MA 252 notes: Commutative algebra

(Distilled from [Atiyah-MacDonald])

Dan Abramovich

Brown University

February 19, 2017

Integral emlements

Definition

Let $A \subset B$. An element $x \in B$ is integral over A if there is a monic polynomial $f(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in A[t]$ such that $f(x) = 0$.

Examples

- $x = \sqrt{2} \in \mathbb{C}$ is integral over $\mathbb{Z}$.
- $x \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if $x \in \mathbb{Z}$ (write $x = m/n$ in rediced form, clear denominators in $f(m/n)$ and reduce moduli a prime dividing m).
- $x = \frac{1+\sqrt{5}}{2} \in \mathbb{C}$ is integral over $\mathbb{Z}$, since $\alpha^2 - \alpha - 1 = 0$, so appearance can be misleading.

Characterization

Proposition

The following are equivlent:

(i) $x \in B$ *integral over* A.

(ii) *The subring* $A[x] \subset B$ *is finite over* A.

(iii) $A[x]$ *is contained in a subring* $C \subset B$ *finite over* A.

(iv) *There is a faithful sub-*$A[x]$*-module* $M \subset B$ *which is finite over* A.

(i)⇒(ii) follows since $A[x] = A1 + Ax + \cdots + Ax^{n-1}$ as $x^n = -(a_1 x^{n-1} + \cdots + a_n)$ etc.
(ii)⇒(iii)⇒(iv) are evident.
(iv)⇒(i) take the characteristic polynomial $f(t)$ of x on generators of M, and we get $f(x) = 0 \in End(M)$ by Cayley-Hamilton.

The set of integral elements

Corollary

If $x_1, \ldots, x_n \in B$ are integral over A then any $A[\{x_i\}] \subset B$ is finite.

Indeed at each stage the extension is finite, and we have seen the result is finite.

Corollary

The set $C \subset B$ of integral element over A is a subring.

Indeed $x_1 \pm x_2, x_1 x_2, x_1/x_2 \in A[x_1, x_2]$.

Definition

The ring $C \subset B$ of integral element over A is the integral closure of A in B.

Remark

For arbitrary $f : A \to B$, we consider $f(A) \subset B$.

Integral closure

Definition

Let $C \subset B$ be the integral closure of A in B.

- $A \subset B$ is integrally closed if $C = A$.
- We say B is integral over A if $C = B$.

Corollary

If $A \subset B \subset C$ with $B/A, C/B$ integral then C/A integral.

If $x \in C$ satisfies $x^n + b_1 x^{n-1} + \cdots + b_n = 0$, then $A[b_1, \ldots, b_n][x]$ is finite over $A[b_1, \ldots, b_n]$ which is finite over A.

Corollary

Let C be the integral closure of A in B. Then C is integrally closed in B.

Indeed if $x \in B$ is integral over C then it is integral over A.

Integrality and fractions

Proposition

Say B/A integral.

(i) *$\mathfrak{b} \subset B$ and $\mathfrak{a} = A \cap \mathfrak{b}$ then $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$.*

(ii) *If $S \subset A$ multiplicative then $B[S^{-1}]/A[S^{-1}]$ integral.*

(i) lift $\bar{x} \in B/\mathfrak{b}$ to $x \in B$ and use the same equation, modulo $\mathfrak{a}$.
(ii) For $x/s \in B[S^{-1}]$ divide the equation of x by s^n.

Remark

The opposite is false.

Integrality, fields, and primes

Proposition

If $A \subset B$ are domains, B/A integral. Then B is a field if and only if A a field.

If A a field and $y \neq 0 \in B$ then the equation $y^n + \ldots + a_n = 0$ of smallest degree has $a_n \neq 0$, so $y^{-1} = -(y^{n-1} + \cdots + a_{n-1})/a_n$.
If B a field, $x \neq 0 \in A$ then $y = 1/x \in B$ has equation $y^m + a_1 y^{n-1} + \cdots + a_n = 0$ so $y = -(a_1 + \cdots + a_n x^{n-1}) \in A$.

