CHAPTER V: INTEGRAL EXTENSIONS; NORMAL RINGS

§1: INTEGRAL EXTENSIONS

(5.1) Definition: Let $A \subseteq B$ be an extension of rings.

(a) B is called a finite A-algebra if B is finitely generated as an A-module.

(b) An element $b \in B$ is called integral over A if the ring extension $A \subseteq A[b]$ is finite (that is, the A-subalgebra $A[b]$ of B is finite over A).

(c) The extension $A \subseteq B$ is called an integral extension (and B is called integral over A) if every element $b \in B$ is integral over A.

(5.2) Theorem: Let $A \subseteq B$ be a ring extension and $b \in B$. The following are equivalent:

(a) b is integral over A.

(b) There is a positive integer $n \in \mathbb{N}$ and elements $a_0, \ldots, a_{n-1} \in A$ such that $b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0 = 0$.

(c) There is a finite A-algebra B_1 with $A \subseteq B_1 \subseteq B$ and $b \in B_1$.

(d) There is a faithful $A[b]$-module M which is finitely generated as A-module.

Proof: We show: (a) $\Rightarrow$ (c) $\Rightarrow$ (d) $\Rightarrow$ (b) $\Rightarrow$ (a)

(a) $\Rightarrow$ (c): Set $B_1 = A[b]$.

(c) $\Rightarrow$ (d): Set $B_1 = M$. Since $A[b] \subseteq B_1$, B_1 is an $A[b]$-module. Moreover, since $1_A = 1_B \in B_1$, $\mathrm{ann}_{A[b]}(B_1) = 0$. (Note: If $A \subseteq B$ is a ring extension we always assume that $1_A = 1_B$.)

(d) $\Rightarrow$ (b): Suppose that $M = Am_1 + \ldots + Am_n$. M is an $A[b]$-module, thus for all $1 \leq i \leq n$ there are elements $a_{ij} \in A$ such that $bm_i = \sum_{j=1}^{n} a_{ij} m_j$. Hence for all $1 \leq i \leq n$:

$$\sum_{j=1}^{n} (a_{ij} - b\delta_{ij}) m_j = 0.$$

Let $\sigma = (a_{ij} - b\delta_{ij})_{i,j}$ be the $n \times n$-matrix with entries in $A[b]$ and let σ^* be its adjoint matrix. Then $\sigma^*\sigma = \det(\sigma) \cdot I_{n\times n}$ where $I_{n \times n}$ is the $n \times n$ identity matrix.

Note that:

$$\sigma\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \text{ and therefore } \sigma^*\sigma\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \det(\sigma)\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

This shows $\det(\sigma) \in \mathrm{ann}_{A[b]}(M) = (0)$ and hence $\det(\sigma) = 0$. Evaluation of $\det(\sigma)$ yields an integral equation: $b^n + a_{n-1}b^{n-1} + \ldots + a_0 = 0$ with $a_i \in A$.

(b) $\Rightarrow$ (a): $A[b]$ is a homomorphic image of the polynomial ring $A[x]$. Thus $A[b] = \{g(b) \mid g(x) \in A[x]\}$. Let $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \in A[x]$ with $f(b) = 0$. Since $f(x) \in A[x]$ is monic for every $g(x) \in A[x]$ there are polynomials $q(x), r(x) \in A[x]$ with $r(x) = 0$ or $\deg(r(x)) < \deg(f(x)) = n$ such that $g(x) = q(x)f(x) + r(x)$. Hence $g(b) = r(b)$ and $1, b, \ldots, b^{n-1}$ is a generating system of the A-module $A[b]$.

(5.3) Corollary: (a) Let $A \subseteq B$ be a finite extension of rings. Then B is integral over A.
(b) Let $A \subseteq B \subseteq C$ be ring extensions and let $c \in C$ be integral over A. c is integral over B.

Proof: (a) For every $b \in B$ $M = B$ is an $A[b]$-module which is finite as an A-module. Since $A[b] \subseteq B$ and $1_A = 1_B$: $\mathrm{ann}_{A[b]}(M) = 0$. Apply (5.2).
(b) trivial

(5.4) Example: $\mathbb{Z} \subseteq \mathbb{Z}[i]$ is an integral extension.

(5.5) Lemma: Let $A \subseteq B \subseteq C$ be ring extensions such that B is finite over A and C is finite over B. Then C is finite over A.

Proof: Let $b_1, \ldots, b_r \in B$ with $B = Ab_1 + \ldots + Ab_r$ and $c_1, \ldots, c_s \in C$ with $C = Bc_1 + \ldots + Bc_s$. Then $C = \sum_{i,j} Ab_ic_j$.

(5.6) Lemma: Let $A \subseteq B$ be an extension of rings and consider $\overline{A} = \{b \in B \mid b \text{ integral over } A\}$. $\overline{A}$ is an intermediate ring, $A \subseteq \overline{A} \subseteq B$, which is integral over A.

Proof: Let $b, c \in \overline{A}$. We have to show that $b \pm c$ and $b.c$ are in $\overline{A}$. Consider the A-subalgebra $A[b,c] = (A[b])[c] \subseteq B$. c is integral over A, thus c is integral over $A[b]$ and $(A[b])[c]$ is a finite $A[b]$-algebra. Since $A[b]$ is a finite A-algebra, the A-algebra $A[b,c]$ is finite and $A[b,c] \subseteq \overline{A}$.

(5.7) Definition: (a) Let $A \subseteq B$ be an extension of rings. The intermediate ring $\overline{A} = \{ b \in B \mid b \text{ integral over } A \}$ is called the integral closure of A in B. If $A = \overline{A}$, then A is called integrally closed in B.

(b) Let A be a domain, $K = Q(A)$ its field of quotients. The integral closure of A in $Q(A)$ is called the integral closure of A.

(c) Let A be a domain. A is called normal if A is integrally closed in its field of quotients $Q(A)$.

(5.8) Proposition: Every factorial domain is normal.

