Introduction to Rings and Modules

Lecture 17, Friday June 16 2023

Ari Feiglin

Definition 17.0.1:

Suppose $R \subseteq S$ are rings and $s \in S$, then $R[s]$ is the smallest subring of S which contains both R and s:

$$R[s] = \left\{ a_n s^n + a_{n-1} s^{n-1} + \cdots + a_1 s + a_0 \;\middle|\; n \in \mathbb{N}_0,\, a_i \in R \right\}$$

Note if $s^k \in R$ then

$$R[s] = \left\{ a_k s^k + \cdots + a_0 \;\middle|\; a_i \in R \right\}$$

Definition 17.0.2:

An R-module M is **faithful** if

$$\mathrm{Ann}_R(M) = (0)$$

meaning for every $r \in R$, there exists an $m \in M$ where $rm \neq 0$.

Proposition 17.0.3:

Suppose $R \subseteq S$ are commutative. Let $s \in S$, then the following are equivalent

(1) s is integral over R.

(2) $R[s]$ is a finitely-generated R-module.

(3) There exists a ring T such that $R[s] \subseteq T \subseteq S$ and T is finitely-generated as an R-module.

(4) There exists a faithful $R[s]$-module M which is finitely-generated as an R-module.

Proof:

Firstly, $2 \Rightarrow 3$ is trivial, take $T = R[s]$. And for $3 \Rightarrow 4$ let $M = T$, which is finitely-generated as an R-module. Suppose $\alpha \in \mathrm{Ann}_{R[s]}(T)$ so $\alpha t = 0$ for every $t \in T$. Since T is a ring, take $1 \in T$, so we get $\alpha = 0$. Thus T is a faithful $R[s]$-module.

Now for $1 \Rightarrow 2$, we know that

$$s^n + b_{n-1}s^{n-1} + \cdots + b_0 = 0$$

for $b_i \in R$ since s is integral over R. Then we claim

$$R[s] = \left\langle 1, s, \dots, s^{n-1} \right\rangle$$

It is sufficient to show that every s^m is generated by these elements, since every element in $R[s]$ is a linear combination of s^ms. For $m < n$ this is trivial, and note that

$$s^n = -b_{n-1}s^{n-1} - \cdots - b_0$$

so it is true for $m = n$. We will show this is true for exponents s^{n+m}, we proved the base case for $m = 0$ already. Now we know by our inductive hypotehsis

$$s^m = a_{n-1}s^{n-1} + \cdots + a_0$$

and so

$$s^{m+1} = a_{n-1}s^n + a_{n-2}s^{n-1} + \cdots + a_0 s$$

and since s^n is a linear combination of $1, s, \dots, s^n$ so is s^{m+1} as required.

Finally for $4 \Rightarrow 1$, suppose M is a faithful $R[s]$-module, which is also finitely generated as an R-module. Suppose $M = \langle m_1, \dots, m_n \rangle$, now for $m \in M$ we have

$$m = a_1 m_1 + \cdots + a_n m_n$$

for some $a_i \in R$, and this is true for sm_i in particular

$$sm_i = a_{i,1} m_1 + \cdots + a_{i,n} m_n$$

and thus we have that

$$\begin{pmatrix} sm_1 \\ \vdots \\ sm_n \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

Thus

$$(sI_n - A) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$$

notice that $sI_n - A$ is a matrix with coefficients in $R[s]$. The adjugate of matrices are defined still in commutative rings as there is no need for division, so we can multiply both sides by $\mathrm{adj}(sI_n - A)$ and get

$$\det(sI_n - A) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$$

Thus $\det(sI_n - A)m_i = 0$ for every i and thus $\det(sI_n - A)m = 0$ for every $m \in M$, so $\det(sI_n - A) \in \mathrm{Ann}_{R[s]}(M)$. Thus we have $\det(sI_n - A) = 0$, but we also know $\det(sI_n - A)$ is the characteristic polynomial of A over R evaluated at s (which is in $R[s]$), meaning $p_A(s) = 0$. Since p_A is a monic polynomial over R, we have that s is then integral over R. ■

Proposition 17.0.4:

Suppose $R \subseteq S$ are commutative rings, then

$$T = \{s \in S \mid s \text{ is integral over } R\}$$

is a subring of S.

