## Math 513 Tom Tucker <br> NOTES FROM CLASS 9/29

We were proving the following:
Theorem 12.1. 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. $(\Rightarrow)$ We did last time.
$(\Leftarrow)$ We will denote $\mathrm{T}_{L / K}(x y)$ 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 $\left[a_{i j}\right]$ where $a_{i j}=\left(m_{i}, m_{j}\right)$ since we want

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

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 $y \in L$.

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 $A=\left[a_{i j}\right]$ above with

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

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 $\theta$, then

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

from what we proved earlier. Similarly, we have

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

There is a trick to finding the determinant of such a matrix. Recall the van der Monde matrix in $V:=V\left(\theta_{1}, \ldots, \theta_{n}\right)$. It is the matrix

$$
\left(\begin{array}{lll}
1 & \cdots & 1 \\
\theta_{1} & \cdots & \theta_{n} \\
\cdots & \cdots & \cdots \\
\theta_{1}^{n} & \cdots & \theta_{n}^{n}
\end{array}\right)
$$

1

The determinant of this matrix is

$$
\operatorname{det}(V)=\prod_{i<j}\left(\theta_{i}-\theta_{j}\right)
$$

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

$$
\operatorname{det}(A)=\operatorname{det}(V) \operatorname{det}\left(V^{T}\right)=\operatorname{det}(V)^{2}=\left(\prod_{i<j}\left(\theta_{i}-\theta_{j}\right)\right)^{2} \neq 0
$$

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 $f_{i}\left(u_{j}\right)=\delta_{i j}$ where $\delta_{i j}$ is the Kronecker delta, which means that $\delta_{i j}=0$ if $i \neq j$ and $\delta_{i j}=1$ if $i=j$. Since $f_{i}(x)=\left(v_{j}, x\right)$ for some $v_{j} \in W$, we obtain a dual basis $v_{1}, \ldots, v_{n}$ with the property that

$$
\left(v_{i}, u_{j}\right)=\delta_{i j} .
$$

Thus, we have the following.
Theorem 12.2. (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

$$
\mathrm{T}_{L / K}\left(v_{i}, u_{j}\right)=\delta_{i j} .
$$

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

Definition 12.3. Let $L \supseteq K$ be a separable field extension. Let $M$ be a submodule of $L$. We define $M^{\dagger}$ to be set

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

Remark 12.4. It is clear that $M \subseteq N \Rightarrow M^{\dagger} \supseteq N^{\dagger}$, by definition of the dual module.

Lemma 12.5. Let $M$ be an $A$-submodule of $L$ for which

$$
M=B u_{1}+\cdots+B u_{n}
$$

for $u_{1}, \ldots, u_{n}$ a basis for $L$ over $K$. Then $M^{\dagger}$ is equal to $B v_{1}+\cdots+B v_{n}$ 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 $T_{L / K}\left(x u_{i}\right) \in A$ for each $u_{i}$. Writing $x$ as $\sum_{i=1}^{n} \alpha_{i} v_{i}$ with $\alpha_{i} \in K$, we see that $T_{L / K}\left(x u_{i}\right)=\alpha_{i}$, so $T_{L / K}\left(x u_{i}\right) \in R$ if and only if $\alpha_{i} \in R$. This completes our proof.
Theorem 12.6. 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 $u^{\prime}=\prod_{i=1}^{m} y_{i}$ and multiplying through by $\left(\prod_{i=1}^{m} y_{i}\right)^{m}$ converts this into an integral monic equation in $u^{\prime}$ 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

$$
B \subseteq B^{\dagger} \supseteq A v_{1}+\cdots+A v_{n}
$$

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.