Proof: Let A be a factorial domain, $y \in Q(A)$ integral over A and $y \neq 0$. Then there are relatively prime elements $b, c \in A$ with $y = b/c$. Let $a_0, \ldots, a_{n-1} \in A$ with $y^n + a_{n-1} y^{n-1} + \ldots + a_0 = 0$. Thus $b^n = (-c)(a_{n-1} b^{n-1} + \ldots + a_0 c^{n-1})$. If $p \in A$ is a prime element with $p \mid c$, then $p \mid b$ contradicting $\gcd(b,c) = 1$. Hence c is a unit in A and $y \in A$.

(5.9) Examples: (a) The factorial domains $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[x_1, \ldots, x_n]$ and $K[x_1, \ldots, x_n]$ are normal. (K a field and $x_1, \ldots, x_n$ variables).

(b) $\mathbb{Z}[i]$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[i]$.

Proof: Let $\overline{\mathbb{Z}}$ denote the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[i]$. Since $i \in \overline{\mathbb{Z}}$ we have that $\mathbb{Z}[i] \subseteq \overline{\mathbb{Z}}$. $\mathbb{Z}[i]$ is normal, thus $\mathbb{Z}[i] = \overline{\mathbb{Z}}$.

(5.10) <u>Proposition</u>: Let $A \subseteq B \subseteq C$ be extensions of rings. C is integral over A if and only if C is integral over B and B is integral over A.

<u>Proof</u>: "$\Rightarrow$" trivial

"$\Leftarrow$" Let $c \in C$. Since c is integral over B there is an $n \in \mathbb{N}$, $n > 0$, and elements $b_i \in B$ such that $c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0$. Each b_i, $0 \le i \le n-1$, is integral over A and the A-algebra $A[b_0, \ldots, b_{n-1}]$ is finite. Since c is integral over $A[b_0, \ldots, b_{n-1}]$ the $A[b_0, \ldots, b_{n-1}]$-algebra $A[b_0, \ldots, b_{n-1}, c]$ is finite. By (5.5) the A-algebra $A[b_0, \ldots, b_{n-1}, c]$ is finite. c is integral over A by (5.2).

(5.11) <u>Corollary</u>: Let $A \subseteq B$ be a ring extension and $\overline{A}$ the integral closure of A in B. $\overline{A}$ is integrally closed in B.

(5.12) <u>Proposition</u>: Let $A \subseteq B$ be an extension of rings, $S \subseteq A$ a multiplicative set, $J \subseteq B$ an ideal and $I = J \cap A$ its contraction to A. Suppose that B is integral over A. Then:

(a) $A/I \subseteq B/J$ is an integral extension.

(b) $S^{-1}A \subseteq S^{-1}B$ is an integral extension.

<u>Proof</u>: (a) A/I is considered a subring of B/J. Let $\overline{b} = b + J \in B/J$ with $b \in B$. b satisfies an integral equation: $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ where $a_i \in A$ and $n > 0$. Thus $\overline{b}^n + \overline{a}_{n-1}\overline{b}^{n-1} + \cdots + \overline{a_0} = 0$ in B/J with $\overline{a}_i = a_i + I \in A/I$.

(b) Let $b/s \in S^{-1}B$ where $b \in B$ and $s \in S \subseteq A$. b is integral over A, thus $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ for $n > 0$ and some $a_i \in A$. Then $\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_0}{s^n} = 0$ and $a_i/s^{n-i} \in S^{-1}A$. b/s is integral over $S^{-1}A$.

(5.13) <u>Proposition</u>: Let $A \subseteq B$ be an extension of rings, $S \subseteq A$ a multiplicative subset. If A is integrally closed in B, then $S^{-1}A$ is integrally closed in $S^{-1}B$.

Proof: Let $b \in B$, $s \in S$ with b/s integral over $S^{-1}A$. Then there is an $n > 0$ and $\alpha_i \in S^{-1}A$ such that: $(*)$ $(b/s)^n + \alpha_{n-1}(b/s)^{n-1} + \_\_\_ + \alpha_0 = 0$.
Write $\alpha_i = a_i/s_i$ with $a_i \in A$ and $s_i \in S$ and set $t = (\prod_{i=0}^{n-1} s_i)s^n$; $t_n = \prod_{i=0}^{n-1} s_i$, and $t_j = (\prod_{i=0, i\neq j}^{n-1} s_i)s^{n-j}$ for $0 \leq j \leq n-1$. Multiplying $(*)$ by t yields:

$$0 = (t^n b^n + a_{n-1}t_{n-1}b^{n-1} + \_\_\_ + a_0 t_0)/1 \in S^{-1}B.$$

Thus there is an element $v \in S$ so that:

$$(**) \quad v(t^n b^n + a_{n-1}t_{n-1}b^{n-1} + \_\_\_ + a_0 t_0) = 0 \text{ in } B.$$

Multiply $(**)$ by r^{n-1} where $r = v t_n \in S$. Then

$$(rb)^n + \tilde{a}_{n-1}(rb)^{n-1} + \_\_\_ + \tilde{a}_0 = 0$$

where $\tilde{a}_i \in A$. Since A is integrally closed in B, $rb \in A$ and thus $b/s = (rb)/(rs) \in S^{-1}A$.

(5.14) Corollary: Let A be a normal domain and $S \subseteq A \setminus (0)$ a multiplicative subset. $S^{-1}A$ is a normal domain.

(5.15) Corollary: Let A be an integral domain. A is normal if and only if A_m is normal for all $m \in m\text{-Spec}(A)$.

Proof: "$\Rightarrow$" by (5.14)
"$\Leftarrow$": By (1.52): $A = \bigcap_{m \in m\text{-Spec}(A)} A_m$. If $x \in Q(A)$ is integral over A, then x is integral over A_m for all $m \in m\text{-Spec}(A)$. Thus $x \in A_m$ for all $m \in m\text{-Spec}(A)$ and $x \in A$.

(5.16) Lemma: Let A be a domain, $Q(A) = K$ its field of quotients and $K \subseteq L$ an extension of fields. If $\alpha \in L$ is algebraic over K then there is an element $t \in A \setminus (0)$ so that $t\alpha$ is integral over A.

