Math 430 Tom Tucker
NOTES FROM CLASS 9/22

Back to showing that $\mathcal{O}_K$ is Dedekind. All we need is to do is show that $\mathcal{O}_K$ is Noetherian and one-dimensional. For R-modules (R a ring), it is easy to see that M satisfies the Noetherian ascending chain condition if and only if every submodule of M is finitely generated (as an R-module).

Proposition 8.1. *Let R be a ring, let M' and M'' be Noetherian R-modules and let*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

be an exact sequence of R-modules. Then M is Noetherian.

Proof. We denote the map from M' into M as i and the map from M to M'' as ϕ. It will suffice to show that every submodule N of M is finitely generated. Since $\phi(N)$ is a submodule N of M'' it is finitely generated by, say, $x_1, \ldots, x_m$. Since $N \cap i(M')$, which we denote as N', is a submodule of $i(M')$, it is finitely generated by, say, $y_1, \ldots, y_n$. For each x_i, let $z_i \in N$ have the property that $\phi(z_i) = x_i$ and let N'' be the module they generate in N. Then N is generated by $y_1, \ldots, y_n, z_1, \ldots, z_m$ since given any $t \in N$ we can write $\phi(t) = \sum_{i=1}^m r_i \phi(z_i)$, so

$$\phi(t) - \sum_{i=1}^m r_i z_i \in N \cap i(M),$$

and $N = N' + N''$. □

Corollary 8.2. *Let A be a Noetherian ring and let M be a finitely generated A-module. Then M is a Noetherian A-module*

Proof. We proceed by induction on the number of generators of M as an A-module. If M has one generator, then it is isomorphic to some quotient of A, so we're done. Otherwise, let $x_1, \ldots, x_n$ generate M and write

$$0 \longrightarrow Rx_n \longrightarrow M \longrightarrow M/(Rx_n) \longrightarrow 0.$$

Then $M/(Rx_n)$ is generated by the images of $x_1, \ldots, x_{n-1}$, so must be Noetherian by the inductive hypothesis. By the Lemma above, M must be Noetherian. □

Corollary 8.3. *Let A be a Noetherian ring and let $B \supseteq A$ be finitely generated as an A-module. Then B is a Noetherian ring.*

Proof. By the corollary above, B is a Noetherian A-module, so every ideal of B is finitely generated as an A-module, hence also as a B-module. □

Theorem 8.4. *Let A be a Dedekind domain with field of fractions K. Let L be a finite separable extension of A. Then the integral closure B of A in L is a Dedekind domain.*

From some work we've done, all we'll have to do is show that B is contained in a finitely generated A-module. We'll use something called a dual basis, the existence of which is proven using the separable basis theorem. All we need to do is show it is Noetherian.

The separable basis theorem. Here is the basic set-up for today. Let L be a finite algebraic extension of degree n over K. Since L is a vector space over K and multiplication by an element x in L preserves the K-structure of L, we see that

$$r_x : z \mapsto xz$$

is a K-linear invertible map from L to L. Given a basis $m_1, \ldots, m_n$ for L over K, we can write

$$r_x m_i = \sum_{i=1}^{n} a_{ij} m_j$$

for $m_1, \ldots, m_n$. We have the usual definitions for the norm and trace of r_x below

$$\mathrm{T}_{L/K}(x) := \mathrm{T}_{L/K}(r_x) = \sum_{i=1}^{n} a_{ii}$$
$$\mathrm{N}_{L/K}(x) := \mathrm{N}_{L/K}(r_x) = \det([a_{ij}]).$$

In other words, if r_x gives the matrix M, then the trace is the sum of the diagonal elements and the norm is the product of the diagonal elements. It turns out that this definition doesn't depend on the choice of basis. This is a standard fact from linear algebra. It follows from the fact that for any matrix $n \times n$ M and any invertible $n \times n$ matrix U, we have

$$\mathrm{T}_{L/K}(M) = \mathrm{T}_{L/K}(UMU^{-1})$$

and

$$\mathrm{N}_{L/K}(M) = \mathrm{N}_{L/K}(UMU^{-1}).$$

You may recall in fact that the characteristic polynomial $\det(\lambda I - [a_{ij}])$ of a matrix is invariant under conjugation, and that by putting a matrix into upper-triangular form $[a_{ij}]$, the norm $\mathrm{N}_{L/K}(M)$ is $(-1)^n$ times the constant term of the characteristic polynomial and that $\mathrm{T}_{L/K}(M)$ is -1 times the the coefficient of λ^{n-1}. Recall that by Cayley-Hamilton each $b \in L$ must satisfy its own characteristic polynomial $P(\lambda) = 0$ where $P(\lambda) = \det(\lambda I - [a_{ij}])$. Thus, when $L = K(b)$, the polynomial $P(\lambda)$ has the same degree as the minimal polynomial for b

over K and must therefore be the minimal monic polynomial for b over K. This gives us an easy definition of the trace and norm in terms of the minimal polynomial for b over K. Suppose that the minimal monic for b over K is given by

$$f(b) = b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0.$$

Then

$$\mathrm{T}_{K(b)/K}(b) = -a_{n-1} = \sum_{b_i} -b_i$$

and

$$\mathrm{N}_{K(b)/K}(b) = (-1)^n a_0 = (-1)^n \prod_{b_i} b_i,$$

where the b_i are the conjugates of b_i in an algebraic closure of K.

Let $(\cdot,\cdot)$ be the bilinear pairing given by $(a,b) = T_{L/K}(ab)$ for $a, b \in L$. It is easy to see that this is a K-bilinear pairing. We'll work towards showing the following.

Theorem 8.5. *The trace pairing given above is nondegenerate if and only if L is separable over K.*

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 8.6. *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,

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

On the other hand, writing

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

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.

□