MATH200C, LECTURE 10

GOLSEFIDY

Existence of primary decomposition in a Noetherian ring.

Similar to the proof of existence of a decomposition into *irreducible elements* we define an *irreducible ideal* and decompose a given ideal into irreducible ideals. Next we show in a Noetherian ring an irreducible ideal is primary.

Definition 1. *We say a proper ideal $\mathfrak{a} \trianglelefteq A$ is irreducible if for proper ideals $\mathfrak{b}$ and $\mathfrak{c}$ the following holds*

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \Rightarrow (\mathfrak{a} = \mathfrak{b} \text{ or } \mathfrak{a} = \mathfrak{c}).$$

Lemma 2. *In a Noetherian ring any proper ideal can be written as an intersection of finitely many irreducible ideals.*

Proof. Suppose to the contrary that there is a proper ideal that cannot be written as an intersection of finitely manny irreducible ideals; that means

$$\Sigma := \{\mathfrak{a} \trianglelefteq A |\ \mathfrak{a} \neq A, \mathfrak{a} \neq \text{intersection of finitely many irreducible ideals }\}$$

is not empty. Since A is Noetherian, Σ has a maximal element $\mathfrak{a}_0$. Since $\mathfrak{a}_0 \in \Sigma$, it is proper and it is not irreducible. So there are proper ideals $\mathfrak{b}$ and $\mathfrak{c}$ such that $\mathfrak{a}_0 = \mathfrak{b} \cap \mathfrak{c}$, $\mathfrak{a}_0 \subsetneq \mathfrak{b}$, and $\mathfrak{a}_0 \subsetneq \mathfrak{c}$. Since $\mathfrak{a}_0$ is a maximal element of Σ, $\mathfrak{b}, \mathfrak{c} \not\in \Sigma$; this means $\mathfrak{b} = \bigcap_{i=1}^n \mathfrak{q}_i$ and $\mathfrak{c} = \bigcap_{i=1}^m \mathfrak{q}'_i$ for some irreducible ideals $\mathfrak{q}_i$ and $\mathfrak{q}'_i$. Hence

$$\mathfrak{a}_0 = (\bigcap_{i=1}^n \mathfrak{q}_i) \cap (\bigcap_{i=1}^m \mathfrak{q}'_i),$$

which means $\mathfrak{a}_0$ can be written as an intersection of finitely many irreducible ideals; and this is a contradiction. □

Lemma 3. *In a Noetherian ring, an irreducible ideal is primary.*

Proof. Suppose $\mathfrak{q}$ is an irreducible ideal of A. Let $\overline{A} := A/\mathfrak{q}$. Since $\mathfrak{q}$ is irreducible in A, 0 is irreducible in $\overline{A}$. To show $\mathfrak{q}$ is primary, it is (necessary and) sufficient to show any zero-divisor of $\overline{A}$ is nilpotent. Suppose x is a zero-divisor of $\overline{A}$; that means there is a non-zero element y in $(0:x)$. Consider the chain of ideals

$$(0:x) \subseteq (0:x^2) \subseteq \cdots.$$

Since A is Noetherian, there is a positive integer n such that

$$(0:x^n) = (0:x^{n+1}).$$

Claim. $\langle y \rangle \cap \langle x^n \rangle = 0$.

Proof of Claim. Suppose $z \in \langle y \rangle \cap \langle x^n \rangle$; then $zx = 0$ as $z \in \langle y \rangle$ and $yx = 0$. Since $z \in \langle x^n \rangle$, $z = ax^n$ for some $a \in A$. Hence $0 = zx = ax^{n+1}$, which means $a \in (0:x^{n+1}) = (0:x^n)$. And so $z = ax^n = 0$.

Since 0 is irreducible, x and y are zero-divisors (and so they are not units), and $y \neq 0$, we have that $x^n = 0$; as we desired. □

Theorem 4. *In a Noetherian ring any proper ideal has a reduced primary decomposition.*

Proof. This is an immediate corollary of the previous lemmas. □

Corollary 5. *In a Noetherian ring A,* $\mathrm{Spec}(A)$ *has only finitely many minimal elements $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$; in particular* $\mathrm{Spec}(A) = \overline{\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}}$.

Proof. Since A is Noetherian, 0 is decomposable. So the set of minimal elements of $\mathrm{Spec}(A)$ is the same as the set of minimal elements of $\mathrm{Ass}(0)$. Hence there are only finitely many such ideals.

