Integral Ring Extensions

Suppose $A \subset B$ is an extension of commutative rings. We say that an element $b \in B$ is **integral** over A if $b^n + a_1 b^{n-1} + \cdots + a_n = 0$, for some $a_j \in A$. We say that the ring B is **integral** over A if every element of B is integral over A.

For any $b \in B$, there is the subring $A[b] \subset B$, the smallest subring of B containing A and b.

Proposition 1 *The following conditions are equivalent:*

(i) $b \in B$ *is integral over* A.
(ii) *The subring* $A[b] \subset B$ *is finitely generated as an* A*-module.*
(iii) $A[b] \subset C \subset B$*, where* C *is some subring of* B *which is finitely generated as an* A*-module.*
(iv) $A[b] \subset M \subset B$*, where* M *is some* $A[b]$*-submodule of* B *which is finitely generated as an* A*-module.*
(v) *There exists an* $A[b]$*-module* M *which is finitely generated as an* A*-module and faithful as an* $A[b]$*-module. (Faithful means if* $c \in A[b]$ *and* $cm = 0$ *for all* $m \in M$*, then* $c = 0$*.)*

Proof (i) $\Leftrightarrow$ (ii): If b is a root of a monic, degree n polynomial over A, then $A[b]$ is spanned as an A-module by $\{1, b, b^2, \ldots, b^{n-1}\}$. Conversely, if $A[b]$ is spanned as an A-module by finitely many elements, then at most finitely many powers of b, say $\{1, b, b^2, \ldots, b^{n-1}\}$, appear in formulas for these elements. It follows that these powers of b span $A[b]$ as an A-module, hence b^n is an A-linear combination of lower powers of b.

(ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv): Completely trivial.

(iv) $\Rightarrow$ (v): The module M of (iv) is faithful as an $A[b]$-module since $1 \in M$, where $1 \in A$ is the multiplicative identity.

(v) $\Rightarrow$ (i): Say M is spanned by $\{m_1, \ldots, m_n\}$ over A. Each element $bm_i = \sum_{j=1}^{n} a_{ij} m_j$, for suitable $a_{ij} \in A$. Let $T = (a_{ij})$, an $n \times n$ matrix over A. Then $(bI - T)$ is an $n \times n$ matrix with entries in B, and the column vector $(m_1, \ldots, m_n)^T$ is in the kernel of $(bI - T)$, regarded as a transformation $M^n \to M^n$. If $(bI - T)^*$ is the adjugate matrix of $(bI - T)$, then $(bI - T)^*(bI - T) = \det(bI - T)I$, a scalar diagonal matrix over $A[b]$. It follows that $\det(bI - T)m_i = 0$ for all i, hence $\det(bI - T) = 0$, since M is a faithful $A[b]$-module. But $\det(bI - T) = 0$ is a monic, degree n polynomial equation for b over A. ∎

(Remark: If A is Noetherian then another condition equivalent to (i) through (v) above is that $A[b] \subset M$, for some finitely generated A-module M. Because then $A[b]$ is finitely generated as A-module, by the Noetherian assumption.)

Corollary 1 *If a ring* $B \supset A$ *is finitely generated as an* A*-module, then every element of* B *is integral over* A. □

Corollary 2 *The set of all elements of* B *which are integral over* A *forms a subring of* B.

Proof If $b, c \in B$ are integral over A, then the ring $A[b, c]$ is finitely generated as A-module. Specifically, a spanning set for $A[b, c]$ over A will exist of the form $\{b^i c^j\}$, $0 \le i < n$, $0 \le j < m$. It follows from Corollary 1 that all elements of $A[b, c]$, for example $b + c$ and bc, are integral over A. ∎

The subring $\hat{A} \subset B$ consisting of all elements of B which are integral over A is called the integral closure of A in B. We say that A is integrally closed in B if $\hat{A} = A$.

Corollary 3 *If* $A \subset B \subset C$ *are three rings with* B *integral over* A *and* C *integral over* B*, then* C *is integral over* A.

Proof An element $c \in C$ is integral over $A[b_1, \ldots, b_n]$, where the b_j are coefficients of some monic polynomial over B with root c. Each b_i is integral over A, so $A[b_1, \ldots, b_n, c]$ is finitely generated as an A-module. A specific set of A-module generators will have the form of a set of monomials in the elements b_i and c, with bounded exponents. ∎

Corollary 4 *The integral closure of A in B is integrally closed in B, that is, $\hat{\hat{A}} = \hat{A} \subset B$.*

Proof Apply Corollary 3 to $A \subset \hat{A} \subset \hat{\hat{A}}$. ∎

Suppose the ring A is an integral domain, with field of fractions K. We say that A is an integrally closed domain if A is integrally closed in K.