Proof: If $\alpha \in L$ is algebraic over K, there is an $n > 0$ and elements $\beta_i \in K$ such that $\alpha^n + \beta_{n-1}\alpha^{n-1} + \_\_\_ + \beta_0 = 0$. Write $\beta_i = a_i/t$ with $a_i \in A$ and $t \in A \setminus (0)$. Then $(t\alpha)^n + (a_{n-1})(t\alpha)^{n-1} + \_\_\_ + a_0 t^{n-1} = 0$ and $t\alpha$ is integral over A.

(5.17) <u>Lemma</u>: Let A be a domain, $K = Q(A)$ its field of quotients and $K \subseteq L$ an algebraic field extension. Let B denote the integral closure of A in L. Then:
(a) $Q(B) = L$, that is, the field of quotients of B is L.
(b) The K-vector space L has a basis consisting of elements of B.

<u>Proof</u>: (a) Let $\alpha \in L$. By assumption α is algebraic over K and by (5.16) there is an element $t \in A \setminus (0)$ with $t\alpha$ integral over A. Thus $t\alpha \in B$ and $\alpha \in Q(B)$ since $A \subseteq B$.
(b) Let $\{\alpha_i\}_{i\in I}$ be a basis of L over K. For each $i \in I$ there is an element $t_i \in A \setminus (0)$ with $t_i\alpha_i \in B$. $\{t_i\alpha_i\}_{i\in I}$ is a basis of L over K.

<u>Recall</u>: Let $K \subseteq L$ be a finite field extension. For every $\alpha \in L$ the map $\ell_\alpha : L \longrightarrow L$ with $\ell_\alpha(\beta) = \alpha\beta$ defines a K-linear operator of the K-vector space L. The characteristic polynomial of ℓ_α is denoted by $P_{L/K}(\alpha, x) \in K[x]$ and the minimal polynomial of ℓ_α is denoted by $m(\alpha, x)$. Note that $m(\alpha, x)$ is the minimal polynomial of the (algebraic) element $\alpha \in L$ over the subfield K.

(5.18) <u>Theorem</u>: Let A be a normal domain, $K = Q(A)$ its field of quotients and $K \subseteq L$ a finite field extension. The following are equivalent:
(a) α is integral over A.
(b) $m(\alpha, x) \in A[x]$
(c) $P_{L/K}(\alpha, x) \in A[x]$

<u>Proof</u>: Since $m(\alpha, x)$ is monic and $P_{L/K}(\alpha, x)$ has leading coefficient $(-1)^r$: (b)$\Rightarrow$(a) and (c)$\Rightarrow$(a).
(a)$\Rightarrow$(b): Let $f = m(\alpha, x) \in K[x]$ and $h \in A[x]$ monic with $h(\alpha) = 0$. By definition of the minimal polynomial there is a polynomial $g \in K[x]$ with $h = f \cdot g$. Let $\overline{K} = \overline{L}$ denote the algebraic closure of K and L. Then $g = \prod_{i=1}^{m} (x - \beta_i)$ and $f = \prod_{j=1}^{n} (x - \alpha_j)$ where $\beta_i, \alpha_j \in \overline{K}$ and $\alpha = \alpha_1$. Let $\overline{A}$ be the integral closure of A in $\overline{K} = \overline{L}$. Since $h(\alpha_j) = 0$ for all $1 \le j \le n$ and $h(x) \in A[x]$ monic we obtain that $\alpha_j \in \overline{A}$ for all $1 \le j \le n$.

The coefficients of f are elementary symmetric functions in the α_j $(1 \leq j \leq n)$. This implies that the coefficients of f are in $\bar{A} \cap K$. Since A is normal, $\bar{A} \cap K = A$.

(a) $\Rightarrow$ (c): We know that $P_{L/K}(\alpha, x) \mid m(\alpha, x)^r$ for some $r \in \mathbb{N}$. Let $h \in A[x]$ be monic with $h(\alpha) = 0$. Then $P_{L/K}(\alpha, x) \mid h(x)^r$ and the same argument as above applies.

(5.19) Example: Let A be a factorial domain, $K = Q(A)$ its field of quotients and $d \in A$ a square free element of A, that is, $d = p_1 \cdots p_r$ where p_i are prime elements of A with $p_i \notin (p_j)$ if $i \neq j$. Suppose that 2 is a prime element of A and let B denote the integral closure of A in $L = K(\sqrt{d}) \supsetneq K$. Obviously, $\{1, \sqrt{d}\}$ is a basis of L over K and $L = \{a + b\sqrt{d} \mid a, b \in K\}$. Question: When is $a + b\sqrt{d} \in B$?

By (5.18): $a + b\sqrt{d} \in B \Leftrightarrow m(a + b\sqrt{d}, x) \in A[x]$

Note that if $b \neq 0$, then $m(a+b\sqrt{d}, x) = (x - (a + b\sqrt{d}))(x - (a - b\sqrt{d})) = x^2 - 2ax + a^2 - b^2 d \in K[x]$.

Thus $m(a + b\sqrt{d}, x) \in A[x] \Leftrightarrow 2a \in A$ and $a^2 - b^2 d \in A$.

Claim: $A + A\sqrt{d} \subseteq B \subseteq (A + A\sqrt{d}) \cup \{a + b\sqrt{d} \mid a, b \notin A \text{ and } 2a, 2b \in A\}$.

Pf of Cl: If $a + b\sqrt{d} \in B$ with $b \neq 0$ then $2a, a^2 - b^2 d \in A$. Thus $(2b)^2 d \in A$. Suppose $b = u/v$ with $u, v \in A$ relatively prime. If $p \in A$ is a prime element with $p \mid v$ then $p^2 \mid 4u^2 d$ and $p^2 \mid 4d$ since $\gcd(u, v) = 1$. Since d is square free $p^2 \mid 4$ and $p = 2$. By a similar argument v is not divided by 4 and $2b \in A$. Similarly, if $a \in A$ then $b \in A$ and if $b \in A$ then $a \in A$.

Suppose now that $A = \mathbb{Z}$ and $d \in \mathbb{Z}$ is a square free integer.

