

Lecture 10.

1) Integral closure, cont'd.

2) Localization

BONUS: Proof of Thm (I) in Section 1.3

Refs: [AM], Section 5.3, Chapter 3; [V], Section 9.3

1) A is comm'v unital ring, B is an A -algebra. Recall (Section 2 of Lecture 9, the integral closure:

$$\bar{A}^B = \{b \in B \mid b \text{ is integral over } A\}, \text{ } A\text{-subalgebra in } B.$$

1.0) Fraction fields.

Suppose A is a domain. We can form its fraction field $\text{Frac}(A)$. By definition, it consists of fractions $\frac{a}{b}$ w. $a, b \in A$, $b \neq 0$.

In $\text{Frac}(A)$ we have $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$. The fractions are added & multiplied in the usual way. A direct check shows that $\text{Frac}(A)$ is a field.

Note that A has a ring embedding into $\text{Frac}(A)$: $a \mapsto \frac{a}{1}$.

Moreover, every embedding $\varphi: A \hookrightarrow L$ factors as

$A \hookrightarrow \text{Frac}(A) \hookrightarrow L$, where the latter is $\frac{a}{b} \mapsto \frac{\varphi(a)}{\varphi(b)}$.

Examples:

- $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$.
- For a field F , we have $\text{Frac}(F[x_1, \dots, x_n]) = F(x_1, \dots, x_n)$, the field of rational functions in n variables.

- Let $d \in \mathbb{Z}$, not a complete square. Then $\mathbb{Z}[\sqrt{d}]$ is a domain & $\text{Frac}(\mathbb{Z}[\sqrt{d}]) = \mathbb{Q}[\sqrt{d}]$.

1.1) Normal domains.

Let A be a domain.

Definition:

i) The normalization of A is $\bar{A}^{\text{Frac}(A)}$, integral closure of A in $\text{Frac}(A)$.

ii) A is normal if A coincides w. its normalization.

Special cases:

1) L is a field, $A \subset L$ is a subring. Claim: \bar{A}^L is normal.

Indeed, \bar{A}^L is integr. closed in L & $\text{Frac}(\bar{A}^L) \subset L \Rightarrow \bar{A}^L$ closed in $\text{Frac}(\bar{A}^L)$.

2) UFD \Rightarrow normal: let A be UFD & $\frac{a}{b} \in \text{Frac}(A)$ w. coprime $a, b \in A$. Need to show: $\frac{a}{b}$ is integral over $A \Rightarrow \frac{a}{b} \in A$ i.e. b is invertible. Let $f(x) = x^k + c_{k-1}x^{k-1} + \dots + c_1x + c_0$ ($c_i \in A$) be s.t. $f\left(\frac{a}{b}\right) = 0 \Rightarrow 0 = b^k f\left(\frac{a}{b}\right) = a^k + \sum_{i=0}^{k-1} c_i a^i b^{k-i}$

The sum is divisible by b . So $a^k \equiv 0 \pmod{b}$. Since a & b are coprime, this implies that b is invertible.

Exercise: Let L be a field & $A_1, A_2 \subset L$ be normal subrings. Prove that $A_1 \cap A_2$ is normal. Prove the analogous claim for infinite intersections.

1.2) Examples of computation of integral closure.

Example 1: compute the integral closure of $A = \mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ is a square-free number. We need to understand when $\beta \in \mathbb{Q}(\sqrt{d})$, $\beta = a + b\sqrt{d}$ ($a, b \in \mathbb{Q}$), is integral over \mathbb{Z} .

Lemma 1: TFAE

(i) β is integral over \mathbb{Z} ,

(ii) $2a, a^2 - b^2d \in \mathbb{Z}$.

Proof: We set $\bar{\beta} := a - b\sqrt{d}$. Note that: $\beta + \bar{\beta} = 2a$, $\beta\bar{\beta} = a^2 - b^2d$, rational numbers. So $(x - \beta)(x - \bar{\beta}) = x^2 - 2ax + (a^2 - b^2d)$

So (ii) \Rightarrow (i).

