CHAPTER I: SEPARABILITY AND THE MODULE OF DIFFERENTIALS

§1: THE MODULE OF DIFFERENTIALS

General assumptions: all rings commutative with 1
all homomorphisms of rings map 1 into 1
all modules are unitary: $\forall\, m \in M: 1 \cdot m = m$

(1.1) Definition: R a ring; M an R-module; $d: R \longrightarrow M$ a map. d is a derivation from R into M if d satisfies:

(a) $\forall\, a,b \in R: \quad d(a+b) = d(a) + d(b)$

(b) (Productrule) $\forall\, a,b \in R: \quad d(ab) = a\,d(b) + b\,d(a)$

(1.2) Remark: $d: R \longrightarrow M$ a derivation

(a) $d(1) = d(1)+d(1) \Longrightarrow d(1) = 0$

(b) $u \in R^*$ a unit $\Longrightarrow 0 = d(1) = d(uu^{-1}) = u\,d(u^{-1}) + u^{-1}d(u) \Longrightarrow d(u^{-1}) = -d(u)/u^2$

(c) $\ker(d) = \{a \in R \mid d(a) = 0\}$ is a subring of R.

(1.3) Examples: (a) $I \subseteq \mathbb{R}$ an open interval, R the ring of differentiable functions $f: I \longrightarrow \mathbb{R}$ with continuous derivations. M the set of continuous functions $g: I \longrightarrow \mathbb{R}$. M is an R-module (in the natural way). Define:

$d: R \longrightarrow M$ by $d(f) = f'$.

d is a derivation in the sense of (1.1).

(b) S a ring, $R = S[x_1, \ldots, x_n]$ the polynomial ring over S (in n variables). The partial derivations $\partial/\partial x_j: R \longrightarrow R$ defined by: for

$$f = \sum{}' s_{(i)}\, x_1^{i_1} \cdots x_n^{i_n}\,; \quad \frac{\partial f}{\partial x_j} = \sum i_j\, s_{(i)}\, x_1^{i_1} \cdots x_j^{i_j - 1} \cdots x_n^{i_n}$$

are derivations in the sense of (1.1). Similarly, partial derivations over-

polynomial rings in infinitely many variables and over power series rings are defined.

(1.4) Definition: k a ring; R a k-algebra; M an R-module.
(a) A k-linear derivation $d: R \longrightarrow M$ is called a k-derivation.
(b) $\mathrm{Der}_k(R,M) := \{ d: R \longrightarrow M \mid d \text{ a } k\text{-derivation} \}$
$\mathrm{Der}_{\mathbb{Z}}(R,M) := \mathrm{Der}(R,M)$.
Note that every derivation is a $\mathbb{Z}$-derivation.

(1.5) Remark: (a) $\varphi: k \longrightarrow R$ a morphism of rings; M an R-module; $d: R \longrightarrow M$ a derivation. d is a k-derivation $\Longleftrightarrow d(k) = d(\varphi(k)) = 0$.
Pf: "$\Rightarrow$": $a \in k$, $d(a) = d(a \cdot 1) = a\,d(1) + 1\,d(a) = a\,d(1) \Rightarrow d(a) = 0$
"$\Leftarrow$": $r \in R, a \in k$: $d(ar) = a\,d(r) + r\,d(a) = a\,d(r)$
(b) Every derivation is a $\mathbb{Z}$-derivation.
Pf: $n \in \mathbb{Z}$, $n > 1$: by induction $d(n) = d(n-1) + d(1) = d(n-1) = 0$
$d(-1+1) = d(0) = d(-1) + d(1) = 0 \Rightarrow d(-1) = 0$
$n \in \mathbb{Z}$, $n > 1$: $d(-n) = (-1)\,d(n) + n\,d(-1) = 0$. Now use (a).
(c) $d: R \longrightarrow M$ a k-derivation; $\varphi: M \longrightarrow N$ an R-map. Then $\varphi \circ d$ is a k-derivation
Pf: $r, t \in R$: $\varphi \circ d(rt) = \varphi(r\,d(t) + t\,d(r)) = r\,\varphi d(t) + t\,\varphi d(r)$.
(d) $\mathrm{Der}_k(R,M)$ is an R-module (in a natural way). Associate:
$M \rightsquigarrow \mathrm{Der}_k(R,M)$; $\varphi: M \longrightarrow N$, then $\mathrm{Der}_k(R,M) \longrightarrow \mathrm{Der}_k(R,N)$ defined by $d \mapsto \varphi \circ d$, is an R-map.
This defines a functor $\mathrm{Der}_k(R,-)$ from R-mod to R-mod.

(1.6) Definition: Let $\delta: R \longrightarrow N$ be a k-derivation. δ is called a universal k-derivation and N a module of differentials of R over k if for any k-derivation $d: R \longrightarrow M$ there is a unique R-linear map $\varphi: N \longrightarrow M$

so that the diagram $R \xrightarrow{d} M$, $R \xrightarrow{\delta} N \xrightarrow{\varphi} M$ commutes, i.e. $d = \varphi\delta$.

A module of differentials is denoted by $\Omega_{R/k}$. If $k = \mathbb{Z}$, $\Omega_{R/\mathbb{Z}} = \Omega_R$.

(1.7) Remark: (a) If a module of differentials exists it is unique up to unique isomorphism.

(b) Suppose $\Omega_{R/k}$ exists with universal derivation $\delta: R \longrightarrow \Omega_{R/k}$. For all R-modules M the map:

$$\begin{aligned} \mathrm{Hom}_R(\Omega_{R/k}, M) &\xrightarrow{\cong} \mathrm{Der}_k(R, M) \\ \varphi &\longmapsto \varphi\delta \end{aligned}$$

is an isomorphism of R-modules.

Pf: Surjectivity follows from the definition of $(\Omega_{R/k}, \delta)$.

Injectivity follows from the uniqueness part of the definition of $(\Omega_{R/k}, \delta)$.

(c) Conversely, if N is an R-module, $d: R \longrightarrow N$ a k-derivation so that

$$\begin{aligned} \mathrm{Hom}_R(N, M) &\xrightarrow{\cong} \mathrm{Der}_k(R, M) \\ \varphi &\longmapsto \varphi d \end{aligned}$$

is an isomorphism for all R-modules M, then (N, d) is a module of differentials, i.e. $N \cong \Omega_{R/k}$ and d is a universal k-derivation.

(1.8) Theorem: k a ring, $R = k[x_i]_{i \in I}$ the polynomial ring over k. Then $\Omega_{R/k}$ exists. Moreover, $\Omega_{R/k}$ is a free R-module with basis $\{\delta x_i\}_{i \in I}$ and universal k-derivation $\delta = \oplus \partial/\partial x_i$.

Proof: Let $N = \oplus_{i \in I} R e_i$ be a free R-module with basis $\{e_i\}_{i \in I}$ and

$$\begin{aligned} \delta: R &\longrightarrow N \\ f &\longmapsto (\partial f/\partial x_i \, e_i)_{i \in I}. \end{aligned}$$

δ is a k-derivation from R to N.

Let $d: R \longrightarrow M$ be a k-derivation with $d(x_i) = m_i$ for all $i \in I$.

