4. *Integral elements*

4.1 Definition. Let R be a commutative ring, T an R-algebra and $u \in T$. Then u is called **integral** over R if and only if there exists a monic polynomial $f \in R[x]$ with $f(u) = 0$.

4.2 Definition. A ring extension $R \subseteq T$ is called integral if every element of T is integral over R.

4.3 Theorem. Let R be a commutative ring, T an R-algebra and $u \in T$. Then the following are equivalent:

(1) u is integral over R.
(2) $R[u]$ is finitely generated as an R-module.
(3) $R[u] \subseteq A \subseteq T$ for some ring A that is finitely generated as an R-module.
(4) There exists a faithful $R[u]$-module that is finitely generated as an R module.
(5) $R[u]$ is integral over R.

Proof. $(1 \Rightarrow 2)$ $R[u]$ is generated as an R-module by the powers of u. Since u is integral over R, there exists an $n \in \mathbb{N}$ and $r_0, \dots, r_{n-1} \in R$ such that $u^n = r_{n-1}u^{n-1} + \dots + r_1 u + r_0$, and by induction, every power of u is expressible as an R-linear combination of 1, $u, \dots, u^{n-1}$.
$(2 \Rightarrow 3)$ Take $A = R[u]$.
$(3 \Rightarrow 4)$ Take A as the faithful $R[u]$ module.
$(4 \Rightarrow 5)$ Let M be a faithful $R[u]$-module, generated by $m_1, \dots, m_n$ as an R-module, and let $w \in R[u]$. Then $\varphi_w(m) = wm$ (scalar multiplication by w) is an R-module endomorphism of M, $\varphi_w \in \mathrm{End}_R(M)$. Let $C = (c_{ij})$ in $M_n(R)$ be a matrix with with $\varphi_w(m_k) = c_{1k}m_1 + c_{2k}m_2 + \dots + c_{nk}m_n$ then C represents $\varphi_w \in \mathrm{End}_R(M)$ with respect to the system of generators $m_1, \dots, m_n$.

By Cayley-Hamilton (3.5), $\chi(\varphi_w) = 0$, where $\chi(x) = \det(xI_n - C)$ is the characteristic polynomial of C. $0 = \chi(\varphi_w) = \varphi_{\chi(w)}$, means that scalar multiplication by $\chi(w)$ is the 0-mapping on M, in other words, $\chi(w) \in \mathrm{Ann}_{R[w]}(M)$. Since M is a faithful $R[u]$ module, $\chi(w) = 0$ follows. $\square$

4.4 Definition. Let R be a commutative ring, I an ideal of R, T an R-algebra and $u \in T$. Then u is called **integral** over I if and only if there exists a monic polynomial $f \in R[x]$ whose coefficients (apart from the leading coefficient) are all in I with $f(u) = 0$.

4.5 Theorem. Let R be a commutative ring, I an ideal of R, T an R-algebra and $u \in T$. Then the following are equivalent:

(1) u is integral over I.

(2) $R[u]$ is finitely generated as an R-module and $u \in \sqrt{IR[u]}$.

(3) $R[u] \subseteq A \subseteq T$ for some ring A that is finitely generated as an R-module and $u \in \sqrt{IA}$.

(4) There exists a faithful $R[u]$-module M that is finitely generated as an R module and for some $k \in \mathbb{N}$, $u^k M \subseteq IM$.

Proof. $(1 \Rightarrow 2)$ There exists an $n \in \mathbb{N}$ and $r_0, \ldots, r_{n-1} \in I$ such that $u^n = r_{n-1}u^{n-1} + \ldots + r_1 u + r_0$. Therefore $u \in \sqrt{IR[u]}$ and $R[u]$ is generated as an R-module by $1, u, \ldots, u^{n-1}$.

$(2 \Rightarrow 3)$ Take $A = R[u]$.

$(3 \Rightarrow 4)$ Take A as the faithful $R[u]$ module.

