Lecture 15 – Integral dependence

Recall that given a field extension $k \subseteq k'$, we say that an element $\alpha \in k'$ is **algebraic** over k if there is a some polynomial $f \in k[x]$ such that $f(\alpha) = 0$.

We now generalise this concept, but in a stronger form, to general rings.

Definition. Let $A \subseteq B$ be rings, and let $b \in B$. We say b is **integral** over A if we can find a polynomial

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \qquad a_i \in A,$$

such that $f(b) = 0$.

Remark. It is crucial in this definition that the coefficient of x^n is 1.

Example. Consider $\mathbb{Z} \subset \mathbb{Q}$. Then $b \in \mathbb{Q}$ is integral over $\mathbb{Z} \Leftrightarrow x \in \mathbb{Z}$.

$\Leftarrow$: If $b \in \mathbb{Z}$, then take $f = x - b$, so b is integral over $\mathbb{Z}$.

$\Rightarrow$: Let $b = p/q$, and assume that $\gcd(p, q) = 1$. If

$$x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0,$$

then we get

$$p^n + c_{n-1}p^{n-1}q + \cdots + c_0 q^n = 0.$$

Since q divides all the other terms, q divides p^n, and since $\gcd(q, p) = 1$ this can only happen if $q = 1$. Hence $p/q \in \mathbb{Z}$.

Example. Let k be a field, and consider $k[x] \subseteq k(x)$. Then similarly $f \in k(x)$ is integral over $k[x]$ if and only if $f \in k[x]$. The proof is exactly the same as in the previous example: In $k[x]$ we have unique factorisation into irreducibles, so we can write $f = p/q$ with $p, q \in k[x]$ having no common factor, and the rest of the proof goes through.

Example. Given $A \subseteq B$, every element $a \in A$ is integral over A, by taking the polynomial $x - a$.

Definition. Given $A \subseteq B$ and $b \in B$, we let $A[b] \subseteq B$ be the smallest subring of B containing A and b. Explicitly

$$A[b] = \{\sum_{i=1}^{k} a_i b^i \mid a_i \in A\} \subseteq B.$$

More generally, given $b_1, \ldots, b_n \in B$, we let

$$A[b_1, \ldots, b_n] = \{\sum a_{i_1 \cdots i_n} b_1^{i_1} \cdots b_n^{i_n} \mid a_i \in A\} \subseteq B.$$

Theorem. *Let $A \subset B$, and let $b \in B$. The following are equivalent:*

1. *b is integral over A.*
2. *$A[b]$ is a finitely generated A-module.*
3. *There is a ring C with $A[b] \subseteq C \subseteq B$ such that C is a finitely generated A-module.*

Proof. (1) $\Rightarrow$ (2): The ring $A[b]$ is generated by the infinite set $1, b, b^2, \cdots$. If b is integral, we can write

$$b^k = -(a_{k-1}b^{k-1} + \cdots + a_0),$$

and therefore

$$b^{k+m} = (a_{k-1}b^{k+m-1} + \cdots + a_0 b^m)$$

So we can always express b^{k+m} in terms of b^i for $i < k+m$. This gives that $1, b, \ldots, b^{k-1}$ generate $A[b]$.

(2) $\Rightarrow$ (3): Obvious, take $C = A[b]$.

(3) $\Rightarrow$ (1): We need the following

Lemma (Ch. 2, Lemma 2.4). [7] *Let M be a finitely generated A-module, generated by k elements, and let $\phi\colon M \to M$ be a homomorphism. Then we can find $a_0, \cdots, a_{k-1} \in A$ such that*

$$\phi^k + a_{k-1}\phi^{k-1} + \cdots + a_0 = 0 \in \mathrm{Hom}_A(M, M).$$

where $\phi^i = \overbrace{\phi \circ \cdots \circ \phi}^{i}$.

Take now $M = C$, $\phi\colon C \to C$ given by $\phi(c) = bc$. The lemma ensures that we can find $a_i \in A$ such that

$$\phi^k + a_{k-1}\phi^{k-1} + \cdots + a_0 = 0 \in \mathrm{Hom}_A(C, C).$$

Inserting $1 \in C$ on both sides gives

$$b^k + a_{k-1}b^{k-1} + \cdots + a_0 = 0,$$

so b is integral over A. □

Example. Consider $\mathbb{Z} \subseteq \mathbb{Q}$ again, and take for instance $\frac{1}{2} \in \mathbb{Q}$. In this case $\frac{1}{2}$ is not integral over $\mathbb{Z}$, and equivalently the ring

$$\mathbb{Z}[1/2] = \mathbb{Z}_2 \subseteq \mathbb{Q}$$

is not a finite $\mathbb{Z}$-module.

