Lecture 10. Integral extensions

Definition 4.20. *Suppose $A \subset B$ are commutative rings. We say that $b \in B$ is* **integral** *over A if there exist $m \geq 1$ and $a_0, a_1, \ldots, a_{m-1} \in A$ such that*

$$b^m + a_{m-1}b^{m-1} + \ldots + a_1 b + a_0 = 0.$$

We say that B is integral over A if all elements of B are integral over A.

In other words, $b \in B$ is integral over A if there exists a **monic** polynomial $f \in A[X]$ such that $f(b) = 0$.

▶ Let $A = \mathbb{Z}$ and $B = \mathbb{Q}$. The elements of $\mathbb{Q}$ integral over $\mathbb{Z}$ are exactly the integers: if $b = p/q$ in lowest terms satisfies a monic equation of degree m over $\mathbb{Z}$, then multiplying by q^m shows that q divides p^m, so $q = \pm 1$.

▶ Let $A = \mathbb{Z}$ and $B = \mathbb{Q}(i)$. The elements of B integral over $\mathbb{Z}$ are the Gaussian integers $\mathbb{Z}[i]$.

▶ Let $A = \mathbb{Z}[\sqrt{-3}]$ and $B = \mathbb{Q}(\sqrt{-3})$. Then $\omega = (-1 + \sqrt{-3})/2 \notin A$ is integral over A, since $\omega^2 + \omega + 1 = 0$. The elements of B integral over A are the Eisenstein integers $\mathbb{Z}[\omega]$.

More generally, in algebraic number theory one studies the **ring of integers** $\mathcal{O}_K$ of a number field K (a finite extension of $\mathbb{Q}$), defined as

$$\mathcal{O}_K = \{b \in K : b \text{ is integral over } \mathbb{Z}\}.$$

That this is a ring is not obvious from the definition, but follows from Corollary 4.23(b) below.

The proof of the following lemma uses Cramer's rule from linear algebra, which we recall for convenience; it holds over any commutative ring R. Let $M \in M_n(R)$ be an n-by-n matrix with entries in R and let $Mx = y$ be a system of n linear equations, where x and y are column vectors with entries in R. Write $M = [m_1 \ m_2 \ \ldots \ m_n]$ where m_i are the columns of M. Then the n linear equations can be written as

$$x_1 m_1 + x_2 m_2 + \ldots + x_n m_n = y.$$

Define new n-by-n matrices $M_j = [m_1 \ m_2 \ \ldots \ m_{j-1} \ y \ m_{j+1} \ \ldots \ m_n]$. Since the determinant is linear in each column and vanishes when two columns coincide,

$$\det M_j = \sum_{i=1}^{n} x_i \det[m_1 \ m_2 \ \ldots \ m_{j-1} \ m_i \ m_{j+1} \ \ldots \ m_n] = x_j \det M.$$

Lemma 4.21. *Let $A \subset B$ be commutative rings and $b \in B$. The following conditions are equivalent:*

i. b *is integral over* A.

ii. $A[b] \coloneqq \{f(b) : f \in A[X]\}$ *is finitely generated over* A *as a module.*

iii. *There exists a subring* $C \subset B$ *such that* $A[b] \subset C$ *and* C *is finitely generated over* A *as a module.*

Proof. *i.* implies *ii.* : By the hypothesis, we have a monic polynomial $g \in A[X]$ of degree m such that $g(b) = 0$. Given $f \in A[X]$, we can divide by g (as g is monic!) and write

$$f = gh + r, \text{ with } h, r \in A[X],$$

where $r = 0$ or $\deg(r) < m$. Then $f(b) = g(b)h(b) + r(b) = r(b)$. Hence $A[b] = \{r(b) : r = 0 \text{ or } \deg(r) < m\} = A \cdot 1 + A \cdot b + \ldots + A \cdot b^{m-1}$.

ii. implies *iii.* : Trivial. Take $C = A[b]$.

iii. implies *i.* : We have $C = Ac_1 + Ac_2 + \ldots + Ac_n$ with $c_i \in C$. Since $b \in C$ and C is a ring, we can write

$$bc_i = \sum_{j=1}^{n} a_{ij} c_j \text{ for some } a_{ij} \in A.$$

Let N be the n-by-n matrix with entries a_{ij} and let x be the column vector with entries c_i. Then $Nx = bx$, or equivalently $(bI_n - N)x = 0$. By Cramer's rule applied to $M = bI_n - N \in M_n(B)$ and $y = 0$, we get $\det M_j = 0$ and hence

$$c_i \det(bI_n - N) = 0 \text{ for all } i.$$

On the other hand, $1 \in C$, hence there exist $a_i \in A$ such that $1 = \sum_{i=1}^{n} a_i c_i$. It follows that

$$\det(bI_n - N) = \sum_{i=1}^{n} a_i c_i \det(bI_n - N) = 0.$$

Let $p(X) = \det(XI_n - N) \in A[X]$. Expanding the determinant shows that $p(X)$ is monic of degree n, and $p(b) = 0$. □

