CHAPTER V: INTEGRAL EXTENSIONS; NORMAL RINGS

§1: INTEGRAL EXTENSIONS

(5.1) Definition: Let $R \subseteq S$ be an extension of rings.

(a) S is called a finite R-algebra if S is finitely generated as an R-module.

(b) An element $b \in S$ is called integral over R if the ring extension $R \subseteq R[b]$ is finite.

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

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

(a) b is integral over R.

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

(c) There is a finite R-algebra S_1 with $R \subseteq S_1 \subseteq S$ and $b \in S_1$.

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

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

(a) $\Rightarrow$ (c): Set $S_1 = R[b]$.

(c) $\Rightarrow$ (d): Set $S_1 = M$. Since $R[b] \subseteq S_1$, S_1 is an $R[b]$-module. Moreover, since $1_R = 1_S \in S_1$, $\operatorname{ann}_{R[b]}(S_1) = 0$. (Note that if $R \subseteq S$ is a ring extension we always assume that $1_R = 1_S$.)

(d) $\Rightarrow$ (b): Suppose that $M = Rm_1 + \ldots + Rm_n$. M is an $R[b]$-module, thus for all $1 \leq i \leq n$ there are elements $a_{ij} \in R$ such that $b m_i = \sum_{j=1}^{n} a_{ij} m_j$. Hence for all $1 \leq i \leq n$, $\sum_{j=1}^{n} (a_{ij} - b\delta_{ij}) m_j = 0$. Let $\sigma = (a_{ij} - b\delta_{ij})_{1 \leq i,j \leq n}$ be the $n \times n$ matrix with entries in $R[b]$ and let σ^* be its adjoint matrix. Then $\sigma^* \sigma = \det(\sigma) I_n$ where I_n is the $n \times n$ identity matrix. Note that:

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

This shows that $\det(\sigma) \in \operatorname{ann}_{R[b]}(M) = 0$ and thus $\det(\sigma) = 0$. Evaluation of $\det(\sigma)$ yields an integral equation $b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$ with $a_i \in R$.

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

(5.3) Corollary: (a) Let $R \subseteq S$ be a finite extension of rings. Then S is integral over R.
(b) Let $R \subseteq S \subseteq T$ be ring extensions. If $c \in T$ is integral over R, then c is integral over S.

Proof: (a) For every $b \in S$, $M = S$ is an $R[b]$-module which is finite as an R-module. Since $R[b] \subseteq S$ and $1_R = 1_S$, $\operatorname{ann}_{R[b]}(M) = 0$. Apply (5.2).
(b) trivial

(5.4) Example: $\mathbb{Z} \subseteq \mathbb{Z}[i]$ and $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{2}]$ are integral extensions.

(5.5) Lemma: Let $R \subseteq S \subseteq T$ be ring extensions such that S is finite over R and T is finite over S. Then T is finite over R.

Proof: Let $b_1, \dots, b_s \in S$ with $S = Rb_1 + \dots + Rb_s$ and $c_1, \dots, c_t \in T$ with $T = Sc_1 + \dots + Sc_t$. Then $T = \sum_{i,j} R b_i c_j$.

(5.6) Lemma: If $R \subseteq S$ is an extension of rings, set $\overline{R} = \{b \in S \mid b \text{ is integral over } R\}$. $\overline{R}$ is an intermediate ring, i.e. $R \subseteq \overline{R} \subseteq S$, and $\overline{R}$ is integral over R.

Proof: Let $b, c \in \overline{R}$. We have to show that $b \pm c$ and $b \cdot c$ are in $\overline{R}$. Consider the R-subalgebra $R[b,c] = (R[b])[c] \subseteq S$. The element c is integral over R, thus c is

integral over $R[b]$ and $(R[b])[c]$ is a finite $R[b]$-algebra. Since $R[b]$ is a finite R-algebra, by (5.5) the R-algebra $R[b,c]$ is finite and thus $R[b,c] \subseteq \overline{R}$.

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

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

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

(5.8) Proposition: Every factorial domain is normal.

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

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

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

Proof: (b) Let $\overline{\mathbb{Z}}$ denote the integral closure of $\mathbb{Z}$ in $\mathbb{Q}[i]$. Since $i \in \mathbb{Z}$, $\mathbb{Z}[i] \subseteq \overline{\mathbb{Z}}$. Since $\mathbb{Z}[i]$ is normal, $\mathbb{Z}[i] = \overline{\mathbb{Z}}$.

(5.10) Proposition: Let $R \subseteq S \subseteq T$ be extensions of rings. T is integral over R if and only if T is integral over S and S is integral over R.

Proof: "$\Leftarrow$": Let $c \in T$. Since c is integral over S, there is an $n \in \mathbb{N}$, $n > 0$, and elements $b_i \in S$

such that $c^n + b_{n-1}c^{n-1} + \dots + b_0 = 0$. Each b_i is integral over R and the R-algebra $R[b_0, \dots, b_{n-1}]$ is finite. Since c is integral over $R[b_0, \dots, b_{n-1}]$ the $R[b_0, \dots, b_{n-1}]$-algebra $R[b_0, \dots, b_{n-1}, c]$ is finite. By (5.5) the R-algebra $R[b_0, \dots, b_{n-1}, c]$ is finite and c is integral over R by (5.2).

(5.11) Corollary: Let $R \subseteq S$ be a ring extension and $\overline{R}$ the integral closure of R in S. Then $\overline{R}$ is integrally closed in S.

(5.12) Proposition: Let $R \subseteq S$ be an integral extension of rings, $W \subseteq R$ a multiplicative subset, $J \subseteq S$ an ideal, and $I = J \cap R$ its contraction to R. Then:
(a) $R/I \subseteq S/J$ is an integral extension.
(b) $W^{-1}R \subseteq W^{-1}S$ is an integral extension.

Proof: (a) Let $\overline{b} = b + J \in S/J$ with $b \in S$. b satisfies an equation $b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$ where $a_i \in R$ and $n > 0$. Thus $\overline{b}^n + \overline{a}_{n-1}\overline{b}^{n-1} + \dots + \overline{a}_0 = 0$ in S/J with $\overline{a}_i = a_i + I \in R/I$.
(b) Let $b/s \in W^{-1}S$ where $b \in S$ and $s \in W \subseteq R$. b is integral over R, thus $b^n + a_{n-1}b^{n-1} + \dots + a_0 = 0$ for $n > 0$ and some $a_i \in R$. Then $(b/s)^n + (a_{n-1}/s)(b/s)^{n-1} + \dots + (a_0/s^n) = 0$ where $a_i/s^{n-i} \in W^{-1}R$. b/s is integral over $S^{-1}R$.

(5.13) Proposition: Let $R \subseteq S$ be an extension of rings, $W \subseteq R$ a multiplicative subset. If R is integrally closed in S, then $W^{-1}R$ is integrally closed in $W^{-1}S$.

Proof: Let $b \in S$, $s \in W$ with b/s integral over $W^{-1}R$. Then there are $\alpha_i \in W^{-1}R$ and $n \in \mathbb{N}$, $n > 0$, so that (*) $(b/s)^n + \alpha_{n-1}(b/s)^{n-1} + \dots + \alpha_0 = 0$. Write $\alpha_i = a_i/s_i$ with $a_i \in R$ and $s_i \in W$ 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: $0 = (t_n b^n + a_{n-1}t_{n-1}b^{n-1} + \dots + a_0 t_0)/1 \in W^{-1}S$. Thus there is an element $v \in W$ so that (**) $v(t_n b^n + a_{n-1}t_{n-1}b^{n-1} + \dots + a_0 t_0) = 0$ in S. Multiply (**) by r^{n-1} where $r = vt_n \in W$. Then $(rb)^n + a_{n-1}(rb)^{n-1} + \dots + a_0 t_0 r^{n-1} = 0$. Since R is

integrally closed in S, $rb \in R$ and thus $b/s = (rb)/(rs) \in W^{-1}R$.

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

(5.15) Corollary: Let R be an integral domain. R is normal if and only if R_m is normal for all $m \in m\mathrm{Spec}(R)$.

Proof: "$\Longrightarrow$": By (5.14)

"$\Longleftarrow$": By (1.66) $R = \bigcap_{m \in m\mathrm{Spec}(R)} R_m$. If $x \in Q(R)$ is integral over R, then x is integral over R_m for all $m \in m\mathrm{Spec}(R)$. Thus $x \in R_m$ for all $m \in m\mathrm{Spec}(R)$ and $x \in R$.

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

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

(5.17) Lemma: Let R be a domain, $K = Q(R)$ its field of quotients, and $K \subseteq L$ an algebraic field extension. Let S denote the integral closure of R in L. Then:

(a) $Q(S) = L$, that is, L is the field of quotients of S.