$(4 \Rightarrow 1)$ Let M be a faithful $R[u]$-module, generated by $m_1, \ldots, m_n$ as an R-module. Let $w = u^k$ such that $wM \subseteq IM$. Then $\varphi_w(m) = wm$ (scalar multiplication by w) is an R-module endomorphism of M. Let $C = (c_{ij})$ in $M_n(R)$ be a matrix with with $\varphi_w(m_k) = c_{1k}m_1 + c_{2k}m_2 + \ldots + c_{nk}m_n$ and $c_{ij} \in I$ for all i, j. Then C represents $\varphi_w \in \operatorname{End}_R(M)$ with respect to the system of generators $m_1, \ldots, m_n$.

By Cayley-Hamilton (3.5), $\chi(\varphi_w) = 0$, where $\chi = \det(xI_n - C)$ is the characteristic polynomial of C, whose coefficients (apart from the leading coefficient) are all in I. $0 = \chi(\varphi_w) = \varphi_{\chi(w)}$, means that scalar multiplication by $\chi(w)$ is the 0-mapping on M, in other words, $\chi(w) \in \operatorname{Ann}_{R[w]}(M)$. Since M is a faithful $R[u]$ module, $\chi(w) = 0$ follows. As $w = u^k$ we have also found a monic polynomial satisfied by u whose coefficients (except for the leading coefficient) are in I. □

If $R \subseteq T$ are commutative rings and T is finitely generated as an R-module, then T is also finitely generated over R as a ring, but the converse does not hold in general, viz. the polynomial ring $R[x]$. Integrality provides the answer to the question when the converse does hold. Note the analogy to field extensions, where finitely generated by algebraic elements equals finite-dimensional.

4.6 Proposition. Let R be a commutative ring and T a commutative R-algebra. Then the following are equivalent:

(1) T is finitely generated as an R-module.

(2) T is finitely generated over R a a ring and integral over R.

(3) T is finitely generated by integral elements over R as a ring.

Proof. $(1 \Rightarrow 2)$ by 4.3. $(2 \Rightarrow 3)$ holds a fortiori. To see $(3 \Rightarrow 1)$, assume T is generated as a ring over R by $t_1, \dots, t_m$. Then T is generated as an R-module by monomials $t_1^{k_1} t_2^{k_2} \dots t_m^{k_m}$. If each t_i is integral over R then for each i there exists an exponent n_i such that every power of t_i is expressible as an R-linear combination of $1, t, \dots, t^{n_i}$, and therefore T is generated as an R-module by monomials $t_1^{k_1} t_2^{k_2} \dots t_m^{k_m}$ with $0 \le k_i \le n_i$. $\square$

4.7 Corollary. Let R be a commutative ring, T an R-algebra and $a, b \in T$ with $ab = ba$. If both $R[a]$ and $R[b]$ are finitely generated as R-modules then so is $R[a, b]$. In particular, if a and b are commuting integral elements over R, then $a - b$ and ab are integral over R, too.

4.8 Corollary. Let $R \subseteq T$ be commutative rings. Then the set of all elements of T integral over R form a ring.

Commutativity is essential here. If the integral elements a and b do not commute, neither their sum nor their product needs to be integral over R.

4.9 Definition. Let $R \subseteq T$ be commutative rings. The ring

$$R' = \{t \in T \mid t \text{ is integral over } R\}$$

is called **the integral closure of R in T**. R is called **integrally closed in T** if $R' = R$. “The” integral closure of a domain R is the integral closure in its quotient field. R is called **integrally closed** if R is integrally closed in its quotient field.

4.10 Proposition. Let R be a commutative ring, $R \subseteq S$ an integral ring extension and u integral over S. Then u is integral over R.

Proof. Suppose $u^n + a_{n-1}u^{n-1} + \dots + a_0 = 0$ with $a_0, \dots, a_{n-1} \in S$. Then $R[a_0, \dots, a_{n-1}]$ is finitely generated integral over R. Let $g_1, \dots, g_m$ be generators of $R[a_0, \dots, a_{n-1}]$ as an R-module. Then $R[a_0, \dots, a_{n-1}, u]$ is generated as an R-module by the elements $g_i u^k$ for $1 \le i \le m$ and $1 \le k \le n - 1$. $\square$

4.11 Corollary (Transitivity of integral extensions). Let $R \subseteq S \subseteq T$ be commutative rings. If T is integral over S and S is integral over T then T is integral over R.