Case 1: $d \equiv 1 \pmod 4$

Suppose $a, b \in \mathbb{Z} \setminus (2)$. Then $a^2 - b^2 d \equiv 0 \pmod 4$ and $(a/2)^2 - (b/2)^2 d \in \mathbb{Z}$.

Then $B = \mathbb{Z}[1/2 + 1/2\sqrt{d}] = \{a + b(1/2 + 1/2\sqrt{d}) \mid a, b \in \mathbb{Z}$.

Case 2: $d \equiv 2 \pmod 4$

If $a, b \in \mathbb{Z} \setminus (2)$, then $a^2 - b^2 d \not\equiv 0 \pmod 4$ and $(a/2)^2 - (b/2)^2 d \notin \mathbb{Z}$. Thus $B = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.

Case 3: $d \equiv 3 \pmod 4$

If $a, b \in \mathbb{Z} \setminus (2)$, then $a^2 - b^2 d \not\equiv 0 \pmod 4$ and $B = \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.

(5.20) Lemma: Let $A \subseteq B$ be an extension of rings with B integral over A. Suppose that B is a domain. A is a field if and only if B is a field.

Proof: "$\Rightarrow$": Let $b \in B$. Since b is integral over A, $b \in Q(B)$ is algebraic over A. Every intermediate ring $A \subseteq C \subseteq Q(A[b]) = A(b)$ is a field. Hence $A[b]$ is a field.
"$\Leftarrow$": Let $a \in A$ with $a \neq 0$. Since B is a field, $a^{-1} \in B$ and there are $a_i \in A$ so that $(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \text{—} + a_0 = 0$. Then

$$a^{-1} = -(a_{n-1} + a_{n-2}a + \text{—} + a_0 a^{n-1}) \in A$$

and A is a field.

(5.21) Definition: Let $A \subseteq B$ be an extension of rings, $P \in \operatorname{Spec}(A)$ and $Q \in \operatorname{Spec}(B)$ prime ideals. We say that Q is lying over P if $Q \cap A = P$.

(5.22) Theorem: Let $A \subseteq B$ be an integral extension of rings. Then:
(a) "Lying over": For every prime ideal $P \subseteq A$ there is a prime ideal $Q \subseteq B$ which lies over P, that is, $Q \cap A = P$.
(b) If $Q_1 \subseteq Q_2$ are prime ideals of B which lie over the same prime ideal P of A then $Q_1 = Q_2$.
(c) Let $Q \subseteq B$ be a prime ideal lying over $P \subseteq A$. Q is a maximal ideal of B if and only if P is a maximal ideal of A.

Proof: (c) Consider the integral extension $A/P \subseteq B/Q$ and apply (5.20).
(b) Consider the integral extension $A/P \subseteq B/Q_1$ and replace A by A/P and B by B/Q_1. Thus we may assume that $A \subseteq B$ is an integral extension of domains and $Q \subseteq B$ is a prime ideal with $Q \cap A = (0)$. Suppose that $b \in Q$ and $b \neq 0$. Then there is a minimal $n \in \mathbb{N}$ so that there is an integral equation: $b^n + a_{n-1}b^{n-1} + \text{—} + a_0 = 0$ with $a_i \in A$. Since $a_0 \in Q \cap A = (0)$ we obtain $b(b^{n-1} + a_{n-1}b^{n-2} + \text{—} + a_1) = 0$. B is a domain, thus $b^{n-1} + a_{n-1}b^{n-2} + \text{—} + a_1 = 0$, a contradiction to n minimal.

(a) $S = A - P$ is a multiplicative subset of A and B and the ring extension $A_p = S^{-1}A \subseteq S^{-1}B$ is integral. This yields a commutative diagram:

$$\begin{array}{ccc} B & \xrightarrow{i_{B,S}} & S^{-1}B \\ \text{integral} \uparrow & & \uparrow \text{integral} \\ A & \xrightarrow{i_{A,S}} & A_p = S^{-1}A \end{array}$$

Let $m \subseteq S^{-1}B$ be a maximal ideal. By (c) $n = m \cap S^{-1}A$ is a maximal ideal of A, thus $n = PA_p$. The ideal $Q = i_{B,S}^{-1}(m)$ is a prime ideal of B which lies over $P \subseteq A$.

(5.23) Corollary: Let $A \subseteq B$ be an integral extension of rings. If $Q_0 \subsetneq Q_1 \subsetneq — \subsetneq Q_r$ is a chain of distinct prime ideals of B, then $P_0 \subsetneq P_1 \subsetneq — \subsetneq P_r$, where $P_i = A \cap Q_i$, is a chain of distinct prime ideals of A. In particular, $\dim A \geq \dim B$.

(5.24) Corollary: (Going-up) Let $A \subseteq B$ be an integral extension of rings and $P_0 \subseteq P_1 \subseteq — \subseteq P_r$ a chain of prime ideals of A. Let $Q_0 \subseteq B$ be a prime ideal that is lying over P_0. Q_0 extends to a chain of prime ideals $Q_0 \subseteq Q_1 \subseteq — \subseteq Q_r$ in B with $Q_i \cap A = P_i$ for $0 \leq i \leq r$.

Proof: By induction on r. For $r = 0$ there is nothing to show.
$r-1 \to r$: Suppose we have constructed a chain of prime ideals $Q_0 \subseteq Q_1 \subseteq — \subseteq Q_{r-1}$ in B with $Q_i \cap A = P_i$ for $0 \leq i \leq r-1$. Then $A/P_{r-1} \subseteq B/Q_{r-1}$ is an integral extension. By (5.22) there is a prime ideal $\overline{Q}_r \subseteq B/Q_{r-1}$ with $\overline{Q}_r \cap (A/P_{r-1}) = \overline{P}_r = P_r/P_{r-1}$. Let $Q_r \subseteq B$ be the preimage of $\overline{Q}_r$. Then $Q_{r-1} \subseteq Q_r$ and $Q_r \cap A = P_r$.

(5.25) Corollary: Let $A \subseteq B$ be an integral extension of rings. Then:
(a) $\dim A = \dim B$
(b) If $Q \in \mathrm{Spec}(B)$ and $P = Q \cap A \in \mathrm{Spec}(A)$, then $\mathrm{ht}\, P \geq \mathrm{ht}\, Q$.
(c) If $Q \in \mathrm{Spec}(B)$ and $P = Q \cap A \in \mathrm{Spec}(A)$, then $\dim A/P = \dim B/Q$.