(b) The K-vector space L has a basis consisting of elements of S.

Proof: (a) Let $\alpha \in L$. By assumption α is algebraic over K and by (5.16) there is an element $t \in R-(0)$ with $t\alpha$ integral over R. Thus $t\alpha \in S$ and $\alpha \in Q(S)$, since $R \subseteq S$.

(b) Let $\{\alpha_i\}_{i \in I}$ be a basis of L over K. For each $i \in I$ there is an element $t_i \in R-(0)$ with $t_i\alpha_i \in S$. $\{t_i\alpha_i\}_{i \in I}$ is a basis of L over K.

Let $K \subseteq L$ be a finite field extension. For every $\alpha \in L$ the map $l_\alpha : L \to L$ with $l_\alpha(\beta) = \alpha\beta$ for all $\beta \in L$ defines a K-linear operator on 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) Theorem: Let R be a normal domain, $K = Q(R)$ its field of quotients, and $K \subseteq L$ a finite field extension. For an element $\alpha \in L$ the following are equivalent:

(a) α is integral over R.

(b) $m(\alpha, x) \in R[x]$

(c) $P_{L/K}(\alpha, x) \in R[x]$

Proof: $m(\alpha, x)$ is monic and $P_{L/K}(\alpha, x)$ has leading coefficient $(-1)^r$. Hence (b) $\Rightarrow$ (a) and (c) $\Rightarrow$ (a)

(a) $\to$ (b): Let $f = m(\alpha, x) \in K[x]$ and $h \in R[x]$ monic with $h(\alpha) = 0$. By definition of the minimal polynomial there is a polynomial $g \in K[x]$ with $h = fg$. 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 $\overline{R}$ be the integral closure of R in $\overline{K}$. Since $h(\alpha_j) = 0$ for all $1 \leq j \leq n$ and $h(x) \in R[x]$ monic, $\alpha_j \in \overline{R}$ for all $1 \leq j \leq n$. The coefficients of f are elementary symmetric functions in α_j $(1 \leq j \leq n)$. Hence the coefficients of f are in $\overline{R} \cap K$. Since R is normal, $\overline{R} \cap K = R$.

(a) $\to$ (c): It is known that $P_{L/K}(\alpha, x) \mid m(\alpha, x)^r$ for some $r \in \mathbb{N}$. Let $h \in R[x]$ be a monic polynomial 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 R be a factorial domain, $K = Q(R)$ its field of quotients and $d \in R$ a square free element of R, that is, $d = p_1 \cdots p_r$ where p_i are prime elements of R with $p_i \notin (p_j)$ if $i \neq j$. Suppose that 2 is a prime element in R and let S denote the integral closure of R in $L = K(\sqrt{d}) \neq K$. 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 $a+b\sqrt{d} \in S$?

By (5.18) $a+b\sqrt{d} \in S \iff m(a+b\sqrt{d}, x) \in R[x]$. 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 $a+b\sqrt{d} \in S \iff 2a \in R$ and $a^2 - b^2 d \in R$.

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

Pf of cl.: If $a+b\sqrt{d} \in S$ with $b \neq 0$, then $2a, a^2 - b^2 d \in R$. Thus $(2b)^2 d \in R$. Suppose that $b = u/v$ with $u, v \in R$ relatively prime. If $p \in R$ 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 $2b \in R$. Similarly, if $a \in R$, then $b \in R$ and if $b \in R$, then $a \in R$.

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

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

Suppose $a, b \in \mathbb{Z} - (2)$. Then $a^2 - b^2 d \equiv 0 \pmod 4$ and $(a/2)^2 - (b/2)^2 d \in \mathbb{Z}$. Then $S = \mathbb{Z}[1/2 + 1/2\sqrt{d}] = \{a + b(1/2 + 1/2\sqrt{d}) \mid a,b \in \mathbb{Z}\}$.

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

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

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

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

§2: GOING-UP AND GOING-DOWN

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

Proof: "$\Rightarrow$": The field extension $R \subseteq Q(S)$ is algebraic. Hence every intermediate ring $R \subseteq T \subseteq Q(S)$ is a field and S is a field.
"$\Leftarrow$": Let $a \in R-(0)$. Since S is a field, $a^{-1} \in S$ and there are $a_i \in R$ such that $(a^{-1})^n + a_{n-1}(a^{-1})^{n-1} + \dots + a_0 = 0$ implying $a^{-1} = -(a_{n-1} + a_{n-2}a + \dots + a_0 a^{n-1}) \in R$ and R is a field.

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

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

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

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

$$\begin{array}{ccc} S & \xrightarrow{i_{S,W}} & W^{-1}S \\ \text{integral} \uparrow & & \uparrow \text{integral} \\ R & \xrightarrow{i_{R,W}} & R_P = W^{-1}R \end{array}$$

Let $m \subseteq W^{-1}S$ be a maximal ideal. By (c) $n = m \cap W^{-1}R$ is a maximal ideal of R_P and $n = PR_P$. The ideal $Q = i^{-1}_{S,W}(m)$ is a prime ideal of S which lies over $P \subseteq R$.

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

(5.24) Corollary: (Going-up) Let $R \subseteq S$ be an integral extension of rings and $P_0 \subseteq P_1 \subseteq \dots \subseteq P_r$ a chain of prime ideals of R. Let $Q_0 \subseteq S$ be a prime ideal which lies over P_0. Then Q_0 extends to a chain of prime ideals $Q_0 \subseteq Q_1 \subseteq \dots \subseteq Q_r$ in S with $Q_i \cap R = P_i$ for all $0 \leq i \leq r$.

Proof: We only have to show: If $P_0 \subseteq P_1$ are prime ideals of R and $Q_0 \in \operatorname{Spec}(S)$ with $Q_0 \cap R = P_0$, then there is a prime ideal $Q_1 \subseteq S$ with $Q_0 \subseteq Q_1$ and $Q_1 \cap R = P_1$. Consider the integral extension $R/P_0 \subseteq S/Q_0$. By (5.22) there is a prime ideal $\overline{Q_1} \subseteq S/Q_0$ with $\overline{Q_1} \cap R/P_0 = P_1/P_0$. Let Q_1 be the contraction of $\overline{Q_1}$ to S. Then $Q_0 \subseteq Q_1$ and $Q_1 \cap R = P_1$.

(5.25) Corollary: Let $R \subseteq S$ be an integral extension of rings. Then:

(a) $\dim R = \dim S$

(b) If $Q \in \operatorname{Spec}(S)$ and $P = R \cap Q$, then $ht\, P \geq ht\, Q$.

(c) If $Q \in \operatorname{Spec}(S)$ and $P = R \cap Q$, then $\dim R/P = \dim S/Q$.

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

(b) By (5.23).

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

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

Proof: With $W = R - P$ the extension $W^{-1}R = R_P \subseteq W^{-1}S$ is integral. By (5.25) $r = ht\, P = \dim R_P = \dim W^{-1}S$. Let $\tilde{Q} \subseteq W^{-1}S$ be a prime ideal with $ht\, \tilde{Q} = r$. $\tilde{Q}$ is maximal in $W^{-1}S$ and thus $\tilde{Q} \cap R_P = PR_P$. Let $Q \in \mathrm{Spec}(S)$ with $QW^{-1}S = \tilde{Q}$. Then $ht\, Q = ht\, \tilde{Q} = r$ and $P = Q \cap R$.

(5.27) Notation: If $\varphi: R \longrightarrow S$ is a morphism of rings and $I \subseteq S$ an ideal, we set $I \cap R := \varphi^{-1}(I)$ (although R may not be contained in S).

(5.28) Lemma: Let $\varphi: R \longrightarrow S$ be a morphism of rings and $P \subseteq R$ a prime ideal. There is a prime ideal $Q \subseteq S$ with $\varphi^{-1}(Q) = P$ if and only if $\varphi^{-1}(\varphi(P)S) = P$.

Proof: "$\Longrightarrow$": Obvious, since $\varphi(P)S \subseteq Q$.
"$\Longleftarrow$": Set $W = R - P$. Then $P \cap W = \varphi^{-1}(\varphi(P)S) \cap W = \emptyset$, hence $\varphi(P)S \cap \varphi(W) = \emptyset$ and $\varphi(P)W^{-1}S$ is a proper ideal. Let m be a maximal ideal of $W^{-1}S$ containing $\varphi(P)W^{-1}S$. Then $m \cap W^{-1}R = PR_P$. Moreover, $Q = m \cap S$ is a prime ideal with $Q \cap R = (m \cap S) \cap R = m \cap R = m \cap W^{-1}R \cap R = pR_P \cap R = P$.