Proposition 2 *A UFD is integrally closed.*

Proof This is the same as the familiar result that the only rational roots of monic polynomials with integer coefficients are themselves integers. Namely if $r = p/q$ is a fraction in lowest terms in K with $r^n + a_1 r^{n-1} + \ldots + a_n = 0$ and $a_j \in A$, multiply by q^n to see that q divides p^n in A. But this contradicts p, q relatively prime unless q is a unit, that is, $r \in A$. ∎

Next consider an algebraic field extension $K \subset L$, where K is the field of fractions of some integral domain A. Every element of L is the root of some polynomial with coefficients in A, since one can take the minimal monic polynomial for x over K and clear denominators.

Proposition 3 *Suppose $x \in L$ is the root of a polynomial over A with leading coefficient $a \in A$. Then x is integral over $A[1/a]$ and ax is integral over A.*

Proof Divide the relation $ax^n + bx^{n-1} + \cdots + c = 0$ by a to see the first statement. Multiply this relation by a^{n-1} to see the second statement. ∎

In the situation above, $A \subset K \subset L$, denote by B the integral closure of A in L. From the last Proposition, it follows that L is the field of fractions of B. It also follows that if $|L : K|$ is finite and if $\{x_1, \ldots, x_n\}$ is a vector space basis of L over K, then for some $a \in A$ the elements $\{ax_1, \ldots, ax_n\}$ belong to B and, of course, still form a vector space basis of L over K.

In general, an element $x \in L$ might satisfy some monic polynomial over A and yet its minimum monic polynomial over K might not have coefficients in A. For example, if A is not integrally closed in its own field of fractions K and if $L = K$, this certainly occurs. An example of a domain which is not integrally closed is $\mathbb{Z}[\sqrt{5}]$. The element $(1 + \sqrt{5})/2$ satisfies the monic equation $x^2 - x - 1 = 0$.

Proposition 4 *Suppose A is an integrally closed domain with field of fractions K. If $K \subset L$ is an algebraic extension and if $x \in L$ is integral over A, then, in fact, the minimum polynomial for x over K has all its coefficients in A.*

Proof Say $g(T)$ is a monic polynomial over A which has x as a root. Then the minimum polynomial, $f(T)$, for x over K divides $g(T)$ in $K[T]$, hence all the conjugates x_j of x in some larger field are integral over A. But $f(T) = \prod_j (T - x_j)$ has coefficients which are sums of products of the x_j, hence these coefficients are also integral over A. Since these coefficients belong to K, and A is integrally closed in K, the coefficients of $f(T)$ all belong to A, as claimed. ∎

We now want to continue studying the situation of an integrally closed integral domain A, with field of fractions K, and the integral closure $B \supset A$ inside some finite algebraic extension $L \supset K$. Very important special cases are when $A = \mathbb{Z}$ and $K = \mathbb{Q}$, in which case B is the ring of algebraic integers in some finite extension of $\mathbb{Q}$, and when $A = k[z]$ and $K = k(z)$, the field of rational functions in one variable over some field k, e.g. $k = \mathbb{C}$. In this case, L is a "function field in one variable," that is, a finitely generated extension of k of transcendence degree one, and B turns out to be the affine coordinate ring of a *nonsingular* affine algebraic curve, in particular, a Riemann surface.

Proposition 5 *If $K \subset L$ is a finite separable extension and if A is Noetherian, then B is Noetherian. If A is a PID, (e.g. $A = \mathbb{Z}$ or $k[z]$), then B is a free module of rank n over A, where $n = |L : K|$.*

Proof This takes some steps. We exploit the trace, $\mathrm{Tr} : L \to K$. Separability implies $\mathrm{Tr} \neq 0$. Of course, in characteristic 0, $\mathrm{Tr}(1) = n = |L : K|$, so separability is kind of behind the scenes in the argument that $\mathrm{Tr} \neq 0$. In both characteristic 0 and characteristic p, separability is used to make sense of the trace as a K-valued function which is a sum of field homomorphisms. After that, linear independence of characters is needed in characteristic p to conclude $\mathrm{Tr} \neq 0$. The formula $\mathrm{Tr}(1) = n$ remains correct, but if $p \mid n$ then $n = 0$.

Consider the symmetric K-bilinear pairing, $Tr : L \times L \to K$, defined by $\mathrm{Tr}(x, y) = \mathrm{Tr}(xy)$. For each $y \neq 0 \in L$, there exists elements $x \in L$ with $\mathrm{Tr}(x, y) \neq 0$, since any element of L can be written xy for suitable x, and $\mathrm{Tr} \neq 0$ on L. Thus, the pairing Tr defines a K-linear *injection* $L \to L^* = \mathrm{Hom}_K(L, K)$ which assigns to $y \in L$ the K-linear functional $t_y(x) = \mathrm{Tr}(x, y) = \mathrm{Tr}(xy) \in K$. Since L is finite dimensional over K, the trace form thus defines an isomorphism $L \cong L^*$.

