Differentiale und Körpererweiterungen

Robert W. Berger

Sommersemester 1996

Inhaltsverzeichnis

1 Differentialmoduln **1**
Definitionen 1
Existenz der universellen Derivation 3
Zweiseitige Derivationen 4
Erste Konstruktion der universellen Derivation 5
Ausdehnung von Derivationen 5
Definitionen und Grundeigenschaften 6
Konstruktion der universellen Ausdehnung 10
Vergrößerung des Konstantenrings 15

2 Separable und inseparable Körpererweiterungen **17**
Inseparabilität einer Körpererweiterung 17
Separable Körpererweiterungen 20
Beliebige Körpererweiterungen 24
Der Hauptsatz 28
Separabilität und lineare Disjunktheit 29
Separabilität bei nicht endlich erzeugten Körpererweiterungen 33
Tensorielle Ausdehnung und Separabilität 35

Literaturverzeichnis **41**

Index **42**

Kapitel 1

Differentialmoduln

Definitionen

Im folgenden seien P, R kommutative (unitäre) Ringe, $\rho : P \to R$ ein (unitärer) Ringhomomorphismus und M ein (unitärer) R–Modul. Vermöge ρ fassen wir R als P-Algebra auf. In Anlehnung an die aus der Analysis bekannten Summen- und Produktregeln der Differentialrechnung definiert man

Definition 1.1 *Eine* Derivation (erster Ordnung) von R nach M *ist eine Abbildung* $\mathrm{D} : R \to M$ *mit:*

$$\left.\begin{array}{lrcll} 1. & \mathrm{D}(x+y) & = & \mathrm{D}(x)+\mathrm{D}(y) & \textit{(Summenregel)} \\ 2. & \mathrm{D}(x\cdot y) & = & x\cdot\mathrm{D}(y)+y\cdot\mathrm{D}(x) & \textit{(Produktregel)} \end{array}\right\} \textit{für alle } x,y \in R$$

D *heißt* ρ–Derivation *oder auch* Derivation über P *(Derivation von R/P), wenn außerdem gilt*

3. $\mathrm{D} \circ \rho = 0$.

Statt $\mathrm{D}(x)$ *schreiben wir auch einfach* $\mathrm{D}x$.
Ist T eine beliebige Teilmenge vom R, so bezeichnen wir mit $R\mathrm{D}T$ den von der Menge $\{\mathrm{D}t \mid t \in T\}$ erzeugten R-Untermodul von M.

Anmerkung 1.2 *Die Eigenschaft, Derivation über P zu sein, bedeutet, daß die Derivation P-linear ist.*

Anmerkung 1.3 (Quotientenregel) *Ist D eine Derivation von R, $r \in R$ und $t \in R$ eine Einheit von R, dann gilt die „Quotientenregel“:*
$\mathrm{D}\left(\frac{r}{t}\right) = \frac{1}{t^2}\cdot(t\cdot\mathrm{D}r - r\cdot\mathrm{D}t)$

Beweis: Wegen $t\cdot\frac{r}{t} = r$ gilt auf Grund der Produktregel $t\cdot\mathrm{D}\left(\frac{r}{t}\right)+\frac{r}{t}\cdot\mathrm{D}(t) = \mathrm{D}(r)$. Da t Einheit ist, liefert die Multiplikation mit $\frac{1}{t}$ die Behauptung. q.e.d.

Beispiel 1.4

- Die Nullabbildung $R \to \{0\}$ ist eine Derivation von R, die sogenannte „triviale Derivation“ .
- Sei $R = P[X]$ Polynomring in X, $\rho : P \hookrightarrow R$ die Inklusionsabbildung und $\mathrm{D}f := f'$ die formale Ableitung nach X, so ist $\mathrm{D} : R \to R$ eine Derivation von R über P nach R.
- Allgemeiner: Sei $R = P[\{X_\iota \mid \iota \in I\}]$ Polynomring über P in beliebig vielen Unbestimmten X_i, bezeichne $\mathrm{D}_\iota f := \frac{\partial f}{\partial X_\iota}$ die formale partielle Ableitung von f nach X_ι und sei $M = \bigoplus_{\iota \in I} R \cdot \mathrm{D}X_\iota$ der freie R-Modul mit der Basis $\{\mathrm{D}X_\iota \mid \iota \in I\}$, so sind die $\mathrm{D}_\iota : R \to R$ Derivationen von R über P nach R und $\mathrm{D} : R \to M$ mit $\mathrm{D}f := \sum \frac{\partial f}{\partial X_\iota} \cdot \mathrm{D}X_\iota$ eine Derivation von R über P nach M .