Proof: (a) By (5.23) $\dim A \geq \dim B$ and $\dim A \leq \dim B$ by (5.24).

(b) By (5.23)

(c) Apply (a) to the integral extension $A/P \subseteq B/Q$.

(5.26) Corollary: Let $A \subseteq B$ be an integral extension of rings and $P \subseteq A$ a prime ideal of finite height. Then there is a prime ideal $Q \subseteq B$ with $\mathrm{ht}\, Q = \mathrm{ht}\, P$ and $P = Q \cap A$.

Proof: With $S = A - P$ the extension $S^{-1}A = A_P \subseteq S^{-1}B$ is integral. By (5.25) $r = \mathrm{ht}\, P = \dim A_P = \dim S^{-1}B$. Let $\tilde{Q} \subseteq S^{-1}B$ be a prime ideal with $\mathrm{ht}\, \tilde{Q} = r$. $\tilde{Q}$ is maximal in $S^{-1}B$ and therefore $\tilde{Q} \cap A_P = PA_P$. Let $Q \in \mathrm{Spec}(B)$ with $QS^{-1}B = \tilde{Q}$. Then $\mathrm{ht}\, Q = \mathrm{ht}\, \tilde{Q} = r$ and $P = Q \cap A$.

Recall from algebra: A finite extension of fields $K \subseteq L$ is called normal if one of the following equivalent conditions is satisfied:

(a) If $g(x) \in K[x]$ is an irreducible polynomial and $\alpha \in L$ with $g(\alpha) = 0$ then $g(x)$ splits completely into linear factors over L; $g(x) = \varepsilon \prod_{i=1}^{n} (x - \alpha_i)$ where $\varepsilon \in K$, $\alpha_i \in L$, and $\alpha = \alpha_1$.

(b) For all $\alpha \in L$ every conjugate of α is in L. (The conjugates of α are the roots of the minimal polynomial of α over K.)

(c) Let $\overline{K} = \overline{L}$ be the algebraic closure of K and L. For every $\sigma \in \mathrm{Aut}_K(\overline{K})$ we have that $\sigma|_L \in \mathrm{Aut}_K(L)$, that is, $\sigma(L) \subseteq L$.

Also note that $|\mathrm{Aut}_K(L)| \leq [L:K]$.

(5.27) Proposition: Let A be a normal domain, $K = Q(A)$ its field of quotients, and $K \subseteq L$ a finite normal field extension. Let B be the integral closure of A in L, and let $P \in \mathrm{Spec}(A)$, $Q_1, Q_2 \in \mathrm{Spec}(B)$ be prime ideals with $Q_1 \cap A = Q_2 \cap A = P$. Then there is an automorphism $\sigma \in \mathrm{Aut}_K(L)$ with $\sigma(Q_2) = Q_1$, that is, Q_1 and Q_2 are conjugate over K. In particular, there are only finitely many prime ideals $Q \subseteq B$ lying over $P \subseteq A$.

Proof: Put $G = \mathrm{Aut}_K(L) = \{\sigma_1, \ldots, \sigma_r\}$. It is easy to verify that each σ_j defines an automorphis of B (by restriction) and that $\sigma_j(Q) \in \mathrm{Spec}(B)$ for all $Q \in \mathrm{Spec}(B)$. Let

$P \in \mathrm{Spec}(A)$ and $Q_1, Q_2 \in \mathrm{Spec}(B)$ be as above. Suppose $Q_2 \neq \sigma_j^{-1}(Q_1)$ for all $1 \le j \le r$. By (5.22)(b): $Q_2 \nsubseteq \sigma_j^{-1}(Q_1)$ for all $1 \le j \le r$. Thus $Q_2 \nsubseteq \bigcup_{j=1}^r \sigma_j^{-1}(Q_1)$. Pick an element $x \in Q_2 - \bigcup_{j=1}^r \sigma_j^{-1}(Q_1)$ and consider $y := [\prod_{j=1}^r \sigma_j(x)]^q$ where $q = 1$ if $\mathrm{char}(K) = 0$ and $q = p^\nu$ if $\mathrm{char}(K) = p$. ν is given as follows: The extension $K \subseteq L$ splits into

$$K \subseteq K' = \mathrm{Fix}(L; G) \subseteq L$$

where $K \subseteq K'$ is purely inseparable and $K'^q \subseteq K$ for $q = p^\nu$ and some $\nu \in \mathbb{N}$. Obviously, $\prod_{j=1}^r \sigma_j(x) \in K'$ and therefore $y \in K$. Since $x \in B$ is integral over A, $y \in K$ is integral over A and since A is normal: $y \in A$. Suppose that $\sigma_1 = \mathrm{id}_L$, then $\sigma_1(x) = x$ and y is a multiple of x. Hence $y \in Q_2 \cap A = P = Q_1 \cap A$. This implies $[\prod_{j=1}^r \sigma_j(x)]^q \in Q_1$ and therefore $\sigma_j(x) \in Q_1$ for some $1 \le j \le r$, a contradiction. Hence $Q_2 = \sigma_j^{-1}(Q_1)$ for some $1 \le j \le r$.

(5.28) <u>Remark</u>: Let A be a normal domain, $Q(A) = K$ its field of quotients and $K \subseteq L$ a finite field extension. Then there is a field extension $L \subseteq E$ such that $K \subseteq E$ is finite and normal. Let B_L be the integral closure of A in L and B_E the integral closure of A in E. We have integral extensions $A \subseteq B_L \subseteq B_E$ and for every $P \in \mathrm{Spec}(A)$ there are only finitely many $\tilde{Q} \in \mathrm{Spec}(B_E)$ lying over P. Thus there are only finitely many $Q \in \mathrm{Spec}(B_L)$ lying over P.