Choose a vector space basis $\{b_1, \ldots, b_n\}$ of L over K, with all $b_j \in B$. Let $\{b_1^*, \ldots, b_n^*\} \subset L$ denote the dual basis with respect to the trace form identification $L \cong L^*$. Specifically, the $\{b_j^*\}$ are characterized by the relations $\mathrm{Tr}(b_i b_j^*) = \delta_{ij}$.

I claim that $B \subset \oplus_j A b_j^*$, the free rank n module over A spanned by the $\{b_j^*\}$ inside L. In particular, if A is Noetherian, then B is Noetherian as an A-module, so it is certainly Noetherian as a ring. (Ideals in B are also A-submodules of B.) If, further, A is a PID, then it follows that B is a *free* A-module of rank no greater than n. The rank must be exactly n, since B contains vector space bases of L over K, such as the basis $b_1, \ldots, b_n$ we started with, and these n elements are certainly linear independent over A.

How do we prove $B \subset \oplus_j A b_j^*$? The key is that if $b' \in B \subset L$, then $\mathrm{Tr}(b') \in A \subset K$, since $\mathrm{Tr}(b') \in K$ is a sum of conjugates of b', hence integral over A. But we are assuming A is integrally closed in K. So, now, if $b \in B$, write $b = \sum_{i=1}^n c_i b_i^* \in L$, with $c_i \in K$. I will show all $c_i \in A$. Since $b_j \in B$, we have $b b_j \in B$, hence, by the key remark $\mathrm{Tr}(b b_j) \in A$. But $\mathrm{Tr}(b b_j) = \mathrm{Tr}(\sum_{i=1}^n c_i b_i^* b_j) = c_j$, since Tr is K-linear and $\mathrm{Tr}(b_i^* b_j) = \delta_{ij}$. ∎

When $A = \mathbb{Z}$ and $K = \mathbb{Q}$, there is another important point of view which shows that the integral closure $B \supset Z$ in a finite algebraic extension $L \supset Q$ is a free Z-module. If $n = |L : Q|$, let $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n) : L \to \mathbb{C}^n$ be the embedding in affine space over the complex numbers defined by the n distinct field embeddings $\sigma_j : L \to \mathbb{C}$. So, if $x \in L$, the coordinates of $\sigma(x)$ are the conjugates of x.

Proposition 6 *In any bounded region in $\mathbb{C}^n$, with respect to the usual norm, there exist only finitely many vectors $x = \sigma(x)$, with $x \in B \subset L$.*

Proof If all the conjugates x_j of x satisfy $\|x_j\| < r$, then the coefficients of the minimum polynomial $f(T) = \prod_j (T - x_j)$ of x are bounded by some simple function of r. Since these coefficients are ordinary integers, there are only finitely many polynomials $f(T)$ whose coefficients satisfy these bounds.

One now proceeds to show that $\sigma(B) \subset \mathbb{C}^n$ is a discrete lattice, an additive subgroup isomorphic to $\mathbb{Z}^n$, with no accumulation points. Begin by choosing $0 \neq b_1 \in B$ with $\|\sigma(b_1)\|$ as small as possible. On the real line in $\mathbb{C}^n$ containing $\sigma(b_1)$, the points of $\sigma(B)$ consist only of integral multiples of $\sigma(b_1)$, an additive copy of $\mathbb{Z}$. Then choose $b_2 \in B$ so that $\sigma(b_2)$ is as close as possible to this first line but not on this first line. Argue that the points in $\sigma(B)$ which belong to the real plane spanned by $\sigma(b_1)$ and $\sigma(b_2)$, consist exactly of the $\mathbb{Z}$-linear combinations of $\sigma(b_1)$ and $\sigma(b_2)$, and form a discrete lattice isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$. Continue until the maximal rank, namely n, of subgroups of $\sigma(B)$ is reached. Details are left to the reader, or, as Descartes wrote when he was too lazy to write out detailed proofs of his assertions, "I would not wish to deny the reader the pleasure of providing the remainder of the proof." ∎

Proposition 7 *Suppose A is an integrally closed domain, B the integral closure of A in some finite separable extension of the fraction field of A. Suppose $Q \subset B$ is a non-zero prime ideal of B, lying over $P \subset A$. If $0 \neq x \in Q$, then $0 \neq \mathrm{N}(x) \in P$, where N is the field norm. In particular, P is non-zero.*

Proof $\mathrm{N}(x)$ is a power of the constant coefficient of the minimal monic polynomial $0 = f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ for x over A. In B, x divides this constant coefficient, hence the coefficient belongs to $Q \cap A = P$. ∎