Anmerkung 1.5 *Ist R° der in R enthaltene Primring, so ist jede Derivation von R stets eine Derivation über R°.*

Beweis: Es genügt zu zeigen, daß für jede Derivation D stets gilt $D1 = 0$, wenn 1 das Einselement von R bezeichnet. Es gilt sogar allgemeiner $De = 0$ für jedes Idempotent e von R:
Aus $e \cdot e \cdot e = e$ bzw. $e \cdot e = e$ folgt nach der Produktregel

$$\begin{aligned} e \cdot \mathrm{D}e + e \cdot \mathrm{D}e + e \cdot \mathrm{D}e &= \mathrm{D}e \\ e \cdot \mathrm{D}e + e \cdot \mathrm{D}e &= \mathrm{D}e \end{aligned}$$

Durch Subtraktion der beiden Gleichungen folgt $e \cdot \mathrm{D}e = 0$ und daher
$\mathrm{D}e = e \cdot \mathrm{D}e + e \cdot \mathrm{D}e = 0$ q.e.d.

Anmerkung 1.6 *Mit D_1 und D_2 ist auch $\mathrm{D}_1 + \mathrm{D}_2$ eine Derivation von R über P nach M. Ferner ist für alle $r \in R$ auch $r \cdot \mathrm{D}_1$ eine Derivation von R über P nach M. Die Derivationen von R über P nach M bilden also in natürlicher Weise einen R-Modul $\mathrm{Der}_P(R, M)$.*

Beispiel 1.7 Betrachte wie in Beispiel 1.4 $R := P[X_1 \ldots, X_n]$.
Dann ist $\mathrm{Der}_P(R, R) = \bigoplus_{i=1}^{n} R \cdot \frac{\partial}{\partial X_i}$ freier R-Modul mit der Basis $\{\frac{\partial}{\partial X_1}, \ldots, \frac{\partial}{\partial X_n}\}$.

Beweis: Sei D eine beliebige Derivation von R über P nach R. Auf Grund der Summen- und Produktregel zusammen mit der P-Linearität sieht man, daß für ein beliebiges Polynom $f \in R$ gilt: $\mathrm{D}f = \sum_{i=1}^{n} \frac{\partial f}{\partial X_i} \cdot \mathrm{D}X_i$. Also ist $\mathrm{D} = \sum_{i=1}^{n} (\mathrm{D}X_i) \cdot \frac{\partial}{\partial X_i}$. Ferner sind wegen $\frac{\partial X_i}{\partial X_j} = \delta_{ij}$ die $\{\frac{\partial}{\partial X_1}, \ldots, \frac{\partial}{\partial X_n}\}$ linear unabhängig über R. q.e.d.

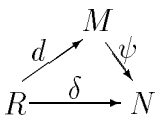
Einen Überblick über die verschiedenen Derivationen einer Ringerweiterung R/P erhält man, indem man nach Kähler [Kä] den sogenannten „universellen Differentialmodul“ $\Omega(R/P)$ bildet:

Ist $\mathrm{D} : R \to M$ eine Derivation von R/P und $\varphi : M \to N$ ein R-Modulhomomorphismus, dann ist offenbar $\varphi \circ \mathrm{D}$ eine Derivation von R/P nach N. Wir nennen dann $\varphi \circ \mathrm{D}$ eine *Spezialisierung* von D.

Definition 1.8 *Eine Abbildung* $\mathrm{d} : R \to M$ *heißt* universelle Derivation von R über P, *wenn gilt:*

1. d *ist eine Derivation von* R *über* P.