Suppose $V(\mathfrak{a}) = \overline{\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}}$ and $\mathfrak{p} \in \mathrm{Spec}(A)$. Then there is i such that $\mathfrak{p}_i \subseteq \mathfrak{p}$. Hence $\mathfrak{p}|\mathfrak{p}_i|\mathfrak{a}$, which implies $\mathfrak{p} \in V(\mathfrak{a})$; and claim follows. □

Integral extensions

Definition 6. *(1) Suppose A is a subring of B; in this case we say B/A is a ring extension.*

(2) We say $b \in B$ is integral over A if there is a monic polynomial $f(x) := \sum_{i=0}^{n} a_i x^i \in A[x]$ such that $f(b) = 0$; that means $\sum_{i=0}^{n} a_i b^i = 0$.

(3) We say B/A is an integral extension if any $b \in B$ is integral over A.

Proposition 7. *Suppose A is a subring of B; the following statements are equivalent:*

(1) $b \in B$ is integral over A.
(2) $A[b]$ is a finitely generated A-module.
(3) There is a subring C of B such that $A[b] \subseteq C$ and C is a finitely generated A-module.
(4) There is a faithful $A[b]$-module M that is a finitely generated A-module.

Recall. Suppose M is an R-module. Then $\mathrm{Ann}(M) := \{r \in R \mid \forall x \in M, rx = 0\}$ is an ideal of R; and we say M is a faithful R-module if $\mathrm{Ann}(M) = 0$. For a commutative ring R, $r \mapsto l_r$, where $l_r(x) := rx$ defines a ring homomorphism from R to $\mathrm{End}_R(M)$ and its kernel is $\mathrm{Ann}(M)$.

Proof. (1)⇒(2) Suppose $f(x) \in A[x]$ is a monic polynomial and $f(b) = 0$. For any $g(x) \in A[x]$, by long division (notice that since $f(x)$ is monic, the process of long division is feasible), there are $q(x), r(x) \in A[x]$ such that $g(x) = f(x)q(x) + r(x)$ and $\deg r < \deg f$. Hence $g(b) = r(b) = \sum_{i=0}^{\deg f-1} a_i b^i$ for some $a_i \in A$; therefore $A[b] = \sum_{i=0}^{\deg f-1} Ab^i$, which means $A[b]$ is generated by $\{1, b, \ldots, b^{\deg f-1}\}$ as an A-module.

(2)⇒(3) Let $C := A[b]$.

(3)⇒(4) Let $M := C$; notice that for any $r \in A[b]$, $r \cdot 1 = r$ implies that C is a faithful $A[b]$-module.

(4)⇒(1) Let $l_b : M \to M, l_b(x) := bx$. Since $A[b]$ is commutative, $l_b \in \mathrm{End}_A(M)$. Since M is a finitely generated A-module, there are $a_i \in A$ such that

$$l_b^n + \overline{a}_{n-1} l_b^{n-1} + \cdots + \overline{a}_1 l_b + \overline{a}_0 = 0$$

in $\mathrm{End}_A(R)$, where $\overline{a}_i := l_{a_i}$[1]. This means

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 \in \mathrm{Ann}(M) = 0;$$

and claim follows. □

INTEGRAL CLOSURE

Lemma 8. *Suppose B/A is a ring extension, $b_1, \ldots, b_n \in B$ are integral over A. Then $A[b_1, \ldots, b_n]$ is a finitely generated A-module.*

[1] We have proved such a result earlier, based on this result we showed Nakayama's lemma.

$A[b_1, \ldots, b_n]$ is the subring of B that is generated by A and b_i's. This can be viewed as the image of evaluation at $(b_1, \ldots, b_n)$:

$$\phi : A[x_1, \ldots, x_n] \to B, \phi(f(x_1, \ldots, x_n)) := f(b_1, \ldots, b_n).$$