Proposition. *Assume $b_1, b_2 \in B$ are integral over A. Then $A[b_1, b_2]$ is a finitely generated A-module.*

Proof. Consider the chain of rings

$$A \subseteq A[b_1] \subseteq A[b_1, b_2] \subseteq B$$

Then b_2 is integral over $A \Rightarrow b_2$ is integral over $A[b_1]$, so $A[b_1, b_2] = A[b_1][b_2]$ is a finitely generated $A[b_1]$-module. If it is generated by $c_1, \ldots, c_k$ and $A[b_1]$ is generated as an A-module by $d_1, \ldots, d_l$, one checks that $A[b_1, b_2]$ is generated as an A-module by $\{c_i d_j\}$:

$$\begin{aligned} x \in A[b_1, b_2] \Rightarrow x &= \sum_{i=1}^{k} f_i c_i, \qquad f_i \in A[b_i] \\ &= \sum_{i=1}^{k} \sum_{j=1}^{l} a_{ij} c_i d_j. \end{aligned}$$

[7] It is perhaps useful to think of this lemma as a version of the Cayley–Hamilton theorem. If A is an $(n \times n)$ matrix with coefficients in a field k, then recall its characteristic polynomial is given by

$$\det(xI_n - A) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in k[x],$$

where for instance $a_{n-1} = -tr(A)$ and $a_0 = (-1)^n \det(A)$. The Cayley–Hamilton theorem says that we have an equality of $(n \times n)$-matrices

$$A^n + a_{n-1}A^{n-1} + \cdots + a_0 = 0.$$

□

Corollary. *Let $A \subseteq B$. The set of elements of B which are integral over A forms a subring of B.*

Proof. We must show that given $b_1, b_2 \in B$ integral over A, then also $b_1 \pm b_2$ and $b_1 b_2$ are integral over A. But b_1 and b_2 being integral over A implies $A[b_1, b_2]$ is a finitely generated A-module, and we have $b_1 \pm b_2, b_1 b_2 \in A[b_1, b_2]$. These then satisfy condition (3) of the theorem above, so are integral. □

Definition. Given $A \subseteq B$, we call the ring

$$C = \{b \in B \mid b \text{ integral over } A\}$$

the **integral closure** of A in B. If A is equal to its integral closure, we say it is **integrally closed** in B.

Proposition. *The integral closure C of A in B is itself integrally closed in B.*

Proof. Assume $b \in B$ is integral over C, then we can write

$$b^n + c_{n-1} b^{n-1} + \cdots + c_0 = 0, \qquad c_i \in C.$$

We have that b is integral over $A[c_0, \cdots, c_{n-1}]$, so $A[c_0, \cdots, c_{n-1}, b]$ is a finitely generated $A[c_0, \cdots, c_{n-1}]$-module. The ring $A[c_0, \cdots, c_{n-1}]$ is itself a finitely generated A-module, since the c_i are integral over A. Then $A[c_0, \cdots, c_{n-1}, b]$ is a finitely generated A-module. Therefore b is integral over A, so $b \in C$. □

Example. The ring $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

Example. The integral closure of $\mathbb{Z}$ in $\mathbb{C}$ is called the ring of **algebraic integers**, i.e. a complex number z is an algebraic integer if we can find integers $a_0, \cdots, a_{n-1}$ such that

$$z^n + a_{n-1} z^{n-1} + \cdots + a_0.$$

The most important special case is the following. Given an integral domain A, it is contained in its field of fractions K. We say A is **integrally closed** if it is integrally closed in K.

Example. The ring $\mathbb{Z}$, and more generally every unique factorisation domain, is integrally closed.

Example. The ring $\mathbb{Z}[\sqrt{5}]$ is *not* integrally closed (which means that it does not have unique factorisation). The fraction field

$$K = \{\frac{a + b\sqrt{5}}{c + d\sqrt{5}} \mid a, b, c, d \in \mathbb{Z}\} = \mathbb{Q}(\sqrt{5}) \subset \mathbb{R},$$

and in particular we have the golden ratio $\varphi = \frac{1+\sqrt{5}}{2} \in K$. But we have

$$\varphi^2 - \varphi - 1 = 0,$$

so φ is integral over $\mathbb{Z}$, hence over $\mathbb{Z}[\sqrt{5}]$. One checks that $\varphi \notin \mathbb{Z}[\sqrt{5}]$.

Example. Consider the ring $k[x^2, x^3] \subseteq k[x]$. Concretely, we have

$$k[x^2, x^3] = \{\sum_{i=0}^{n} a_i x^i \mid a_i \in k, a_1 = 0\}.$$

Let K be the fraction field of $k[x^2, x^3]$. We have an element $a = x^3/x^2 \in K$, and moreover

$$a^2 = x^4/x^2 = x^2/1,$$

so a is a zero of the polynomial $t^2 - x^2$. This shows that a is integral over $k[x^2, x^3]$. One can also check that $a \notin k[x^2, x^3]$, so $k[x^2, x^3]$ is not integrally closed.