Math 531
Notes from 9/27
Let's also keep in mind that we can always put a polynomial in upper-triangular or even Jordan canonical form when working with the norm and the trace. Here are some basic properties of norm and trace, most of which are elementary. Let's remember as well that every element $x \in L$ will satisfy the characteristic polynomial of the matrix $r_{x}$ (multiplication by $x$ ).
when $L=K(x)$, we have

$$
N_{L / K}(x)=(-1)^{n} a_{0}
$$

and

$$
T_{L / K}(x)=-a_{n-1}
$$

where

$$
F(T)=T^{n}+a_{n-1} T^{n-1}+\cdots+a_{0}
$$

is a polynomial of minimal degree for $x$ over $K$. This follows from the Cayley-Hamilton theorem, which says that $F(T)$ must be the characteristic polynomial for the matrix coming from the linear map

$$
r_{x}: a \longrightarrow x a
$$

on $L$.

## Proposition 11.1.

Let $L$ be a finite dimensional extension of a field $K$ and let $x, y \in L$ and $a \in K$. Then:
(1) $\mathrm{T}_{L / K}(x+y)=\mathrm{T}_{L / K}(x)+\mathrm{T}_{L / K}(y)$;
(2) $\mathrm{T}_{L / K}(a x)=a \mathrm{~T}_{L / K}(x)$;
(3) $\mathrm{N}_{L / K}(x y)=\mathrm{N}_{L / K}(x) \mathrm{N}_{L / K}(y)$;
(4) $\mathrm{N}_{L / K}(a x)=a^{[L: K]} \mathrm{N}_{L / K}(x)$;
(5) $\mathrm{T}_{L / K}(a)=[L: K] a$;
(6) Let $E$ be a subfield of $L$ containing $K$, i.e. $K \subseteq E \subseteq L$. Then $\mathrm{T}_{L / K}(x)=\mathrm{T}_{E / K}\left(\mathrm{~T}_{L / E}(x)\right)$.

Proof. It is obvious that the trace is additive and we know from linear algebra that the determinant is multiplicative. Moreover $r_{x y}=r_{x} r_{y}$ and $r_{x}+r_{y}=r_{x+y}$. Properties 1-5 are obvious from this plus the definition of the norm and trace (in the case of norm, remember we can suppose we are in upper triangular form).

To prove property 6 , let $a_{1}, \ldots, a_{m}$ be a basis for $E$ over $K$ and let $b_{1}, \ldots, b_{n}$ be a basis for $L$ over $E$. Then the $a_{\ell} b_{k}$ form a basis for $L / K$.

We write

$$
x b_{i}=\sum_{j=1}^{n} \beta_{i j}(x) b_{j}
$$

where $\beta_{i j}(x) \in E$ (we treat $\beta_{i j}$ as a function in $x$ ). Similarly for any $y \in E$, we write

$$
y a_{k}=\sum_{\ell=1}^{m} \alpha_{k \ell}(y) a_{\ell} .
$$

Now, $\mathrm{T}_{L / E}(x)=\sum_{i=1}^{n} \beta_{i i}(x)$ and $\mathrm{T}_{E / K}(y)=\sum_{k=1}^{n} \alpha_{k k}(y)$. Thus,

$$
\mathrm{T}_{E / K}\left(\mathrm{~T}_{L / K}(x)\right)=\sum_{i=1}^{n} \sum_{k=1}^{n} \alpha_{k k}\left(\beta_{i i}(x)\right) .
$$

On the other hand, writing

$$
x a_{k} b_{i}=\sum_{j=1}^{m} \sum_{\ell=1}^{n} \alpha_{k \ell}\left(\beta_{i j}(x)\right) a_{\ell} b_{j},
$$

we see that

$$
\mathrm{T}_{L / K}(x)=\sum_{i=1}^{n} \sum_{k=1}^{m} \alpha_{k k}\left(\beta_{i i}(x)\right),
$$

so we are done.

We'll prove transitivity of the norm (the analogue of Property 6 for norms) later with Galois theory. Trying to do the same argument for the norm is more complicated. You have to choose a basis $b_{1}, \ldots, b_{n}$ for $L$ over $E$. Then we choose different bases

$$
a_{i k}, k=1, \ldots, m
$$

for each $K$-subvector space $b_{i} E$ of $L$ so that $\beta_{i i}(x)$ is upper-triangular over $b_{i} E$. Then the argument goes through the same way.

Proposition 11.2. Let $x \in L$. Let $F(T)=T^{d}+a_{d-1} T^{d-1}+\cdots+a_{0}$ be a polynomial of minimal degree for $x$ over $K$.

$$
\mathrm{T}_{L / K}=[L: K(x)]\left(-a_{d-1}\right) .
$$

Proof. Since $\mathrm{T}_{L / K(x)}(x)=[L: K(x)] x$ and

$$
\mathrm{T}_{K(x) / K}([L: K(x)] x)=[L: K(x)] \mathrm{T}_{K(x) / K}(x)=[L: K(x)]\left(-a_{d-1}\right),
$$

this follows immediately from property 6 above.
Proposition 11.3. If $L$ is not separable over $K$, then $\mathrm{T}_{L / K}$ is identically 0.

Proof. This follows immediately from the above. If $\alpha \in L^{\text {sep }}$, we have [ $L: K(\alpha)$ is divisible by the characteristic of $K$. If $\alpha \in L \backslash L^{\text {sep }}$, then $\alpha$ satisfies a polynomial of the form $T^{p^{e}}-\gamma$, which has next to last term equal to 0 , so $T_{L / L^{\operatorname{sep}}}(\alpha)=0$.

Theorem 11.4. Let $L \supseteq K$ be a finite extension of fields. Then the bilinear form $(x, y)=\mathrm{T}_{L / K}(x y)$ is nondegenerate $\Leftrightarrow L$ is separable over $K$.

Proof. $(\Rightarrow)$ This direction is easy. We'll do the contrapositive. If $L$ is not separable over $K$, then not only is $(x, y)=\mathrm{T}_{L / K}(x y)$ degenerate, it is identically 0 .
$(\Leftarrow)$ First a quick note. We will denote $\mathrm{T}_{L / K}(x y)$ as $(x, y)$. Choosing a basis $m_{1}, \ldots, m_{n}$ and writing $x$ and $y$ as vectors in terms of the $m_{i}$ we can write

$$
\mathbf{x} A \mathbf{y}^{T}
$$

for some matrix $A$. The matrix $A$ is given by $\left[a_{i j}\right]$ where $a_{i j}=\left(m_{i}, m_{j}\right)$ since we want

$$
\left(\sum_{i=1}^{n} r_{i} m_{i}, \sum_{j=1}^{n} r_{j} m_{j}\right)=\sum_{i=1}^{n} \sum_{j=1}^{n} r_{i} r_{j}\left(m_{i}, m_{j}\right) .
$$

It is easy to see that that the form will be nondegenerate if and only if $A$ is invertible, since $A \mathbf{y}=0$ if and only $(x, y)=0$ for every $y \in L$.

Let $\theta$ generate $L$ over $K$. Then $1, \theta, \ldots, \theta^{n-1}$ for $n=[L: K]$. Let's calculate the matrix giving us $(x, y)=\mathrm{T}_{L / k}(x y)$ for this basis.