On the other hand, note that $\beta \mapsto \bar{\beta}$ is a homomorphism $\mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{Z}[\sqrt{d}]$. So for $f(x) \in \mathbb{Z}[x]$ we have $f(\bar{\beta}) = \overline{f(\beta)}$. So if $f(\beta) = 0$, then $f(\bar{\beta}) = 0$. In particular, if β is integral over \mathbb{Z} , then β is integral. By Proposition 1 of Section 2 of Lecture 9, $\beta + \bar{\beta}, \beta\bar{\beta} \in \mathbb{Q}$ are integral over \mathbb{Z} . But \mathbb{Z} is UFD, hence normal. So elements of \mathbb{Q} integral over \mathbb{Z} are integers. (ii) follows. \square

Exercise (Number thy): If $d \equiv 2$ or $3 \pmod{4}$, then (ii) \Leftrightarrow $a, b \in \mathbb{Z}$;

if $d \equiv 1 \pmod{4}$, then (ii) \Leftrightarrow either $a, b \in \mathbb{Z}$ or $a, b \in \mathbb{Z} + \frac{1}{2}$.

Corollary: i) $\mathbb{Z}[\sqrt{d}]$ is normal $\Leftrightarrow d \equiv 2$ or $3 \pmod{4}$.

If $d \equiv 1 \pmod{4}$, then the normal'n of $\mathbb{Z}[\sqrt{d}]$ is $\left\{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \text{ or } a, b \in \mathbb{Z} + \frac{1}{2} \right\}$.

ii) $\mathbb{Z}[\sqrt{-5}]$ is normal but not UFD.

Example 2: Consider the ring $A = \mathbb{C}[x, y]/(y^2 - f(x))$, $f(x) \in \mathbb{C}[x]$

Exercise: This ring is a domain $\Leftrightarrow f(x)$ is not a complete square

Fact (going beyond what we cover in this class) A is normal $\Leftrightarrow f(x)$ has no repeated roots (\Leftrightarrow the curve $\{(x, y) \mid y^2 = f(x)\}$ is "non-singular" – compute the Jacobian vector of $(x, y) \mapsto y^2 - f(x)$).

We consider the special case $f(x) = x^3$ and describe the normalization in this case. Let's write \bar{x}, \bar{y} for the images of x, y in A .

Exercise: the elements $\bar{x}^k, \bar{x}^k \bar{y}$ for $k \geq 0$ form a basis in A (for any f , in fact).

Lemma 2: The integral closure of A in $K := \text{Frac}(A)$ coincides w. $\mathbb{C}[\underline{y/x}]$ (and so is isomorphic to the polynomial algebra). In particular, A isn't normal.

Proof: We have $\bar{y}^2 = \bar{x}^3$ in A . So for $t := \bar{y}/\bar{x} \in K$ we have $t^2 = \bar{x}$ meaning t is integral over A . Let $\tilde{A} := \mathbb{C}[t] \subset K$ (exercise: t is transcendental over \mathbb{C}). We have $\bar{x} = t^2, \bar{y} = t^3$ so $A \subset \tilde{A}$. But for any domain $A' \subset K$ have $\text{Frac}(A') \subset K$. Since $A \subset \tilde{A}$ have $K = \text{Frac}(\tilde{A})$. Since \tilde{A} is generated by an element integral over A , its integral over A . As we've seen in Section 1.1, \tilde{A} is

normal. So \tilde{A} is the normalization of A and A is not normal \square

1.3) Finiteness of integral closures.

Let A be a domain, $K = \text{Frac}(A)$, $K \subset L$ finite field ext'n.

Q: Is \tilde{A}^L finite over A ?

A: It's complicated...

Theorem: Assume that one of the following holds:

(I) A is Noeth'n & normal, $\text{char } K=0$.

(II) A is a fin. gen'd algebra over a field or over \mathbb{Z} .

Then \tilde{A}^L is finite over A .

Proof under (I) will appear as a bonus.

Example: Let $A = \mathbb{Z}$, L is a finite extension of \mathbb{Q} . The ring \tilde{A}^L is called the ring of algebraic integers in L (crucially important for Alg. Number thy). Both (I) & (II) apply, so Thm $\Rightarrow \tilde{A}^L$ is finite over \mathbb{Z} , i.e. is a fin. gen'd abelian group.

Fact/Premium exercise: As an abelian group, $\tilde{A}^L \cong \mathbb{Z}^n$, where $n = \dim_{\mathbb{Q}} L$.

(Hint: observe that since \tilde{A}^L is a domain, $n\alpha = 0$ for $\alpha \in \tilde{A}^L$ implies $n=0$ or $\alpha=0$, so $\tilde{A}^L \cong \mathbb{Z}^n$ for some n . Then observe that $\forall \beta \in L \exists k \in \mathbb{Z} \setminus \{0\}$ s.t. $k\beta \in \tilde{A}^L$)

2) Localization.