(5.29) Lemma: Let R be a domain with quotient field $K = Q(R)$ and $K \subseteq L$ an algebraic field extension. If S is the integral closure of R in L and $\sigma \in \mathrm{Aut}_K(L)$, then $\sigma(S) \subseteq S$.

Proof: If $\alpha \in S$ and $f(x) \in R[x]$ a monic polynomial with $f(\alpha) = 0$, then $\sigma(f(\alpha)) = f(\sigma(\alpha)) = 0$ and $\sigma(\alpha) \in S$.

(5.30) Lemma: Let $R \subseteq S$ be an integral extension, R and S domains, R normal, and

$K=Q(R)$ the quotient field of R. Let $P\subseteq R$ be a prime ideal, $\alpha\in PS$, and $f(x)=m(x,\alpha)$ the minimal polynomial of α over K. The coefficients of $f(x)$ are in P, except for the highest one.

Proof: By (5.18) $f(x)=m(\alpha,x)\in R[x]$. After a finite extension of $Q(S)$ and replacing S by the integral closure of R in that extension field, we may assume that $f(x)=\prod_{i=1}^{n}(x-\alpha_i)$ where $\alpha_1=\alpha$ and $\alpha_i\in S$ for all $1\leq i\leq n$. Moreover, with $L=Q(S)$ there are $\sigma_i\in Aut_K(L)$ with $\sigma_i(\alpha)=\alpha_i$. Then $\alpha_i=\sigma_i(\alpha)\in PS$ and the coefficients of $f(x)$ are in $PS\cap K=PS\cap R=P$, since R is normal.

(5.31) Theorem: (Going down) Let R be a normal domain, $K=Q(R)\subseteq L$ an algebraic field extension and S the integral closure of R in L. If $P_0\subseteq P_1\subseteq\dots\subseteq P_r$ is a chain of prime ideals of R and $Q_r\subseteq S$ a prime ideal with $Q_r\cap R=P_r$, then there is a chain of prime ideals $Q_0\subseteq Q_1\subseteq\dots\subseteq Q_r$ in S with $Q_i\cap R=P_i$ for all $0\leq i\leq r$.

Proof: It suffices to show: if $P_0\subseteq P_1$ are prime ideals of R and $Q_1\subseteq S$ a prime ideal with $Q_1\cap R=P_1$, then there is a prime ideal $Q_0\subseteq S$ with $Q_0\subseteq Q_1$ and $Q_0\cap R=P_0$. Consider the ring extension $R_{P_1}\hookrightarrow S_{Q_1}$. (Note that in general, S_{Q_1} is not integral over R_{P_1}.) We want to show that there is a prime ideal $\tilde{Q}_0\subseteq S_{Q_1}$ lying over $P_0R_{P_1}$. Then with $Q_0=\tilde{Q}_0\cap S$, $Q_0\cap R=\tilde{Q}_0\cap R_{P_1}\cap R=P_0R_{P_1}\cap R=P_0$ and $Q_0\subseteq Q_1$.

By Lemma (5.28) it suffices to show that $P_0S_{Q_1}\cap R_{P_1}=P_0R_{P_1}$, or equivalently, $P_0S_{Q_1}\cap R=P_0$. Let $0\neq z=y/t\in P_0S_{Q_1}\cap R$ where $y\in P_0S$ and $t\in S-Q_1$. By (5.30) the minimal polynomial of y over K is of the form $x^n+a_1x^{n-1}+\dots+a_n=0$ where $a_i\in P_0$. Since $z\in R$, $K(t)=K(y)$ and $x^n+a_1/z\,x^{n-1}+\dots+a_n/z^n=0$ is the minimal polynomial of t over K. Since $t\in S$, by (5.18) $a_i/z^i\in R$ for all $1\leq i\leq n$. With $b_i=a_i/z^i\in R$, $t^n+b_1t^{n-1}+\dots+b_n=0$ and $z^ib_i=a_i\in P_0$. If $z\notin P_0$, then $b_i\in P_0$ for all $1\leq i\leq n$ and hence $t^n\in P_0S\subseteq P_1S\subseteq Q_1$ and $t\in Q_1$, a contradiction.

(5.32) Corollary: Let $R \subseteq S$ be an integral extension, R and S domains, and R normal. Then 'going-down' holds, that is, if $P_0 \subseteq P_1$ are prime ideals of R and $Q_1 \subseteq S$ is a prime ideal with $Q_1 \cap R = P_1$, then there is a prime ideal $Q_0 \subseteq S$ with $Q_0 \subseteq Q_1$ and $Q_0 \cap R = P_0$.

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 $\sigma \in \mathrm{Aut}_K(\overline{K})$, $\sigma|_L \in \mathrm{Aut}_K(L)$, that is, $\sigma(L) \subseteq L$.

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

(5.33) Proposition: Let R be a normal domain, $K = Q(R)$ its field of quotients, and $K \subseteq L$ a finite normal field extension. Let S be the integral closure of R in L, and let $P \in \mathrm{Spec}(R)$, $Q_1, Q_2 \in \mathrm{Spec}(S)$ be prime ideals with $Q_1 \cap R = Q_2 \cap R = P$. 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 $Q \in S$ lying over $P \subseteq R$.

Proof: Set $G = \mathrm{Aut}_K(L) = \{\sigma_1, \ldots, \sigma_r\}$ with $\sigma_1 = \mathrm{id}_L$. Each σ_j defines by restriction an an automorphism of S with $\sigma_j(Q) \in \mathrm{Spec}(S)$ for all $Q \in \mathrm{Spec}(S)$. Let $P \in \mathrm{Spec}(R)$ and $Q_1, Q_2 \in \mathrm{Spec}(S)$ as above. Suppose $Q_2 \neq \sigma_j^{-1}(Q_1)$ for all $1 \leq j \leq r$. By (5.22)(b), $Q_2 \not\subseteq \sigma_j^{-1}(Q_1)$ for all $1 \leq j \leq r$. Thus $Q_2 \not\subseteq \bigcup_{j=1}^{r} \sigma_j^{-1}(Q_1)$. 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 $\mathrm{char}(K) = p$ and ν is given by: 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 hence $y \in K$. Moreover, $y \in K$ is integral over R and thus $y \in R$, since R is normal. Note that $\sigma_1(x) = x$ and that y is a multiple of x. Hence $y \in Q_2 \cap R = P = Q_1 \cap R$ and $[\prod_{j=1}^{r} \sigma_j(x)]^q \in Q_1$. Thus $\sigma_j(x) \in Q_1$ for some $1 \leq j \leq r$, a contradiction. Hence $Q_2 = \sigma_j^{-1}(Q_1)$ for some $1 \leq j \leq r$.

(5.34) Remark: Let R be a normal domain, $Q(R) = K$ 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 S_L be the integral closure of R in L and S_E the integral closure of R in E. For every $P \in \operatorname{Spec}(R)$ there are only finitely many $\tilde{Q} \in \operatorname{Spec}(S_E)$ lying over P. Thus there are only finitely many $Q \in \operatorname{Spec}(S_L)$ lying over P.
If R is a non-normal domain, $\overline{R}$ the integral closure of R in $Q(R)$, we may ask again if there are only finitely many prime ideals $Q \subseteq \overline{R}$ which lie over a given prime ideal $P \in \operatorname{Spec}(R)$. The Mori-Nagata theorem shows that this is the case provided that R is a Noetherian domain.

§3: A NORMALIZATION THEOREM

(5.35) **Theorem**: (Noether normalization theorem) Let k be a field, $R = k[x_1, \dots, x_n]/\mathfrak{J}$ a finitely generated k-algebra, and $I \subsetneq R$ an ideal with $I \neq R$. Then there are integers $\delta \leq d$ and elements $y_1, \dots, y_d \in R$ such that:

(a) $y_1, \dots, y_d$ are algebraically independent over k, that is, the natural map from the polynomial ring $\varphi: k[t_1, \dots, t_d] \longrightarrow R$ defined by $\varphi(t_i) = y_i$ and $\varphi|_k = \mathrm{id}_k$ is injective.

(b) R is a finitely generated $k[y_1, \dots, y_d]$-module.

(c) $I \cap k[y_1, \dots, y_d] = (y_{\delta+1}, \dots, y_d)$.

If k is an infinite field, then in addition

(d) For all $1 \leq i \leq \delta$ the elements $y_i \in R$ can be chosen so that $y_i = \sum_{j=1}^{n} a_{ij}(x_j + \mathfrak{J})$ for some $a_{ij} \in k$.