If A is a non-normal domain, $\bar{A}$ the integral closure of A in $Q(A)$, we can ask if there are only finitely many prime ideals $Q \subseteq \bar{A}$ which lie over a given prime ideal $P \in \mathrm{Spec}(A)$. The Mori-Nagata theorem shows that this is true if A is a Noetherian domain.

(5.29) <u>Theorem</u>: (Going Down) Let A be a normal domain, $K = Q(A)$ its field of quotients, and $K \subseteq L$ a finite extension of fields. Let B be the integral closure of A in L and $P_0 \subseteq P_1 \subseteq \dots \subseteq P_r \subseteq A$ a chain of prime ideals in A. If $Q_r \in \mathrm{Spec}(B)$ is a prime ideal with $Q_r \cap A = P_r$ then there is a chain of prime ideals $Q_0 \subseteq Q_1 \subseteq \dots \subseteq Q_r$ in B with $Q_i \cap A = P_i$ for all $0 \le i \le r$.

Proof: There is a finite extension E of L so that E is normal over K. Let C be the integral closure of A in E. $B \subseteq C$ is an integral extension and there is a prime ideal $Q' = Q_r' \in \mathrm{Spec}(C)$ which lies over Q_r. It is enough to construct a chain of prime ideals $Q_0' \subseteq Q_1' \subseteq \ldots \subseteq Q_r' = Q'$ in C with $Q_i' \cap A = P_i$ for $1 \leq i \leq r$. Thus we may assume $E = L$ is normal over K.

The proof is by induction on r. If $r = 0$, there is nothing to show. For the induction step $r-1 \Rightarrow r$ we have to show: if $P_0 \subsetneq P_1$ are prime ideals of A and $Q_1 \subseteq B$ is a prime ideal with $Q_1 \cap A = P_1$ then there is a prime ideal $Q_0 \subseteq B$ with $Q_0 \subseteq Q_1$ and $Q_0 \cap A = P_0$:

$$\begin{array}{ccccc} P_0 & \subsetneq & P_1 & \subseteq & A \\ | & & | & & \cap \\ Q_0 & \subsetneq & Q_1 & \subseteq & B. \end{array}$$

Let $Q_0' \subseteq B$ be a prime ideal with $Q_0' \cap A = P_0$. By going-up there is a prime ideal $Q_1' \subseteq B$ with $Q_0' \subseteq Q_1'$ and $Q_1' \cap A = P_1$. By (5.27) there is an automorphism $\sigma \in \mathrm{Aut}_K(L)$ with $\sigma(Q_1') = Q_1$. Then $\sigma(Q_0') = Q_0 \subseteq Q_1$ and $Q_0 \cap A = Q_0' \cap A = P_0$.

(5.30) Remark: By using Galois theory of infinite (algebraic) extensions one can prove (5.27) and (5.29) without the assumption $[K:L] < \infty$.

§2: DISCRETE VALUATION RINGS ; DEDEKIND DOMAINS

(5.31) Definition: Let K be a field. A discrete valuation of K is a function $v: K \longrightarrow \mathbb{Z}\cup\{\infty\}$ which satisfies the following conditions:

(a) $v(x) = \infty \Longleftrightarrow x = 0$

(b) For all $x,y \in K$: $v(xy) = v(x) + v(y)$, that is, $v|_{K^*}: K^* \longrightarrow (\mathbb{Z},+)$ is a homomorphism of groups.

(c) For all $x,y\in K$: $v(x+y) \geq \min(v(x), v(y))$

A valuation $v: K \longrightarrow \mathbb{Z}\cup\{\infty\}$ is called trivial if $v(K) = \{0,\infty\}$.

(5.32) Remark: (a) There is the more general concept of valuations where the 'value' group $\mathbb{Z}$ is replaced by an (arbitrary) ordered abelian group.

(b) Let $K \subseteq L$ be an extension of fields, $v: L \longrightarrow \mathbb{Z}\cup\{\infty\}$ a discrete valuation of L. The restriction $v|_K$ is a discrete valuation of K. Note that $v|_K$ may by trivial while v is not.

(c) $v(K^*) \subseteq \mathbb{Z}$ is a subgroup of $\mathbb{Z}$, thus $v(K^*) = m\mathbb{Z}$ for some $m\in\mathbb{Z}$. v is trivial if and only if $m=0$. If v is nontrivial, v can be replaced by the (equivalent) valuation $v': K \longrightarrow \mathbb{Z}\cup\{\infty\}$ defined by $v'(x) = (1/m)v(x)$ for $x\in K^*$ and $v'(0) = \infty$. In the following we assume that a nontrivial valuation v of K satisfies $v(K^*) = \mathbb{Z}$.

(5.33) Example: Let A be a factorial domain, $p\in A$ a prime element and $K = Q(A)$ its field of quotients. Every element $\alpha\in K^*$ can be written as $\alpha = p^n(a/b)$ where $a,b\in A$, $p\nmid a$ and $p\nmid b$, and $n\in\mathbb{Z}$. Define $v_p(\alpha) = n$. v_p is a discrete valuation of K. If $A=\mathbb{Z}$, $K=\mathbb{Q}$, and p a prime number, v_p is called the p-adic valuation of $\mathbb{Q}$.

(5.34) Theorem: Let K be a field, $v: K \longrightarrow \mathbb{Z}\cup\{\infty\}$ a discrete valuation of K. Then:

(a) $A_v = \{x\in K \mid v(x) \geq 0\}$ is a subring of K.

(b) The units of A_v are $A_v^* = \{x\in K \mid v(x) = 0\}$.

(c) $m_v = \{x\in K \mid v(x) > 0\}$ is the only maximal ideal of A_v, that is, A_v is a local domain with maximal ideal m_v.

(d) A_v is a principal ideal domain. v is trivial if and only if $A_v = K$.

(e) The prime elements of A_v are the elements $p \in A_v$ with $v(p) = 1$. All prime elements of A_v are associated and m_v is generated by a prime element $p \in A_v$.

Proof: (a) Note that $v(1) = v(1) + v(1)$, thus $v(1) = 0$ and $0 = v(1) = v(-1) + v(-1)$ and $v(-1) = 0$. It is now easy to verify that A_v is a subring of K.