2. *Ist* $\delta : R \to N$ *eine beliebige Derivation von* R *über* P, *so existiert* genau eine R*-lineare Abbildung* $\psi : M \to N$ *mit* $\delta = \psi \circ \mathrm{d}$.
   (D.h. Jede Derivation von R/P *ist auf genau eine Weise Spezialisierung von* d *.)*



Auf Grund dieser Definition ist zunächst klar, daß eine solche universelle Derivation von R/P, falls sie existiert, bis auf natürliche R-Isomorphie eindeutig bestimmt ist. Wir sprechen daher im folgenden von *der* universellen Derivation von R/P und nennen der dazugehörigen Modul M den *Kählerschen Differentialmodul* oder auch den *universellen Differentialmodul* von R über P.
Wir bezeichnen die universelle Derivation von R/P mit $\mathrm{d}_{R/P}$ und den universellen Differentialmodul von R/P mit $\Omega(R/P)$. Falls P der in R enthaltene Primring ist, nennen wir $\mathrm{d}_{R/P}$ die *absolute universelle Derivation von* R. Wir bezeichnen sie dann mit d_R und den zugehörigen *absoluten universellen Differentialmodul von* R mit $\Omega(R)$
Nach Definition ist sofort klar, daß

$$\mathrm{Der}_P(R,R) = \mathrm{Hom}_R\left(\Omega(R/P), R\right) \tag{1.1}$$

ist. Falls R ein Körper und $\Omega(R/P)$ ein endlich erzeugter R-Vektorraum ist, gilt auf Grund der Dualität $\Omega(R/P) \cong \mathrm{Hom}(\mathrm{Der}_P(R,R), R)$. In diesem Falle läßt sich also auch der universelle Differentialmodul aus dem Modul der Derivationen von R nach R berechnen. Im allgemeinen enthält aber der universelle Differentialmodul mehr Information als $\mathrm{Der}_P(R,R)$.

Existenz der universellen Derivation

Obwohl sich später (Satz 1.29) bei der Konstruktion der universellen Ausdehnung einer Derivation ein in gewissem Sinne konstruktiver Existenzbeweis für die universelle Derivation von R/P als Spezialfall ergeben wird, ist es auch nützlich, die folgende abstraktere Konstruktion zu betrachten.

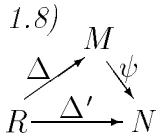
Zweiseitige Derivationen

Sei $R^e := R \otimes_P R$ und M ein zweiseitiger R-Modul (R-Bimodul), für den zusätzlich gilt $r \cdot z = z \cdot r$ für alle $r \in P$. Man kann M in natürlicher Weise auch als R^e-Linksmodul auffassen mittels $x \otimes y \cdot z := x \cdot z \cdot y$ für alle $x, y \in R$ und alle $z \in M$. Ein R-Bimodulhomomorphismus ist dann dasselbe wie ein R^e-Linksmodulhomomorphismus

Definition 1.9 *Eine* zweiseitige Derivation von R über P nach M *ist eine Abbildung* $\Delta : R \to M$ *mit:*

$$\left.\begin{array}{lrcll} 1) & \Delta(x+y) & = & \Delta(x)+\Delta(y) & \textit{(Summenregel)} \\ 2) & \Delta(x\cdot y) & = & x\cdot\Delta(y)+\Delta(x)\cdot y & \textit{(Produktregel)} \\ 3) & \Delta\circ\rho & = & 0 & \end{array}\right\} \textit{für alle } x,y \in R$$

Δ *heißt* universelle zweiseitige Derivation *von R über P, wenn es zu jeder zweiseitigen Derivation Δ' von R genau einen R-Bimodulhomomorphismus ψ gibt mit $\Delta' = \psi \circ \Delta$. (vgl. Definition 1.8)*



Für die Konstruktion der universellen zweiseitigen Derivation von R über P benötigen wir zunächst:

Hilfssatz 1.10 *Sei $\varphi : R \otimes_P R \to R$ der durch die P-bilineare Abbildung $R \times R \to R$ mit $(x,y) \mapsto x \cdot y$ induzierte Ringhomomorphismus und $I := \mathrm{Ker}\,(\varphi)$. Dann gilt $\varphi(x \otimes y) = x \cdot y$ und I wird als R^e-Modul erzeugt von $\{1 \otimes x - x \otimes 1 \mid x \in R\}$.*

Beweis: Zunächst ist klar, daß $\varphi(x \otimes y) = x \cdot y$ und $I \subseteq \mathrm{Ker}\,(\varphi)$ gilt. Ist umgekehrt $\sum x_i \otimes y_i \in \mathrm{Ker}\,(\varphi)$, so gilt $\sum x_i \cdot y_i = 0$ nach Definition von φ. Also ist auch
$\sum (x_i y_i \otimes 1) = (\sum x_i y_i) \otimes 1 = 0$
und daher
$\sum x_i \otimes y_i = \sum x_i \otimes y_i - \sum x_i y_i \otimes 1 = \sum x_i (1 \otimes y_i - y_i \otimes 1) \in I$. q.e.d.