Define $\varphi: N = \bigoplus Re_i \longrightarrow M$ by $\varphi(e_i) = m_i$. Then for all $f \in R$:

$$d(f) = \sum_{i \in I} \partial f/\partial x_i \, m_i$$

(check only on monomials and apply the product rule).
Thus $d = \varphi\delta$. If $\psi: N \longrightarrow M$ is an R-linear map with $d = \psi\delta$, then $d(x_i) = \psi\delta(x_i) = \psi(e_i) = m_i$ and thus $\varphi = \psi$.

(1.9) Lemma: R an k-algebra. Suppose $(\Omega_{R/k}, \delta)$ exists. If $I \subseteq R$ is an ideal, then $I\Omega_{R/k} \subseteq R\delta(I) \subseteq I\Omega_{R/k} + \delta(I)$.

Proof: Let $a \in I$, $r \in R$. Then $a\delta(r) = \delta(ar) - r\delta(a) \Rightarrow I\Omega_{R/k} \subseteq R\delta(I)$, since $\Omega_{R/k}$ is generated by $\delta(R)$. Similarly, $R\delta(I) = I\Omega_{R/k} + \delta(I)$.

(1.10) Theorem: R a k-algebra, $I \subseteq R$ an ideal. Suppose $(\Omega_{R/k}, \delta)$ exists. Then $\Omega_{(R/I)/k}$ exists and $\Omega_{(R/I)/k} = \Omega_{R/k}/R\delta(I)$.

Proof: By (1.9) $I\Omega_{R/k} \subseteq R\delta(I)$, thus $\Omega_{R/k}/R\delta(I)$ is an R/I-module. Consider the commutative diagram:

$$\begin{array}{ccc} R & \xrightarrow{\delta} & \Omega_{R/k} \\ \nu \downarrow & & \downarrow \mu \\ R/I & \xrightarrow{\delta'} & \Omega_{R/k}/R\delta(I) \end{array}$$

where $\delta'(r+I) = \delta(r) + R\delta(I)$. δ' is a k-derivation. Let $d: R/I \longrightarrow M$ be a k-derivation and $d^* = d\nu: R \xrightarrow{\nu} R/I \xrightarrow{d} M$ the composition. d^* is a k-derivation. Thus there is an R-map $\varphi: \Omega_{R/k} \longrightarrow M$ so that

$$\begin{array}{ccc} R & \xrightarrow{\delta} & \Omega_{R/k} \\ & {\scriptstyle d^*}\searrow \quad \swarrow{\scriptstyle \varphi} & \\ & M & \end{array}$$

commutes, i.e. $d^* = \varphi\delta$.
Since $d^*(I) = 0$, $\varphi(\delta(I)) = 0$ and φ factors through $\Omega_{R/k}/R\delta(I)$. The

diagram: $R \xrightarrow{\delta} \Omega_{R/k} \xrightarrow{\varphi} M$

$\nu \downarrow$ $\quad \downarrow \mu$ $\quad \nearrow \psi$

$R/I \xrightarrow{\delta'} \Omega_{R/k/R\delta(I)}$ with $\varphi = \psi\mu$, commutes.

Thus $\psi\delta'\nu = \psi\mu\delta = \varphi\delta = d^* = d\nu$ and $\psi\delta' = d$.

ψ is unique. Suppose there is another R/I-linear map $\psi' : \Omega_{R/k/R\delta(I)} \longrightarrow M$ with $\psi'\delta' = d$. Then $\psi\mu = \psi'\mu$ and $\psi = \psi'$ since μ is surjective.

(1.11) Corollary: k a ring; R a k-algebra. Then $\Omega_{R/k}$ exists. If R is a finitely generated k-algebra, $\Omega_{R/k}$ is a finitely generated R-module.

(1.12) Corollary: There is an exact sequence of R/I-modules:

$$I/I^2 \xrightarrow{\bar{\delta}} \Omega_{R/k}/I\Omega_{R/k} \xrightarrow{\lambda} \Omega_{(R/I)/k} \longrightarrow 0$$

where $\bar{\delta}(a+I^2) = \delta(a) + I\Omega_{R/k}$ and λ the natural map.

A different construction of $\Omega_{R/k}$.

Consider the map $\tau : R \otimes_k R \longrightarrow R$ defined by $\tau(a \otimes b) = ab$. Let $I = \ker(\tau)$. Note that τ is a homomorphism of rings and I is generated by the set $\{1 \otimes a - a \otimes 1 \mid a \in R\}$.

There are 2 (different) R-module structures on $R \otimes_k R$ given by:

$\forall\, a, x, y \in R$: 1) $a(x \otimes y) = (ax) \otimes y = (a \otimes 1)(x \otimes y)$

2) $a(x \otimes y) = x \otimes (ay) = (1 \otimes a)(x \otimes y)$.

Both R-module structures on $R \otimes_k R$ induce the same R-module structure on I/I^2: $a, x \in R \Rightarrow$

$$\begin{aligned}(a \otimes 1)[(1 \otimes x) - (x \otimes 1)] &= a \otimes x - ax \otimes 1 \\ &\equiv (1 \otimes a)[(1 \otimes x) - (x \otimes 1)] \mod I^2 \\ &= 1 \otimes ax - x \otimes a\end{aligned}$$

In the following we consider I/I^2 an R-module via these structures.

The map $\delta' : R \longrightarrow I/I^2$ defined by $\delta'(a) = (1 \otimes a - a \otimes 1) + I^2$ is a k-derivation from R into the R-module I/I^2.

(1.13) Definition: Let R be a ring; M an R-module. Define a multiplication on $R \oplus M$ as follows: $\forall\, a,a' \in R;\ m,m' \in M:\ (a,m)(a',m') = (aa', am' + a'm)$. This defines a ring structure on $R \oplus M$. This ring is called the trivial extension of R by M and is denoted by $R * M$. $R * M$ is a commutative ring with identity $(1,0)$. The canonical embedding $\lambda: R \longrightarrow R * M$ by $\lambda(a) = (a,0)$ is an injective morphism of rings. In the following $R * M$ is considered an R-algebra via λ.

(1.14) Theorem: $(I/I^2, \delta')$ is the module of differentials of R over k.

Proof: Let $d: R \longrightarrow M$ be a k-derivation. Define $\varphi: R \otimes_k R \longrightarrow R * M$ by $\varphi(a \otimes b) = (ab, a\,d(b))$. φ is a morphism of k-algebras with $\varphi(I) \subseteq M \subseteq R * M$. $[\varphi(a \otimes 1 - 1 \otimes a) = (a,0) - (a, d(a)) = (0, d(a))]$. Thus $\varphi|_I : I \longrightarrow M$ is an R-linear map with $\varphi(I^2) = 0$, since $M^2 = 0$ in $R * M$.
Thus φ induces an R-linear map $\varphi: I/I^2 \longrightarrow M$. Let $a \in R$, then

$$\begin{aligned} \varphi\delta'(a) &= \varphi(1 \otimes a - a \otimes 1 + I^2) \\ &= (0, d(a)) \\ &\equiv d(a) \quad \text{where } M \text{ is considered a submodule of } R * M. \end{aligned}$$

Thus $\varphi \circ \delta' = d$. Uniqueness follows since $\delta'(R)$ generates I/I^2 as an R-module.

