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 $r.a := \phi(r)a$

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) $\Rightarrow$ (b). Take

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

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

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

$1, s, s^2, \ldots, s^{n-1}$. $\square$

(b) $\Rightarrow$ (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.

$\square$

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	$\bar{x}$	$\bar{x}^2$	$\frac{\mathbb{Z}x^3}{2\mathbb{Z}x^3}$			
	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}/2 \cong C_2$	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) $\Rightarrow$ (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 $(A - sI)\begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$

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

$$= \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

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

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

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. $\square$

$\det \begin{bmatrix} a_{11} - s & a_{12} & & a_{1n} \\ a_{21} & a_{22} - s & & \\ & & \ddots & \end{bmatrix}$ 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) ⊆ 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 $p(f) = 0$. $\square$

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

Pre-class Warm-up

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

$$u^n + a_{n-1}u^{n-1} + \dots + a_0 = 0$$

$$r^n u^n + r^n a_{n-1} u^{n-1} + \dots + r^n a_0 = 0$$

$$(ru)^n + r a_{n-1} (ru)^{n-1} + \dots = 0$$

Corollary = Theorem 4.2.
Elements of S integral over R form an R-subalgebra.

Proof. We show if $a, b \in S$ are integral over R then so are $a+b$, ab.

$a \in M \subseteq S$, M is fin gen as an R-module $aM \subseteq M$.
Similarly $b \in M' \subseteq S$ same conditions.

If M is gen'd over R by $m_1, \ldots, m_u$
M' .... by $m'_1, \ldots, m'_v$
then $MM' = \{mm' \mid m \in M, m' \in M'\} \subseteq S$

is an an R-module generated by the $m_i m'_j$.

$$ab\, MM' = aM\, bM' \subseteq MM'$$
$$(a+b)MM' \subseteq aMM' + bMM'$$
$$\subseteq MM' + MM' = MM'.$$

Thus ab, $a+b$ satisfy the criterion to be integral over R. $\square$

Why do we go through this elaborate process to show this?

Proposition 4.1. Let R be a commutative 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 $1, s, s^2, \ldots, s^{n-1}$

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 $1, \ldots, s^{n-1}$
where n = degree of that polynomial.

Proof a. "$\Leftarrow$" If $J \ni p$ a monic polynomial of degree n

$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$

Then $x^n = -(a_{n-1}x^{n-1} + \ldots + a_0)$

so s^n lies in the sub R-module generated by $1, \ldots, s^{n-1}$.

so does s^{n+1} etc.

"$\Rightarrow$" If S is generated by $m_1, \ldots, m_t$, $t \leq n$

Cayley-Hamilton $\Rightarrow$ s is a root of a monic $p(x)$ of degree t.

$p \in J$. $\square$

Example. $R = \mathbb{Z}$, $J = (2x^3)$

$R[x]/J$						
degree	0	1	2	3	4	…
	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	…

This is not finitely generated as a $\mathbb{Z}$-module.

$\in S \supseteq R$

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

Proof. "$\Rightarrow$" s integral $\Rightarrow$ $p(s) = 0$, $p \in R[x]$ monic, $R[s] \cong R[x]/(p)$ is finitely generated over R.

"$\Leftarrow$" Use Cor 4.6 with $M = R[s]$. $\square$

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. Apply Cayley-Hamilton.

Take the ring to be $R[x]$.

Let M be an $R[x]$-module where x acts via f.

$(xm := f(m))$.

Take the ideal I to be (x).

Then $f : M \to M$ has image in $IM = M$ so 1_M satisfies

$$p(t) = t^n + a_{n-1} t^{n-1} + \cdots + a_0$$

$$p(1) = 0$$

$$a_i \in I^{?} \subseteq I$$

$$1 + f \cdot q = 0.$$

because $a_{n-1} t^{n-1} + \cdots + a_0$ is divisible by x f.

$$fq = -1 \qquad f(-q) = 1.$$

f is invertible. $\square$

Pre-class Warm-up!!

True or false?

Let J be a maximal ideal of a commutative ring R and let u be an element of R not in J.
Then u is a unit.

A. True 1

B. False 2

e.g. $J = 2\mathbb{Z} \subseteq \mathbb{Z} = R$

$3 \notin J$ is not a unit.

We might also consider:

Let u be an element of R not in any maximal ideal. Then u is a unit.

A. True ✓

B. False

$Ru = (u) = R$ because o/w (u) would be contained in a max. ideal.

Thus $\exists\, v \in R$, $vu = 1$.

u is a unit.

<u>Prop'n</u>. $\bigcap$ maxl ideals $\subseteq \{r \in R \mid 1 + r \text{ is unit}\}$.

Corollary 4.5. S is commutative.