Localizations of rings generalize the fraction fields of domains. To construct a localization of A we need a suitable subset in A .

Definition: A subset $S \subset A$ is **multiplicative** if

- $1 \in S$
- $s, t \in S \Rightarrow st \in S$

Examples:

0) $S = \{\text{all invertible elements in } A\}$ is multiplicative.

1) If A is a domain, then $S = A \setminus \{0\}$ is multiplicative.

1') For general A , $S := \{\text{all nonzero divisors of } A\}$ is multiplicative.

2) For $f \in A$, the subset $S := \{f^n \mid n \geq 0\}$ is multiplicative.

2') For $f_1, \dots, f_k \in A \rightsquigarrow S := \{f_1^{n_1} \dots f_k^{n_k} \mid n_i \geq 0\}$ is multiplicative.

3) Let $\mathfrak{p} \subset A$ be prime ideal $\Rightarrow S := A \setminus \mathfrak{p}$ is multiplicative

$1 \in S \Leftrightarrow 1 \notin \mathfrak{p}; \quad s, t \in S \Leftrightarrow s, t \notin \mathfrak{p} \Rightarrow st \notin \mathfrak{p}$ (the last implication uses that \mathfrak{p} is prime) $\Rightarrow st \in S$.

BONUS: Proof of Theorem in Section 1.3 under assumption (I).

Proof: Let $\dim_K L = n$. Every element $\alpha \in L$ gives the K -linear operator, say, m_α , on L via multiplication. So for $\alpha \in L$ it makes sense to speak about $\text{tr}(\alpha) := \text{tr}(m_\alpha) \in K$.

Step 1: We claim that for $\alpha \in \bar{A}^L$ we have $\text{tr}(\alpha) \in A$. Let $f(x) \in A[x]$ be a monic polynomial w/ $f(\alpha) = 0$. Choose an algebraic extension \tilde{L} of L where $f(x)$ decomposes into linear factors. All eigenvalues of m_α are roots of $f(x)$, hence are integral over A . Therefore $\text{tr}(\alpha)$ - the sum of eigenvalues - is integral over A . But $\text{tr}(\alpha) \in K$ and, since A is normal, we see $\text{tr}(\alpha) \in A$.

Step 2: For $\alpha, \beta \in L$ define $(\alpha, \beta) := \text{tr}(\alpha\beta)$. This is a symmetric K -bilinear form $L \times L \rightarrow K$. We claim that since $\text{char } K = 0$, this bilinear form is nondegenerate. More precisely, for $u \in L \setminus \{0\}$ $\exists m > 0$ s.t. $(u, u^{m-1}) = \text{tr}(u^m) \neq 0$. Let $u_1 = u, u_2, \dots, u_n$ be the eigenvalues of m_u counted w/ multiplicities. Then $\text{tr}(u^m) = \sum_{i=1}^n u_i^m$. If the r.h.s.'s are 0 for all m , then, thx to $\text{char } \tilde{L} = \text{char } K = 0$, we get $u_1 = \dots = u_n = 0$, which is impossible since $u \neq 0$.

Step 3: Thx to the exercise in Section 1.3, we can find a K -basis l_1, \dots, l_n of L w/ $l_i \in \bar{A}^L$. Let ℓ^1, \dots, ℓ^n be the dual basis w.r.t. (\cdot, \cdot) , i.e. $\text{tr}(l_i \ell_j) = \delta_{ij}$, it exists b/c (\cdot, \cdot) is nondegenerate. Let $M := \text{Span}_A (\ell^1, \dots, \ell^n)$. Note that, for $\alpha \in \bar{A}^L$ we have $\alpha = \sum_{i=1}^n (\alpha, \ell_i) \ell^i$. We have $(\alpha, \ell_i) = \text{tr}(\alpha \ell_i) \in A$ b/c $\alpha \ell_i \in A$. So $\alpha \in M \Rightarrow \bar{A}^L \subset M$. But A is Noetherian,

and M is manifestly finitely generated A -module. Hence \bar{A}^L is a finitely generated A -module and we are done. \square

Corollary: Theorem is also true under assumption (II) if A is a finitely generated \mathbb{F} -algebra & $\text{char } \mathbb{F} = 0$.

Sketch of proof: Thanks to the Noether normalization lemma we can replace A w. $\mathbb{F}[x_1, \dots, x_m]$ for some m , this doesn't change \bar{A}^L (exercise). Now we are in the situation of (I) of the theorem. \square

For a proof of (II) w. a finitely generated algebra over an arbitrary field, see [E], Section 13.3.