(1.15) Remark: Both constructions of $\Omega_{R/k}$ are isomorphic.

(1.16) Lemma: Let $N' \xrightarrow{\alpha} N \xrightarrow{\beta} N''$ be a sequence of R-modules. If for all R-modules M the induced sequence:

$$\mathrm{Hom}_R(N', M) \xleftarrow{\alpha^*} \mathrm{Hom}_R(N, M) \xleftarrow{\beta^*} \mathrm{Hom}_R(N'', M)$$

is exact, then $N' \xrightarrow{\alpha} N \xrightarrow{\beta} N''$ is exact.

Proof: (a) $\ker(\beta) \subseteq \mathrm{im}(\alpha)$.
Let $M = N/\mathrm{im}(\alpha)$ and consider the diagram:

$$\begin{array}{ccccc} N' & \xrightarrow{\alpha} & N & \xrightarrow{\beta} & N'' \\ & & \downarrow \nu & \nearrow k & \\ & & N/\mathrm{im}(\alpha) & & \end{array}$$

Since $\alpha^*(\nu)=0$, $\nu \in \operatorname{im}(\beta^*)$ and there is an $h \in \operatorname{Hom}_R(N'', M)$ with $h\beta = \nu = \beta^*(h)$.
Thus $\ker(\beta) \subseteq \operatorname{im}(\alpha)$

(b) $\operatorname{im}(\alpha) \subseteq \ker(\beta)$

Let $M = N''$. Then $\alpha^*\beta^*(id_{N''}) = 0 \Rightarrow \beta\alpha = 0 \Rightarrow \operatorname{im}(\alpha) \subseteq \ker(\beta)$.

(1.17) Theorem: Let $f: k \to R$ and $g: R \to S$ be morphisms of rings. Then there is an exact sequence of S-modules:

$$\Omega_{R/k} \otimes_R S \xrightarrow{\alpha} \Omega_{S/k} \xrightarrow{\beta} \Omega_{S/R} \to 0$$

where

(1) $\alpha(\delta_{R/k}(a) \otimes b) = b\,\delta_{S/k}(g(a))$ for all $a \in R$, $b \in S$.

(2) $\beta(\delta_{S/k}(b)) = \delta_{S/R}(b)$ $\forall$ $b \in S$.

Proof: For any S-module M apply $\operatorname{Hom}_S(-, M)$:

$$\begin{array}{ccccccc}
\operatorname{Hom}_S(\Omega_{R/k} \otimes_R S, M) & \xleftarrow{\alpha^*} & \operatorname{Hom}_S(\Omega_{S/k}, M) & \xleftarrow{\beta^*} & \operatorname{Hom}_S(\Omega_{S/R}, M) & \leftarrow & 0 \\
\downarrow \cong & & & & & & \\
\operatorname{Hom}_R(\Omega_{R/k}, \operatorname{Hom}_S(S, M)) & & \text{is} & & \text{is} & & \\
\downarrow \cong & & & & & & \\
\operatorname{Hom}_R(\Omega_{R/k}, M) & & & & & & \\
\downarrow \cong & & & & & & \\
\operatorname{Der}_k(R, M) & \xleftarrow{\alpha^{**}} & \operatorname{Der}_k(S, M) & \xleftarrow{\beta^{**}} & \operatorname{Der}_R(S, M) & \leftarrow & 0
\end{array}$$

The last sequence is exact.

(1.18) Remark: The exact sequence of (1.17) is part of a long exact sequence. (André - Quillen homology).

§2: SEPARABILITY

(1.19) Theorem: K a field; $K \subseteq L = K(\alpha)$ a simple algebraic field extension. Suppose that $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_n = 1$, is the minimal polynomial of α over K. Let V be an L-vector space and $d: K \longrightarrow V$ a derivation. For all $v \in V$ the following conditions are equivalent:

(a) There is a derivation $\tilde{d}: L \longrightarrow V$ extending d with $\tilde{d}(\alpha) = v$.

(b) $\sum_{i=0}^{n} d(a_i)\alpha^i + f'(\alpha)v = 0$ in V.

Proof: (a) $\Rightarrow$ (b): Let $\tilde{d}: L \longrightarrow V$ be a derivation with $\tilde{d}|_K = d$ and $\tilde{d}(\alpha) = v$.
Since $f(\alpha) = 0$, $0 = \tilde{d}(f(\alpha)) = \sum_{i=0}^{n} d(a_i)\alpha^i + f'(\alpha)v$.

(b) $\Rightarrow$ (a): Since $L = K(\alpha) \cong K[x]/(f)$, we may consider V as a $K[x]$-module.
Define $d_1: K[x] \longrightarrow V$ by $d_1\left(\sum_i b_i x^i\right) = \sum d(b_i)x^i$
and $d_2: K[x] \longrightarrow V$ by $d_2(g) = g'(\alpha)v$.
d_1 and d_2 are derivations from $K[x]$ into V with $d_1|_K = d$ and $d_2|_K = 0$.
Thus $d_1 + d_2$ is an extension of d to $K[x]$. By assumption (b) $(d_1 + d_2)(f) = 0$ and $d_1 + d_2$ factors through L.

(1.20) Proposition: Let $K \subseteq L$ be a separable algebraic field extension. Any derivation from K into an L-vector space V can be uniquely extended to a derivation from L into V.

Proof: Case 1: $K \subseteq L$ is finite.
Then there is an $\alpha \in L$ with $L = K(\alpha)$. Let $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_n = 1$, be the minimal polynomial of α over K. Since α is separable over K, $f'(\alpha) \neq 0$.
If $d: K \longrightarrow V$ is a derivation from K into an L-vector space V, there is a unique $v \in V$ so that $\sum_{i=0}^{n} d(a_i)\alpha^i + f'(\alpha)v = 0$. By (1.19) d extends uniquely.

Case 2: the general case

Write L as a union of finite field extensions of K: $L = \bigcup_{i\in I} E_i$ and let $d: K \longrightarrow V$ be a derivation from K into an L-vector space V. For all $i\in I$ there is a unique extension $d_i: E_i \longrightarrow V$ of d. By uniqueness, if $E_i \subseteq E_j$ then $d_i = d_j|_{E_i}$. Hence the derivation $\tilde{d}: L \longrightarrow V$ with $\tilde{d}(\beta) = d_i(\beta)$ for $\beta \in E_i$ is well defined and unique.

(1.21) Corollary: Let $K \subseteq L$ be a separable field extension. Then $\Omega_{L/K} = 0$.

Proof: Let $\delta: L \longrightarrow \Omega_{L/K}$ be the universal K-derivation. Then $\delta|_K = 0$ and $\delta|_K$ extends uniquely to a derivation from L into $\Omega_{L/K}$. Thus $\delta = 0$. Since $\Omega_{L/K}$ is generated by $\delta(L)$, it follows that $\Omega_{L/K} = 0$.

(1.22) Corollary: Let $K \subseteq L \subseteq E$ be field extensions with $L \subseteq E$ separable algebraic. Then $\Omega_{E/K} \cong \Omega_{L/K} \otimes_L E$.