Corollary

if $\mathfrak{q} \in \operatorname{Spec} B$, B/A integral, $\mathfrak{p} = A \cap \mathfrak{q}$. Then $\mathfrak{q}$ maximal if and only if $\mathfrak{p}$ maximal.

Primes in integral extensions and surjectivity of Spec

Corollary

B/A integral, $\mathfrak{q}, \mathfrak{q}' \in \operatorname{Spec} B$, $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Then $\mathfrak{q} = \mathfrak{q}'$.

We have $B_{\mathfrak{p}}/A_{\mathfrak{p}}$ integral. Let $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$, a maximal ideal. Let $\mathfrak{n} = \mathfrak{q}B_{\mathfrak{p}}$, $\mathfrak{n}' = \mathfrak{q}'B_{\mathfrak{p}}$, so $\mathfrak{n} \subset \mathfrak{n}'$ and $\mathfrak{n} \cap A_{\mathfrak{p}} = \mathfrak{n}' \cap A_{\mathfrak{p}} = \mathfrak{m}$. By the corollary $\mathfrak{n}, \mathfrak{n}'$ are maximal so $\mathfrak{n} = \mathfrak{n}'$. By the correspondence, $\mathfrak{q} = \mathfrak{q}'$.

Theorem

If $A \subset B$ and B/A integral then $\operatorname{Spec} B \to \operatorname{Spec} A$ surjective.

Consider $\mathfrak{p} \in \operatorname{Spec} A$ and the diagram $\begin{array}{ccc} A & \hookrightarrow & B \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ A_{\mathfrak{p}} & \hookrightarrow & B_{\mathfrak{p}} \end{array}$. For a maximal ideal $\mathfrak{n} \subset B_{\mathfrak{p}}$, we have $\mathfrak{n} \cap A_{\mathfrak{p}}$ is maximal, so $\mathfrak{n} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$, in particular $\mathfrak{q} = \beta^{-1}(\mathfrak{n})$ restricts to $\alpha^{-1}(\mathfrak{n} \cap A_{\mathfrak{p}}) = \alpha^{-1}(\mathfrak{p}A_{\mathfrak{p}}) = \mathfrak{p}$.

Going up

Theorem (Going up)

Let B/A integral, $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n \subset A$ primes, $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m \subset B$ primes such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i, i = 1, \ldots, m$. Then there is an extended sequence $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i, i = 1, \ldots, n$.

Suffices to prove: $\mathfrak{p}_1 \subset \mathfrak{p}_2$, $\mathfrak{p}_1 = \mathfrak{q}_1 \cap A$ then there is $\mathfrak{q}_1 \subset \mathfrak{q}_2$ such that $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$.
Reducing to $A/\mathfrak{p}_1 \subset B/\mathfrak{p}_2$ we have by surjectivity $\bar{\mathfrak{q}}_2 \in \operatorname{Spec} B/\mathfrak{p}_2$ with $\bar{\mathfrak{q}}_2 \cap A/\mathfrak{p}_1 = \bar{\mathfrak{p}}_2$.
This gives the required $\mathfrak{q}_2$.

Integral closure and fractions

Proposition

If C is the integral closure of A in B and $S \subset A$ multiplicative then $C[S^{-1}]$ is the integral closure of $A[S^{-1}]$ in $B[S^{-1}]$.

We have seen that $C[S^{-1}]$ is integral over $A[S^{-1}]$.
Let the equation of an integral b/s be
$x^n + (a_1/s_1)x^{n-1} + \cdots + (a_n/s_n) = 0$. Take $t = \prod s_i$ and multiply by $(st)^n$, and get an integral equation for bt, so $bt \in C$ and $b/s = (bt)/(st) \in C[S^{-1}]$.

Integrally closed domains

A domain A is integrally closed if it is integrally closed in its field of fractions K. E.g. every UFD (by the argument of $\mathbb{Z}$).