Proof. Since b_i's are integral over A, there are monic polynomials $f_i(x) \in A[x]$ such that $f_i(b_i) = 0$. By induction on n, we prove that $A[b_1, \ldots, b_n]$ is generated by $\{b_1^{i_1} \cdots b_n^{i_n} | \, 0 \le i_1 < \deg f_1, \ldots, 0 \le i_n < \deg f_n\}$. We proceed by induction on n; we have already proved the base of induction. So we focus on the induction step. For $g \in A[x_1, \ldots, x_{n+1}]$, there are polynomials $g_i \in A[x_1, \ldots, x_n]$ such that $g = \sum_{i=0}^m g_i x_{n+1}^i$. By the induction hypothesis, there are $a_{i,\mathbf{j}} \in A$ such that

$$g_i(b_1, \ldots, b_n) = \sum_{\mathbf{j} \in [0..\deg f_1) \times \cdots [0..\deg f_n)} a_{i,\mathbf{j}} b_1^{j_1} \cdots b_n^{j_n}.$$

Hence

$$\begin{aligned} g(b_1, \ldots, b_{n+1}) &= \sum_{i=0}^m g_i(b_1, \ldots, b_n) b_{n+1}^i = \sum_{i=0}^m \sum_{\mathbf{j}} a_{i,\mathbf{j}} b_1^{j_1} \cdots b_n^{j_n} b_{n+1}^i \\ &= \sum_{\mathbf{j}} b_1^{j_1} \cdots b_n^{j_n} \underbrace{\Big(\sum_{i=0}^m a_{i,\mathbf{j}} b_{n+1}^i\Big)}_{\in A[b_{n+1}] = \sum_{j=0}^{\deg f_{n+1}-1} A b_{n+1}^j} \\ &= \sum_{\mathbf{j}} b_1^{j_1} \cdots b_n^{j_n} \Big(\sum_{j_{n+1}=0}^{\deg f_{n+1}-1} a'_{\mathbf{j},j_{n+1}} b_{n+1}^{j_{n+1}}\Big), \end{aligned}$$

for some $a'_{\mathbf{j},j_{n+1}} \in A$ (and $\mathbf{j} \in [0..\deg f_1) \times \cdots [0..\deg f_n)$); and claim follows. □

Corollary 9. *Suppose B/A is a ring extension. Let*

$$C := \{b \in B | \, b \text{ is integral over } A\}.$$

Then C is a subring of B.

Definition. C is called the integral closure of A in B. We say A is integrally closed in B if $C = A$.

Proof. Suppose $b_1, b_2 \in C$; then by the previous lemma, $A[b_1, b_2]$ is a finitely generated A-module. Hence by Part (3) of Proposition 7, we have that any element of $A[b_1, b_2]$ is integral over A. Therefore $b_1 \pm b_2$ and $b_1 b_2$ are integral over A, which means $b_1 \pm b_2, b_1 b_2 \in C$. Thus C is a subring of B. □

Definition 10. *An integral domain D is called* integrally closed *if it is integrally closed in its field of fractions.*

Example 11. *Because of the rational root criterion a UFD is integrally closed.*

Remark. We will show that being integrally closed is a local property; but we have seen that being a UFD is not a local property. This makes being integrally closed a better "geometric" property.

Lemma 12. *Suppose B/A and C/B are integral extensions; then C/A is an integral extension.*

Proof. For $c \in C$, there are b_i's in B such that

$$c^n + b_{n-1}c^{n-1} + \cdots + b_1 c + b_0 = 0.$$

So c is integral over $A[b_0, \ldots, b_{n-1}]$, which implies that

$$A[b_0, \ldots, b_{n-1}, c] = \sum_{j=0}^{k} A[b_0, \ldots, b_{n-1}]c^j$$

for some k. Since b_i's are integral over A, by an earlier lemma we have

$$A[b_0, \ldots, b_{n-1}] = \sum_{\mathbf{j} \in J} A b_0^{j_0} \cdots b_{n-1}^{j_{n-1}},$$

for some finite set J. Overall we get

$$A[b_0, \ldots, b_{n-1}, c] = \sum_{j=0}^{k} \sum_{\mathbf{j} \in J} A b_0^{j_0} \cdots b_{n-1}^{j_{n-1}} c^j,$$

which implies that $A[b_0, \ldots, b_{n-1}, c]$ is a finitely generated A-module. Thus another application of Proposition 7 implies that c is integral over A; and claim follows. □

Corollary 13. *Suppose B/A is a ring extension and C is the integral closure of A in B; then C is integrally closed in B.*

Proof. Let $\overline{C}$ be the integral closure of C in B. Then $\overline{C}/C$ and C/A are integral. Hence $\overline{C}/A$ is integral, which implies that $\overline{C} \subseteq C$. Therefore $\overline{C} = C$. □