Chapter 4: Integrality and some other things

Given a commutative ring R, we study R-algebras A so that A is finitely generated (or finite) as an R-module.

Examples:

1. The group ring RG. = free R-module with the elements of G as a basis. This is finite over R if G is finite.

2. Let R = Z contained in the rational numbers Q. What subrings of Q are finitely generated as Z-modules?

e.g. is $\mathbb{Z}[\frac{1}{2}]$ finitely generated? No

The only such subring is $\mathbb{Z}$.

3. Inside Q[i], consider Z[i], Z[2i], Z[i/2].

$\mathbb{Z}[i]$ is finitely generated over $\mathbb{Z}$.

$\mathbb{Z}[2i] \subseteq \mathbb{Z}[i]$ is also finitely generated over $\mathbb{Z}$.

$\mathbb{Z}[\frac{i}{2}]$ is not fin. gen over $\mathbb{Z}$.

Defn. A commutative R-algebra A is finite over R if it is finitely generated as an R-module.

Does your neighbor know what an R-algebra is?

Yes ✓

No

Definition R is a commutative ring. An R-algebra A is a ring with a ring homomorphism $\phi : R \to Z(A)$ (so $1_R \mapsto 1_A$). A is an R-module via $r \cdot a := \phi(r)a$

We learn:

- What condition on elements of A produce this finiteness condition
- What are the properties of integers.

Definitions. Let S be an R-algebra.

S should be commutative.

An element s of S is integral over R if and only if $p(s) = 0$ in S where $p(x) \in R[x]$ is a monic polynomial.

monic: the leading coefficient is 1

The algebra S is integral over R if.

every element of S is integral over R.

Not clear: $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right] \subseteq \mathbb{C}$ is integral over $\mathbb{Z}$.

Examples: $1 + i\sqrt{3}$ and $(1+i\sqrt{3})/2$.

$$(1+i\sqrt{3})^2 = 1-3+2i\sqrt{3}$$
$$= -2+2i\sqrt{3}$$
$$= 2(1+i\sqrt{3}) - 4$$

$1+i\sqrt{3}$ is a root of of X^2-2X+4. so is integral over $\mathbb{Z}$.

$$\left(\frac{1+i\sqrt{3}}{2}\right)^2 = \frac{1+i\sqrt{3}}{2} - 1$$

$\frac{1+i\sqrt{3}}{2}$ is a root of X^2-X+1 so is also integral over $\mathbb{Z}$.

$1+i\sqrt{5}$ is integral over $\mathbb{Z}$

$\frac{1+i\sqrt{5}}{2}$ is not integral over $\mathbb{Z}$.

Goal: the integral elements form a sub ring. of S.

Corollary 4.6 plus. Let S be an R-algebra.
TFAE for s in S
(a) s is integral over R.
(b) R[s] is contained in an R-submodule M of S, finitely generated over R, with $sM \subseteq M$
(c) there exists an S-module N and a finitely generated R-submodule M of N, not annihilated by nonzero elements of S, such that $sM \subseteq M$.

Proof (a) ⇒ (b). Take

$$M = R[s] \quad (= \phi(R)[s]) \subseteq S.$$

Then $s \cdot R[s] \subseteq R[s]$.

Show R[s] is finitely generated over R. It is generated by

$1, s, s^2, s^3, \ldots$

If $p(s) = 0$

$p(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$

then $s^n = -(b_{n-1}s^{n-1} + \cdots + b_0)$

so s^n is not needed as a generator of R[s]. Neither are $s^{n+1}, s^{n+2}, \ldots$

R[s] is generated by

$1, s, s^2, \ldots, s^{n-1}$. □

(b) ⇒ (c): In (c) take N = S, M the same. Then $1 \in R[s] \subseteq M$ is not ann. by any non-zero elt of S.

□

Pre-class Warm-up!!!

Is 2 integral over $\mathbb{Z}$?

A Yes ✓

B No

Is 1/2 integral over $\mathbb{Z}$?

A Yes

✓

Some further questions we might discuss (or not!)