(b) $a \in A_v^* \longleftrightarrow v(a) \geq 0$ and $v(a^{-1}) \geq 0$. Since $0 = v(1) = v(a) + v(a^{-1})$ it follows that $v(a) = 0$. On the other hand if $v(a) = 0$ then $v(a^{-1}) = 0$ and $a^{-1} \in A_v$.

(c) Verify that $m_v \subseteq A_v$ is an ideal. Since $A_v^* = A_v - m_v$, m_v is a maximal ideal of A_v and A_v is local.

(d) Let $I \subseteq A_v$ be an ideal with $I \neq (0)$. Pick $a \in I - (0)$ so that for all $b \in I$: $v(b) \geq v(a)$. Let $b \in I$. Then $b = a\,(b/a) \in K$ and $v(b) = v(a) + v(b/a)$. Since $v(a) \leq v(b)$, $v(b/a) \geq 0$ and $b/a \in A_v$. Thus $I = (a)$.

(e) By (d) m_v is generated by any element $p \in A_v$ with $v(p) = 1$. Any such element p generates the prime ideal m_v. Thus p is a prime element. If $q \in m_v$ is a second element with $v(q) = 1$, then $v(p/q) = 0$ and $p/q = \delta \in A_v^*$. Hence p and q are associated.

(5.35) Definition: (a) A local PID which is not a field is called a discrete valuation ring, DVR, for short.

(b) Let K be a field, $v : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ a nontrivial discrete valuation of K. The ring A_v is called the discrete valuation ring associated to v.

(5.36) Theorem: Let A be a DVR, $p \in A$ a prime element, and $K = Q(A)$ its quotient field.

(a) Every element $x \in K^*$ is of the form $x = u p^n$ with $u \in A^*$ and $n \in \mathbb{Z}$. The integer n does not depend on the choice of p.

(b) The map $v : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ defined by $v(0) = \infty$ and $v(x) = n$ for $x \in K^*$ with

$x = up^n$, $u \in A^*$, $n \in \mathbb{Z}$, is a discrete valuation of K with $v(K^*) = \mathbb{Z}$ and $A_v = A$.

<u>Proof</u>: Since A is a local PID, A has exactly one nonzero prime ideal $P \subseteq A$. Moreover, P is generated by a prime element $p \in A$ and every other prime element $q \in A$ is associated to p.

(a) Let $x \in K^*$. Then $x = a/b$ with $a, b \in A$. There are units $u, v \in A^*$ and nonnegative integers $n, m \in \mathbb{N}$ with $a = up^n$ and $b = vp^m$. Thus $x = (uv^{-1})p^{n-m}$. Since every prime element $q \in A$ is associated to p, the exponent $n-m$ is independent of the choice of p.

(b) Obvious

(5.37) <u>Corollary</u>: Let K be a field. Then there is a 1-1 correspondence:

$\{v \text{ a discrete valuation of } K\} \ \widehat{=}\ \{A \subseteq K \text{ a DVR with } Q(A) = K\}$.

(5.38) <u>Theorem</u>: (Characterization of DVRs) Let (A, m) be a local Noetherian domain. The following are equivalent:

(a) A is a DVR.

(b) A is normal and $\dim A = 1$.

(c) A is normal and there is an $a \in A \setminus (0)$ with $m \in \mathrm{Ass}_A(A/(a))$.

(d) m is a nonzero principal ideal.

(e) A is not a field, A is factorial and all prime elements of A are associated.

<u>Proof</u>: (a) $\Rightarrow$ (b): A is a PID, thus A is normal with $\dim A = 1$.

(b) $\Rightarrow$ (c): For all $a \in m - (0)$: $\mathrm{Supp}_A(A/aA) = \{m\}$. Therefore $m \in \mathrm{Ass}_A(A/(a))$.

(c) $\Rightarrow$ (d): Let $a \in A - (0)$ with $m \in \mathrm{Ass}_A(A/aA)$ and let $\bar{b} \in A/aA$ with $\mathrm{ann}_A(\bar{b}) = m$. Let be $b \in A$ be a preimage of $\bar{b}$. Since $\bar{b} \neq 0$, $b \notin aA$ and $mb \subseteq aA$. Thus $mba^{-1} \subseteq A$. mba^{-1} is an ideal of A.

<u>Claim</u>: $mba^{-1} = A$.

Pf of (c): If $mba^{-1} \neq A$ then $mba^{-1} \subseteq m$ since A is local. Thus $m(ba^{-1})^2 \subseteq mba^{-1} \subseteq m$ and so on, that is, $m(ba^{-1})^n \subseteq m$ for all $n \in \mathbb{N}$. Hence $a(ba^{-1})^n \subseteq m$ for all $n \in \mathbb{N}$ and $(ba^{-1})^n \subseteq Aa^{-1} \subseteq K$ for all $n \in \mathbb{N}$. Aa^{-1} is a finite (cyclic) A-submodule of K. We get that the A-algebra $A[ba^{-1}]$ is contained in the finite A-module Aa^{-1}! Aa^{-1} is a faithful $A[ba^{-1}]$-module and by (5.2) ba^{-1} is integral over A. Since A is normal $ba^{-1} \in A$ and hence $b \in aA$, a contradiction.

Hence $mba^{-1} = A$ and $m = (ab^{-1})A$ with $ab^{-1} \in A$.

(d) $\Rightarrow$ (e): Put $m = (p)$ and let $a \in A - (0)$ be any element. Since A is local Noetherian by (4.22) there is an $n \in \mathbb{N}$ with $a \in m^n = (p^n)$ (possibly: $n = 0$) and $a \notin m^{n+1} = (p^{n+1})$. Thus $a = up^n$ with $u \in A^*$. Since p generates a prime ideal, p is a prime element of A. Every element of A can be written (uniquely) as a product of a unit of A and a power of p. Thus A is factorial and all prime elements of A are associated.

