Math 430 Tom Tucker
NOTES FROM CLASS 08/30/21

First a few quick notes:

One quick note on unique factorization. More on this later. In what follows, A will also be an integral domain. We say two elements $a, b \in A$ are associates if $Aa = Ab$.

Definition 2.1. Let A be an integral domain. We say that a non-unit $a \in A$ is *irreducible* if if $a = bc$ means that b or c is a unit.

Definition 2.2. Let A be an integral domain. We say that a non-unit $\pi \in A$ is *prime* if $\pi \mid bc$ implies $\pi \mid b$ or $\pi \mid c$.

Note that a prime is irreducible, since if π is prime and $\pi = bc$, then either $\pi \mid b$ or $\pi \mid c$. Suppose WLOG that $\pi \mid b$. Then we have $bc = w\pi c = \pi$ so $wc = 1$ and thus c is a unit. In general, however, an irreducible need not be prime. Take $\sqrt{6}$ in the ring $\mathbb{Z}[\sqrt{-6}]$, for example.

Now suppose that every element of A has unique factorization into irreducibles, which means that for any $a \in A$ factors into irreducible elements and if furthermore, if we have

$$ub_1 \cdots b_m = wc_1 \cdots c_n$$

for units u, w and irreducibles, $b_1, \dots, b_m, c_1 \dots, c_n$, then we have $m = n$ and permutation σ of $\{1, \dots, m\}$ such that for each a_i, the element $b_{\sigma(i)}$ is an associate of a_i. Note that if A has unique factorization, then every irreducible element of A is prime since if $a \mid bc$, then some associate of a appears in the factorization of b or c and thus a divides b or c.

Thus, in a UFD, everything factors into primes.

Now, a quick note about how to tell when something is integral by looking at its minimal polynomial.

Proposition 2.3. *(Prop. 2.5 from Janusz) Let R be a domain with field of fractions K and let L be an algebraic extension of K. Let $b \in L$ and let $f(X)$ be the minimal polynomial for b that has coefficients in K and leading coefficient 1. Then, the coefficients of f are integral over R whenever b is integral over R. In particular, if R is integrally closed in K and b is integral over R, then the coefficients of f are in R.*

Proof. Suppose that b is integral over R. We can write

$$f(X) = (X - b_1)(X - b_2) \cdots (X - b_n),$$

by extending L to some field E over which f splits. Note that any polynomial satisfied by b is divisible by f in $K[X]$, so if b satisfies an integral polynomial with coefficients in R, so do all of the other b_i.

Hence, if b is integral then so are all of the b_i. The coefficients of f are all in the ring $R[b_1, \ldots, b_n]$, so this also means that the coefficients of f are integral over R as desired. Now, since these coefficients are also in K, they are actually in R if R is integrally closed. $\square$

So, to check if something is integral, all we have to do is check its minimal polynomial. Example, let $\alpha = \sqrt{11}/7$. Its minimal polynomial is $X^2 - 11/49$ which isn't integral over $\mathbb{Z}$, so we're done.

Theorem 2.4. *(Cayley-Hamilton) Let $A \subseteq B$. Suppose that M is a finitely generated A-module with generators $m_1, \ldots, m_n$. Suppose that that M is also a faithful $A[b]$-module (this means the only element that annihilates all of M is 0) and that b acts on the generators m_i in the following way*

$$bm_i = \sum_{j=1}^{n} a_{ij} m_j. \tag{1}$$

Then b satisfies the equation

$$\det \begin{pmatrix} b - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & b - a_{22} & \cdots & -a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n2} & -a_{n1} & \cdots & b - a_{nn} \end{pmatrix} = 0.$$

Proof. Let T be the matrix $bI - [a_{ij}]$. The theorem then says that $\det T = 0$. Notice that we can consider T as an endomorphism of M^n by writing

$$\begin{pmatrix} b - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & b - a_{22} & \cdots & -a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n2} & -a_{n1} & \cdots & b - a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \cdot \\ \cdot \\ x_n \end{pmatrix} = \begin{pmatrix} bx_1 - \sum_{j=1}^{n} a_{1j} x_j \\ \cdot \\ \cdot \\ bx_n - \sum_{j=1}^{n} a_{nj} x_j \end{pmatrix}$$

where the x_i are elements of M. Let $(x_1, \ldots, x_n)$ be $(m_1, \ldots, m_n)$, we obtain

$$\begin{pmatrix} b - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & b - a_{22} & \cdots & -a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n2} & -a_{n1} & \cdots & b - a_{nn} \end{pmatrix} \begin{pmatrix} m_1 \\ \cdot \\ \cdot \\ m_n \end{pmatrix} = \begin{pmatrix} bm_1 - \sum_{j=1}^{n} a_{1j} m_j \\ \cdot \\ \cdot \\ bm_n - \sum_{j=1}^{n} a_{nj} m_j \end{pmatrix} = \begin{pmatrix} 0 \\ \cdot \\ \cdot \\ 0 \end{pmatrix}$$