▶ For example, let $B = k[X, Y]/(X^2 - Y^2)$, and let $x, y \in B$ be the classes of X, Y. The subring $A = k[y] \subset B$ is isomorphic to $k[Y]$, since $(X^2 - Y^2) \cap k[Y] = \{0\}$, and $B = A \cdot 1 + A \cdot x$ since $x^2 = y^2$. Hence B is a finitely generated A-module, so B is integral over A by *iii.* of the lemma.

▶ Geometrically, the inclusion $k[y] \subset B$ in the previous example corresponds to the projection of $\mathcal{V}(X^2 - Y^2)$, the two lines $x = \pm y$ in k^2, onto the y-axis: every fibre is finite (two points, or one point over $y = 0$). Compare this with $k[x] \subset C = k[X, Y]/(XY - 1)$, the projection of the hyperbola $xy = 1$ onto the x-axis: the fibre over $x = 0$ is empty, the hyperbola "escapes to infinity" as $x \to 0$, and indeed y is not integral over $k[x]$, since multiplying an equation $y^m + a_{m-1}(x)y^{m-1} + \ldots + a_0(x) = 0$ by x^m gives $1 + a_{m-1}(x)x + \ldots + a_0(x)x^m = 0$ in $k[x] \subset C$, which is impossible. In general, for k algebraically closed, an integral extension of coordinate rings of affine varieties corresponds to a map of varieties which is onto with finite fibres; we will prove the surjectivity (the lying-over theorem) in Lecture 22.

Definition 4.22. *Let k be a field. We say that A is a k-**algebra** if*

(a) A is a vector space over k

(b) A is a commutative ring (with unity)

(c) $\lambda(a \cdot b) = (\lambda a) \cdot b = a \cdot (\lambda b)$ for all $a, b \in A$ and $\lambda \in k$.

The standard example of a k-algebra is the polynomial ring $k[X_1, \ldots, X_n]$, or more generally a quotient ring $A = k[X_1, \ldots, X_n]/I$ by an ideal I. We say that a k-algebra A is **finitely generated** if it is generated by finitely many elements as an algebra: there exist $a_1, \ldots, a_n \in A$ such that $A = \{f(a_1, \ldots, a_n) : f \in k[X_1, \ldots, X_n]\}$. We write $A = k[a_1, \ldots, a_n]$. In this case, we have a surjective k-algebra homomorphism

$$\pi : k[X_1, \ldots, X_n] \to A$$

given by $\pi(X_i) = a_i$, and A is isomorphic to $k[X_1, \ldots, X_n]/\ker(\pi)$. Thus every finitely generated k-algebra is of the form $k[X_1, \ldots, X_n]/I$.

More generally, let $A \subset B$ be commutative rings. For $b_1, \ldots, b_n \in B$ we write $A[b_1, \ldots, b_n] = \{f(b_1, \ldots, b_n) : f \in A[X_1, \ldots, X_n]\}$ for the subring of B generated by A and $b_1, \ldots, b_n$. We say that B is **finitely generated as an A-algebra** if $B = A[b_1, \ldots, b_n]$ for some $b_1, \ldots, b_n \in B$, or equivalently if B is isomorphic, as an A-algebra, to $A[X_1, \ldots, X_n]/I$ for some n and some ideal I. It is important not to confuse this with the similar sounding statement that B is a finitely generated A-module: $A[X]$ is finitely generated as an A-algebra but not as an A-module.

Corollary 4.23. *Let A and B be commutative rings with $A \subset B$.*

(a) Suppose $B = A[b_1, \ldots, b_n]$ where each b_i is integral over $A[b_1, \ldots, b_{i-1}]$. Then B is finitely generated as an A-module, and hence integral over A.

(b) The integral closure $\overline{A}_B := \{b \in B : b \text{ is integral over } A\}$ is a subring of B.

(c) If C is a ring with $A \subset C \subset B$ such that C is integral over A and B is integral over C, then B is integral over A.

(d) Let B be integral over A. If B is a field, then A is also a field. Conversely, if A is a field, and B is an integral domain, then B is also a field.

