CHAPTER XV

INTEGRAL EXTENSIONS

1. Integral Dependence

Let A and B be commutative rings with A a subring of B. An element x in B is said to be *integral* over A if it satisfies a *monic* polynomial $f(X) \in A[X]$. If A is a field, this is the same thing as saying that x is algebraic over A. However, in general it is not at all the same. For example, if A is a domain with field of fractions K and L is an algebraic extension of K, then each $x \in L$ it satifies an algebraic equation over K and by multiplying by a common denominator, it is not hard to see that it satifies an algebraic equation with coefficients in A. However, generally it will not satisfy such an equation with leading coefficient 1.

Example. Let $A = \mathbf{Z}$ considered as a subring of $B = \mathbf{Q}[\sqrt{5}]$. Note that every element of B is algebraic over $\mathbf{Q}$ so it satisfies an algebraic equation over $\mathbf{Z}$. When is an element $\xi = a + b\sqrt{5}$ with $a, b \in \mathbf{Q}$ integral over $\mathbf{Z}$? To determine this, note that ξ is certainly a root of $f(X) = (X - \xi)(X - \overline{\xi}) = X^2 - 2aX + (a^2 - 5b^2)$, where $\overline{\xi} = a - b\sqrt{5}$. Thus ξ will be integral over $\mathbf{Z}$ if $2a, a^2 - 5b^2 \in \mathbf{Z}$. This will be the case if $a, b \in \mathbf{Z}$, but it is also true for example for the element $(1 + \sqrt{5})/2$.

It is also not too hard to see that if ξ is integral over $\mathbf{Z}$, then $2a, a^2 - 5b^2 \in \mathbf{Z}$.

PROPOSITION. *Let $A \subseteq B$ be commutative rings. The following are equivalent.*
(i) $b \in B$ is integral over A.
(ii) $A[b]$ is a finitely generated A-submodule of B.
(iii) $A[b]$ is contained in some subring C of B which is finitely generated as an A-submodule.
(iv) There exits a faithful $A[b]$-module M which is finitely generated as an A-module.

PROOF. (i) $\Rightarrow$ (ii). Assume $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ with $a_i \in A$. Then b^n (or any higher power) can be expressed as a linear combination over A of the powers $1, b, \ldots, b^{n-1}$. Hence any element of $A[b]$ may be reexpressed as a polynomial in b which involves only the powers $1, b, \ldots, b^{n-1}$.

(ii) $\Rightarrow$ (iii) is clear since $A[b]$ is a subring of B.

(iii) $\Rightarrow$ (iv). Let $M =$ the subring C. Since A is a subring of C, it is clear that C is faithful as an A-module. (Any $x \in A$ which kills C also kills $1 \in A$.)

(iv) $\Rightarrow$ (i). Define $\rho_b \in \mathrm{Hom}_A(M, M)$ by $\rho_b(x) = bx$. Let $\{x_1, \ldots, x_n\}$ be a set of generators for M as an A-module. Then we have

$$\rho_b(x_i) = bx_i = \sum_j p_{ji} x_j, \qquad j = 1, \ldots, n.$$

By the Hamilton-Cayley theorem, ρ_b satisfies the characteristic polynomial $f(X) \in A[X]$ of the matrix $P = (p_{ij})$. That is, $f(\rho_b) = 0$ in the ring $\mathrm{Hom}_A(M, M)$. However, $\rho_{f(b)} = f(\rho_b)$ and since M is faithful as an $A[b]$-module, $f(b) = 0$. Since a characteristic polynomial is always monic, we are done.

Let A be a subring of B where A and B are both commutative rings. We say that B is *integral* over A if every element of B is integral over A. (More generally, if $\phi : A \to B$ is a homomorphism of commutative rings, we say B is integral over A if it is integral over $\phi(A)$.)