Proof:

Since R is integral over itself, $R \subseteq T$ and in particular $1_S = 1_R \in R \subseteq T$. Now suppose $t_1, t_2 \in T$ then let us look at

$$R[t_1, t_2] = \left\{ \sum a_{m,n} t_1^m t_2^n \;\middle|\; a_{m,n} \in R \right\}$$

which is $R[t_1][t_2]$ or the smallest ring containing R, t_1, and t_2. But since

$$t_1^n + a_{n-1} t^{n-1} + \cdots + a_0 = 0, \qquad t_2^m + b_{m-1} t^{m-1} + \cdots + b_0 = 0$$

for $a_i, b_i \in R$. Thus every exponent of t_1 is a linear combination over R of $1, t_1, \dots, t_1^{n-1}$ and similarly exponents of t_2 are linear combinations over R of $1, t_2, \dots, t_2^{m-1}$. Thus the products of exponents t_1 and t_2 are linear combinations of coefficients of the form $t_1^i t_2^j$ for $0 \leq i \leq n-1$ and $0 \leq j \leq m-1$. Thus

$$R[t_1, t_2] = \left\langle t_1^i t_2^j \;\middle|\; 0 \leq i \leq n-1, \, 0 \leq j \leq m-1 \right\rangle$$

So $R[t_1, t_2]$ is a finitely-generated R-module.
So we must show that $t_1 + t_2 \in T$ and $t_1 t_2 \in T$. Since we know

$$R[t_1 + t_2], R[t_1 t_2] \subseteq R[t_1, t_2] \subseteq S$$

Thus by the above proposition, $t_1 + t_2$ and $t_1 t_2$ are integral over R, ie. $t_1 + t_2$, $t_1 t_2 \in T$ as required. Thus T is a ring, and it contains 1_S so it is a subring of S's. ■

Definition 17.0.5:

Suppose $R \subseteq S$ are commutative rings, then

$$\{s \in S \mid s \text{ is integral over } R\}$$

is called the **integral closure of R over S**.

Lemma 17.0.6:

If $R \subseteq S \subseteq T$ such that S is a finitely-generated R-module and T a finitely generated S-module, then T is a finitely generated R-module.

Proof:

Suppose $S = \langle a_1, \ldots, a_n \rangle$ and $T = \langle b_1, \ldots, b_m \rangle$ then every $t \in T$ is of the form

$$t = \sum_{i=1}^{m} s_i b_i = \sum_{i=1}^{m} \sum_{j=1}^{n} r_{i,j} a_j b_i$$

and thus $T = \langle a_j b_i \mid 1 \leq j \leq n,\, 1 \leq i \leq m \rangle$ as required. ∎

Proposition 17.0.7:

If $R \subseteq S \subseteq T$ are rings where S is integral over R, and T is integral over S, then T is integral over R.

Proof:

Suppose $t \in T$, then t is integral over S so

$$t^n + s_{n-1} t^{n-1} + \cdots + s_0 = 0$$

Thus t is integral over $R[s_0, \ldots, s_{n-1}]$ and so $R[s_0, \ldots, s_{n-1}, t]$ is a finitely generated $R[s_0, \ldots, s_{n-1}]$-module. But $R[s_0, \ldots, s_{n-1}]$ is finitely-generated over R since s_i are integral over R. Thus $R \subseteq R[s_0, \ldots, s_{n-1}] \subseteq R[s_0, \ldots, s_{n-1}, t]$ where each successive rings form an integral extension, thus by the lemma above, $R[s_0, \ldots, s_{n-1}, t]$ is a finitely-generated module over R. Thus we have $R \subseteq R[t] \subseteq R[s_0, \ldots, s_{n-1}, t] \subseteq T$ where $R[s_0, \ldots, s_{n-1}, t]$ is finitely-generated so t is integral over R. ∎

Proposition 17.0.8:

Integral closures are integrally closed.

Proof:

Suppose $R \subseteq S$ and T is the integral closure of R over S. Let T' be T's integral closure over S, then $R \subseteq T \subseteq T'$ where T is integral over R and T' over T, thus T' is integral over R so $T' \subseteq T$, meaning $T' = T$. So every element in S which is integral over T is in T, meaning T is integrally closed. ∎