

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 $R = \mathbb{Z}$ contained in the rational numbers \mathbb{Q} . What subrings are finitely generated as \mathbb{Z} -modules?

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

The only such subring is \mathbb{Z} .

3. Inside $\mathbb{Q}[i]$, consider $\mathbb{Z}[i]$, $\mathbb{Z}[2i]$, $\mathbb{Z}[i/2]$.

$\mathbb{Z}[i]$ 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 $\phi: R \rightarrow Z(A)$ (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 $x^2 - 2x + 4$.
 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
 $M = R[s] (= \phi(R)[s])$
 $\subseteq S$.

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

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

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

$$\text{If } p(s) = 0$$

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

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

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

$R[s]$ is generated by

$$1, s, s^2, \dots, s^{n-1} \quad \square$$

(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 $\mathbb{Z}[x] / (2x^3)$

(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	$\overline{\mathbb{Z}x^3}$		
	\mathbb{Z}	\mathbb{Z}	$\mathbb{Z} \cong \mathbb{Z} \cong \mathbb{Z}$	$\mathbb{Z} \cong \mathbb{Z} \cong \mathbb{Z}$	C_2	C_2

Another question: (a) and (b) for $\mathbb{Z}[x]/(x^3)$.

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 $M = Rm_1 + \dots + Rm_n$
 $m_i \in M$. 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 $(A - sI) \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$

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

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

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

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

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

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

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

s is integral over R . \square

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

Theorem 4.3 (Cayley-Hamilton) *commutative*.

Let \mathcal{I} be an ideal of a ring R ,
 M an R -module generated by elements
 m_1, \dots, m_n ,

$f: M \rightarrow M$ an endomorphism. *of R -modules*.

If $f(M) \subseteq \mathcal{I}M$ *JM*

then there is a polynomial

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

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

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

Let $A = (a_{ij})$

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

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

elements of M i.e. vectors. Not allowed.

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

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

If $p(x) = \det(xI - A)$ then

$p(x) \cdot M = 0$, so $p(f) = 0$. \square

and $p_j \in \mathcal{I}^j$.

*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, \dots, m_u

M' \dots

m'_1, \dots, m'_v

then $MM' = \{mm' \mid m \in M, m' \in M'\}$
 $\subseteq S$

is an R -module generated by the m, 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 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 $1, s, s^2, \dots, s^{n-1}$.

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

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

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

$$\text{then } x^n = -(a_{n-1}x^{n-1} + \dots + a_0)$$

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

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.

so does s^{n+1} etc.

" \Rightarrow " If S is generated by m_1, \dots, m_n Cayley-Hamilton $\Rightarrow s$ is a root of a monic $p(x)$ of degree n . $p \in J$. \square

$$e \in S \supseteq R$$

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 $f: M \rightarrow M$ 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 $f: M \rightarrow M$ has image in $I M = M$ so 1_M satisfies

$$p(t) = t^n + a_{n-1}t^{n-1} + \dots + a_0$$
$$p(1) = 0$$

$$a_i \in I' \subseteq I$$

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

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

$$f q = -1 \quad f(-q) = 1$$

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 |

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

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

Thus $\exists v \in R, vu = 1$.
 u is a unit.

Propn. \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, \dots, s_n as an R -algebra, s_i integral.

Induction:

Suppose $R[s_1, \dots, s_t]$ is finite over R .

s_{t+1} is integral over R , hence integral over $R[s_1, \dots, s_t]$

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

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

Then the $u_i v_j$ generate $R[s_1, \dots, s_{t+1}]$ 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 $\mathbb{Z}[i\sqrt{3}]$ is not normal

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

$\mathbb{Z}[i\sqrt{5}]$ 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 $\frac{a}{b} \in K = \text{field of frac. of } R$.

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 $b^n = 1$.

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

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~~ commutes with taking the integral closure.

localization.

Theorem 4.14 (Emmy Noether)

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.

Pre-class Warm-up!!!

True or false?

If R is a normal domain then R is factorial.

A True

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 $1_M: M \rightarrow M$ gives a monic polynomial $p(t) = t^n + a_{n-1}t^{n-1} + \dots + a_0$ $a_i \in J$, $p(1_M) = 0$.

$$1 + \sum_{i=0}^{n-1} a_i = 0, r = -\sum_{i=0}^{n-1} a_i \text{ acts as } 1 \text{ on } M. \quad \square$$

Definition. The Jacobson radical of a ring R is the intersection of the maximal ideals of R . It is denoted $\text{Jac}(R)$.