COROLLARY. *Let $A \subseteq B$ be commutative rings. If $b_1, \ldots, b_n \in B$ are integral over A, then $A[b_1, \ldots, b_n]$ is integral over A.*

PROOF. We prove the corollary for $n = 2$; the general case is similar. Let $b_1, b_2 \in B$ be integral over A. Then $A[b_1]$ is a finitely generated A-module. b_2 is also integral over $A[b_1]$ since it is even integral over A, so $A[b_2][b_1] = A[b_1, b_2]$ is finitely generated as an $A[b_1]$-module. It follows easily that $A[b_1, b_2]$ is finitely generated as an A-module. (Why?) If $x \in A[b_1, b_2]$ then $A[x] \subseteq A[b_1, b_2]$ which is a finitely generated A-module. It follows from part (iii) of the Proposition that x is integral over A.

COROLLARY. *Let $A \subseteq B$ be commutative rings. The set C of all elements $b \in B$ which are integral over A is a subring of B.*

PROOF. Clear.

The subring of B of all elements integral over A is called the *integral closure* of A in B.

Corollary. *If $A \subseteq B \subseteq C$ are commutative rings, and B is integral over A and C is integral over B, then C is integral over A. Thus integrality is transitive.*

PROOF. Let $c \in C$ satisfy the monic polynomial equation

$$c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0 \qquad \text{with } b_i \in B.$$

Then c is integral over $A[b_1, \ldots, b_n]$. Hence, $A[b_1, \ldots, b_n, c]$ is finitely generated as an $A[b_1, \ldots, b_n]$-module. However, $A[b_1, \ldots, b_n]$ is a finitely generated A-module since $b_1, \ldots, b_n$ are integral over A, so $A[b_1, \ldots, b_n, c]$ is a finitely generated A-module. It follows from (iii) that c is integral over A.

Let $A \subseteq B$ be commutative rings, and let $\overline{A}$ be the integral closure of A in B. It follows from the above corollary that the integral closure of $\overline{A}$ in B is just $\overline{A}$ again.

Let A be a *domain*, and let K be its field of fractions. We say that A is *integrally closed* if the integral closure of A in K is just A.

THEOREM. *Every unique factorization domain A is integrally closed.*

PROOF. Exercise. Hint: Assume a/b with $a, b \in A, b \neq 0$ satisfies a monic polynomial with coefficients in A, and show b cannot have any irreducible factors.

Examples. $\mathbf{Z}$, any PID, and $k[X_1, \ldots, X_n]$ where k is a field.

PROPOSITION. *Let $A \subseteq B$ be domains with B is integral over A. Then A is a field if and only if B is a field.*

PROOF. Suppose A is a field. $x \in B$ is algebraic over A so $A[x]$ is a field. It follows that if $x \neq 0$ then x is invertible.

Conversely, suppose B is a field. Let $x \neq 0 \in A$. $1/x \in B$ is integral over A so we have

$$(1/x)^n + a^1(1/x)^{n-1} + \cdots + a_n = 0 \qquad \text{where } a_i \in A.$$

Multiply through by x^{n-1} to obtain

$$1/x = -(a_1 + \cdots + a_n x^{n-1}) \in A.$$

It follows that A is a field.

Note that it follows that if A is a domain then the field of fractions of A cannot be integral over A without being A.

PROPOSITION. *Let $A \subseteq B$ be commutative rings with B integral over A. If $\mathfrak{b}$ is an ideal of B, then $B/\mathfrak{b}$ is integral over $A/A \cap \mathfrak{b}$.*

PROOF. Note first that $A/A \cap \mathfrak{b}$ may be viewed naturally as a subring of $B/\mathfrak{b}$ since $A \cap \mathfrak{b}$ is the kernel of $A \to B/\mathfrak{b}$. Clearly any monic polynomial equation in B with coefficents in A may be read modulo $\mathfrak{b}$ as a polynomial with coefficients in $A \cap \mathfrak{b}$.

COROLLARY. *Let $A \subseteq B$ be commutative rings with B integral over A. Let $\mathfrak{P}$ be a prime ideal in B. Then $\mathfrak{P}$ is maximal if and only if $A \cap \mathfrak{P}$ is maximal.*

PROOF. Consider the integral ring extension $A/A \cap \mathfrak{P} \subseteq B/\mathfrak{P}$. The former is a field if and only if the latter is a field.