The proof requires a lemma:

(5.36) **Lemma**: Let k be a field, $x_1, \dots, x_n$ variables over k, and $F \in k[x_1, \dots, x_n] - k$.

(a) By a substitution of the form $x_i = y_i + x_n^{r_i}$ for $1 \leq i \leq n-1$ and suitable $r_i \in \mathbb{N}$, F can be written as $F = a x_n^m + g_1 x_n^{m-1} + \dots + g_m$ where $m > 0$, $a \in k^*$, and $g_i \in k[y_1, \dots, y_{n-1}]$ for $1 \leq i \leq m$.

(b) If k is an infinite field, the same result as in (a) can be achieved by substituting $x_i = y_i + a_i x_n$ with suitable $a_i \in k$.

Proof: Let $F = \sum a_{(\nu)} x_1^{\nu_1} \cdots x_n^{\nu_n}$ with $(\nu) = (\nu_1, \dots, \nu_n)$ and $a_{(\nu)} \in k$.

(a) Replacing x_i by $x_i = y_i + x_n^{r_i}$, F can be written as a polynomial in $y_1, \dots, y_{n-1}, x_n$:

$$F = \sum a_{(\nu)} (x_n^{r_1} + y_1)^{\nu_1} \cdots (x_n^{r_{n-1}} + y_{n-1})^{\nu_{n-1}} x_n^{\nu_n}$$

$$= \sum a_{(\nu)} \left[x_n^{\nu_n + \nu_1 r_1 + \dots + \nu_{n-1} r_{n-1}} + \text{terms of lower degree in } x_n \right]$$

Let $q - 1 = \max\{\nu_i \mid F \text{ contains a coefficient } a_{(\nu_1, \dots, \nu_i, \dots, \nu_n)} \neq 0\}$ and set $r_i = q^i$. For all $(\nu) = (\nu_1, \dots, \nu_n)$, $(\mu) = (\mu_1, \dots, \mu_n) \in \mathbb{N}^n$ with $a_{(\nu)} \neq 0$, $a_{(\mu)} \neq 0$, and $(\nu) \neq (\mu)$ it follows that $\nu_n + \nu_1 q + \dots + \nu_{n-1} q^{n-1} \neq \mu_n + \mu_1 q + \dots + \mu_{n-1} q^{n-1}$. Hence with

$m = \max\{\nu_n + \nu_1 q + \cdots + \nu_{n-1} q^{n-1} \mid a_{(\nu_1,\ldots,\nu_n)} \neq 0\}$; F can be written as a polynomial in $y_1, \ldots, y_{n-1}, x_n$ of the form $F = a x_n^m +$ terms of lower degree in x_n, where $a \in k^*$.

(b) Write $F = F_0 + \ldots + F_m$ where F_i is a homogeneous polynomial of degree i and $F_m \neq 0$. Substitute $x_i = y_i + a_i x_n$ for $1 \leq i \leq n-1$, then

$$F_m = \sum_{|\nu|=m} a_{(\nu)} (y_1 + a_1 x_n)^{\nu_1} \cdots (y_{n-1} + a_{n-1} x_n)^{\nu_{n-1}} x_n^{\nu_n}$$
$$= F_m(a_1, \ldots, a_{n-1}, 1)\, x_n^m + \text{terms of lower degree in } x_n.$$

Since $F_m \neq 0$, $F_m(x_1, \ldots, x_{n-1}, 1) \neq 0$ and there are $a_1, \ldots, a_{n-1} \in k$ with $F_m(a_1, \ldots, a_{n-1}, 1) \neq 0$ since k is infinite. Then $F(y_1, \ldots, y_{n-1}, x_n) = F_m(a_1, \ldots, a_{n-1}, 1)\, x_n^m +$ terms of lower degree in x_n and $F_m(a_1, \ldots, a_{n-1}, 1) = a \neq 0$.

Proof of (5.35): We first prove the case where I is a principal ideal and $R = k[x_1, \ldots, x_n]$ is the polynomial ring.

Case 1: $R = k[x_1, \ldots, x_n]$ and $I = (F)$, F a nonconstant polynomial.

By (5.34) there are integers $r_i \in \mathbb{N}$ (or elements $a_i \in k$, if k is infinite) such that with $x_i = y_i + x_n^{r_i}$ (or $x_i = y_i + a_i x_n$) $F = a x_n^m + g_1 x_n^{m-1} + \cdots + g_m$, where $a \in k^*$ and $g_i \in k[y_1, \ldots, y_{n-1}]$. Consider the homomorphism of rings: $\varphi : k[y_1, \ldots, y_{n-1}, y_n] \longrightarrow k[x_1, \ldots, x_n]$ defined by $\varphi|_k = \mathrm{id}_k$, $\varphi(y_i) = x_i - x_n^{r_i}$ (or $\varphi(y_i) = x_i - a_i x_n$) for $1 \leq i \leq n-1$ and $\varphi(y_n) = F$. Note that $R = k[y_1, \ldots, y_{n-1}, x_n]$ and that x_n is integral over $k[y_1, \ldots, y_n]$ since $a x_n^m + g_1 x_n^{m-1} + \cdots + g_m - y_n = 0$, where $g_i \in k[y_1, \ldots, y_{n-1}]$. This implies that $\dim(k[y_1, \ldots, y_n]/\ker\varphi) = \dim R = n$. Thus $\ker(\varphi) = 0$ and $y_1, \ldots, y_n$ are algebraically independent over k (as elements of R). Let $\overline{\varphi} = \pi\varphi$ denote the composition map where $\pi : R \longrightarrow R/(F)$ is the natural map. $R/(F)$ is integral over $k[y_1, \ldots, y_n]/\ker\overline{\varphi}$ and thus $\dim k[y_1, \ldots, y_n]/\ker\overline{\varphi} = \dim R/(F) = n-1$. Since (y_n) is a prime ideal of height one and $(y_n) \subseteq \ker\overline{\varphi}$, by dimension reasons $\ker\overline{\varphi} = (y_n)$ and thus $(F) \cap k[y_1, \ldots, y_n] = (y_n)$.

Case 2: Assume that $R = k[x_1, \ldots, x_n]$ and that $I \subseteq R$ is any ideal with $I \neq R$. The proof is by induction on n. We may assume that $I \neq (0)$ and take $F \in I - (0)$. By the first case there are $y_1, \ldots, y_n \in R$ with $y_n = F$ so that the ring extension

$k[y_1,\dots,y_n] \subseteq R$ is finite. If k is infinite, $y_1,\dots,y_{n-1}$ can be chosen to be linear combinations of $x_1,\dots,x_n$ (over k). Apply the induction hypothesis to $k[y_1,\dots,y_{n-1}]$ and the ideal $I \cap k[y_1,\dots,y_{n-1}]$. Then there are elements $t_1,\dots,t_{n-1} \in k[y_1,\dots,y_{n-1}]$ such that:

(i) $k[y_1,\dots,y_{n-1}]$ is a finite $k[t_1,\dots,t_{n-1}]$-module.

(ii) $I \cap k[t_1,\dots,t_{n-1}] = (t_{\delta+1},\dots,t_{n-1})$ for some $\delta \leq n-1$.

(iii) If k is infinite, then for $1 \leq i \leq \delta$: $t_i = \sum_{j=1}^{n-1} b_{ij} y_j$ where $b_{ij} \in k$.

This implies that $R = k[x_1,\dots,x_n]$ is a finite $k[t_1,\dots,t_{n-1},y_n]$-module. In particular, $t_1,\dots,t_{n-1},y_n$ are algebraically independent over k. Let $f \in I \cap k[t_1,\dots,t_{n-1},y_n]$, then $f = g + h y_n$ where $g \in k[t_1,\dots,t_{n-1}]$ and $h \in k[t_1,\dots,t_{n-1},y_n]$. Since $y_n \in I$, it follows that $g \in I \cap k[t_1,\dots,t_{n-1}] = (t_{\delta+1},\dots,t_{n-1})$ and hence $f \in (t_{\delta+1},\dots,t_{n-1},y_n)$. If k is infinite, $y_1,\dots,y_{n-1}$ are linear combinations of $x_1,\dots,x_n$. Thus for $1 \leq i \leq \delta$, t_i is a linear combination of $x_1,\dots,x_n$.

Case 3: $R = k[x_1,\dots,x_n]/J$ and $I \subseteq R$ any ideal.

