Math 531 Tom Tucker
NOTES FROM CLASS 9/24

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 10.1. *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 10.2. *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 10.3. *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. □

What's the problem in general then for showing that $\mathcal{O}_L$ is Dedekind for L a number field? The big problem is showing that it is $\mathcal{O}_L$ is finitely generated as a $\mathbb{Z}$-module. It is integrally closed and we alter one of the Lemmas above to show that it is one-dimensional. Here is the proof of that.

Lemma 10.4. *Let A be a field and let $B \supseteq A$ be an integral domain that is integral over A. Then B is a field.*

Proof. Any nonzero prime $\mathcal{Q}$ of B must intersect A in a nonzero ideal, but A has no nonzero ideals. □

Proposition 10.5. *Let A and B be integral domains with $A \subset B$ and B integral over A. Suppose that A is 1-dimensional. Then B is 1-dimensional.*

Proof. First, note that B cannot be 0-dimensional; that is, it cannot be a field (I'll fix up the proof of this next time). Let $\mathcal{Q}$ be a nonzero prime in B. Then $\mathcal{Q} \cap A = \mathcal{P}$ for $\mathcal{P}$ a nonzero prime of A. Thus, we have a natural inclusion

$$A/\mathcal{P} \subseteq B/\mathcal{Q}.$$

Since B is integral over A, every element of $B/\mathcal{Q}$ is algebraic over $A/\mathcal{P}$. Thus, $B/\mathcal{Q}$ is a field, since any domain that is an algebraic extension of a field is itself a field. □

So all we need to do is show that $\mathcal{O}_L$ is Noetherian for a number field L. We'll show something a little more general. We'll show the following.

Theorem 10.6. *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.

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

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

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 show the following next time.

Theorem 10.7. *The trace pairing given above is nondegenerate if and only if L is separable over K.*