixed field of the Galois group, and hence in F . Note that the proof for $Tr(\alpha)$ works the same way. Now, let E/F be an arbitrary finite extension. Let $T = \{\alpha \in E \mid \alpha \text{ is separable over } F\}$. Let $\alpha \in E$. Note that $[F(\alpha) : F]_i \leq [E : F]_i$ and if $p^l = [E : F]_i$, then α^{p^l} is separable by the major proposition above on separability, and hence in T . Let $\{\sigma_1, \dots, \sigma_r\}$ be the distinct F -embeddings of T into \bar{F} . Then $\{\sigma_1|_T, \dots, \sigma_r|_T\}$ are the distinct F -embeddings of T into \bar{F} . Indeed, we have that $[E : F]_s = [T : F]_s$ as E/T is purely inseparable by construction. Then

$$N_F^E(\alpha) = (\sigma_1(\alpha) \cdots \sigma_r(\alpha))^{[E:F]_i}$$

$$= \sigma_1(\alpha^{[E:F]_i}) \cdots \sigma_r(\alpha^{[E:F]_i})$$

$$= N_T^E(\alpha^{[E:F]_i})$$

which is in F by the separable case above, since T/F was separable by construction. The trace again works the same way.

Properties of Norm and Trace: Let E/F be a finite extension and let $N = N_F^E$ and $Tr = Tr_F^E$. Then

1. For all $\alpha, \beta \in E$, we have that $N(\alpha\beta) = N(\alpha)N(\beta)$ and $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$.
2. If $\alpha \in F$, then $N(\alpha) = \alpha^{[E:F]}$ and $Tr(\alpha) = [E:F]\alpha$.
3. If L is an intermediate field of E/F then $N_F^L \circ N_L^E = N_F^E$ and similarly for trace.

Proof: The proof of these results are an easy exercise.

Remark:

1. If $\alpha \in E \setminus \{0\}$, then $N(\alpha) \neq 0$, so $N_F^E : E^\times \rightarrow F^\times$ is a group homomorphism.
2. Similarly, $Tr_F^E : E \rightarrow F$ is a homomorphism of additive groups. Moreover, if $c \in F$, then $Tr_F^E(c\alpha) = cTr_F^E(\alpha)$, i.e. it is a linear functional on the F -vector space E .

Lemma: Let E/F be a field extension and $\{\sigma_1, \dots, \sigma_r\}$ distinct embeddings of E into L , where L is any field containing E . Then $\{\sigma_1, \dots, \sigma_r\}$ are linearly independent over F .

Proof: We induct on n with the case $n = 1$ being trivial. Suppose $n = 1$ and suppose that there exists $a_1, \dots, a_r \in F$ not all zero such that $a_1\sigma_1 + \dots + a_r\sigma_r = 0$. As the lemma is true by induction for $\leq n-1$, we must have that all the a_i are nonzero. Let $\beta \in E$ such that $\sigma_1(\beta) \neq \sigma_2(\beta)$. Then for all $\alpha \in E$, we have that

$$a_1\sigma(\beta\alpha) + a_2\sigma_2(\beta\alpha) + \dots + a_r\sigma_r(\beta\alpha) = 0$$

and hence

$$a_1\sigma(\beta)\sigma_1(\alpha) + a_2\sigma_2(\beta)\sigma_2(\alpha) + \dots + a_r\sigma_r(\beta)\sigma_r(\alpha) = 0$$

therefore

$$a_1\sigma(\beta)\sigma_1 + a_2\sigma_2(\beta)\sigma_2 + \dots + a_r\sigma_r(\beta)\sigma_r = 0$$

Now dividing by $\sigma_1(\beta)$ we have

$$a_1\sigma_1 + a_2\frac{\sigma_2(\beta)}{\sigma_1(\beta)}\sigma_2 + \dots + a_r\frac{\sigma_r(\beta)}{\sigma_1(\beta)}\sigma_r = 0$$

Subtracting this from the above equation gives

$$a_2\left(1 - \frac{\sigma_2(\beta)}{\sigma_1(\beta)}\right)\sigma_2 + \dots + a_r\left(1 - \frac{\sigma_r(\beta)}{\sigma_1(\beta)}\right)\sigma_r = 0$$

However, as $\sigma_1(\beta) \neq \sigma_2(\beta)$, $\left(1 - \frac{\sigma_2(\beta)}{\sigma_1(\beta)}\right) \neq 0$ and $a_2 \neq 0$ by assumption. This contradicts our induction hypothesis.

Corollary: Let E/F be a separable extension. Then $Tr_F^E \neq 0$.

Proof: Note that $Tr_F^E = \sigma_1 + \sigma_r$ where $\{\sigma_1, \dots, \sigma_r\}$ is the set of distinct F embeddings of E into \bar{F} . Thus by the above theorem it is non-zero.

Hilbert's Satz 90: Let E/F be a finite cyclic extension and $\text{Gal}(E/F) = \langle \sigma \rangle$. Then $N_F^E(\beta) = 1 \Leftrightarrow \beta = \frac{\alpha}{\sigma(\alpha)}$ for some $\alpha \in E$.