First apply case 2 to $k[x_1,\dots,x_n]$ and the ideal J. Hence there is a subalgebra $k[y_1,\dots,y_n] \subseteq k[x_1,\dots,x_n]$ such that $k[x_1,\dots,x_n]$ is a finite $k[y_1,\dots,y_n]$-module and $J \cap k[y_1,\dots,y_n] = (y_{d+1},\dots,y_n)$. If k is infinite, for $1 \leq i \leq d$ the y_i are linear combinations of $x_1,\dots,x_n$. Moreover, R is a finite $k[y_1,\dots,y_d]$-module. Let $I' = I \cap k[y_1,\dots,y_d]$. By case 2 there is a subalgebra $k[t_1,\dots,t_d] \subseteq k[y_1,\dots,y_d]$ so that $k[y_1,\dots,y_d]$ is a finite $k[t_1,\dots,t_d]$-module and $I' \cap k[t_1,\dots,t_d] = (t_{\delta+1},\dots,t_d)$. If k is infinite, for $1 \leq i \leq d$, t_i is a linear combination of $y_1,\dots,y_d$. Then R is a finite $k[t_1,\dots,t_d]$-module and $I \cap k[t_1,\dots,t_d] = (t_{\delta+1},\dots,t_d)$. If k is infinite, for $1 \leq i \leq \delta$, t_i is a linear combination of $x_1,\dots,x_n$.

(5.37) Corollary: Let k be a field and R a finitely generated k-algebra. Then there exists a polynomial ring $k[x_1,\dots,x_d] \subseteq R$ with R integral over $k[x_1,\dots,x_d]$. Furthermore $\dim R = d$. If, in addition, R is a domain, then $\dim R = d = \operatorname{trdeg}_k R$.

§4: DISCRETE VALUATION RINGS; DEDEKIND DOMAINS

(5.38) 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) $v(x) = \infty \iff x = 0$

(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 $v(K) = \{0, \infty\}$.

(5.39) Remark: (a) There is a more general concept of valuations where the value group $\mathbb{Z}$ is replaced by an 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 be 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 $v(K^*) = \mathbb{Z}$.

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

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

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

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

(c) $m_v = \{x \in K \mid v(x) > 0\}$ is the only maximal ideal of R_v, that is, R_v is a local domain.
(d) R_v is a principal ideal domain. v is trivial if and only if $R_v = K$.
(e) The prime elements of R_v are the elements $p \in R_v$ with $v(p) = 1$. All prime elements of R_v are associated and m_v is generated by any prime element $p \in R_v$.

Proof: Note that $v(1) = v(1) + v(1)$, thus $v(1) = 0$ and $0 = v(1) = v(-1) + v(-1)$ and also $v(-1) = 0$.
(a) easy
(b) $a \in R_v^* \iff v(a) \geq 0$ 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 $a^{-1} \in R_v$.
(c) Obviously, $m_v \subseteq R_v$ is an ideal. Since $R_v^* = R_v - m_v$, m_v is a maximal ideal of R_v and R_v is local.
(d) Let $I \subseteq R_v$ 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 $b/a \in R_v$. Thus $I = (a)$.
(e) By (d) m_v is generated by any element $p \in R_v$ with $v(p) = 1$. In particular, if $p \in R_v$ with $v(p) = 1$, then p is a prime element. If $q \in m_v$ is a second element with $v(q) = 1$, then $v(p/q) = 0$ and $p/q \in R_v^*$. Hence p and q are associated.

(5.42) Definition: (a) A local principal ideal domain, which is not a field, is called a discrete valuation ring (DVR).
(b) Let K be a field, $v: K \longrightarrow \mathbb{Z} \cup \{\infty\}$ a nontrivial discrete valuation of K. The ring R_v is called the discrete valuation ring associated to v.

(5.43) Theorem: Let R be a DVR, $p \in R$ a prime element, and $K = Q(R)$ its quotient field.
(a) Every element $x \in K^*$ is of the form $x = up^n$ with $u \in R^*$ 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 $x = up^n$, $u \in R^*$, $n \in \mathbb{Z}$, is a discrete valuation of K with $v(K^*) = \mathbb{Z}$ and $R_v = R$.

Proof: Since R is a local PID, R has exactly one nonzero prime ideal $P \subseteq R$. Moreover, P is generated by a prime element $p \in R$ and every other prime element $q \in R$ is associated to p.
(a) Let $x \in K^*$. Then $x = a/b$ with $a, b \in R$. There are units $u, v \in R^*$ 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 $q \in R$ is associated to p, the exponent $n-m$ is independent of the choice of p.
(b) Obvious

(5.44) Corollary: Let K be a field. Then there is a one-to-one correspondence:
$\{ v$ a discrete valuation of K with $v(K^*) = \mathbb{Z} \} \cong \{ R \subseteq K$ a DVR with $Q(R) = K \}$.

(5.45) Theorem: (Characterization of DVRs) Let (R, m) be a local Noetherian domain. The following are equivalent:
(a) R is a DVR.
(b) R is normal and $\dim R = 1$.
(c) R is normal and there is an $a \in R - (0)$ with $m \in \mathrm{Ass}_R(R/(a))$.
(d) m is a nonzero principal ideal.
(e) R is not a field, R is factorial, and all prime elements of R are associated.

Proof: (a) $\Rightarrow$ (b): R is a PID, thus R is normal with $\dim R = 1$.
(b) $\Rightarrow$ (c): For all $a \in m - (0)$, $\mathrm{Supp}_R(R/aR) = \{m\}$ and $m \in \mathrm{Ass}_R(R/(a))$.
(c) $\Rightarrow$ (d): Let $a \in R - (0)$ with $m \in \mathrm{Ass}_R(R/(a))$ and let $\bar{b} \in R/(a)$ with $\mathrm{ann}_R(\bar{b}) = m$. with $b \in R$ a preimage of $\bar{b}$, $b \notin aR$ and $mb \subseteq aR$. Thus $mba^{-1} \subseteq R$ and mba^{-1} is an ideal of R. We claim that $mba^{-1} = R$. If $mba^{-1} \neq R$, then $mba^{-1} \subseteq m$ and therefore $m(ba^{-1})^2 \subseteq m(ba^{-1}) \subseteq m$ 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 $(ba^{-1})^n \subseteq Ra^{-1} \subseteq K$ for all $n \in \mathbb{N}$. Ra^{-1} is a finite (cyclic) R-submodule of K. Hence the R-algebra $R[ba^{-1}]$ is contained in the finite faithful R-module Ra^{-1}. By (5.2) ba^{-1} is integral over R. Since R is normal, $ba^{-1} \in R$ and hence $b \in aR$, a contradiction. Thus $mba^{-1} = R$ and $m = (ab^{-1})R$ with $ab^{-1} \in R$.

(d) $\Rightarrow$ (e): Set $m=(p)$ and let $a \in R-(0)$ be any element. Since R is a local Noetherian ring, 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 $u \in R^*$. Note that p is a prime element of R. Every element of R can be written (uniquely) as a product of a unit of R and a power of p. Thus R is factorial and all prime elements of R are associated.

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

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

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

(5.48) Theorem: Let R be a Dedekind domain.

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

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

Proof: (a) Let $I = Q_1 \cap \dots \cap Q_r$ be a shortest primary decomposition of I where $Q_i \subseteq R$ are m_i-primary with $m_i \neq m_j$ for $i \neq j$. Since $\dim R = 1$, all the m_i are maximal ideals of R. Let $\varphi_i : R \to R_{m_i}$ be the natural maps. Then $Q_i = \varphi_i^{-1}(Q_i R_{m_i})$. R_{m_i} is a DVR and therefore $Q_i R_{m_i} = m_i^{t_i} R_{m_i}$. Because m_i is maximal, the ideal $m_i^{t_i}$ is m_i-primary and $Q_i = m_i^{t_i}$. This shows that $I = m_1^{t_1} \cap \dots \cap m_r^{t_r}$ and by the Chinese remainder theorem $I = m_1^{t_1} \dots m_r^{t_r}$. 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) Let $a \in I-(0)$. Then there are maximal ideals $m_i \subseteq R$ with $m_i \neq m_j$ for $i \neq j$ so that $I = m_1^{t_1} \cdots m_r^{t_r}$ and $(a) = m_1^{s_1} \cdots m_e^{s_e}$ with $l \geq r$ and $s_i \geq t_i$ for $i \leq r$. Set $t_i = 0$ for $i > r$ and $J = m_1^{s_1 - t_1} \cdots m_e^{s_e - t_e}$. Then $IJ = (a)$.

(5.49) Remark: In general a Dedekind domain is not factorial. For 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 $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

(5.50) Theorem: Let R be a Noetherian domain. The following are equivalent:

(a) R is normal.

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

(c) For every height one prime ideal $P \subseteq R$ the ring R_P is a DVR and $R = \bigcap_{P \text{ prime}, \mathrm{ht} P = 1} R_P$.