Proposition (Integral closedness is local)

Fix a domain A. The following are equivalent:

- *A integrally closed.*
- *$A_{\mathfrak{p}}$ is integrally closed for all primes $\mathfrak{p}$.*
- *$A_{\mathfrak{m}}$ is integrally closed for all maximals $\mathfrak{m}$.*

Let C be the integral closure of A in K. Then $C_{\mathfrak{p}}$ is the integral closure of $A_{\mathfrak{p}}$.
A (resp. $A_{\mathfrak{p}}$) is integrally closed if and only if $A \to C$ (resp. $A_{\mathfrak{p}} \to C_{\mathfrak{p}}$) surjective. Recall that surjectivity (just like injectivity) is a local property. (If we proved just injectivity, complete the proof!)

Integral closure of ideals

Definition

if $\mathfrak{a} \subset A \subset B$ then $b \in B$ is integral over $\mathfrak{a}$ if it satisfies $f(b) = 0$ with $f(t) = t^n + a_1 t^{n-1} + \cdots a_n$ with $a_i \in \mathfrak{a}$. The integral closure of $\mathfrak{a}$ in B is the set of all such.

Lemma

Let C be the integral closure of $A \subset B$ and $\mathfrak{c} = \mathfrak{a}C$. Then the integral closure of $\mathfrak{a}$ in B is the radical $r(\mathfrak{c})$.

If x is integral over $\mathfrak{a}$ then it is integral over A so $x \in C$. The equation gives $x^n \in \mathfrak{a}C = \mathfrak{c}$ so $x \in r(\mathfrak{c})$.
If $x \in r(\mathfrak{c})$ then $x^n = \sum a_i x_i$ with $a_i \in \mathfrak{a}$ and $x_i \in C$. The module $M = A[x_1, \ldots, x_n]$ is finite, and $x^n M \subset \mathfrak{a}M$, so taking characteristic polynomial we get that x^n is integral over $\mathfrak{a}$, so x is integral over $\mathfrak{a}$.

Integrality and fields

Proposition

Let $A \subset B$ be domains, assume $A \subset K := A_{(0)}$ integrally closed, and $x \in B$ integral over $\mathfrak{a} \subset A$. Then x is algebraic over K, and its minimal polynomial $f(t) = t^n + a_1 t^{n-1} + \cdots + a_1$ has $a_i \in r(\mathfrak{a})$.

Since x is integral over A it is algebraic over K. Let L/K be a normal extension containing x, so the conjugates $x_i \in L$. All x_i are also integral over $\mathfrak{a}$, since $f(t)$ divides the integrality equation. The coefficients of $f(t)$ are polynimials in x_i so integral over $\mathfrak{a}$ (by the previous result). Since $A \subset K$ integrally closed, $a_i \in A$. By the previous result they are in $r(\mathfrak{a})$.

Going down

Theorem

$A \subset B$ integral, A, B domains, $A \subset K$ integrally closed.
$A \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_n$ and $B \supset \mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m$ primes, such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$. Then there is an extended chain $B \supset \mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_m \cdots \supset \mathfrak{q}_n$ of primes, such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$.

Again it suffices to take $n = 2, m = 1$. (Localizing at $\mathfrak{p}_1$ we may assume it is maximal.)

Going down - proof

There is $\mathfrak{q}_2 \subset \mathfrak{q}_1$ such that $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$.

Consider the ring $B_{\mathfrak{q}_1}$. By that controversial proposition it suffices to prove that $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A = \mathfrak{p}_2$.
Write $y/s \in B_{\mathfrak{q}_1}\mathfrak{p}_2$ with $y \in B\mathfrak{p}_2$ and $s \in B \setminus \mathfrak{q}_1$. Now y is integral over $\mathfrak{p}_2$. So its minimal equation $y^r + u_1 y^{r-1} + \cdots$ over K has coefficients $u_i \in r(\mathfrak{p}_2) = \mathfrak{p}_2$.
If $x = y/s \in B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A$ then $s = y/x \in K$ so its minimal equation over K has coefficients $v_i = u_i/x^i$, hence $x^i v_i \in \mathfrak{p}_2$. Since s is integral over A we have $v_i \in A$.
But if $x \notin \mathfrak{p}_2$ then $v_i \in \mathfrak{p}_2$ would imply $s \in r(\mathfrak{q}_1) = \mathfrak{q}_1$, a contradiction, so $x \in \mathfrak{p} - 2$ as required.