PROPOSITION. *Let $A \subseteq B$ be commutative rings, and let $\overline{A}$ be the integral closure of A in B. Let S be a multiplicative subset of A. Then $S^{-1}\overline{A}$ is the integral closure of $S^{-1}A$ in $S^{-1}B$. In particular, if B is integral over A, then $S^{-1}B$ is integral over $S^{-1}A$.*

PROOF. Let $b/s \in S^{-1}\overline{A}$ where $b \in \overline{A}$ and $s \in S$. Then b satisfies some polynomial equation

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0 \text{ where } a_i \in A.$$

Divide through by s^n in $S^{-1}B$ to get

$$(b/s)^n + (a_{n-1}/s)(b/s)^{n-1} + \cdots + a_n/s^n = 0.$$

This is a monic polynomial equation with coefficients in $S^{-1}A$.

Conversely, suppose $b/s \in S^{-1}B$ is integral over $S^{-1}A$, and

$$(b/s)^n + (a_{n-1}/s_{n-1})(b/s)^{n-1} + \cdots + a_n/s_n = 0$$

where $a_i \in A, s_i \in S$. Let $t = s_1 s_2 \dots s_n$ and multiply the above equation by $(st)^n$ to get

$$(bt)^n + c_{n-1}(bt)^{n-1} + \cdots + c_n = 0$$

for suitable $c_i \in A$. (What is c_i?) It follows that bt is integral over A, so $b/s = bt/ts \in S^{-1}\overline{A}$.

COROLLARY. *Let $A \subseteq B$ be commutative rings with B integral over A. Suppose $\mathfrak{P} \subseteq \mathfrak{P}'$ are prime ideals of B. Then*

$$\mathfrak{P} \cap A = \mathfrak{P}' \cap A \qquad \Leftrightarrow \qquad \mathfrak{P} = \mathfrak{P}'.$$

PROOF. Suppose $\mathfrak{p} = \mathfrak{P} \cap A = \mathfrak{P}' \cap A$. Let $S = A - \mathfrak{p}$. Note that $S^{-1}\mathfrak{P} \subseteq S^{-1}\mathfrak{P}'$. Also,

$$S^{-1}\mathfrak{P} \cap S^{-1}A = S^{-1}(\mathfrak{P} \cap A) = S^{-1}\mathfrak{p} = S^{-1}(\mathfrak{P}' \cap A) = S^{-1}\mathfrak{P}' \cap S^{-1}A.$$

However, $S^{-1}\mathfrak{p}$ is the unique maximal ideal of $S^{-1}A$. Since $S^{-1}B$ is integral over $S^{-1}A$, it follows that $S^{-1}\mathfrak{P}$ and $S^{-1}\mathfrak{P}'$ are maximal ideals of $S^{-1}B$. Hence, $S^{-1}\mathfrak{P} = S^{-1}\mathfrak{P}'$. Let $x \in \mathfrak{P}'$ so $x/1 = y/s$ where $y \in \mathfrak{P}$ and $s \in S$. It follows that $\exists u \in S$ such that $ux \in \mathfrak{P}$. However, $u \in A - A \cap \mathfrak{P}$ so $u \notin \mathfrak{P}$. Since $\mathfrak{P}$ is prime, it follows that $x \in \mathfrak{P}$. Hence, $\mathfrak{P} = \mathfrak{P}'$.

The corollary does not preclude the possibility that $A \cap \mathfrak{P} = A \cap \mathfrak{P}'$ with $\mathfrak{P} \neq \mathfrak{P}'$ if we *drop* the assumption $\mathfrak{P} \subseteq \mathfrak{P}'$. In fact, that is the normal state of affairs for an integral extension.

Example. Let $A = \mathbf{Z}$ and let $B = \mathbf{Z}[i]$ —the ring of Gaussian integers. The ideals $A(2+i)$ and $A(2-i)$ are not the same, they are both prime, and they both intersect $\mathbf{Z}$ in the ideal $5\mathbf{Z}$. (Proofs?)