Proof: (a) $\Rightarrow$ (b): Since R is normal, R_P is normal for all $P \in \mathrm{Spec}(R)$. Thus R_P is a DVR for all $P \in \mathrm{Spec}(R)$ with $\mathrm{ht} P = 1$. Let $a \in R-((0) \cup R^*)$ and $P \in \mathrm{Ass}_R(R/(a))$. Then $PR_P \in \mathrm{Ass}_{R_P}(R_P/aR_P)$. By (5.45) R_P is a DVR. Hence $\mathrm{ht} P = 1$ and P is a minimal associated prime of (a).

(b) $\Rightarrow$ (c): Obviously, $R \subseteq \bigcap_{P \in \mathrm{Spec}(R), \mathrm{ht} P = 1} R_P$. Let $x = b/a \in Q(R)$, $a, b \in R$, $a \neq 0$, with $x \in R_P$ for all $P \in \mathrm{Spec}(R)$ with $\mathrm{ht} P = 1$. Then $b \in aR_P$ for all prime ideals P of height one. By (b), $b \in aR_P$ for all $P \in \mathrm{Ass}_R(R/(a))$. For all $P \in \mathrm{Ass}_R(R/aR)$ let $s_P \in R-P$ and $c_P \in R$ with $b = a c_P/s_P$. Consider the ideal $I = (a):(b) = \{y \in R \mid yb \in (a)\}$. Then $s_P \in I$ for all $P \in \mathrm{Ass}_R(R/(a))$ and $I \notin \bigcup_{P \in \mathrm{Ass}(R/(a))} P$. Let $Q \in \mathrm{Ass}_R((b)+(a)/(a))$. Since $\mathrm{ann}_R((b)+(a)/(a)) = I$, $I \subseteq Q$. On the other hand $(b)+(a)/(a) \subseteq R/(a)$ and therefore $\mathrm{Ass}_R((b)+(a)/(a)) \subseteq \mathrm{Ass}_R(R/(a))$. This shows that $\mathrm{Ass}_R((b)+(a)/(a)) = \emptyset$ and $(b)+(a)/(a) = (0)$. Hence $b \in (a)$ and $x = b/a \in R$.

(c) $\Rightarrow$ (a): Since R is an intersection of normal domains, R is normal.

§5: THE KRULL-AKIZUKI THEOREM

(5.51) Proposition: Let R be a Noetherian ring with $\mathrm{Spec}(R) = m\mathrm{Spec}(R)$. Every finite R-module has finite length, in particular, R has finite length.

Proof: Let M be a finite R-module. By (2.16) there is a normal series of M: $(0) = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M$ with $M_i/M_{i-1} \cong R/P_i$ where $P_i \in \mathrm{Spec}(R)$ for all $1 \leq i \leq n$. Since $P_i \in m\mathrm{Spec}(R)$ the modules M_i/M_{i-1} are simple.

(5.52) Proposition: Let R be a ring. The following are equivalent:

(a) R is Noetherian and every prime ideal of R is maximal.

(b) Every finite R-module has finite length.

(c) R has finite length (as an R-module).

Proof: (a) $\Rightarrow$ (b): By (5.51) and (b) $\Rightarrow$ (c): trivial

(c) $\Rightarrow$ (a): Suppose that R has finite length as an R-module. Then R is Noetherian and Artinian. By (1.97) every prime ideal of R is maximal.

(5.53) Theorem: Let R be a Noetherian ring and M a finite R-module. The following are equivalent:

(a) $\ell_R(M) < \infty$

(b) M is an Artinian R-module.

(c) If $P \in \mathrm{Ass}_R(M)$ then P is a maximal ideal of R.

(d) $R/\mathrm{ann}(M)$ is an Artinian ring.

Proof: (a) $\Leftrightarrow$ (b): By (1.97)

(a) $\Rightarrow$ (c): Consider a composition series of M: $(0) = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_{n-1} \subsetneq M_n = M$, i.e. the factor modules M_i/M_{i-1} are simple R-modules. Thus $M_i/M_{i-1} \cong R/m_i$ where $m_i \subseteq R$

is a maximal ideal. By (2.10) $\mathrm{Ass}_R(M) \subseteq \{m_1, \dots, m_n\}$.

(c) $\Rightarrow$ (d): By (2.16) the minimal prime ideals of $\mathrm{Ass}_R(M)$ and $\mathrm{Supp}_R(M)$ are the same. Thus $\mathrm{Ass}_R(M) = \{m_1, \dots, m_n\} = \mathrm{Supp}_R(M) = V(\mathrm{ann}(M)) \subseteq m\mathrm{Spec}(R)$ and $\dim R/\mathrm{ann}(M) = 0$. $R/\mathrm{ann}(M)$ is an Artinian ring.

(d) $\Rightarrow$ (a): Every finite module over an Artinian ring is Artinian.

(5.54) Proposition: Let R be a domain. The following are equivalent:

(a) R is Noetherian and $\dim R = 1$.

(b) For every ideal $I \subseteq R$ with $I \neq (0)$ the ring R/I is Artinian.

Proof: (b) $\Rightarrow$ (a): We have to show that every ideal $I \subseteq R$ is finitely generated. Let $I \subseteq R$ be an ideal with $I \neq (0)$ and let $a \in I - (0)$. By assumption $R/(a)$ is Artinian. Thus $R/(a)$ is Noetherian and $I/(a)$ is finitely generated. Then I is finitely generated.

(5.55) Theorem: (Krull-Akizuki) Let R be a Noetherian domain of dimension one and let $Q(R) \subseteq L$ be a finite field extension. Every intermediate ring $R \subseteq S \subseteq L$ is either a field or a Noetherian ring of dimension one.

We need the following lemma:

(5.56) Lemma: Let R be a ring as in (5.55), V a vector space over $Q(R)$ of dimension $s < \infty$, $M \subseteq V$ an R-submodule, and $a \in R - (0)$. Then $\ell_R(M/aM) \leq s \cdot \ell_R(R/(a))$.

Proof of (5.55): Let $J \subseteq S$ be a nonzero ideal and $b \in J - (0)$. Since b is algebraic over $Q(R)$, there are elements $a_i \in R$, $a_r \neq 0$, with $a_r b^r + a_{r-1} b^{r-1} + \dots + a_0 = 0$. We may assume that $a_0 \neq 0$. Then $a_0 \in Sb \subseteq J$. Apply (5.56) to $L = V$ and $M = S$ to obtain:

$$\ell_S(S/J) \leq \ell_R(S/J) \leq \ell_R(S/a_0 S) \leq [L:K]\, \ell_R(R/a_0 R) < \infty$$

The statement follows with (5.54).

Proof of (5.56): We may assume that M generates the $Q(R)$-vector space V.

Case 1: M is a finite R-module, say $M = Rm_1 + \cdots + Rm_t$. Then $s \le t$ and after renumbering $m_1, \dots, m_s$ is a basis of the $Q(R)$-vector space V. $m_1, \dots, m_s$ is also a basis of the free R-submodule $U = Rm_1 + \cdots + Rm_s \subseteq M$. For all $s+1 \le i \le t$ there are elements $\lambda_{ij} \in Q(R)$ so that $m_i = \sum_{j=1}^{s} \lambda_{ij} m_j$. Hence there is an element $b \in R - (0)$ with $bM \subseteq U$ and the R-module M/U has a nontrivial annihilator $b \in \operatorname{ann}_R(M/U)$. Since $\dim R = 1$ and $\operatorname{ann}_R(M/U) \neq 0$, the ring $R/\operatorname{ann}(M/U)$ is Artinian. M/U is a finite $R/\operatorname{ann}(M/U)$-module and hence $\ell_R(M/U) < \infty$.

Let $a \in R - (0)$. For all $n \ge 1$ there is an exact sequence $0 \to U/a^nU \to M/a^nM \to M/U \to 0$. Note that $U/a^nU \cong (R/(a)^n)^s$ and therefore $\ell_R(U/a^nU) = s\,\ell_R(R/(a^n)) < \infty$. This implies:

$$(*)\quad \ell_R(M/a^nM) \le \ell_R(M/a^nU) = \ell_R(M/U) + \ell_R(U/aU) < \infty.$$

Since a is a nonzero divisor on M and U: $M/aM \cong aM/a^2M \cong \cdots \cong a^{n-1}M/a^nM$ and $U/aU \cong aU/a^2U \cong \cdots \cong a^{n-1}U/a^nU$. From the exact sequences:

$0 \to a^{n-1}M/a^nM \to M/a^nM \to M/a^{n-1}M \to 0$ and $0 \to a^{n-1}U/a^nU \to U/a^nU \to U/a^{n-1}U \to 0$

we obtain by induction on n that $\ell_R(M/a^nM) = n\,\ell_R(M/aM)$ and $\ell_R(U/a^nU) = n\,\ell_R(U/aU)$. Then $(*)$ yields for all $n \in \mathbb{N}$: $n\,\ell_R(M/aM) \le \ell_R(M/U) + ns\,\ell_R(R/(a))$ and therefore for all $n \in \mathbb{N}$: $\ell_R(M/aM) \le (1/n)\,\ell_R(M/U) + s\,\ell_R(R/(a))$. Since $\ell_R(M/U) < \infty$, $\ell_R(M/aM) \le s\,\ell_R(R/(a))$.