4.12 Corollary (Integral closure is integrally closed). Let $R \subseteq T$ be commutative rings and R' the integral closure of R in T. Then R' is integrally closed in T.

4.13 Theorem. Let R be an integrally closed domain with quotient field K, L a field containing K, and $u \in L$ algebraic over K. Then u is integral over R iff the minimal polynomial of u over K is in $R[x]$.

Proof. Assume u integral over R. Let f be the minimal polynomial of u over K and $\bar{L}$ its splitting field over L. Over $\bar{L}$, $f(x) = (x-u)(x-u_1)\dots(x-u_m)$. Since u and the u_i are roots of the same irreducible polynomial on $K[x]$ there exists for each i an isomorphism $\varphi\colon K[u] \to K[u_i]$ with $\varphi(u) = u_i$ and $\varphi(k) = k$ for all $k \in K$. If u is a root of some monic $g \in R[x]$, then $0 = \varphi(0) = \varphi(g(u)) = g(u_i)$ shows u_i to be a root of the same monic $g \in R[x]$. All u_i are integral over R. Therefore the coefficients of f (as sums of products of the roots) are also integral over R. At the same time, the coefficients are in K, therefore, R being integrally closed, the coefficients of f are in R. $\square$

4.14 Lemma. Let $K \subseteq F$ be an algebraic extension of fields and $R \subseteq K$ a domain integrally closed in K.

(i) $u \in F$ is integral over R if and only if its minimal polynomial over K is in $R[x]$.

(ii) Let P be a prime ideal of R. $u \in F$ is integral over P if all coefficients of its minimal polynomial over K (apart from the leading coefficient) are in P.

Proof. Ad (i). Let $f \in K[x]$ be the minimal polynomial of u over K and $g \in R[x]$ with $g(u) = 0$. Then f divides g in $K[x]$. Let $u_1, \dots, u_n$ be the roots of f in its splitting field $\bar{K}$ over F, then all u_i are also roots of g and therefore integral over R. Let R' be the integral closure of R in $\bar{K}$. The coefficients of f (as elementary symmetric polynomials in the u_i are in R'. As they are also in K, they are in $R' \cap K = R$.

Ad (ii). Let f, g as before, and all coefficients (except leading coefficient) of g in P. The roots of f are integral over P, and therefore in $\sqrt{PR'}$. The coefficients of f are, as elementary symmetric polynomials in the u_i, in the subring generated by the u_i in $\bar{K}$, which is contained in $\sqrt{PR'}$. As they are also in K, the coefficients of f are in $K \cap \sqrt{PR'} = \sqrt{P} = P$.

$\square$

4.15 Corollary. Let R be a domain with quotient field K and $u \in L$ algebraic over K. Then u is integral over R iff the coefficients of the minimal polynomial of u over K are integral over R.

4.16 Lemma. Let $R \subseteq T$ be commutative rings and $u \in T$ an invertible element. Then u^{-1} is integral over R if and only if $u^{-1} \in R[u]$.

Proof. An equation showing u^{-1} to be integral over R, such as

$$(u^{-1})^n = a_{n-1}(u^{-1})^{n-1} + \ldots + a_1(u^{-1}) + a_0,$$

can be multiplied by u^{n-1} to show u^{-1} to be in $R[u]$:

$$u^{-1} = a_{n-1} + \ldots + a_1 u^{n-2} + a_0 u^{n-1}.$$

Conversely, an equation showing $u^{-1} \in R[u]$, can be multiplied by an appropriate power of u^{-1} to show u^{-1} integral over R. $\square$

4.17 Proposition. Let $R \subseteq L$ be an integral extension of domains. Then R is a field if and only if L is a field.

Proof. If R is a field then L is an algebraic extension of a field and therefore a field. If L is a field and u is a non-zero element of R then u has an inverse u^{-1} in L, which by the previous lemma is in $R[u] = R$. Therefore R is a field. $\square$

4.18 Definition. Ler $R \subseteq T$ be commutative rings. We introduce names for a few properties that the ring extension $R \subseteq T$ may or may not satisfy:

Lying over. For every prime ideal $P \trianglelefteq R$ there exists a prime ideal $\tilde{P} \trianglelefteq T$ with $\tilde{P} \cap R = P$.