Proof: By (1.17) the sequence

$$(*) \qquad \Omega_{L/K} \otimes_L E \xrightarrow{\alpha} \Omega_{E/K} \xrightarrow{\beta} \Omega_{E/L} \longrightarrow 0$$

is exact. By (1.21) $\Omega_{E/L} = 0$ and α is surjective. In order to show injectivity, let M be an L-vector space. $(*)$ yields an exact sequence

$$\operatorname{Hom}_E(\Omega_{L/K} \otimes_L E, M) \xleftarrow{\alpha^*} \operatorname{Hom}_E(\Omega_{E/K}, M) \longleftarrow 0$$

$$\text{is}$$

$$\operatorname{Der}_K(L, M) \xleftarrow{\alpha^{**}} \operatorname{Der}_K(E, M) \longleftarrow 0$$

where $\alpha^{**}(d) = d|_L$. By (1.20) α^{**} is surjective. Thus α is injective by (1.16).

(1.23) Proposition: Let $K \subseteq L$ be a finite field extension. If $\Omega_{L/K} = 0$, then L is separable over K.

Proof: Let K_0 be the separable closure of K in L and suppose that $K_0 \neq L$. Then there is an intermediate field $K_0 \subseteq K_1 \subseteq L$ with $[L:K_1] = p$ where $\operatorname{char} K = p > 0$. By (1.17) Ω_{L/K_1} is a homomorphic image of $\Omega_{L/K}$ and $\Omega_{L/K_1} = 0$ by assumption. It suffices to show that $\Omega_{L/K_1} \neq 0$.
Let $\alpha \in L - K_1$. Since L is purely inseparable over K_1, $\alpha^p = a \in K_1$ and $f(x) = x^p - a$ is the minimal polynomial of α over K_1. Let V be a nonzero vector space over L and $d: K_1 \longrightarrow V$ the trivial derivation, i.e. $d = 0$. For all $v \in V$ the equation $d(1)\alpha^p - d(a) + f'(\alpha)v = 0$ holds. By (1.19) d extends to a derivation $\tilde{d}: L \longrightarrow V$ with $\tilde{d}(\alpha) = 0$. Thus $\tilde{d} \neq 0$ if $v \neq 0$. Moreover, $0 \neq \tilde{d} \in \operatorname{Der}_{K_1}(L, V) \cong \operatorname{Hom}_L(\Omega_{L/K}, V)$ and $\Omega_{L/K_1} \neq 0$.

(1.24) Definition: Let K be a field and R a K-algebra. R is called separable over K if for any field extension $K \subseteq L$ the tensor product $R \otimes_K L$ is reduced.

(1.25) Remark: Let $k \subseteq L$ be an algebraic field extension. Then there are possibly two different notions of separability. We will call L separable algebraic over K when refering to the concept of separability from field theory. The new definition is simply called 'separable'.

(1.26) Proposition: Let K be a field, R a K-algebra. Then:
(a) If R is separable over K then any K-subalgebra of R is separable over K.
(b) R is separable over K if and only if every finitely generated K-subalgebra of R is separable over K.
(c) R is separable over K if and only if for every finitely generated field extension $K \subseteq L$ the tensor product $R \otimes_K L$ is reduced.
(d) If R is separable over K and if $K \subseteq K'$ is a field extension then $R \otimes_K K'$ is separable over K'.

Proof: (a) Since K is a field, every K-module is flat over K. Thus

$$R_0 \otimes_K L \subseteq R \otimes_K L$$

for every K-subalgebra R_0 of R and every field extension $K \subseteq L$.

(b) By (a) we only need to show the backward direction. Write $R = \varinjlim_{i \in I} R_i$ where $\{R_i\}$ is the directed set of all finitely generated K-subalgebras of R. Let $K \subseteq L$ be a field extension. Since the tensor product commutes with direct limits we have $R \otimes_K L = (\varinjlim_{i \in I} R_i) \otimes_K L = \varinjlim_{i \in I} (R_i \otimes_K L)$. The direct limit of reduced algebras is reduced.

(c) By a similar argument as in (a). If $K \subseteq L$ is an arbitrary field extensions, write L as a direct limit of finitely generated fields over K.

(d) obvious.

(1.27) Exercise: Let K be a field, R a reduced K-algebra. Show:

(a) If x is a variable over K, then $R \otimes_K K(x)$ is reduced.

(b) If $K \subseteq L$ is a finite separable algebraic field extension and if R has only finitely many minimal prime ideals, then $R \otimes_K L$ is reduced.

(c) Let R be reduced with only finitely many minimal prime ideals. If $K \subseteq L$ is a separable algebraic field extension, then $R \otimes_K L$ is reduced. If $K \subseteq L$ is a field extension which is separable in the sense of (1.24) then $R \otimes_K L$ is reduced.

(1.28) Proposition: Let $K \subseteq L$ be an algebraic field extension. The following are equivalent:

(a) $K \subseteq L$ is separable algebraic.

(b) $K \subseteq L$ is separable in the sence of Definition (1.24).

Proof: By Proposition (1.26) we may assume that $K \subseteq L$ is finite.

(a) $\Rightarrow$ (b): Set $L = K(\alpha) = K[x]/(f)$ where $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_n = 1$, is the minimal polynomial of α over K. By assumption f only has simple roots in the algebraic

closure $\overline{K}$ of K. Let $K \subseteq K'$ be a field extension. Then

$$L \otimes_K K' \cong K'[x]/(f).$$

Let $f = f_1 \cdots f_r$ be a factorization of f into irreducible factors in $K'[x]$. Since f is separable, for all $i, j \in \{1, \ldots, r\}$ with $i \neq j$, f_i and f_j are relatively prime. By the Chinese Remainder Theorem:

$$K'[x]/(f) \cong K'[x]/(f_1) \times \cdots \times K'[x]/(f_r)$$

and $K'[x]/(f)$ is a product of fields.

(b) $\Rightarrow$ (a): Let K_0 be the separable closure of K in L and assume that $K_0 \neq L$. Let $\operatorname{char} K = p > 0$. Then there is an element $\alpha \in L - K_0$ with $\alpha^p = a \in K_0$. By Proposition (1.26) $L \otimes_K K_0$ is separable over K_0. Since L and $K_0(\alpha)$ are subalgebras of $L \otimes_K K_0$, by (1.26) $K_0(\alpha)$ is separable over K_0. But the ring

$$K_0(\alpha) \otimes_{K_0} K_0^{p^{-1}}$$

is not reduced. Since $K_0(\alpha) \otimes_{K_0} K_0(\alpha) \not\cong K_0(\alpha)$ (as K_0-algebras), the element $\alpha \otimes 1 - 1 \otimes \alpha$ is nonzero in $K_0(\alpha) \otimes_{K_0} K_0^{p^{-1}}$. But $(\alpha \otimes 1 - 1 \otimes \alpha)^p = 0$.

(1.29) Definition: A field extension $K \subseteq L$ is called separably generated, if L admits a separating transcendence basis, i.e., if there is a transcendence basis $\{w_i\}_{i \in I}$ of L over K so that L is separable algebraic over $K(w_i)_{i \in I}$.