Case 2: M arbitrary. Let $\{M_\tau\}_{\tau \in T}$ be the set of all finite R-submodules of M. Then for all $\tau \in T$: $\ell_R(M_\tau/aM_\tau) \le s\,\ell_R(R/(a))$ implying $\ell_R(M_\tau + aM/aM) = \ell_A(M_\tau/M_\tau \cap aM) \le \ell_R(M_\tau/aM_\tau) \le s\,\ell_R(R/(a))$. Choose $\tau_0 \in T$ such that $\ell_R(M_{\tau_0} + aM/aM)$ is maximal. If $M_{\tau_0} + aM \neq M$ pick $z \in M - (M_{\tau_0} + aM)$ and consider $M_{\tau_1} = M_{\tau_0} + Rz$. Then $M_{\tau_1} + aM = M_{\tau_0} + Rz + aM \supsetneq M_{\tau_0} + aM$ and $M_{\tau_0} + aM/aM \subsetneq M_{\tau_1} + aM/aM$. This implies that $\ell_R(M_{\tau_1} + aM/aM) \not\le \ell_R(M_{\tau_0} + aM/aM)$, a contradiction. Thus $M = M_{\tau_0} + aM$ and $\ell_R(M/aM) = \ell_R(M_{\tau_0} + aM/aM) \le s\,\ell_R(R/(a))$.

(5.56) Remark: The Krull-Akizuki theorem fails for Noetherian domains R of dimension ≥ 2. For example, let K be a field and $K[x,y] \subseteq V \subseteq K(x,y)$ where V is a rank 2 valuation ring.

§6: FINITENESS OF THE INTEGRAL CLOSURE

(5.58) Definition: Let $K \subseteq L$ be a finite extension of fields of degree $[L:K] = n < \infty$. For an element $\alpha \in L$ let $\varphi_\alpha : L \longrightarrow L$ denote the K-linear map $\varphi_\alpha(t) = \alpha t$ for all $t \in L$. Define:

(a) $P_{L/K}(\alpha, x) := \det(x - \varphi_\alpha)$ the characteristic polynomial of α

(b) $N_{L/K}(\alpha) := \det(\varphi_\alpha)$ the norm of α

(c) $Tr_{L/K}(\alpha) := \text{trace}(\varphi_\alpha)$ the trace of α

(5.59) Facts from field theory: Let $K \subseteq L$ be a finite extension of fields with $[L:K] = n < \infty$.

(a) There is a unique intermediate field $K \subseteq K_s \subseteq L$ such that

(i) $K \subseteq K_s$ is a separable field extension

(ii) $K_s \subseteq L$ is a purely inseparable field extension, that is, if $\text{char}(K) = 0$ then $K_s = L$ and if $\text{char}(K) = p > 0$ then $L^q \subseteq K_s$ with $q = p^r$ for some $r \in \mathbb{N}$. Note that $K_s = \{\alpha \in L \mid \alpha \text{ is separable over } K\}$.

(iii) $r_i = [L:K_s]$ is called the inseparable degree of the extension $K \subseteq L$ while $r_s = [K_s:K]$ is called the separable degree of L over K. Then $n = [L:K] = r_i r_s$.

(iv) There are exactly r_s mutually distinct K-morphisms $\tau : K \longrightarrow \overline{L}$ where $\overline{L}$ is the algebraic closure of L and K.

(b) Let $\tau_1, \ldots, \tau_{r_s} : L \longrightarrow \overline{L}$ be the r_s mutually distinct K-morphisms from L into $\overline{L}$ with $\tau_1 = id_L$ the natural embedding. For an element $\alpha \in L$ the elements $\tau_j(\alpha) = \alpha^{(j)}$, $1 \le j \le s$, are called the conjugates of α. Note that $\alpha = \alpha^{(1)}$ and possibly $\alpha^{(j)} = \alpha^{(k)}$ for $j \neq k$. Then

(i) $P_{L/K}(\alpha, x) = \prod_{j=1}^{r_s} (x - \alpha^{(j)})^{r_i} \in K[x]$

(ii) $N_{L/K}(\alpha) = \prod_{j=1}^{r_s} \alpha^{(j) r_i} \in K$

(iii) $Tr_{L/K}(\alpha) = r_i \sum_{j=1}^{r_s} \alpha^{(j)} \in K$.

In particular, $Tr_{L/K}(\alpha) = 0$ if $r_i > 1$ or equivalently, if L is inseparable over K. If L is separable over K then $Tr_{L/K}(\alpha) = \sum_{j=1}^{n} \alpha^{(j)}$. If $[L:K] = n$, then $\deg P_{L/K}(\alpha, x) = n$ with $P_{L/K}(\alpha, x) = x^n \pm a_{n-1} x^{n-1} \pm \cdots \pm a_0$ where $a_{n-1} = Tr_{L/K}(\alpha)$ and $a_0 = N_{L/K}(\alpha)$. Norm and trace are elements of K.

(c) (i) The norm function: $N_{L/K}: L^* \longrightarrow K^*$ with $\alpha \longmapsto N_{L/K}(\alpha)$ is a homomorphism of groups.
(ii) The trace function $Tr_{L/K}: L \longrightarrow K$ with $\alpha \longmapsto Tr_{L/K}(\alpha)$ is a K-linear transformation.

(5.60) Definition: Assumptions as in (5.59). Let $\alpha \in L$ be an element.
(a) If $P'_{L/K}(\alpha, X)$ denotes the formal derivative of the characteristic polynomial, the element $\delta_{L/K}(\alpha) = P'_{L/K}(\alpha, \alpha) \in L$ is called the different of α over L.
(b) The element $D(\alpha) = (-1)^t N_{L/K}(\delta_{L/K}(\alpha)) \in K$ where $t = \frac{1}{2} n(n-1)$ is called the discriminant of α over L.

(5.61) Lemma: With the assumptions and notations of (5.59) for an element $\alpha \in L$ the following conditions are equivalent:
(a) $D(\alpha) \neq 0$
(b) $\delta_{L/K}(\alpha) \neq 0$
(c) L is separable over K with $L = K(\alpha)$.

Proof: (a) $\Longleftrightarrow$ (b): trivial
(b) $\Longrightarrow$ (c): If $\delta_{L/K}(\alpha) \neq 0$ then α is a simple root of $P_{L/K}(\alpha, X)$. Since the characteristic polynomial divides a power of the minimal polynomial, in this case $P_{L/K}(\alpha, X)$ is the minimal polynomial. Moreover, $P_{L/K}(\alpha, X)$ is a separable polynomial. Thus $[K(\alpha) : K] = n$ and $L = K(\alpha)$ is separable over K.
(c) $\Longrightarrow$ (b): $P_{L/K}(\alpha, X)$ is the minimal polynomial of α over K and $P_{L/K}(\alpha, X)$ has only simple roots. Thus $\delta_{L/K}(\alpha) \neq 0$.

(5.62) Lemma: Let $K \subseteq L$ be a finite separable field extension, $[L:K] = n$, and $\alpha \in L$. Then:

$$D(\alpha) = (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq k < l \leq n} (\alpha^{(k)} - \alpha^{(l)})^2 = \det \begin{bmatrix} 1 & \alpha^{(1)} & \cdots & \alpha^{(1)n-1} \\ 1 & \alpha^{(2)} & \cdots & \alpha^{(2)n-1} \\ & & & \\ 1 & \alpha^{(n)} & \cdots & \alpha^{(n)n-1} \end{bmatrix}.$$

Proof: If $K \subseteq L$ is a finite separable field extension of degree n, then there are exactly n mutually distinct K-morphisms $\tau_i : L \longrightarrow \overline{K}$. $\alpha \in L$ has exactly n conjugates $\alpha^{(1)}, \ldots, \alpha^{(n)}$ with $\alpha = \alpha^{(1)}$, $P_{L/K}(\alpha, x) = \prod_{j=1}^{n} (x - \alpha^{(j)})$, and $P'_{L/K}(\alpha, \alpha) = \prod_{j=2}^{n} (\alpha - \alpha^{(j)}) = \delta_{L/K}(\alpha)$. For $1 \leq j \leq n$: $\delta_{L/K}^{(j)}(\alpha) = \prod_{k=1, k \neq j}^{n} (\alpha^{(j)} - \alpha^{(k)})$ and $N_{L/K}(\delta_{L/K}(\alpha)) = \prod_{j=1}^{n} \prod_{k=1, k \neq j}^{n} (\alpha^{(j)} - \alpha^{(k)}) = (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq k < j \leq n} (\alpha^{(k)} - \alpha^{(j)})^2$. Note that the double product has exactly $n(n-1)$ factors. Collecting factors $\alpha^{(k)} - \alpha^{(j)}$ and $\alpha^{(j)} - \alpha^{(k)}$ gives the formula. The rest is the Vandermond determinant from linear algebra.