(e) $\Rightarrow$ (a): Let $I \subseteq A$ be a nonzero ideal. We want to show that I is principal. Let $p \in A$ be a prime element. Every element $a \in I - (0)$ can be written as $a = up^n$ where $u \in A^*$, $n \in \mathbb{N}$. Let $a_0 \in I - (0)$ with $a_0 = up^m$, $u \in A^*$ and $m \in \mathbb{N}$ minimal. If $b \in I - (0)$, then $b = vp^t$ where $v \in A^*$ and $t \in \mathbb{N}$ with $t \geq m$. Thus $(vu^{-1})p^{t-m} \in A$ and $b = (vu^{-1})p^{t-m} a_0 \in (a_0)$. Thus $I = (a_0)$.

(5.39) Definition: A Noetherian domain A is called a Dedekind domain if A is normal and $\dim A = 1$.

(5.40) Remark: Let A be a Noetherian domain of positive dimension. A is a Dedekind domain if and only if for all $P \in \operatorname{Spec}(A)$ with $P \neq (0)$ the ring A_P is a DVR.

(5.41) Theorem: Let A be a Dedekind domain.

(a) Every nonzero ideal $I \subseteq A$ can be written uniquely (up to order) as a product of finitely many maximal ideals.

(b) For every nonzero ideal $I \subseteq A$ there is a nonzero ideal $J \subseteq A$ so that IJ is principal.

Proof: (a) Let $I = Q_1 \cap \ldots \cap Q_r$ be a shortest primary decomposition of I where $Q_i \subseteq A$ are m_i-primary with $m_i \neq m_j$ for $i \neq j$. Since $\dim A = 1$ all the m_i are maximal ideals of A. Let $\varphi_i : A \longrightarrow A_{m_i}$ be the canonical morphism. Then $Q_i = \varphi_i^{-1}(Q_i A_{m_i})$. A_{m_i} is a DVR and therefore $Q_i A_{m_i} = m_i^{t_i} A_{m_i}$. Because m_i is maximal the ideal $m_i^{t_i}$ is m_i-primary and therefore $Q_i = m_i^{t_i}$. This shows that $I = m_1^{t_1} \cap \ldots \cap m_r^{t_r}$ and by the Chinese remainder theorem: $I = m_1^{t_1} m_2^{t_2} \ldots m_r^{t_r}$. For uniqueness note that the $m_i^{t_i}$ are exactly the m_i-primary components of I. Those are unique since I has only minimal associated primes.

(b) Pick an element $a \in I - (0)$. Then there are maximal ideals $m_i \subseteq A$ with $m_i \neq m_j$ for $i \neq j$ so that $I = m_1^{t_1} \ldots m_r^{t_r}$ and $(a) = m_1^{s_1} \ldots m_\ell^{s_\ell}$ with $\ell \geq r$ and $s_i \geq t_i$, where $t_i = 0$ for $i > r$. With $J = m_1^{s_1 - t_1} \ldots m_\ell^{s_\ell - t_\ell}$: $IJ = (a)$.

(5.42) Remark: (without proof) Every domain which satisfies (a) or (b) of (5.41) is a Dedekind domain. (without the assumption that A is Noetherian).

(5.43) Remark: In general a Dedekind domain is not factorial. Example: By (5.19) the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-5})$ is $\mathbb{Z}[\sqrt{-5}]$. $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain but $\mathbb{Z}[\sqrt{-5}]$ is not factorial since $2.3 = 6 = (1+\sqrt{-5})(1-\sqrt{-5})$.

(5.44) Theorem: Let A be a Noetherian domain. The following are equivalent:

(a) A is normal.

(b) For every height one prime ideal $P \subseteq A$ the ring A_P is a DVR and for all $a \in A - [(0) \cup A^*]$ every prime ideal of $\mathrm{Ass}_A(A/aA)$ is minimal, that is, the ideal aA has no embedded primes.

(c) For every height one prime ideal $P \subseteq A$ the ring A_P is a DVR and $A = \bigcap_{\substack{P \in \mathrm{Spec}(A) \\ \mathrm{ht}\,P = 1}} A_P$.

Proof: (a) $\Rightarrow$ (b): Since A is normal A_P is normal for all $P \in \mathrm{Spec}(A)$. Thus A_P is a DVR for all $P \in \mathrm{Spec}(A)$ with $\mathrm{ht}\,P = 1$. Let $a \in A - [(0) \cup A^*]$ and $P \in \mathrm{Ass}_A(A/aA)$.

Then $PA_P \in \mathrm{Ass}_{A_P}(A_P/aA_P)$. By (5.38) A_P is a DVR. Hence ht $P = 1$ and P is a minimal associated prime of aA.

(b) $\Rightarrow$ (c): Obviously,
$$A \subseteq \bigcap_{\substack{P \in \mathrm{Spec}(A)\\ \mathrm{ht}\, P = 1}} A_P .$$

Let $x = b/a \in Q(A)$, $a, b \in A$, $a \neq 0$, with $x \in A_P$ for all $P \in \mathrm{Spec}(A)$ with ht $P = 1$. Then $b \in aA_P$ for all primes P of height one. By (b): $b \in aA_P$ for all $P \in \mathrm{Ass}_A(A/aA)$. For all $P \in \mathrm{Ass}_A(A/aA)$ let $s_P \in A - P$ and $c_P \in A$ with $b = a \cdot c_P/s_P$. Consider the ideal $I = (a) : (b) = \{y \in A \mid yb \in (a)\}$. Then $s_P \in I$ for all $P \in \mathrm{Ass}_A(A/aA)$ and
$$I \nsubseteq \bigcup_{P \in \mathrm{Ass}_A(A/aA)} P .$$

Let $Q \in \mathrm{Ass}_A\left((b)+(a)/(a)\right)$. Since $\mathrm{ann}_A\left((b)+(a)/(a)\right) = I$ we obtain the $I \subseteq Q$. But $(b)+(a)/(a) \subseteq A/(a)$ and therefore $\mathrm{Ass}_A\left((b)+(a)/(a)\right) \subseteq \mathrm{Ass}_A\left(A/(a)\right)$. This shows that $\mathrm{Ass}_A\left((b)+(a)/(a)\right) = \emptyset$ and $(b)+(a)/(a) = (0)$. Hence $b \in (a)$ and $x = b/a \in A$.

(c) $\Rightarrow$ (a): A is normal since A is an intersection of normal domains.