(1.30) Theorem: A separably generated field extension is separable.

Proof: Let $K \subseteq L$ be a separably generated field extension and let $\{w_i\}_{i \in I}$ be a separating transcendence basis of L over K. Let K' be any extension field of K. The ring $K(w_i)_{i \in I} \otimes_K K'$ is a localization of the polynomial ring $K'[w_i]_{i \in I}$ and thus a domain. Let E be the quotient field of $K(w_i)_{i \in I} \otimes_K K'$. Since L is separable over $K(w_i)$ the ring $L \otimes_{K(w_i)} E$ is reduced. Then $L \otimes_K K'$ is reduced since

$$L \otimes_K K' = L \otimes_{K(w_i)} (K(w_i) \otimes_K K') \subseteq L \otimes_{K(w_i)} E.$$

(1.31) Theorem: Let K be a field of characteristic $p>0$ and let L be a finitely generated field extension. The following are equivalent:

(a) L is separable over K.

(b) The ring $L\otimes_K K^{p^{-1}}$ is reduced.

(c) L is separably generated over K.

Proof: (a) $\Rightarrow$ (b): Definition (1.24)

(c) $\Rightarrow$ (a): Theorem (1.30)

(b) $\Rightarrow$ (c): Let $L=K(x_1,\dots,x_n)$ where $x_1,\dots,x_r$, $r\le n$, is a transcendence basis of L over K. Suppose that $x_{r+1},\dots,x_q$ are separable algebraic over $K(x_1,\dots,x_r)$ while x_{q+1} fails to be separable over $K(x_1,\dots,x_r)$. Put $y=x_{q+1}$ and let $f\in K[x_1,\dots,x_r][y]$ be the minimal polynomial of y over $K(x_1,\dots,x_r)$. Since y is inseparable over $K(x_1,\dots,x_r)$, there is a monic polynomial $g\in K(x_1,\dots,x_r)[y]$ with $f(y)=g(y^p)$. After clearing denominators there is an irreducible polynomial $G(x_1,\dots,x_r,y^p)\in K[x_1,\dots,x_r,y]$ with $G(x_1,\dots,x_r,y^p)=0$.

1. case: $\partial G/\partial x_i=0$ for all $1\le i\le r$.

In this case G is a polynomial in $x_1^p,\dots,x_r^p,y^r$ and there is a polynomial $H(x_1,\dots,x_r,y)\in K^{p^{-1}}[x_1,\dots,x_r,y]$ with $G(x_1,\dots,x_r,y^p)=H(x_1,\dots,x_r,y)^p$. Since G is irreducible, $K(x_1,\dots,x_r,y)=K(x_1,\dots,x_r)[y]=Q\big(K[x_1,\dots,x_r,y]/G(x_1,\dots,x_r,y^p)\big)$. This implies:

$$\begin{aligned}K(x_1,\dots,x_r,y)\otimes_K K^{p^{-1}} &= Q\big(K[x_1,\dots,x_r,y]/(G(x_1,\dots,x_r,y^p))\big)\otimes_K K^{p^{-1}}\\ &\cong K^{p^{-1}}(x_1,\dots,x_r)[y]/(G(x_1,\dots,x_r,y^p)\\ &= K^{p^{-1}}(x_1,\dots,x_r)[y]/(H^p).\end{aligned}$$

Since $K(x_1,\dots,x_r,y)\otimes_K K^{p^{-1}}\subseteq L\otimes_K K^{p^{-1}}$, this contradicts assumption (b).

2. case: $\partial G/\partial x_i\neq 0$ for some $1\le i\le r$.

Assume that $\partial G/\partial x_1\neq 0$. Then x_1 is separable over $K(x_2,\dots,x_r,y)$ and we replace the transcendence basis $x_1,\dots,x_r$ by $x_2,\dots,x_r,y$. The extension $K\subseteq K(x_2,\dots,x_r,y,x_1,x_{r+1},\dots,x_q)$ is separably generated and we proceed by induction.

(1.32) Remark: If $K \subseteq L$ is an infinitely generated field extension, then $K \subseteq L$ may be separable, but not separably generated. For example, if K is a field and x a variable over K, $\operatorname{char} K = p > 0$, then $K(x) \subseteq K((x))$ is not separably generated.

Let K be a field of characteristic $p > 0$. Define the following subfield of the algebraic closure $\overline{K}$ of K:

$$K^{p^{-\infty}} := \bigcup_{n \in \mathbb{N}} K^{p^{-n}}$$

(1.33) Corollary: Let K be a field of characteristic $p > 0$, L a finitely generated extension field of K. The following are equivalent:

(a) $L \otimes_K K^{p^{-1}}$ is reduced.

(b) $L \otimes_K K^{p^{-\infty}}$ is reduced.

Proof: (a) $\Rightarrow$ (b): By Theorem (1.31) L is separable over K.

(b) $\Rightarrow$ (a): $L \otimes_K K^{p^{-1}} \subseteq L \otimes_K K^{p^{-\infty}}$.

(1.34) Proposition: Let $K \subseteq L$ be a finitely generated field extension. There is a finite purely inseparable field extension $K \subseteq K'$ such that $K' \subseteq L(K')$ is separable.

Proof: If $\operatorname{char} K = 0$, there is nothing to show. If $\operatorname{char} K = p > 0$, put $E = K^{p^{-\infty}}$.

Claim: The ring $D = E \otimes_K L$ is local Noetherian of dimension 0.

Pf of cl: $E \otimes_K L$ is the localization of a finitely generated E-algebra. Thus D is Noetherian. Let $\sum_{i=1}^{n} a_i \otimes b_i \in E \otimes_K L$. By construction of E there is an integer $q = p^e$ for some $e \in \mathbb{N}$ with $a_i^q \in K$ for all $1 \leq i \leq n$. Thus

$$\left(\sum_{i=1}^{n} a_i \otimes b_i\right)^q = \sum_{i=1}^{n} a_i^q \otimes b_i^q = 1 \otimes \left(\sum_{i=1}^{n} a_i b_i\right)^q.$$

Hence either $1 \otimes (\sum a_i b_i)^q = 0$ or $1 \otimes (\sum a_i b_i)^q$ a unit. Thus every element of D outside the nilradical is invertible and the nilradical is the maximal ideal of D.

D is a local Noetherian ring of dimension 0.
Consider a finite system of generators of the nilradical of D:

$$x_j = \sum_{i=1}^{m} a_{ij} \otimes b_{ij} \quad \text{for } 1 \le j \le n.$$

Let $K' = K(a_{ij})_{1 \le i \le m, 1 \le j \le n}$. K' is a finite purely inseparable extension of K with $K'^{p^{-\infty}} = K^{p^{-\infty}} = E$. Thus $E \otimes_{K'} L(K')$ is also a local Noetherian ring of dimension 0. There is a surjective homomorphism of rings

$$\varphi: E \otimes_K L \longrightarrow E \otimes_{K'} L(K')$$

and $\mathrm{nil}(E \otimes_K L) \subseteq \ker(\varphi)$. Thus $E \otimes_{K'} L(K')$ is a field and by (1.31) $L(K')$ is separable over K'.

