
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 $a_0, a_1, \dots, a_{m-1} \in A$ such that

$$b^m + a_{m-1}b^{m-1} + \dots + a_1b + a_0 = 0.$$

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 the characterisation of integral elements given in Lemma 4.21 below.

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. $A[b] := \{f(b) : f \in A[X]\}$ 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.

We will need 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 $M = [m_1 \ m_2 \ \dots \ m_n]$ where m_i are the columns of M . Then the n linear equations can be written as

$$x_1m_1 + x_2m_2 + \dots + x_nm_n = y.$$

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

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

Proof. (of Lemma 4.21) i. implies ii. : By the hypothesis, we have a monic polynomial $g \in A[X]$ 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 $\deg(r) < \deg(g) = m$. Then, $f(b) = g(b)h(b) + r(b)$. Hence, $A[b] = \{r(b) : r = 0 \text{ or } \deg(r) < m\} = A \cdot 1 + A \cdot b + \dots + A \cdot b^{m-1}$.

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

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

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

Consider the n -by- n matrix N with entries a_{ij} and x be the column vector with entries c_i . Then, we have $Nx = bx$ or equivalently $(N - bI_n)x = 0$. By Cramer's rule applied to $M = N - bI_n$, we get the equations

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

($\det M_j = 0$ since $y = 0$.) 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

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

Let $p(X) = \det(N - XI_n)$. We have $p(X) \in A[X]$ is a monic polynomial satisfying $p(b) = 0$. $\square$

► For example, consider the ring $B = k[X, Y]/(X^2 - Y^2)$ and its subring isomorphic to $A = k[Y]$ generated by $Y + (X^2 - Y^2)$. It is easy to see B is finite as an A -module. Indeed, $B = A \cdot 1 + A \cdot X$. Hence, B is integral over A .

Corollary 4.22. *Let A and B be commutative rings with $A \subset B$.*

- (a) *Suppose $B = A[b_1, \dots, b_n]$ with $b_i \in B$ such that b_i are integral over $A[b_1, \dots, b_{i-1}]$ for all i . Then B is integral over A and B is finitely generated as an A -module.*
- (b) *The integral closure $\bar{A}_B := \{b \in B : b \text{ integral over } A\}$ is a subring of B .*
- (c) *Let C be 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) Let $B = A[b, b']$ and b' is integral over $A[b]$ and b is integral over A . Then by Lemma 4.21, we see that $A[b]$ is a finitely generated A -module, and $A[b, b']$ is a finitely generated $A[b]$ -module. It follows that $A[b, b']$ is finitely generated as an A -module. Then, again by Lemma 4.21, it follows that B is integral over A . The general case follows from this by recursion.

(b) Given $b, b' \in B$ integral over A from (a) we get $A[b, b'] \subset B$ is finitely generated over A and so integral over A .

(c) Let $b \in B$ integral over C , then we have an equation

$$b^m + c_{m-1}b^{m-1} + \dots + c_1b + c_0 = 0 \text{ for some } c_0, \dots, c_{m-1} \in C$$

Let $C' = A[b, c_0, \dots, c_{m-1}] \subset B$. The ring $A[c_0, \dots, c_{m-1}]$ is integral over A , and by part (a), C' is integral over A . Hence, b is integral over A .

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

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

Then, we have $a^{-1} = -(a_{n-1} + a_{n-2}a + \dots + a_0a^{n-1}) \in A$.

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

$$b^m + a_{m-1}b^{m-1} + \dots + a_1b + a_0 = 0 \text{ with } a_i \in A$$

Since B is an integral domain, we can assume that $a_0 \neq 0$. Then,

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

□

Definition 4.23. A is said to be **integrally closed** in B if $\overline{A}_B = A$. Assuming that A is an integral domain, we can see A embedded in its field of fractions: $A \subset \text{Frac}(A)$. We say that an integral domain is **normal** if it is integrally closed in its field of fractions. If A is an integral domain, the integral closure of A in $\text{Frac}(A)$ is called the **normalisation** of A .

► The ring $k[X_1, \dots, X_n]$ is normal.

◁ More generally, a ring which is a UFD is normal.

◁ The ring $A = k[x, y]/(y^2 - x^3)$ is not normal. Indeed, the element $t = y/x \in \text{Frac}(A)$ satisfies the monic equation $t^2 - x = 0$ (and $t^3 - y = 0$). Show that the normalisation of A is isomorphic to $k[t]$.

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

```

Definition 4.24. 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 $\lambda \in k$.

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

$$\pi : k[X_1, \dots, X_n] \rightarrow A$$

given by $\pi(X_i) = a_i$ and A is isomorphic to $k[X_1, \dots, X_n]/\ker(\pi)$.

More generally, if $A \subset B$ are commutative rings. We say that B is **finitely generated as an A -algebra** if B is isomorphic to $A[X_1, \dots, X_n]/I$ for some n and ideal I in which case we can write $B = A[b_1, \dots, b_n]$ for some $b_i \in B$. It is important not to confuse this with the similar sounding statement that says that B is a finitely generated A -module.

► Let $A \subset B$ be commutative rings. It follows easily from Lemma 4.21 that B is finitely generated as an A -module if and only if B is finitely generated as an A -algebra and integral over A .

We say that $a_1, \dots, a_n$ are **algebraically independent** if there is no non-zero polynomial $F \in k[X_1, \dots, X_n]$ such that $F(a_1, \dots, a_n) = 0$. This is equivalent to the injectivity of the homomorphism π .