Going up. If $P \subseteq Q$ are prime ideals of R and $\tilde{P}$ a prime ideal of T with $\tilde{P} \cap R = P$ then there exists a prime ideal $\tilde{Q}$ of T with $\tilde{P} \subseteq \tilde{Q}$ and $\tilde{Q} \cap R = Q$.

Going down. If $P \subseteq Q$ are prime ideals of R and $\tilde{Q}$ a prime ideal of T with $\tilde{Q} \cap R = Q$ then there exists a prime ideal $\tilde{P}$ of T with $\tilde{P} \subseteq \tilde{Q}$ and $\tilde{P} \cap R = P$.

Incomparability. For any two prime ideals $\tilde{P}$ and $\tilde{Q}$ of T with $\tilde{P} \cap R = \tilde{Q} \cap R$ neither $\tilde{P} \subseteq \tilde{Q}$ nor $\tilde{Q} \subseteq \tilde{P}$ holds.

Let $R \subseteq T$ be commutative rings, P a prime ideal of R and $S = R \setminus P$. If Q is an ideal of T, then $Q \cap R \subseteq P$ if and only if $Q \cap S = \emptyset$. Since S is a multiplicative subset of T containing (0), we know there exist ideals of T not intersecting S, and among them ideals maximal with this property, which are necessarily prime. The question is now whether an ideal maximal among those not intersecting S actually intersects R in P and vice versa. It turns out that the properties "incomparability" and "going up" can be characterized in this way.

4.19 Proposition. Let $R \subseteq T$ be commutative rings. Then the following are equivalent:

(1) $R \subseteq T$ satisfies "going up".

(2) For every prime ideal P of R, if Q is an ideal of T maximal with respect to the property $Q \cap (R \setminus P) = \emptyset$ then $Q \cap R = P$.

Since ideals maximal with respect to avoiding a multiplicative set S with $0 \notin S$ are guaranteed to exist and are prime, we get:

4.20 Corollary. "Going up" implies "lying over".

4.21 Proposition. Let $R \subseteq T$ be commutative rings. Then the following are equivalent:

(1) $R \subseteq T$ satisfies "incomparability".

(2) For every prime ideal P of R, if Q is a prime ideal of T with $Q \cap R = P$ then Q is maximal with respect to the property $Q \cap (R \setminus P) = \emptyset$.

4.22 Theorem. Let $R \subseteq T$ be an integral extension of rings. Then "incomparability" and "going up" (and therefore "lying over") hold.

Proof. To show "going up", we assume P is a prime ideal of R and $\tilde{P}$ an ideal of T maximal with respect to the property $\tilde{P} \cap (R \setminus P) = \emptyset$; we must show $\tilde{P} \cap R = P$. Suppose otherwise and choose $u \in P \setminus \tilde{P}$. Then, by maximality of $\tilde{P}$, there exists an $s \in (R \setminus P) \cap (\tilde{P} + Tu)$, $s = q + tu$ with $q \in \tilde{P}$ and $t \in T$. t is integral over R, i.e.,

$$t^n + c_{n-1}t^{n-1} + \ldots + c_0 = 0$$

with coeffiecients $c_i \in R$. Multiplying by u^n, we get

$$(tu)^n + c_{n-1}u(tu)^{n-1} + \ldots + u^n c_0 = 0.$$

Since $tu + q = s$, $tu \equiv s \mod \tilde{P}$, and therefore

$$s^n + c_{n-1}us^{n-1} + \ldots + u^n c_0 \equiv 0 \pmod{\tilde{P}}.$$

The left side of this congruence is in R, so it is actually in $\tilde{P} \cap R \subseteq P$. Since $u \in P$ we get $s^n \in P$ and therefore $s \in P$, a contradiction.