(1.35) Corollary: Let K be a field, and R a K-algebra with only finitely many minimal prime ideals. The following are equivalent:
(a) R is separable over K.
(b) For every finite purely inseparable field extension K' of K the ring $R \otimes_K K'$ is reduced.

Proof: (b)$\Rightarrow$(a): By (1.26) it suffices to show that $R \otimes_K L$ is reduced for every finitely generated field extension $K \subseteq L$. By (1.34) there is a finite purely inseparable field extension $K \subseteq K'$ with $L(K')$ separable over K'. By assumption (a) $R \otimes_K K'$ is reduced. Since K' is finite over K, $R \otimes_K K'$ only has finitely many minimal prime ideals. By exercise (1.27) $(R \otimes_K K') \otimes_{K'} L(K') \cong R \otimes_K L(K')$ is reduced and thus $R \otimes_K L$ reduced since $R \otimes_K L \subseteq R \otimes_K L(K')$.

§3: p-BASES

Let $K \subseteq L$ be a field extension, $\operatorname{char} K = p > 0$.

(1.36) **Definition:** (a) $x_1, \dots, x_n \in L$ are called p-independent if $[L^p(K, x_1, \dots, x_n) : L^p(K)] = p^n$, or equivalently, if $\{x_1^{\alpha_1} \dots x_n^{\alpha_n} \mid 0 \le \alpha_i < p\}$ is linearly independent over $L^p(K)$.
(b) A subset $B \subseteq L$ is called p-independent if every finite subset of B is p-independent.
(c) A subset $B \subseteq L$ is a p-basis of L over K if B is p-independent and $L = L^p(K, B)$.

(1.37) **Lemma:** Let $C \subseteq L$ be a p-independent subset. Then C can be extended to a p-basis of L over K.

Proof: Zorn's lemma yields the existence of a maximal p-independent subset $B_0 \subseteq L$ with $C \subseteq B_0$. If $L \neq L^p(K, B_0)$ then $L^p(K, B_0) \subseteq L$ is a proper purely inseparable field extension. Let $\alpha \in L - L^p(K, B_0)$, then $y^p - \alpha^p \in L^p(K, B_0)[y]$ is the minimal polynomial of α over $L^p(K, B_0)$. By the maximality of the set B_0 there are elements $x_1, \dots, x_n \in B_0$ such that the set $\{\alpha, x_1, \dots, x_n\}$ is p-dependent over K. Hence there are elements $q_i \in L^p(K, B_0)$ so that $\sum_{i=0}^{p-1} q_i \alpha^i = 0$, where not all of the q_i are zero. Thus the minimal polynomial of α over $L^p(K, B_0)$ has degree $t \le p-1$, a contradiction.

(1.38) **Remark:** Let B be a p-basis of L over K. Then the set
$$\Gamma_B = \{x_1^{\alpha_1} \dots x_n^{\alpha_n} \mid 0 \le \alpha_i < p;\ n \in \mathbb{N};\ x_1, \dots, x_n \in B\}$$
is a basis of the $L^p(K)$-vector space L.

(1.39) **Lemma:** Let B be a p-basis of L over K and let $d : B \to L$ be a map. d extends uniquely to a K-derivation $D \in \operatorname{Der}_K(L) = \operatorname{Der}_K(L, L)$.

Proof: $\Gamma_B = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid 0 \le \alpha_i < p;\ n \in \mathbb{N};\ x_1, \dots, x_n \in B\}$ is a basis of the $L^p(K)$-vector space L. Define an $L^p(K)$-linear map $D: L \longrightarrow L$ by:

$$D(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = \sum_{i=1}^{n} \alpha_i\, x_1^{\alpha_1} \cdots x_i^{\alpha_i - 1} \cdots x_n^{\alpha_n}\, d(x_i).$$

D is a K-derivation which extends d. Uniqueness is obvious.

(1.40) Remark: It is known from Algebra that if $K \subseteq L$ is a finite extension then L is separable over K if and only if $L = L^p(K)$. In this case any p-basis of L over K is empty.

(1.41) Remark: Note that Lemma (1.37) implies that the extension $K \subseteq L$ admits a p-basis.

(1.42) Theorem: Let $B \subseteq L$ be a subset. The following are equivalent:

(a) B is a p-basis of L over K.

(b) $\{\delta(x) \mid x \in B\}$ is a basis of the L-vector space $\Omega_{L/K}$, where $\delta: L \to \Omega_{L/K}$ is the universal K-derivation.

Proof: First note that $\Omega_{L/K} = \Omega_{L/L^p(K)}$.

(a) $\Rightarrow$ (b): If B is a p-basis of L over K, then $\{\delta(x) \mid x \in B\}$ generates the L-vector space $\Omega_{L/K}$. Let $x_i \in B$, $a_i \in L$ with $\sum_{i=1}^{n} a_i \delta(x_i) = 0$ and $x_i \neq x_j$ for $i \neq j$. If $a_i \neq 0$ for some $1 \le i \le n$, then there are elements $l_i \in L$ so that $\sum_{i=1}^{n} a_i l_i \neq 0$. By (1.39) there is a K-derivation $D: L \longrightarrow L$ with $D(x_i) = l_i$. Thus there is an L-linear map $\varphi: \Omega_{L/K} \longrightarrow L$ so that the diagram

$$\begin{array}{ccc} L & \xrightarrow{D} & L \\ {\scriptstyle\delta}\downarrow & \nearrow_{\varphi} & \\ \Omega_{L/K} & & \end{array}$$

commutes, i.e. $D = \varphi\delta$. Thus $\varphi(\sum_i a_i \delta(x_i)) = \sum_i a_i \varphi(\delta(x_i)) = \sum a_i D(x_i) = \sum a_i l_i \neq 0$, a contradiction.

(b) $\Rightarrow$ (c): Suppose that B is not a p-basis of L over K, and suppose first

that B is p-independent. Then there are $x_1, \dots, x_n \in B$ so that

$$\sum_{(\alpha)} b_{(\alpha)} x_1^{\alpha_1} \cdots x_n^{\alpha_n} = 0$$

where $(\alpha) = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ with $0 \le \alpha_i < p$, $b_{(\alpha)} \in L^p(K)$, and not all $b_{(\alpha)} = 0$. We may suppose that $x_2, \dots, x_n$ are p-independent. Then there is an $(\alpha) = (\alpha_1, \dots, \alpha_n)$ with $\alpha_1 \neq 0$ and $b_{(\alpha)} \neq 0$. Hence:

(i) The minimal polynomial of x_1 over $L^p(K, x_2, \dots, x_n)$ has degree $t \le p-1$.

(ii) Since L is purely inseparable over $L^p(K)$, x_1 is purely inseparable over $L^p(K, x_2, \dots, x_n)$.

Thus $x_1 \in L^p(K, x_2, \dots, x_n)$. Let $f \in L^p(K)[t_2, \dots, t_n]$ with $f(x_2, \dots, x_n) = x_1$. Then

$$\delta(x_1) = \sum_{i=2}^{n} (\partial f / \partial t_i)(x_2, \dots, x_n)\, \delta(x_i),$$

a contradiction, since $\delta(x_1), \dots, \delta(x_n)$ are linearly independent. Thus B is p-independent. If B is not a p-basis by (1.37) B can be extended to a p-basis B' of L over K. By (a) $\Rightarrow$ (b), the elements $\{\delta(y) \mid y \in B'\}$ form a basis of $\Omega_{L/K}$. Thus $B = B'$ and B is a p-basis.