(5.63) Definition: Let $K \subseteq L$ be a finite separable field extension with $[L:K] = n$. For elements $\omega_1, \ldots, \omega_n \in L$ define the discriminant of $\omega_1, \ldots, \omega_n$ by:

$$\Delta_{L/K}(\omega_1, \ldots, \omega_n) = \det\left((\omega_i^{(j)})_{1 \leq i,j \leq n} \right)^2$$

where $\omega_i^{(1)}, \ldots, \omega_i^{(n)}$ are the conjugates of ω_i.

(5.64) Lemma: With assumption as in (5.63):

(a) $\Delta_{L/K}(\omega_1, \ldots, \omega_n) = \det\left(\mathrm{Tr}_{L/K}(\omega_i \omega_j)_{1 \leq i,j \leq n} \right)$

(b) $\Delta_{L/K}(\omega_1, \ldots, \omega_n) \neq 0$ if and only if $\omega_1, \ldots, \omega_n$ is a basis of the K-vector space L.

Proof: (a) $\Delta_{L/K}(\omega_1, \ldots, \omega_n) = \det\left((\omega_i^{(j)}) \right)^2 = \det\left((\omega_i^{(j)}) \right) \det\left((\omega_i^{(j)})^T \right) = \det\left(\left(\sum_{k=1}^{n} \omega_i^{(k)} \omega_j^{(k)} \right)_{i,j} \right) = \det\left(\mathrm{Tr}_{L/K}(\omega_i \omega_j)_{i,j} \right)$.

(b) Since $K \subseteq L$ is a finite separable extension, $L = K(\alpha)$ for some $\alpha \in L$. Then $\omega_j = \sum_{i=1}^{n} a_{ij} \alpha^{i-1}$ for some $a_{ij} \in K$ and $\omega_j^{(k)} = \sum_{i=1}^{n} a_{ij} \alpha^{(k) i-1}$ for all $1 \leq j, k \leq n$. Thus

$$\begin{bmatrix} \omega_1 \\ \omega_2 \\ \vdots \\ \omega_n \end{bmatrix} = (a_{ij})_{i,j} \begin{bmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \omega_1^{(k)} \\ \omega_2^{(k)} \\ \vdots \\ \omega_n^{(k)} \end{bmatrix} = (a_{ij})_{i,j} \begin{bmatrix} 1 \\ \alpha^{(k)} \\ \vdots \\ \alpha^{(k) n-1} \end{bmatrix}.$$

This implies $(\omega_j^{(k)})_{j,k} = (a_{ij})_{i,j} \left(\alpha^{(k) i-1} \right)_{i,k}$ and $\det\left(\omega_j^{(k)} \right) = \det\left(a_{ij} \right) \det\left(\alpha^{(k) i-1} \right)$. Therefore by (5.62) $\Delta_{L/K}(\omega_1, \ldots, \omega_n) = \det\left(a_{ij} \right)^2 D(\alpha)$. By (5.61) $D(\alpha) \neq 0$. This shows that $\Delta_{L/K}(\omega_1, \ldots, \omega_n) \neq 0$ if and only if $\det\left((a_{ij})_{i,j} \right) \neq 0$. This equivalent to $\omega_1, \ldots, \omega_n$ being a basis of L over K.

(5.65) Corollary: Let $K \subseteq L$ be a finite field extension. L is separable over K if and only if $Tr_{L/K} \neq 0$ (i.e. the trace is a nonzero linear map from L to K).

Proof: If $K \subseteq L$ is inseparable and $n > 1$, then $Tr_{L/K} = 0$ by (5.59). Suppose that $K \subseteq L$ is separable and $\omega_1, \ldots, \omega_n$ is a basis of L over K. By (5.64): $\Delta_{L/K}(\omega_1, \ldots, \omega_n) = \det(Tr_{L/K}(\omega_i \omega_j)) \neq 0$ and $Tr_{L/K} \neq 0$.

For the remainder of this section let $K \subseteq L$ be a finite field extension with $[L:K] = n$, R a Noetherian normal domain with $R \subseteq K$ and $Q(R) = K$, and S the integral closure of R in L. Under these assumptions

(a) S is a normal domain

(b) $S \cap K = R$

(c) There is a basis $\omega_1, \ldots, \omega_n$ of the K-vector space L with $\omega_1, \ldots, \omega_n \in S$.

(d) $L = K \cdot S = Q(S)$.

(5.66) Theorem: Suppose there is a K-linear map $t: L \longrightarrow K$ with:

(a) $t(S) \subseteq R$

(b) $t \neq 0$.

Then S is a finite R-module.

Proof: Let $\omega_1, \ldots, \omega_n \in S$ be a K-basis of L and set $M = \sum_{i=1}^{n} R\omega_i \subseteq S$. Since $\omega_1, \ldots, \omega_n$ is a basis of L over K, M is a free R-module with $M \cong R^n$. For any R-submodule U of L put $\widetilde{U} = \{x \in L \mid t(xU) \subseteq R\}$. $\widetilde{U}$ is an R-submodule of L and if $U_1 \subseteq U_2 \subseteq L$ are submodules of L then $\widetilde{U}_2 \subseteq \widetilde{U}_1$. Thus $\widetilde{S} \subseteq \widetilde{M}$, since $M \subseteq S$. For all $b \in S$, $bS \subseteq S$ and hence $t(bS) \subseteq t(S) \subseteq R$ by (a). Thus $S \subseteq \widetilde{S} \subseteq \widetilde{M}$ and it suffices to show that $\widetilde{M}$ is a finite R-module, since R is Noetherian. Consider the map $\varphi: \widetilde{M} \longrightarrow R^n$ defined by $\varphi(m) = (t(m\omega_1), \ldots, t(m\omega_n))$. Since t is K-linear, the map φ is R-linear. We claim that φ is injective. Obviously, $\varphi(m) = 0$ if and only if $t(m\omega_i) = 0$ for all $1 \leq i \leq n$. Hence

if $\varphi(m)=0$ then $t(mM)=0$. If $m\neq 0$, the K-linear map $\varphi_m : L \longrightarrow L$ defined by $\varphi_m(\lambda)=m\lambda$ is injective and surjective and $mw_1, \ldots, mw_n$ is a basis of L over K. Thus if $m\neq 0$ and $t(mM)=0$ then $t(L)=0$ since t is K-linear, a contradiction to (b). Thus S and $\widetilde{M}$ are isomorphic to R-submodules of R^n. Since R is Noetherian, S is a finite R-module.

(5.67) Corollary: Let $K \subseteq L$ be a finite separable field extension and $R \subseteq K$ a normal Noetherian domain with field of quotients $K=Q(R)$. The integral closure S of R in L is a finite R-module. In particular, S is a Noetherian ring.

Proof: The trace function $Tr_{L/K} = t : L \longrightarrow K$ satisfies conditions (a) and (b) of (5.66).

(5.68) Corollary: Let R be a Dedekind domain, $K=Q(R)$ its field of quotients, and $K \subseteq L$ a finite separable field extension. The integral closure S of R in L is a finite R-module and a Dedekind domain.

(5.69) Corollary: Let $\mathbb{Q} \subseteq L$ be a finite field extension. The integral closure S of $\mathbb{Z}$ in L is a finite $\mathbb{Z}$-module and a Dedekind domain.

(5.70) Remark: Let R be a Noetherian domain of dimension one, $K=Q(R)$ its field of quotients and $K \subseteq L$ a finite field extension. By the Krull-Akizuki theorem the integral closure S of R in L is a Noetherian domain of dimension one. Since S is normal, S is a Dedekind domain. There are examples where S is not a finite R-module.

(5.71) Remark: Let k be a field, R a finitely generated k-algebra and a domain, $K=Q(R)$ its field of quotients, and $K \subseteq L$ a finite field extension. The integral closure of R in L is a finite R-module. In particular, the integral closure of R in K is a finite R-module (without proof).