To show "incomparability", we assume $\tilde{P} \cap R = P$ and must show that $\tilde{P}$ is maximal with respect to not intersecting $S = R \setminus P$. Suppose there exists $\tilde{Q}$ with $\tilde{P} \subset \tilde{Q}$ and $\tilde{Q} \cap S = \emptyset$. Choose $u \in \tilde{Q} \setminus \tilde{P}$. u is integral over R. So in particular there exists a monic polynomial f in $R[x]$ with $f(u) \in \tilde{P}$. Let $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ be of minimal degree with this property. Clearly, $\deg f = n \geq 1$. Since $u^n + a_{n-1}u^{n-1} + \ldots + a_0 \in \tilde{P} \subseteq \tilde{Q}$ and $u \in \tilde{Q}$, it follows that $a_0 \in \tilde{Q} \cap R = P$. Now $u(u^{n-1} + a_{n-1}u^{n-2} + \ldots + a_1) \in \tilde{P}$, but no factor is in $\tilde{P}$, a contradiction. □

4.23 Theorem. If $R \subseteq T$ is an integral extension of domains and R is integrally closed then "going down" holds.

Proof. Suppose $P_0 \subseteq P_1$ prime ideals of R and Q_1 a prime ideal of T with $Q_1 \cap R = P_1$. Let $S_0 = R \setminus P_0$, $S_1 = T \setminus Q_1$, and $S = S_0 S_1 = \{rs \mid r \in S_0,\ s \in S_1\}$. S is a multiplicative set containing S_0 and S_1. We will show $P_0 T \cap S =$. Once we have shown this we are done, because then there exists an ideal Q_0 of T maximal with respect to $P_0 T \subseteq Q_0$ and $Q_0 \cap S =$, which is prime, and does what we want.

So, suppose $r \in S_0$ and $s \in S_1$ with $rs \in P_0 T$. Let $f = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ be the minimal polynomial of rs over K. As rs is integral over P_0, the coefficients $a_0, \ldots, a_{n-1}$ are in P_0. Let

$$g(x) = x^n + \frac{a_{n-1}}{r}x^{n-1} + \frac{a_{n-2}}{r^2}x^{n-2} + \ldots + \frac{a_0}{r^n}$$

then $g(s) = 0$ and g must be the minimal polynomial of s over K (or else we could construct a polynomial in $K[x]$ of degree less than n satisfied by rs). Therefore $b_k = a_k / r^{n-k} \in R$ for $0 \leq k < n$. Now $r^{n-k} b_k = a_k \in P_0$ and $r \notin P_0$ implies $b_k \in P_0$ for $0 \leq k < n$ and s is therefore integral over P_0. So $s \in \sqrt{P_0 T} \subseteq Q_1$, a contradiction. $\square$

The length of a chain of ideals $I_0 \supseteq I_1 \supseteq I_2 \supseteq \ldots$ is defined as the number of proper inclusions occurring in the chain.

4.24 Definition. Let P be a prime ideal in a ring R. The **height of** P is the maximal length of a chain of prime ideals descending from P: $\mathrm{ht}(P) = n \in \mathbb{N}_0$ if n is maximal such that there exists a chain of prime ideals $P \supset P_1 \supset \ldots \supset P_n$, and $\mathrm{ht}(P) = \infty$ if there are chains of prime ideals of arbitrary length descending from P.)

4.25 Definition. The **Krull dimension** $\dim(R)$ of a ring R is the supremum of the heights of the prime ideals of R.

Note that a zero-dimensional commutative ring is either a field or else a ring with zero-divisors in which every prime ideal is maximal; and that an integral domain is one-dimensional if and only if every prime ideal other than (0) is maximal.

4.26 Theorem. Let $R \subseteq T$ be commutative rings.

(1) If "incomparability" holds and P is a prime ideal of R then for every prime ideal Q of T with $Q \cap R = P$ we have $\mathrm{ht}(Q) \leq \mathrm{ht}(P)$.

(2) If "going up" holds and P is a prime ideal of R of finite height then there exists a prime ideal Q of R with $Q \cap R = P$ and $\mathrm{ht}(Q) \geq \mathrm{ht}(P)$.

4.27 Corollary. If both "incomparability" and "going up" hold for $R \subseteq T$ (in particular, if $R \subseteq T$ is an integral extension) then for every prime ideal P of R there exists a prime ideal Q of R with $Q \cap R = P$ and $\mathrm{ht}(Q) = \mathrm{ht}(P)$.