(1.43) Definition: Consider the following diagram of field extensions:

$$\begin{array}{ccc} K & \longrightarrow & L \\ \downarrow & & \downarrow \\ L' & \longrightarrow & E \end{array}$$

L and L' are called linearly disjoint over K if the natural map: $L \otimes_K L' \longrightarrow L[L'] \subseteq E$ is an isomorphism. Here $L[L']$ denotes the subring of E which is generated by L and L'.

(1.44) Theorem: Let $K \subseteq L, L' \subseteq E$ be field extension as in (1.43). The following conditions are equivalent:

(a) L and L' are linearly disjoint over K.

(b) If $\alpha_1, \dots, \alpha_n \in L$ are linearly independent over K, then $\alpha_1, \dots, \alpha_n$ are linearly

independent over L'.

(c) If $\beta_1, \dots, \beta_n \in L'$ are linearly independent over K, then $\beta_1, \dots, \beta_n$ are linearly independent over L.

Proof: It suffices to show (a)$\Leftrightarrow$(b).

(a)$\Rightarrow$(b): Let $\alpha_1, \dots, \alpha_n \in L$ be linearly independent over K, and let $\gamma_i \in L'$ with $\sum_{i=1}^n \gamma_i \alpha_i = 0$. Since $\sum \alpha_i \otimes \gamma_i \in L \otimes_K L'$ is mapped to $\sum \alpha_i \gamma_i = 0$ in $L[L']$, it follows that $\sum \alpha_i \otimes \gamma_i = 0$. If $\{e_j\}_{j \in J}$ and $\{f_{j'}\}_{j' \in J'}$ are bases of L and L' over K, then $\{e_j \otimes f_{j'}\}$ is a basis of $L \otimes_K L'$ over K. This implies that $\gamma_i = 0$ for all $1 \le i \le n$.

(b)$\Rightarrow$(a): Suppose that $\sum_{i=1}^n x_i \otimes \gamma_i \longmapsto \sum_{i=1}^n x_i \gamma_i = 0$ under the natural map $L \otimes_K L' \longrightarrow L[L']$. Assume that $x_1, \dots, x_r$ are linearly independent over K, while $x_{r+1}, \dots, x_n$ can be expressed as linear combinations of $x_1, \dots, x_r$. Then $\sum x_i \otimes \gamma_i = \sum_{i=1}^r x_i \otimes z_i$ for some $z_i \in L'$ and $\sum_{i=1}^r x_i z_i = 0$. By assumption (b) $z_i = 0$ for all $1 \le i \le r$ and the morphism $L \otimes_K L' \longrightarrow L[L']$ is injective. Surjectivity is trivial.

(1.45) Theorem: Let $K \subseteq L$ be an extension of fields with $\operatorname{char} K = p > 0$. Then:

(a) If L is separable over K, then L and $K^{p^{-\infty}}$ are linearly disjoint over K.

(b) If for some $n \in \mathbb{N}$ L and $K^{p^{-n}}$ are linearly disjoint over K, then L is separable over K.

Proof: (a) Let $\alpha_1, \dots, \alpha_n \in L$ be linearly independent over K and let $\gamma_1, \dots, \gamma_n \in K^{p^{-\infty}}$ with $\sum_{i=1}^n \gamma_i \alpha_i = 0$. With $K_1 = K(\gamma_1, \dots, \gamma_n)$, $[K_1 : K] < \infty$ and there is an $m \in \mathbb{N}$ with $K_1^{p^m} \subseteq K$. Since L is separable over K, the ring $A = L \otimes_K K_1$ is reduced. Moreover, A is a finite L-module and an Artinian ring. Consider the morphism of rings:

$$A = L \otimes_K K_1 \xrightarrow{\sigma} L$$
$$x \otimes y \longmapsto (xy)^{p^m}.$$

Let $P = \ker(\sigma)$.

Claim: P is the only prime ideal of A.

Pf of Cl: Since L is a field, P is prime. If $f = \sum x_i \otimes y_i \notin P$, then $(\sum x_i y_i)^{p^m} \neq 0$ and $f^{p^m} = (\sum x_i y_i)^{p^m} \otimes 1$ is a unit of A. Hence f is a unit.

Since A is a reduced local Artinian ring, A is a field and thus isomorphic to the subfield $L[K_1] \subseteq \overline{L}$, where $\overline{L}$ is the algebraic closure of L. In particular, L and K_1 are linearly disjoint over K.

By assumption $\sum y_i \alpha_i = 0$ with $\alpha_1, \dots, \alpha_n \in L$ linearly independent over K. By (1.44) $\alpha_1, \dots, \alpha_n$ are also linearly independent over K_1 and hence $y_i = 0$ for all $1 \leq i \leq n$. Thus L and $K^{p^{-\infty}}$ are linearly disjoint.

(b) Suppose that for some $n \in \mathbb{N}$, L and $K^{p^{-n}}$ are linearly disjoint. Then L and $K^{p^{-1}} \subseteq K^{p^{-n}}$ are linearly disjoint and $L \otimes_K K^{p^{-1}} \cong L[K^{p^{-1}}] = L(K^{p^{-1}}) \subseteq \overline{L}$. In particular, $L[K^{p^{-1}}]$ and $L \otimes_K K^{p^{-1}}$ are fields. By (1.26) it suffices to show that every finitely generated K-subalgebra A of L is separable over K. If $Q(A)$ denotes the field of quotients of A, then $Q(A) \otimes_K K^{p^{-1}}$ is reduced as subalgebra of $L \otimes_K K^{p^{-1}}$. By (1.31) $Q(A)$ is separable over K. Apply (1.26) again to conclude that A is separable over K.

(1.46) Proposition: Let $K \subseteq L \subseteq E$ be field extensions with $\operatorname{char} K = p > 0$. Let $L \subseteq E$ be separable. Then

(a) If $K \subseteq L$ is separable then $K \subseteq E$ is separable.

(b) If K is perfect (i.e. $K = K^p$) then any p-basis of L over K can be extended to a p-basis of E over K.

Proof: (a) Let $K \subseteq K'$ be a finitely generated field extension. By (1.26) it suffices to show that $E \otimes_K K'$ is reduced. Note that $E \otimes_K K' = E \otimes_L (L \otimes_K K')$ and T is a localization of a finitely generated L-algebra. Since $K \subseteq L$ separable, T is reduced. Thus the total ring of quotients $Q(T)$ of T is a product of

finitely many fields: $Q(T) = \prod_{i=1}^{r} L_i$, where each field L_i is finitely generated over L. Thus $E \otimes_L T \subseteq E \otimes_L Q(T) \cong \prod_{i=1}^{r} E \otimes_L L_i$. Since E is separable over L, each $E \otimes_L L_i$ is reduced. Hence $E \otimes_L T$ is reduced and E is separable over K.