Examples. 1. $R = \mathbb{Z}$ $\text{Jac}(\mathbb{Z}) = \{0\}$

2. $R = k[x]/(x^5)$ then $\text{Jac}(R) = (x)/(x^5)$.

$\text{Jac}(\mathbb{Z}/p^3\mathbb{Z}) = p\mathbb{Z}/p^3\mathbb{Z}$
 $\mathbb{Z} \rightarrow \mathbb{Z}/p^3\mathbb{Z}$ does give a surjection $\text{Jac } \mathbb{Z} \rightarrow \text{Jac}(\mathbb{Z}/p^3\mathbb{Z})$

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 -module

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

b. If m_1, \dots, 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 -module

Or: If $N \subseteq M$ is a finitely generated submodule and $N + JM = M$ then $N = M$.

(Or: $JM \subseteq \bigcap \text{maxL submodules of } M$)

Proof. a. $JM = M \Rightarrow \exists r \in J$
with $(1-r)M = 0$

Also $1-r$ is a unit in R , because $r \in J$. (If $1-r$ is not a unit $(1-r)$

is a proper ideal, \subseteq some maximal ideal I . Now $1 = (1-r) + r \in I$
 $\in I$ \in every maximal ideal.

Contradiction.)

$1-r$ acts invertibly and $\alpha = 0$, on M .

$M = 0$. \square

b. Let $N = Rm_1 + \dots + Rm_n$ so

$$N + JM = M.$$

Consider M/N . Then

$$J(M/N) = (JM + N)/N = M/N.$$

Thus $M/N = 0$, $N = M$. \square

Nakayama says.

M is f.g.

$$N + JM = M \Rightarrow N = M.$$

This is useful e.g., taking projective resolutions (esp. over a local ring).

$$\begin{array}{c} R^{n_1} \longrightarrow R^{n_0} \longrightarrow M \longrightarrow 0 \\ \searrow \quad \nearrow \\ \quad K_0 \end{array}$$

find generators for K_0 .

How useful is Nakayama's lemma when $R = \mathbb{Z}$?

Here $J = 0$

$$N + 0 \cdot M = M \Rightarrow N = M$$

1 2 3 4 5 6 7 8 9 10
Not useful Very useful

Define $\text{Jac}(M) = \bigcap \text{maxl submodules of } M$.

Let M be finitely generated.

$$\text{Then } N + \text{Jac}(M) = M$$

$\Rightarrow N = M$ must be true.

(assuming every proper submodule of M is contained in a maxl submodule — TRUE.)

Proof. If $N \neq M$ then $N \subseteq M_1 \subsetneq M$, M_1 max in M
 $N + \text{Jac} M \subseteq M_1 \neq M$, contradiction
so $N = M$.

Fact: $\text{Jac}(R) \cdot M \subseteq \text{Jac} M$.

Pre-class Warm-up

Consider the statement:

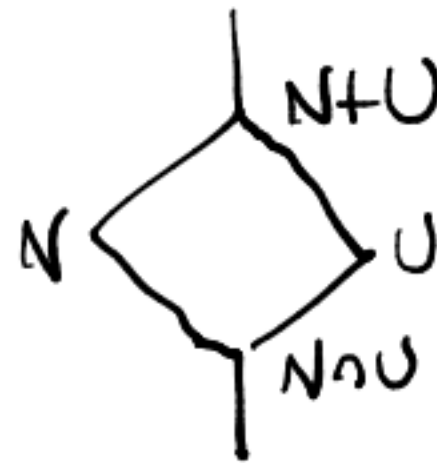
Let N, U be submodules of M . Then $N/(N \cap U)$ is isomorphic to a submodule of M/U .

How would you prove this?

- A The snake lemma.
- B Quote some other well-known theorem.
- C Localize.
- D Do an argument with elements.
- E None of the above!

2nd isomorphism theorem

$$N/(N \cap U) \cong (N+U)/U \subseteq M/U.$$



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 $Q_1 = 0$. *from S* *from R*

We only need find a prime Q of S with $R \cap Q = P$. *Why?*

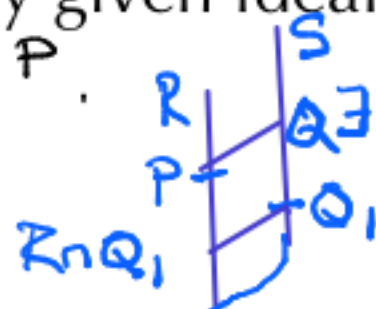
Localize: S_P is integral over R_P .

We may assume R is local with maximal ideal P .

If $U = R - P$, replace R by $R[U^{-1}]$, S by $S[U^{-1}]$

Assuming all this, any maximal ideal of S containing PS has preimage containing P , and therefore equal to P .

