Math 430 Tom Tucker
NOTES FROM CLASS 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

$$r_x : a \longrightarrow xa$$

on L.

Proposition 9.1. *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 transitivity of trace. □

Proposition 9.2. *If L is not separable over K, then $\mathrm{T}_{L/K}$ is identically 0.*

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

Theorem 9.3. *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. ($\Rightarrow$) Follows immediately from the above.

($\Leftarrow$) We will denote $\mathrm{T}_{L/K}(xy)$ as (x, y). Recall the following: 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 $[a_{ij}]$ where $a_{ij} = (m_i, m_j)$ since we want

$$(\sum_{i=1}^{n} r_i a_i, \sum_{j=1}^{n} s_j a_j) = \sum_{i=1}^{n}\sum_{j=1}^{n} r_i s_j (a_i, a_j).$$

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 $y \in L$.

Now, since L is separable over K, we can write $L = K(\theta)$ for $\theta \in L$ and use $1, \theta, \ldots, \theta^{n-1}$ as a basis for L over K. Then we can write the matrix $A = [a_{ij}]$ above with

$$a_{ij} = (\theta^i, \theta^j) = \mathrm{T}_{L/K}(\theta^{i+j}).$$

It isn't too hard to calculate these coefficients explicitly. In fact, if $\theta_1, \ldots, \theta_n$ are the roots of the minimal polynomial of θ, then

$$\mathrm{T}_{L/K}(\theta) = \sum_{\ell=1}^{n} \theta_\ell,$$

from what we proved earlier. Similarly, we have

$$\mathrm{T}_{L/K}(\theta^{i+j}) = \sum_{\ell=1}^{n} \theta_\ell^{i+j}.$$

There is a trick to finding the determinant of such a matrix. Recall the van der Monde matrix in $V := V(\theta_1, \ldots, \theta_n)$. It is the matrix

$$\begin{pmatrix} 1 & \cdots & 1 \\ \theta_1 & \cdots & \theta_n \\ \cdots & \cdots & \cdots \\ \theta_1^n & \cdots & \theta_n^n \end{pmatrix}$$

The determinant of this matrix is

$$\det(V) = \prod_{i<j} (\theta_i - \theta_j).$$

It is easy to check that $VV^T = A$ (a messy but easy calculation). Thus,

$$\det(A) = \det(V)\det(V^T) = \det(V)^2 = \left(\prod_{i>j} (\theta_i - \theta_j)\right)^2 \neq 0,$$

since $\theta_i \neq \theta_j$ for $i \neq j$ and we are done.

□

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 9.4. *(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 9.5. 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 9.6. It is clear that $M \subseteq N \Rightarrow M^\dagger \supseteq N^\dagger$, by definition of the dual module.

Lemma 9.7. *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 9.8. *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 is 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. $\square$