(b) Let B be a p-basis of L over K. By Lemma (1.37) it is enough to show that B is p-independent over K as a subset of E. Suppose that $\alpha_1, \ldots, \alpha_n \in L$ are linearly independent over $L^p = L^p(K)$. Let $\beta_i^p \in E^p = E^p(K)$, $\beta_i \in E$, with $\sum_{i=1}^{n} \beta_i^p \alpha_i = 0$. Since E is separable over L, by (1.45) the field E and $L^{p^{-1}}$ are linearly disjoint over L. Moreover, $\alpha_1^{p^{-1}}, \ldots, \alpha_n^{p^{-1}} \in L^{p^{-1}}$ are linearly independent over L. By (1.44) $\alpha_1^{p^{-1}}, \ldots, \alpha_n^{p^{-1}}$ are linearly independent over E. The equation $\sum_{i=1}^{n} \beta_i^p \alpha_i = 0$ implies that $\sum \beta_i \alpha_i^{p^{-1}} = 0$ and hence $\beta_i = 0$ for all $1 \le i \le n$.

(1.47) Theorem: Let $K \subseteq L$ be a field extension. The following are equivalent:

(a) L is separable over K.

(b) The canonical map $\alpha: \Omega_K \otimes_K L \longrightarrow \Omega_L$ is injective.

(Ω_K denotes the module of differentials $\Omega_{K/P}$, where P is the prime field of K).

Proof: (a) $\Rightarrow$ (b): Case 1: $P = \mathbb{Q}$.

Let Γ be a transcendence basis of K over P. By (1.22) the set $\{\delta(x) \mid x \in \Gamma\}$ is a basis of the K-vector space Ω_K. Since Γ extends to a transcendence basis of L over P, α is injective.

Case 2: $\operatorname{char} K = p > 0$

By (1.46) a p-basis of K over P extends to a p-basis of L over P. Thus α is injective.

(b) $\Rightarrow$ (a): We may assume that $\operatorname{char} K = p > 0$. Let C be a p-basis of K over P. Since α is injective, C extends to a p-basis B of L over P. By (1.45) it suffices to show that L and $K^{p^{-1}}$ are linearly disjoint over K. Consider the sets: $C' = \{x^{p^{-1}} \mid x \in C\} \subseteq B' = \{y^{p^{-1}} \mid y \in B\}$. Obviously, C' is a p-basis of $K^{p^{-1}}$ over P and B' is a p-basis of $L^{p^{-1}}$ over P. Then $\Gamma_{C'} = \{(x_1^{\alpha_1} \cdots x_n^{\alpha_n})^{p^{-1}} \mid n \in \mathbb{N}, x_i \in C', 0 \le i < p\}$ is a basis

of the K-vector space $K^{p^{-1}}$. Define Γ_B, accordingly and set $\Gamma_C = \{\gamma_j\}_{j\in J}$. In particular, $\Gamma_C \subseteq \Gamma_B$, and Γ_C is linearly independent over L.

Let $\{\alpha_i\}_{i\in I}$ be a basis of L over K. Then $\{\alpha_i \otimes \gamma_j\}$ is a basis of the K-vector space $L\otimes_K K^{p^{-1}}$. Let $\varphi: L\otimes_K K^{p^{-1}} \longrightarrow L[K^{p^{-1}}]$ be the natural map. If $x = \sum \lambda_{ij}(\alpha_i \otimes \gamma_j) = \sum_{j=1}^{m}(\sum_{i=1}^{n}\lambda_{ij}\alpha_i)\otimes\gamma_j \in L\otimes_K K^{p^{-1}}$, $\lambda_{ij}\in K$, with $\varphi(x)=0$. Then $\varphi(x) = \sum_{j=1}^{m}(\sum_{i=1}^{n}\lambda_{ij}\alpha_i)\gamma_j = 0$ and $\sum_{i=1}^{n}\lambda_{ij}\alpha_i = 0$ for all $1\le j\le m$, since $\gamma_1,\dots,\gamma_m$ linearly independent over L. Since $\alpha_1,\dots,\alpha_n$ are linearly independent over K, $\lambda_{ij}=0$ for all $1\le i\le n$, $1\le j\le m$. Thus $x=0$ and φ is injective.

(1.48) Theorem: Let $K\subseteq L$ be a separable field extension with $\mathrm{char}(K)=p>0$. If B is a p-basis of L over K then:

(a) B is algebraically independent over K.

(b) The extension $K(B)\subseteq L$ is separable.

Proof: (a) Let $\beta_1,\dots,\beta_n \in B$ be algebraically dependent over K and let $f\in K[x_1,\dots,x_n]$, $f\neq 0$, with $f(\beta_1,\dots,\beta_n)=0$. We may assume that f has minimal total degree among all nonzero polynomials $g\in K[x_1,\dots,x_n]$ with $g(\beta_1,\dots,\beta_n)=0$. We may write

$$f(x_1,\dots,x_n) = \sum_{0\le i_1,\dots,i_n<p} h_{(i)}(x_1^p,\dots,x_n^p)\,x_1^{i_1}\cdots x_n^{i_n}.$$

Since $\beta_1,\dots,\beta_n$ are p-independent over K, for all (i) $h_{(i)}(\beta_1^p,\dots,\beta_n^p)=0$. Thus $f = h_{(i)}(x_1^p,\dots,x_n^p)\in K[x_1^p,\dots,x_n^p]$ for some (i). There is a polynomial $g\in K^{p^{-1}}[x_1,\dots,x_n]$ with $f(x_1,\dots,x_n) = g(x_1,\dots,x_n)^p$. If the total degree of f is d, then g is the sum of monomials $a_{j_1\dots j_n}x_1^{j_1}\cdots x_n^{j_n}$ of total degree $<d$. By the minimality of the total degree of f, the elements $\beta_1^{j_1}\cdots\beta_n^{j_n}$ with $j_1+\cdots+j_n<d$ are linearly independent over K. Since L is separable over K, L and $K^{p^{-1}}$ are linearly disjoint over K and thus the set $\{\beta_1^{j_1}\cdots\beta_n^{j_n} \mid j_1+\cdots+j_n<d\}$ is linearly independent over $K^{p^{-1}}$ and therefore $g(\beta_1,\dots,\beta_n)\neq 0$, a contradiction.

(b) By Theorem (1.47) it suffices to show that the natural morphism:

$\varphi: \Omega_{K(B)} \otimes_{K(B)} L \longrightarrow \Omega_L$ is injective. Consider the commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Omega_K \otimes_K L & \longrightarrow & \Omega_L & \longrightarrow & \Omega_{L/K} & \longrightarrow & 0 \\
 & & \uparrow \mathrm{id} & & \uparrow \varphi & & \uparrow \nu & & \\
 & & \Omega_K \otimes_K L & \longrightarrow & \Omega_{K(B)} \otimes_{K(B)} L & \longrightarrow & \Omega_{K(B)/K} \otimes_{K(B)} L & \longrightarrow & 0
\end{array}$$

It suffices to show that ν is injective. Since $K(B) = K(B)^p(K, B)$ and B p-independent over K, B is also a p-basis of $K(B)$ over K. Thus ν is an isomorphism and φ is injective.