Integral closure in a finite extension field

Proposition

Let A be integrally closed in K, L/K a finite separable extension, B the integral closure of A in L. Then there is a basis v_i of L/K such that $B \subset \sum Av_i$.

Suppose $v \in L$. Then it satisfies $\sum a_i v^{r-i} = 0$ for $a_i \in A$, $a_0 \neq 0$. It follows that $a_0 v$ is integral over A. So we can rescale elements of a basis to get a basis $\{u_i\} \subset B$.

Since L/K separable the bilinear form $Tr(xy)$ is nondegenerate.

Let $\{v_i\} \subset L$ be the dual basis: $Tr(v_i u_j) = \delta_{ij}$.

For $x \in B$ write $x = \sum x_i v_i$. Now $xu_i \in B$ so $Tr(xu_i) \in A$ as the coefficient of the polynimial of xu_i.

Now $Tr(xu_i) = Tr(\sum_j x_j v_j u_i) = \sum_j x_j Tr(v_j u_i) = x_i \in A$ so $B \subset \sum Av_j$.

Challenge: what about purely inseparable?

Valuation rings

Definition

Let B be a domain, $K = B_{(0)}$.
We say B is a valuation ring if every $x \in K$ has either $x \in B$ or $x^{-1} \in B$.

The condition says that two elements can be compared: $x \preccurlyeq y$ if $y/x \in B$, with $x \approx y$ if $x/y \in B^\times$.
Fields are valuation rings. $\mathbb{Z}_{(p)}$ and any $D_{\mathfrak{m}}$ for PID D and $\mathfrak{m}$ maximal is a valuation ring. $\mathbb{Z}_p$ is a valuation ring.

Basic properties

Proposition

Assume $B \subset K$ a valuation ring. Then (1) B is local, (2) $B \subset B' \subset K \Rightarrow B'$ a valuation ring, and (3) B is integrally closed.

Writ $\mathfrak{m} = B \setminus B^\times$. We claim $\mathfrak{m}$ an ideal (and then it is maximal and B local). Indeed if $a \in B, x \in \mathfrak{m} \Rightarrow ax \notin B^\times \Rightarrow ax \in \mathfrak{m}$.
If$x, y \in \mathfrak{m}$ nonzero then either xy^{-1} or $yx^{-1} \in B$, so
$x + y = (xy^{-1} + 1)y = x(1 + yx^{-1}) \in \mathfrak{m}$, giving (1).
(2) is immediate.
If $x \in K$ is integral then $x^n + b_1 x^{n-1} + \cdots + b_n = 0$ so if we had $x^{-1} \in B$ then $x = -(b_1 + b_2 x^{-1} + \cdots + b_n x^{-(n-1)} \in B$ anyway.

Construction of many valuation rings

Consider K and an algebraically closed field Ω. Consider the set $\mathcal{P} = \{(A, f) | A \subset K, f : A \to \Omega\}$, partially ordered by containment/restrictions. Zorn's Lemma applies, so maximal elements dominating any given one (A, f) exist. If $\Omega \supset K$ then $B = K$ itself is a maximal element. If B a valuation ring and $\Omega \supset B/\mathfrak{m}$ the algebraic closure then it is already maximal. What about the others?

Theorem

maximal elements (B, g) are valuation rings.

Lemmas

Lemma

B is local and $\mathfrak{m} = \mathrm{Ker} g$ the maximal ideal.

$g(B) \subset \Omega$ a domain, so $\mathfrak{m}$ is prime. Extend $B_{\mathfrak{m}} \to \Omega$ by $g(b/s) = g(b)/g(s)$, well defined as $s \notin \mathfrak{m}$. By maimality $B = B_{\mathfrak{m}}$ local and the kernel is $\mathfrak{m}$.