Proof. Ad 1) Every chain of prime ideals descending from Q contracts to a chain of the same length descending from P, hence $\mathrm{ht}(P) \geq \mathrm{ht}(Q)$.
Ad 2) "Lying over" and repeated applications of "going up" allow us to construct for every prime ideal chain descending from P a chain of prime ideals in T of the same length descending from some Q with $Q \cap R = P$. □

4.28 Definition. The **co-height** of a prime ideal P of a commutative ring R is the maximal length of a chain of prime ideals ascending from P (in other words, $\text{co-ht}(P) = \dim(R/P)$.)

4.29 Theorem. Let $R \subseteq T$ be commutative rings. If "going up" and "incomparability" hold (in particular, if $R \subseteq T$ is an integral extension) then for every prime ideal P of R and prime ideal Q of T with $Q \cap R = P$ we have $\text{co-ht}(Q) = \text{co-ht}(P)$.

Proof. Easy. □

4.30 Theorem. Let S be a multiplicative subset of a domain R. If R is integrally closed then so is $S^{-1}R$.

Proof. Let K be the quotient field of R and $S^{-1}R$, $u \in K$ integral over $S^{-1}R$; to show $u \in S^{-1}R$.

$$u^n + \frac{a_{n-1}}{s_{n-1}} u^{n-1} + \ldots + \frac{a_0}{s_0} = 0 \qquad a_i \in R,\ s_i \in S$$

By multiplication with $s = s_0 \ldots s_{n-1}$ we get

$$su^n + r_{n-1}a_{n-1}u^{n-1} + \ldots + r_0 a_0 = 0 \qquad r_i,\ a_i \in R.$$

Multiplication with s^{n-1} shows su to be integral over R; therefore $su \in R$, and $u \in S^{-1}R$. □

4.31 Theorem. Let R_α, $\alpha \in A$ be a collection of integral domains all contained in a field K. If every R_α is integrally closed (in its quotient field) then so is $\bigcap_{\alpha \in A} R_\alpha$. The same holds for "integrally closed in K".

Proof. Easy. □

Since every domain R satisfies $R = \bigcap_{P\text{prime}} R_P = \bigcap_{M\text{maximal}} R_M$, we see:

4.32 Corollary. Let R be an integral domain. Then the following are equivalent:

(1) R is integrally closed.

(2) For every prime ideal P of R, R_P is integrally closed.

(3) For every maximal ideal M of R, R_M is integrally closed.

A commutative ring R is called **normal** if for every prime ideal P of R the localization R_P is an integrally closed domain. We have seen that the concepts of normal and integrally closed coincide in the case of an integral domain.

4.33 Definition. Let R be a commutative ring, T an R-algebra and $u \in T$. Then u is called **almost integral** over R if and only if there exists a finitely generated R-submodule B of T with $R[u] \subseteq B$.

Comparing the definition of "almost integral" with the preceding theorem, we see that

(i) "integral" implies "almost integral"

(ii) for Noetherian R, the notions of "integral" and "almost integral" coincide.

(For Noetherian R, every R-submodule of a finitely generated R-module is finitely generated, such that "almost integral" implies condition (1) of 4.3.)

4.34 Lemma. If R is a domain with quotient field K, then $u \in K$ is almost integral over R if and only if $R[u]$ is a fractional ideal of R, i.e., if there exists a non-zero $d \in R$ such that $dw \in R$ for every $w \in R[u]$, or equivalently, such that $du^n \in R$ for all $n \in \mathbb{N}$:

Proof. If u is almost intgral and $R[u] \subseteq B$, where $b_1, \ldots, b_m$ generate B as an R-module then there exists a non-zero common denominator d with $db_i \in R$ $(1 \leq i \leq m)$ and hence $dR[u] \subseteq dB \subseteq R$. Conversely, if there exists $d \in R$, $d \neq 0$, with $dR[u] \subseteq R$ then $R[u] \subseteq d^{-1}R$, and $d^{-1}R$ is finitely generated (even cyclic) as an R-module. □

4.35 Definition. A domain D with quotient field K is called **completely integrally closed** if every element of K that is almost integral over D lies in D.

As we have seen, for Noetherian domains the notions of "integrally closed" and "completely integrally closed" coincide.