THEOREM. *Let $A \subseteq B$ be commutative rings with B integral over A. Suppose $\mathfrak{p}$ is a prime ideal in A. Then there is a prime ideal $\mathfrak{P}$ in B such that $\mathfrak{P} \cap A = \mathfrak{p}$.*

PROOF. Let $S = A - \mathfrak{p}$. Then $S^{-1}B$ is integral over $S^{-1}A = A_{\mathfrak{p}}$. Let $\mathfrak{P}'$ be any maximal ideal of $S^{-1}B$, and consider $\mathfrak{P}' \cap A_{\mathfrak{p}}$. The latter ideal is maximal so it is the unique maximal ideal $S^{-1}\mathfrak{p}$ of $A_{\mathfrak{p}}$. Also, it is not hard to see (as earlier) that the pull back of $S^{-1}\mathfrak{p}$ to A is just $\mathfrak{p}$. However, we have a commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ S^{-1}A & \longrightarrow & S^{-1}B \end{array}$$

so the pull back $\mathfrak{P}$ of $\mathfrak{P}'$ to B intersects A in $\mathfrak{p}$.

The theorem may be interpreted as saying that the induced map $\operatorname{spec}(B) \to \operatorname{spec}(A)$ given by $\mathfrak{P} \mapsto A \cap \mathfrak{P}$ is onto provided B is integral over A. Some of the other results above may also be rephrased in suggestive ways in terms of the spectra. For example, $\operatorname{spec}(B) \to \operatorname{spec}(A)$ carries $\max(B)$ onto $\max(A)$.

PROPOSITION. *Let A be a domain. The following are equivalent.*
(i) A is integrally closed.
(ii) $A_{\mathfrak{p}}$ is integrally closed for each $\mathfrak{p} \in \operatorname{spec}(A)$.
(iii) $A_{\mathfrak{m}}$ is integrally closed for each $\mathfrak{m} \in \max(A)$.

PROOF. Let K be the field of fractions of A. Note that if $\mathfrak{p}$ is a prime ideal, then since A is a domain, $A_{\mathfrak{p}}$ may be identified with a subring of K, and K is also the field of fractions of $A_{\mathfrak{p}}$. Let B be the integral closure of A in K, and let $i : A \to B$ be the inclusion homomorphism. Then A is integrally closed if and only if i is an epimorphism. View everything as an A-module. Then i is an epimorphism if and only if $i_{\mathfrak{p}} : A_{\mathfrak{p}} \to B_{\mathfrak{p}}$ is an epimorphism for each $\mathfrak{p} \in \operatorname{spec}(A)$ (and similarly for maximal ideals). However, $B_{\mathfrak{p}} = S^{-1}B$ ($S = A - \mathfrak{p}$) is the integral closure of $A_{\mathfrak{p}}$ in $K_{\mathfrak{p}} = K$. Hence, $i_{\mathfrak{p}}$ is an epimorphism if and only if $A_{\mathfrak{p}}$ is integrally closed.

Exercises.

1. Show as indicated in the text that if $\xi = a + b\sqrt{5} \in \mathbf{Q}[\sqrt{5}]$ is integral over $\mathbf{Z}$, then $2a, a^2 - 5b^2 \in \mathbf{Z}$.

2. Prove that every UFD is integrally closed. Give an example of an integrally closed domain which is not a UFD.

3. Show that $A = \mathbf{Z} + \mathbf{Z}\sqrt{5}$ is not integrally closed. Hint: The field of fractions of A is $\mathbf{Q} + \mathbf{Q}\sqrt{5} = \mathbf{Q}[\sqrt{5}]$.

4. Let B be a commutative ring and let G be a finite group of ring automorphisms of B. Let A be the set of invariants of G, i.e., $A = \{x \in B \mid \alpha(x) = x, \text{all } \alpha \in G\}$.
   (a) Show that A is a subring of B.
   (b) Show that B is integral over A.