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

Proof. "$\Rightarrow$" Suppose S is generated by finitely many elements as an R-module. These elements also generate S as an R-algebra. These elements are integral over R by criterion:

"$uM \subseteq M$, M finite over R"
$\Rightarrow u$ integral over R. Take $M=S$

"$\Leftarrow$" Suppose S is gen'd by $s_1, \ldots, s_n$ as an R-algebra, s_i integral.

Induction:

Suppose $R[s_1, \ldots, s_t]$ is finite over R. s_{t+1} is integral over R, hence integral over $R[s_1, \ldots, s_t]$

$R[s_1, \ldots, s_{t+1}]$ has generators $u_1, \ldots, u_d$ as $R[s_1, \ldots, s_t]$-module, say,

$R[s_1, \ldots, s_t]$ has generators $v_1, \ldots, v_e$ as an R-module.

Then the $u_i v_j$ generate $R[s_1, \ldots, s_{t+1}]$ as an R-module.

$\square$

4.2 Normal domains

Definition. Let R be an integral domain. Then R is normal if and only if it equals its own integral closure in its field of fractions.

If $R \subset S$, the integral closure of R in S is $\{s \in S \mid s \text{ is integral of } R\}$.

Examples Z [i√3] is not normal.

$\frac{1+i\sqrt{3}}{2}$ is integral over $\mathbb{Z}$, $\frac{1+i\sqrt{3}}{2} \in \mathbb{Q}(i\sqrt{3})$

Z[i√5] is normal It is the integers in $\mathbb{Q}(i\sqrt{5})$.

Proposition 4.10 UFD

Let R be a ring. If R is factorial, then R is normal.

Proof. Let $\frac{a}{b} \in K$ = field of frac. of R. Suppose a, b are relatively prime and

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \dots + c_0 = 0.$$

not divis by b unless b = 1.

$$a^n + \underbrace{c_{n-1}ba^{n-1} + \dots + b^n c_0}_{\text{divis by } b} = 0.$$

Thus $\frac{a}{b} \in R$. $\square$

The normalization of R is its integral closure in its field of fractions.

Example: $\mathbb{Z}$ is its own integral closure in $\mathbb{Q}$.

The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$.

A finite degree field extension $K \supseteq \mathbb{Q}$ is called an algebraic number field. The integral closure of $\mathbb{Z}$ in K is the corresponding ring of algebraic integers.

$\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$, $\mathbb{Z}[i]$ are Euclidean

$\mathbb{Z}$ hence factorial.

$\mathbb{Z}(i\sqrt{5})$ is not a UFD

$(1+i\sqrt{5})(1-i\sqrt{5}) = 6 = 2 \cdot 3$.

The extra things in Eisenbud's book:

Lemma 4.11 is used to prove:

Corollary 4.12.
If R is a normal domain then any monic irreducible polynomial in $R[x]$ is prime.

Proposition 4.13.
~~Normalization~~ localization commutes with taking the integral closure.

Theorem 4.14 (Emmy Noether~~ian~~)
If R is a finitely generated domain over a field or over the integers, and L is a finite extension field of the field of fractions of R, then the integral closure of R in L is a finitely generated R-module.

Rings of algebra integers are finitely generated as abelian groups.

Nakayama's Lemma

First a lemma coming from the Cayley-Hamilton theorem again:

Corollary 4.7
Let M be a finitely generated R-module, J an ideal of R so that $JM = M$.
Then there is an element r in J that acts as the identity on M; i.e. $(1-r)M = 0$.

Proof. Cayley Hamilton applied to $1_M : M \to M$ gives a monic polynomial $p(t) = t^n + a_{n-1}t^{n-1} + \dots + a_0$
$a_i \in J$, $p(1_M) = 0$.
$1 + \sum_{i=0}^{n-1} a_i = 0$, $r = -\sum_{i=0}^{n-1} a_i$ acts as 1 on M. $\square$

Definition. The Jacobson radical of a ring R is the intersection of the maximal ideals of R.

Examples.

True or false?
Let p be a prime. The Jacobson radical of the localization $\mathbb{Z}_{(p)}$ is zero.

A True B False

Corollary 4.8 (Nakayama's lemma)

Let J be an ideal contained in the Jacobson radical of R, let M be a finitely generated R-modul

a. If $JM = M$ then $M = 0$.

b. If $m_1, \ldots , m_n$ in M have images in M / JM that generate it as an R-module then these same elements generate M as an R-modul

Cohen-Seidenberg Lying Over and Going Up

Proposition 4.15
Suppose $R \subset S$ is an integral extension of rings. Given a prime P of R, there exists a prime Q of S with $R \cap Q = P$. In fact, Q may be chosen to contain any given ideal Q_1 that satisfies $R \cap Q_1 \subset P$.

Proof.
Factor out Q_1 and $R \cap Q_1$ to assume $Q_1 = 0$.
We only need find a prime Q of S with $R \cap Q = P$.
Localize: S_P is integral over R_P.
We may assume R is local with maximal ideal P.