Lemma

For $0 \neq x \in K$ consider the subring $B[x] \subset K$ and ideal $\mathfrak{m}[x]$. Then either $\mathfrak{m}[x] \neq B[x]$ or $[\mathrm{x}^{-1}] \neq \mathrm{B}[\mathrm{x}^{-1}]$.

If $\sum v_j x^{-j} = \sum u_i x^i$ are minimal degeree relations with $u_i, v_j \in \mathfrak{m}$, then multiply one to cancel out and get e.g. $(1 - v_0)x^n = v_1 x^{n-1} + \cdots + v_n$, but $1 - v_0$ is a unit so we get $x^n = \sum_{i=1}^{n} w_i x^i$ which can be substitute to shorten the given one, contradicting assumption.

Proof of theorem

If (B, g) maximal then B a valuation ring.

May assume $\mathfrak{m}[x] \neq B[x] \subset K$. So $\mathfrak{m}[x] \subset \mathfrak{n} \subset B[x]$ maximal. $\mathfrak{m} \subset \mathfrak{n} \cap B \subsetneq B$ so $frn \cap B = \mathfrak{m}$. get inclusion $B/\mathfrak{m} \subset B[x]/\mathfrak{n} = B/\mathfrak{m}[\bar{x}]$. Whether or not $\bar{x}$ algebraic it has a place in Ω, so by maximality $B[x] = B$ and $x \in B$.

Chracterizing integral closure

Corollary

If $\tilde{A}$ the integral closure of $A \subset K$ then $\tilde{A} = \cap_{A \subset B \text{ valuation of } K} B$.

First, any $B \supset \tilde{A}$ since B integrally closed.
Note that if $x \in A[x^{-1}]$ then $x \in \tilde{A}$. Assume $x \notin \tilde{A}$ then $x^{-1} \notin A[x^{-1}]^{\times}$. So there is a maximal ideal $x^{-1} \in \mathfrak{m} \subset A[x^{-1}]^{\times}$. The morphism $A \to A[x^{-1}]/\mathfrak{m}$ extends to $B \to \Omega$ for some valuation ring B containing A, x^{-1}, and since $x^{-1} \in \mathfrak{m}$ we have $x \notin B$.

Extensions of homomorphisms

Proposition

$A \subset B$ fin. gen., domain, $0 \neq v \in B$. There is $0 \neq u \in A$ s.t. any $f : A \to \Omega$ with $f(u) \neq 0$ extends to $g : B \to \Omega, g(v) \neq 0$.

By induction assume $B = A[x]$.

- If x transcendental, write $v = h(x)$ for some polynomial $h \in A[t]$, and take $u = a_0$ say. Write $\bar{h}[t] \in \Omega[t]$ for the image under f, nonzero since $f(a_0) \neq 0$. we have some $\xi \in \Omega$ such that $\bar{h}(\xi) \neq 0$, and define $g : A[x] \to \Omega$ by $g(x) = \xi$.
- If x is algebraic then v^{-1} is algebraic. Set $\sum a_i x^i = 0$ and $\sum b_i v^{-i} = 0$. Let u be the product of leading terms. Then f extends to $A[u^{-1}]$ since Ω a field, and to a morphism $g' : C \to \Omega$ on a valuation ring C containing $A[u^{-1}]$ by the big extension theorem. Note x, v^{-1} are integral over $A[u^{-1}]$. So $x, v^{-1} \in C$, in particular $B \subset C$ and $v \in C^\times$, so $g'(v) \neq 0$. The restriction $g = g'_B$ works.

Weak Nullstellensatz, first installement

Proposition

$A \subset B$ fin. gen., domain, $0 \neq v \in B$. There is $0 \neq u \in A$ s.t. any $f : A \to \Omega$ with $f(u) \neq 0$ extends to $g : B \to \Omega, g(v) \neq 0$.

Theorem

A finitely generated algebra B over a field k is a field if and only if it is a finite extension of k.

Indeed, one can take $v = 1 \in B$ and consider $f : A \to \Omega = \bar{k}$.