Math 568
Notes from 10/6

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

$$r_x : a \longrightarrow xa$$

on L.

Proposition 8.1.

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) $\mathrm{T}_{L/K}(ax) = a\,\mathrm{T}_{L/K}(x)$;
(3) $\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\,\mathrm{N}_{L/K}(y)$;
(4) $\mathrm{N}_{L/K}(ax) = a^{[L:K]}\,\mathrm{N}_{L/K}(x)$;
(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 $r_{xy} = r_x r_y$ 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

$$xb_i = \sum_{j=1}^{n} \beta_{ij}(x) b_j$$

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

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

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

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

On the other hand, writing

$$xa_k b_i = \sum_{j=1}^{n} b_j \beta_{ij}(x) a_k = \sum_{j=1}^{n} \sum_{\ell=1}^{m} \alpha_{k\ell}(\beta_{ij}(x)) a_\ell b_j,$$

we see that

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

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

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

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

Proposition 8.2. *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.*

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

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

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

this follows immediately from property 6 above. □

Proposition 8.3. *If L is not separable over K, then $\mathrm{T}_{L/K}$ is identically 0.*

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

Theorem 8.4. *Let $L \supseteq K$ be a finite extension of fields. Then the bilinear form $(x, y) = \mathrm{T}_{L/K}(xy)$ is nondegenerate $\Leftrightarrow$ L is separable over K.*

Proof. ($\Rightarrow$) This direction follows immediately from the Proposition above.

($\Leftarrow$) Next time.

□

Before proving the other direction of the theorem above, we will use it to show that the integral closure of a Dedekind domain in a finite separble extension is a Dedekind domain.

Now, given a bilinear from (x, y) on a vector space W, we get a map from $\psi : W \longrightarrow W^*$, where W^* is the dual of W by sending $x \in W$ to the map $f(y) = (x, y)$. When the form is nondegenerate this map is injective. Thus, by dimension counting, when W is finite dimensional and the form is nondegenerate, we get an isomorphism of vector spaces. In particular, we can do the following. Let $u_1, \ldots, u_n$ be a basis for W over V. Then for each u_i, there is a map $f_i \in W^*$ such that $f_i(u_j) = \delta_{ij}$ where δ_{ij} is the Kronecker delta, which means that $\delta_{ij} = 0$ if $i \neq j$ and $\delta_{ij} = 1$ if $i = j$. Since $f_i(x) = (v_j, x)$ for some $v_j \in W$, we obtain a dual basis $v_1, \ldots, v_n$ with the property that

$$(v_i, u_j) = \delta_{ij}.$$

Thus, we have the following.

Theorem 8.5. *(Dual basis theorem) Let $L \supseteq K$ be a finite, separable extension of fields. Let $u_1, \ldots, u_n$ be basis for L as a K-vector space. Then there is a basis $v_1, \ldots, v_n$ for L as a K-vector space such that*

$$\mathrm{T}_{L/K}(v_i, u_j) = \delta_{ij}.$$

Proof. Since $(x, y) = \mathrm{T}_{L/K}(xy)$ is a nondegenerate bilinear form on L (considered as a K-vector space), we may apply the discussion above. □

Definition 8.6. Let $L \supseteq K$ be a separable field extension. Let M be a submodule of L. We define $M^\dagger$ to be set

$$\{x \in L \mid T_{L/K}(xy) \in A \text{ for every } y \in M\}$$

Remark 8.7. It is clear that $M \subseteq N \Rightarrow M^\dagger \supseteq N^\dagger$, by definition of the dual module.

As usual, A is a Dedekind domain with field of fractions K and B is the integral closure of A in a finite separable extension L of K.

Lemma 8.8. *Let M be an A-submodule of L for which*

$$M = Bu_1 + \cdots + Bu_n$$

for $u_1, \ldots, u_n$ a basis for L over K. Then $M^\dagger$ is equal to $Bv_1 + \cdots + Bv_n$ for $v_1, \ldots, v_n$ a dual basis for $u_1, \ldots, u_n$ with respect to the bilinear form induced by the trace.

Proof. Let $x \in L$. Then $x \in M^\dagger$ if and only if $T_{L/K}(xu_i) \in A$ for each u_i. Writing x as $\sum_{i=1}^{n} \alpha_i v_i$ with $\alpha_i \in K$, we see that $T_{L/K}(xu_i) = \alpha_i$, so $T_{L/K}(xu_i) \in R$ if and only if $\alpha_i \in R$. This completes our proof. □

Theorem 8.9. *Let A be a Dedekind domain with field of fractions K and let $L \supseteq K$ be a finite, separable extension of fields. Let B be the integral closure of A in L. Then B a finitely generated A-module. In particular B is Noetherian as a ring and is therefore Dedekind.*

Proof. We already know that B is 1-dimensional, integrally closed, and an integral domain. We need only show that it is Noetherian.

Then $B \subset B^\dagger$ since B is integral over A (recall B integral over A means that the coefficients of the minimal polynomial for B over A are all in A). Now, we choose a basis $u_1, \ldots, u_n$ for L over K. I claim that we can choose the u_i to be in B. This is because for any $u \in L$ we have

$$u^m + \frac{x_{m-1}}{y_{m-1}} u^{m-1} + \cdots + \frac{x_0}{y_0} = 0$$

with x_i and y_i in A. Replacing u with $u' = \prod_{i=1}^{m} y_i$ and multiplying through by $(\prod_{i=1}^{m} y_i)^m$ converts this into an integral monic equation in u' as we've seen before. Thus, we can take our basis u_i, replace each u_i with a multiple of u_i and still have a basis. Let $v_1, \ldots, v_n$ be a dual basis for $u_1, \ldots, u_n$ with respect to the trace form. Then the A-module generated by the v_i contains $B^\dagger$. So we have

$$B \subseteq B^\dagger \supseteq Av_1 + \cdots + Av_n$$

which implies that B is contained in a finitely generated A-module, which in turn implies that B is Noetherian as an A-module. Hence, B is Noetherian as a B-module and is a Noetherian ring. □