Proof. (a) We first show by induction on n that B is a finitely generated A-module. For $n = 1$ this is $i. \Rightarrow ii.$ of Lemma 4.21. For $n \geq 2$, put $B' = A[b_1, \ldots, b_{n-1}]$, so that $B = B'[b_n]$. By induction $B' = \sum_i Au_i$ for finitely many $u_i \in B'$, and since b_n is integral over B', Lemma 4.21 gives $B = \sum_j B'v_j$ for finitely many $v_j \in B$. Hence $B = \sum_{i,j} Au_iv_j$ is a finitely generated A-module. Now for every $b \in B$, condition $iii.$ of Lemma 4.21 holds with $C = B$, so b is integral over A.

(b) Every $a \in A$ is a root of $X - a$, so $A \subset \overline{A}_B$; in particular $1 \in \overline{A}_B$. If $b, b' \in \overline{A}_B$, then b' is also integral over $A[b]$, so $A[b, b']$ is integral over A by (a); in particular $b \pm b'$ and bb' lie in $\overline{A}_B$. Hence $\overline{A}_B$ is a subring of B.

(*c*) Let $b \in B$. Since b is integral over C, we have an equation

$$b^m + c_{m-1}b^{m-1} + \ldots + c_1 b + c_0 = 0 \text{ for some } c_0, \ldots, c_{m-1} \in C.$$

Each c_i is integral over A, hence over $A[c_0, \ldots, c_{i-1}]$, and the equation shows that b is integral over $A[c_0, \ldots, c_{m-1}]$. By part (*a*), applied to the generators $c_0, \ldots, c_{m-1}, b$ in this order, the ring $A[c_0, \ldots, c_{m-1}, b] \subset B$ is integral over A. Hence b is integral over A.

(*d*) Let B be a field, and let $a \in A$ be a non-zero element. Then $a^{-1} \in B$, and we want to show that $a^{-1} \in A$. Since B is integral over A, there is a relation

$$a^{-n} + a_{n-1}a^{-n+1} + \ldots + a_0 = 0 \text{ with } \ a_i \in A.$$

Multiplying by a^{n-1}, we get $a^{-1} = -(a_{n-1} + a_{n-2}a + \ldots + a_0 a^{n-1}) \in A$.

Conversely, suppose A is a field and B is an integral domain. Let $b \in B$ be a non-zero element, and choose an equation

$$b^m + a_{m-1}b^{m-1} + \ldots + a_1 b + a_0 = 0 \text{ with } \ a_i \in A$$

of smallest possible degree m. If $a_0 = 0$ then, since B is an integral domain and $b \neq 0$, we may cancel b and obtain a monic equation of smaller degree, contradicting the choice of m. Hence $a_0 \neq 0$, and

$$b^{-1} = -a_0^{-1}(b^{m-1} + a_{m-1}b^{m-2} + \ldots + a_1) \in B.$$

□

▶ Let $A \subset B$ be commutative rings. Then B is finitely generated as an A-module if and only if B is finitely generated as an A-algebra and integral over A. Indeed, module generators are algebra generators, and integrality follows from *iii.* of Lemma 4.21; the converse is Corollary 4.23(a).

Definition 4.24. *A is said to be* **integrally closed** *in B if $\overline{A}_B = A$. If A is an integral domain, we regard A as a subring of its field of fractions* $\mathrm{Frac}(A)$*. We say that an integral domain A is* **normal** *if it is integrally closed in* $\mathrm{Frac}(A)$*, and the integral closure of A in* $\mathrm{Frac}(A)$ *is called the* **normalisation** *of A.*

◁ Show that a UFD is normal (the argument given for $\mathbb{Z}$ at the start of this lecture works verbatim). In particular, $k[X_1, \ldots, X_n]$ is normal.

◁ Let $A = k[X, Y]/(Y^2 - X^3)$, and let $x, y \in A$ be the classes of X, Y. Show that $x \mapsto t^2$, $y \mapsto t^3$ identifies A with the subring $k[t^2, t^3]$ of $k[t]$, so that A is an integral domain with $\mathrm{Frac}(A) = k(t)$. The element $t = y/x \in \mathrm{Frac}(A)$ is not in A but satisfies the monic equation $t^2 - x = 0$ (and $t^3 - y = 0$), so A is not normal. Show that the normalisation of A is $k[t]$.

Macaulay2 can tell you whether a ring is normal, and compute the normalisation if not:

```
R = QQ[x,y]/(y^2-x^3)
isNormal R
S = integralClosure R
describe S
icFractions R
```

The last command shows that the new variable w of S is the fraction y/x, and

$$S = \mathbb{Q}[w, x, y]/(wy - x^2,\, wx - y,\, w^2 - x) \simeq \mathbb{Q}[w],$$

as the relations allow one to eliminate $x = w^2$ and $y = w^3$.