Proof: Let $|\sigma| = n$, so that $\sigma^n = 1$. First suppose that $\beta = \frac{\alpha}{\sigma(\alpha)}$. Then

$$\begin{aligned} N_F^E(\beta) &= \beta\sigma(\beta) \cdots \sigma^{n-1}(\beta) \\ &= \frac{\alpha}{\sigma(\alpha)} \sigma\left(\frac{\alpha}{\sigma(\alpha)}\right) \sigma^{n-1}\left(\frac{\alpha}{\sigma(\alpha)}\right) \\ &= \frac{\alpha}{\sigma(\alpha)} \frac{\sigma(\alpha)}{\sigma^2(\alpha)} \cdots \frac{\sigma^{n-1}(\alpha)}{\sigma^n(\alpha)} \end{aligned}$$

But $\sigma^n(\alpha) = \alpha$, and hence the above expression is 1. For the reverse direction, suppose that $N(\beta) = 1$. By the lemma on embeddings, we know that $\{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\}$ is linearly independent over F . Let $g = 1 + \beta\sigma + (\beta\sigma(\beta))\sigma^2 + \cdots + (\beta\sigma(\beta)\sigma^2(\beta) \cdots \sigma^{n-2}(\beta))\sigma^{n-1}$. Then $g \neq 0$. So, choose $u \in E$ such that $g(u) \neq 0$, and let $\alpha = g(u)$. Then we have

$$\begin{aligned} \beta\sigma(\alpha) &= \beta\sigma(u + \beta\sigma(u) + (\beta\sigma(\beta))\sigma^2(u) + \cdots + (\beta\sigma(\beta)\sigma^2(\beta) \cdots \sigma^{n-2}(\beta))\sigma^{n-1}(u)) \\ &= \beta\sigma(u) + \beta\sigma(\beta)\sigma^2(u) + \cdots + (\beta\sigma(\beta)\sigma^2(\beta) \cdots \sigma^{n-1}(\beta))u \end{aligned}$$

But as $(\beta\sigma(\beta)\sigma^2(\beta) \cdots \sigma^{n-2}(\beta)) = N_F^E(\beta) = 1$, we have

$$\begin{aligned} &= u + \beta\sigma(u) + \beta\sigma(\beta)\sigma^2(u) + \cdots + (\beta\sigma(\beta)\sigma^2(\beta) \cdots \sigma^{n-2}(\beta))\sigma^{n-1}(u) \\ &= g(u) = \alpha \end{aligned}$$

Hence $\beta = \frac{\alpha}{\sigma(\alpha)}$, as desired.

Additive Version of Hilbert's Satz 90: Let E/F be a finite cyclic extension, and $\text{Gal}(E/F) = \langle \sigma \rangle$. Then $\text{Tr}_F^E(\beta) = 0 \Leftrightarrow \beta = \alpha - \sigma(\alpha)$ for some $\alpha \in E$. Read in Lang or try mimicing the proof above.

Note: Let F be a field and \bar{F} its algebraic closure. Then the roots of $x^n - 1$ form a finite subgroup of \bar{F}^\times . Such subgroups are cyclic. A **primitive n th root of unity over F** is a cyclic generator for this subgroup.

Theorem: Let E/F be a finite extension and suppose that F contains a primitive n th root of unity, where $\text{Char } F \nmid n$. Then E/F is cyclic of degree $d \mid n \Leftrightarrow E = F(\alpha)$ where $\alpha^n \in F$.

Proof: For the forward direction, let ω be a primitive n th root of unity in F . Then $\zeta = \omega^{n/d}$ is a primitive d th root of unity. Certainly ζ^{-1} is in F , thus $N_F^E(\zeta^{-1}) = (\zeta^{-1})^{[E:F]} = (\zeta^{-1})^d = 1$. Hence it is in the kernel of the norm map. Therefore, $\zeta^{-1} = \frac{\alpha}{\sigma(\alpha)}$ for some $\alpha \in E$, where $\langle \sigma \rangle = \text{Gal}(E/F)$, by Satz 90. Therefore, $\sigma(\alpha) = \zeta\alpha$, and in general, we have that $\sigma^i(\alpha) = \zeta^i\alpha$. Hence, since $\alpha, \zeta\alpha, \dots, \zeta^{d-1}\alpha$ are distinct, we have that $[F(\alpha) : F]_s \geq d$. Thus, $[F(\alpha) : F] = d$, and thus $E = F(\alpha)$. Also, note that $\sigma(\alpha^d) = \sigma(\alpha)^d = (\zeta\alpha)^d = \alpha^d$, hence $\alpha^d \in E_{\langle \sigma \rangle} = F$, and hence $(\alpha^d)^{n/d} = \alpha^n \in F$.

For the reverse direction, Let $a = \alpha^n \in F$. Then α is a root of $x^n - a \in F[x]$. Since ω , a primitive n th root of unity, is in F , we have that $x^n - a$ splits in $F(\alpha) \in E$. So, E/F is normal, and since $\text{Char } F \nmid n$, $x^n - a$ is separable and so α is separable, and hence E/F is separable. Therefore E/F is Galois. Let $f(x) = \text{Irr}(\alpha, F)$. We know that $f(x) \mid x^n - a$. Let $\omega^{i_1}\alpha, \dots, \omega^{i_k}\alpha$ be the roots of $f(x)$. So $\sigma_{i_j} : F(\alpha) \rightarrow F(\alpha)$ sending α to $\omega^{i_j}\alpha$ is an automorphism of E fixing F . Then $\text{Gal}(E/F) = \{\sigma_{i_1}, \dots, \sigma_{i_k}\}$. Define

$$\phi : \text{Gal}(E/F) \rightarrow \{\omega^i \mid 0 \leq i \leq n-1\} \quad (\text{cyclic and isomorphic to } C_n)$$
$$\sigma_{i_j} \rightarrow \omega^{i_j}$$

Then ϕ is an injective group homomorphism, and since subgroups of cyclic groups are cyclic, $\text{Gal}(E/F)$ is cyclic of order $d \mid n$ by Lagrange.