Is Z[x] / (2x^3)

(a) finitely generated as a ring? Yes

(b) finitely generated as an abelian group? No

Degree	0	1	2	3	4	5
elements	1	$\bar{x}$	$\bar{x}^2$	$\mathbb{Z}x^3 / 2\mathbb{Z}x^3$		
	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\cong C_2$	C_2	C_2	C_2

Another question: (a) and (b) for Z[x]/(x^3).

Yes and Yes.

Goal: the integral elements form a sub ring.

Corollary 4.6 plus. Let S be an R-algebra. TFAE for s in S

(a) s is integral over R.

(b) R[s] is contained in an R-submodule M of S, finitely generated over R, with $sM \subseteq M$

(c) there exists an S-module N and a finitely generated R-submodule M of N, not annihilated by nonzero element of S, such that $sM \subseteq M$.

(c) ⇒ (a) Let $M = Rm_1 + \cdots + Rm_n$, $m_i \in M$. Let s satisfy $sM \subseteq M$

Write $sm_i = \sum a_{ij} m_j$, $a_{ij} \in R$, for each i.

Let $A = (a_{ij})$

Now $(A - sI)\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$

$$\operatorname{adj}(A - sI)(A - sI)\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \operatorname{adj}(A - sI) \cdot \begin{bmatrix} 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

$$\det(A - sI) \cdot I \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

$\det(A - sI)\, m_i = 0$

so $\det(A - sI) \cdot M = 0$

and $\det(A - sI) = 0$.

If $p(t) = \det(A - tI)$ then p is monic and $p(s) = 0$.

s is integral over R. □

$\det \begin{bmatrix} a_{11} - s & a_{12} & & a_{1n} \\ a_{21} & a_{22} - s & & \\ & & \ddots & \end{bmatrix}$ is monic.

Theorem 4.3 (Cayley-Hamilton) commutative.

Let J I be an ideal of a ring R,

M an R-module generated by elements

m_1, ... m_n,

f : M -> M an endomorphism. of R-modules.

If $f(M) \subseteq IM$ JM

then there is a polynomial

$$p(x) = x^n + p_1 x^{n-1} + \cdots + p_n$$

so that p(f) = 0, with $p_j \in I^j$ J^j $\forall j$.

Proof. Write $f(m_i) = \sum a_{ij} m_j$, $a_{ij} \in I$ J

Let $A = (a_{ij})$

Regard M as an R[x]-module with x acting as f.

Now $(xI - A)\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = 0$

elements of M i.e. vectors. Not allowed

$$\operatorname{adj}(xI-A)\cdot(xI-A)\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

$$\det(xI-A)I\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

If $p(x) = \det(xI - A)$ then $p(x)\cdot M = 0$, so $p(f) = 0$. □

and $p_j \in J^j$.

$\operatorname{adj} B \cdot B = \det(B)\cdot I$

Math 4242: entries of B are in a field.

Questions:

1. Could we present this proof to undergraduates in Math 4242? Why, or why not? Yes

No Most

2. How many points in this proof are troubling to you?

0 1 2 3 4

Question:

Let R be a subring of S, u an element of S and r an element of R.

Is it obvious that if u is integral over R then ru is also integral over R?

A Yes

B No

Corollary = Theorem 4.2.

Elements of S integral over R form an R-subalgebra.

Proposition 4.1. Let R be a ring, J an ideal of $R[x]$, $S = R[x] / J$.
Let s be the image of x in S.

a. S is generated by $\leq n$ elements as an R-module if and only if J contains a monic polynomial of degree $\leq n$.
In this case S is generated by

b. S is a finitely generated free R-module if and only if J can be generated by a monic polynomial.
In this case S is freely generated by

Corollary. s is integral over R if and only if $R[s]$ is finitely generated as an R-module.

Corollary 4.4. Let M be a finitely generated R-module.

a. If $f : M \to M$ is an epimorphism of R-modules, then f is an isomorphism.

Proof.

Corollary 4.5.

An R-algebra S is finite over R if and only if S is generated as an R-algebra by finitely many integral elements.

The extra things in Eisenbud's book