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 $f(\alpha) = 0$.

Example. For the field extension $\mathbb{Q} \subset \mathbb{R}$, the element $\sqrt{2}$ is algebraic over $\mathbb{Q}$ since $x^2 - 2 \in \mathbb{Q}[x]$ has $\sqrt{2}$ as a 0. The element $\pi \in \mathbb{R}$ is not algebraic over $\mathbb{Q}$.

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

Definition. Let $A \subseteq B$ be rings, and let $b \in B$. We say b is **integral** over A if there is a polynomial $f \in A[x]$ of the form

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

such that $f(b) = 0$.

Remark. It is crucial in this definition that f is **monic**, i.e. that the coefficient of the highest order term 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

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

so

$$p^n = -q(c_{n-1}p^{n-1} + \cdots + c_0 q^{n-1})$$

Now q divides p^n, and since $\gcd(q, p) = 1$ this can only happen if $q = \pm 1$. 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 $x - a$.

Example. If $k \subseteq k'$ is a field extension, then $b \in k'$ is integral over k if and only if it is algebraic over k: A polynomial $f = a_n x^n + \cdots + a_0 \in k[x]$ with b as a root gives a monic polynomial f/a_n with b as a root.

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 $A \subseteq B$, 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 (Cf. Ch. 2, Lemma 2.4)**.** *Let M be an A-module generated by elements $x_1, \ldots, x_n \in M$, $a_{ij} \in A, 1 \leq i, j \leq n$ be elements such that for every j we have*

$$\sum_{i=1}^{n} a_{ij}x_j = 0$$

Let X be the matrix (a_{ij}). Then $\det(X)x = 0$ for all $x \in M$.

Proof. Let X be the $(n \times n)$-matrix with coefficients in A given by a_{ij}. Let Y be the adjugate matrix, that is the matrix with entries b_{ij}, where b_{ij} is the (j,i)-th minor of X. We then have the matrix product equality $YX = \det(X)I_n$. Fixing some i, this means that

$$\sum_{j=1}^{n}\sum_{k=1}^{n} b_{ij}a_{jk}x_k = \det(X)x_i.$$

On the other hand we have

$$\sum_{j=1}^{n}\sum_{k=1}^{n} b_{ij}a_{jk}x_k = \sum_{j=1}^{n} b_{ij}\left(\sum_{k=1}^{n} a_{jk}x_k\right) = \sum_{j=1}^{n} b_{ij}0 = 0$$

Since $\det(X)x_j = 0$ for every generator of M, the claim follows. □

Take now $M = C$. There exist $x_1, \ldots, x_n \in C$ generating C as an A-module. We can therefore find elements $d_{ij} \in A$ such that $bx_j = \sum_{i=1}^{n} d_{ij}x_i$ holds for all j. Taking $a_{ij} = b\delta_{ij} - d_{ij}$, the x_j and a_{ij} now satisfy the assumptions of the lemma above. Letting $X = (a_{ij})$, we have

$$\det(X) = b^n - \sum_{i=1}^{n} d_{ii}b^{n-1} + \cdots,$$

and $\det(X)x = 0$ for every $x \in C$. Since $1 \in C$, we have $\det(X)1 = \det(X) = 0$, showing that 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 $\{c_i d_j\}$:

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

□

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.