by equation (1). Now, recall from linear algebra (exercise) that there is a matrix U, called the *adjoint* of T, for which $UT = (\det T)I$. We obtain

$$\begin{pmatrix} \det T & 0 & \cdots & 0 \\ 0 & \det T & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \det T \end{pmatrix} \begin{pmatrix} m_1 \\ \cdot \\ \cdot \\ m_n \end{pmatrix} = \begin{pmatrix} (\det T)m_1 \\ \cdot \\ \cdot \\ (\det T)m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \cdot \\ \cdot \\ 0 \end{pmatrix}$$

so $(\det T)m_i = 0$ for each m_i. Hence $(\det T) = 0$, since $(\det T) \in A[b]$ and $A[b]$ acts faithfully on M. □

Corollary 2.5. *Let $A \subseteq B$ and let $b \in B$. If $A[b] \subseteq B' \subseteq B$ for a ring B' that is finitely generated as an A-module, then b is integral over A.*

Proof. Since $b \in B'$, multiplication by b sends B' to B'. Moreover, the resulting map is A-linear (by distributivity of multiplication). The action of $A[b]$ on B' must be faithful since $c \cdot 1 = 0$ implies $c = 0$.

Let $m_1, \ldots, m_n$ generate B' as an A-module. Then, for each i with $1 \le i \le n$, we can write

$$bx_i = \sum_{j=1}^{n} a_{ij}x_j.$$

Clearly, the equation

$$\det \begin{pmatrix} b - a_{11} & -a_{21} & \cdots & -a_{n1} \\ -a_{12} & b - a_{22} & \cdots & -a_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{1n} & -a_{2n} & \cdots & b - a_{nn} \end{pmatrix} = 0$$

is integral. □

For now, let's note the following corollary.

Corollary 2.6. *Let $A \subseteq B$. Then the set of all elements in B that are integral over A is a ring.*

Proof. We need only show that the elements in B that are integral over A forms a ring. If α and β are integral over A, then $A[\alpha, \beta]$ is finitely generated as an A-module. Hence, $-\alpha$, $\alpha + \beta$, and $\alpha\beta$ are all integral over A since they are contained in $A[\alpha, \beta]$, by the Cayley-Hamilton theorem above. □

The following is immediate.

Corollary 2.7. *Let K be an extension of $\mathbb{Q}$. Then the set of all elements in K that are integral over $\mathbb{Z}$ is a ring.*

Again let $A \subseteq B$. The set B' of elements of B that are integral over A is a ring. We call this ring B' the *integral closure of A in B*.

Definition 2.8. Let K be a number field (a finite extension of $\mathbb{Q}$). The *ring of integers* of K is the integral closure of $\mathbb{Z}$ in K. We denote is as $\mathcal{O}_K$.

Ask if people have seen localization.

Definition 2.9. We say that a domain B is integrally closed if it is *integrally closed* in its field of fractions.

Proposition 2.10. *Let $A \subseteq B$, where A and B are domains. The ring B is integrally closed over A if and only if B is integrally closed in its field of fractions.*

Proof. Exercise. □

Example 2.11. Any unique factorization domain is integrally closed. (Exercise.)

Let's do a preview of what properties we want rings of integers to have. First let's recall some features of $\mathbb{Z}$:

(1) $\mathbb{Z}$ is Noetherian.

(2) $\mathbb{Z}$ is 1-dimensional.

(3) $\mathbb{Z}$ is a unique factorization domain.

(4) $\mathbb{Z}$ is a principal ideal domain.

Recall what a Noetherian ring is.

Definition 2.12. A ring R is *Noetherian* if every ideal is finitely generated as an R-module. Equivalently, R is if every ascending chain of ideals terminates.

Incidentally, we will later see that the conditions (1) and (2) are often equivalent in the situations we examine.

The rings $\mathcal{O}_K$ will have the properties that

(1) $\mathcal{O}_K$ is Noetherian.

(2) $\mathcal{O}_K$ is 1-dimensional.

(3) $\mathcal{O}_K$ has unique factorization *for ideals*.

(4) $\mathcal{O}_K$ is *locally* a principal ideal domain.

(5) It is possible that $\mathcal{O}_K$ is not a unique factorization domain and that it is not a principal ideal domain.

In fact, any subring B of a number field K that is integral over $\mathbb{Z}$ will be Noetherian and 1-dimensional. That is the Krull-Akizuki theorem which we will eventually prove.

We used the work "locally" above. Let's define it.