Why not equal to R ? Why isn't $PS \cap R = R$?



We prove that $PS \neq S$.

If $PS = S$ then 1 is an S -linear combination of finitely many elements of P .

Letting S' be the subring generated over R by the coefficients; then 1 is in PS' , so $PS' = S'$.

S and hence S' are integral over R .

Thus S' is a finitely generated R -module.

By Nakayama's lemma, $S' = 0$, a contradiction. \square

The Krull dimension of R is the largest d so that \exists a chain of prime ideals $P_0 \subset P_1 \subset \dots \subset P_d$ of R .

e.g. $K\text{-dim}(\text{field } k) = 0$

e.g. $K\text{-dim}(\text{PID}) = 1$

Should Eisenbud have explained more? Yes No

Lemma 4.16.

Let $R \subseteq S$ be domains. If $K(S)$ is algebraic over $K(R)$ then any nonzero ideal of S intersects R nontrivially.

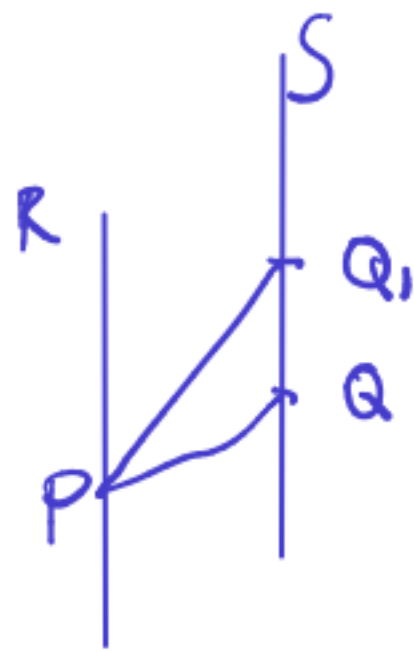
= field of fractions of S !

Proof. It suffices to consider a principal ideal bS .

Now b satisfies an equation

$$a_n b^n + \dots + a_1 b + a_0 = 0$$

a_i in $K(R)$. Multiplying by a common denominator and dividing by a power of b if necessary, we may assume $a_0 \neq 0$, $a_i \in R$. Now a_0 is in bS .



Corollary 4.18 (Incomparability).

Suppose $R \subseteq S$ is an integral extension of rings. Two distinct primes of S having the same intersection with R are incomparable.

Proof. If $Q \subsetneq Q_1 \subsetneq S$ are primes with $R \cap Q = R \cap Q_1 = P \subsetneq R$ then factoring out P in R and Q in S reduces to a situation where S is a domain, $Q = 0$ and $Q_1 \cap R = 0$.

Why factor out these?

Integral equations persist modulo P , so S is still integral over R and $K(S)$ is algebraic over $K(R)$.

Lemma 4.16 $\Rightarrow Q_1 = 0 = Q$ as required \square

Application.

If S is an integral extension of the ring R then R and S have the same Krull dimension

Proof. If $Q_0 \subset \dots \subset Q_d \subset S$ is a chain of prime ideals of S , then $R \cap Q_0 \subset \dots \subset R \cap Q_d$ is a chain ... of R . They are distinct by incomparability, so $\dim S \leq \dim R$.

Given a chain of prime ideals

$$P_0 \subset \dots \subset P_d \subset R$$

we find Q_0 (prime in S) with

$$Q_0 \cap R = P_0. \text{ Find } Q_1 \supseteq Q_0$$

Examples of Krull dimension.

$$(\text{prime in } S), Q_1 \cap R = P_1.$$

Repeat to get

$$Q_0 \subset \dots \subset Q_d \text{ in } S.$$

$$\dim R \leq \dim S. \quad \square$$

Example

If k is a field we will see that

$$\dim k[x_1, \dots, x_n] = n.$$

which is not obvious.

Another result that always seems to be included here in books on commutative algebra

Corollary 4.17.

If $R \subseteq S$ is an integral extension of domains, then S is a field if and only if R is a field

Proof. Observe: $K(S)$ is algebraic over $K(R)$.

Suppose R is a field. We show S is a field. Let $0 \neq b \in S$.
 $Sb \cap R \neq \{0\}$ (by Lemma)

$0 \neq r \in Sb \cap R$. r is a unit in R .
 r is a unit in S

$bS = S$, b is a unit.

Suppose S is a field.

$\nexists I \subseteq R$ is a prime ideal

$\exists Q \subseteq S$ prime with

$Q \cap R = I$ (by Lying Over)

Such $Q = \{0\}$ so $I = 0$.

Therefore R is a field, \square