Satz 1.11 *Die Abbildung $\Delta : R \to I$ mit $\Delta(x) := 1 \otimes x - x \otimes 1 \in I$ ist universelle zweiseitige Derivation von R über P.*

Beweis: Die Summenregel für Δ ist klar, ebenso, daß $\Delta(P) = 0$ ist. Produktregel: Seien $x, y \in R$. Dann ist $\Delta(x \cdot y) = 1 \otimes (xy) - (xy) \otimes 1 = x \cdot (1 \otimes y - y \otimes 1) + (1 \otimes x - x \otimes 1) \cdot y = x \cdot \Delta(y) + \Delta(x) \cdot y$. Also ist Δ eine zweiseitige Derivation von R über P. Sei nun $\Delta' : R \to N$ eine beliebige zweiseitige Derivation von R über P. Durch $(x,y) \mapsto x \cdot \Delta' y \in N$ wird eine P-bilineare Abbildung von $R \times R$ nach N definiert. Sei $\Psi : R \otimes_P R \to N$ die durch diese induzierte P-lineare Abbildung

und $\psi : I \to N$ die Einschränkung von Ψ auf I. Dann ist $\psi(1 \otimes x - x \otimes 1) = \Delta'(x)$ für alle $x \in R$, also $\Delta' = \psi \circ \Delta$. Außerdem rechnet man sofort nach, daß ψ sogar ein R-Bimodulhomomorphismus ist.(Ψ dagegen nicht!). Ferner ist ψ durch Δ' eindeutig bestimmt, da I nach Hilfssatz 1.10 durch $\Delta(R)$ erzeugt wird. Also ist Δ universelle zweiseitige Derivation von R. q.e.d.

Erste Konstruktion der universellen Derivation

Aus der universellen zweiseitigen Derivation Δ von R/P läßt sich nun leicht die universelle Derivation im Sinne von Definition 1.8 bilden:
Zunächst kann man jeden R-Linksmodul M auch als R-Bimodul auffassen durch die Definition $z \cdot r := r \cdot z$ für alle $r \in R$ und alle $z \in M$. Jede Derivation $\mathrm{D} : R \to M$ von R über P ist mit dieser Definition von M als R-Bimodul auch eine zweiseitige Derivation von R über P. Also gibt es zu D einen R-Bimodulhomomorphismus $\tilde{\psi} : I \to M$ mit $\mathrm{D} = \tilde{\psi} \circ \Delta$. Es ist $\tilde{\psi}(I^2) = (0)$; denn für alle $z \in I$ und $x \in R$ gilt $\tilde{\psi}\left((1 \otimes x - x \otimes 1) \cdot z\right) = (1 \otimes x - x \otimes 1) \cdot \tilde{\psi}(z)$
$= \tilde{\psi}(z) \cdot x - x \cdot \tilde{\psi}(z) = 0$ nach Definition der Bimodulstruktur auf M. Daher induziert $\tilde{\psi}$ in natürlicher Weise einen R^e-Homomorphismus $\psi : I/I^2 \to M$. Sei ferner $\mathrm{d} := \chi \circ \Delta$, wobei $\chi : I \to I/I^2$ den kanonischen Homomorphismus bezeichnet, so gilt $\mathrm{D} = \psi \circ d$. Auf I/I^2 stimmen Rechts- und Linksmultiplikation mit Elementen von R überein (vgl. oben), also ist d auch eine (gewöhnliche) Derivation und ψ eine R-lineare Abbildung. Ferner wird I/I^2 als R-Modul von $\mathrm{d}(R)$ erzeugt, und daher ist ψ mit $\mathrm{D} = \psi \circ \mathrm{d}$ durch D eindeutig bestimmt. Es folgt:

Satz 1.12 *Sei I wie in Hilfssatz 1.10. Sei ferner* $\mathrm{d} : R \to I/I^2$ *definiert durch* $\mathrm{d}(x) := 1 \otimes x - x \otimes 1 \bmod I^2$.
Dann gilt: d *ist die universelle Derivation von R über P.*

Ausdehnung von Derivationen

Bei der Frage, ob sich eine gegebene Derivation $\mathrm{D} : R \to M$ auf einen Oberring S von R fortsetzen läßt, erkennt man sehr schnell, daß dies im allgemeinen nicht möglich ist:

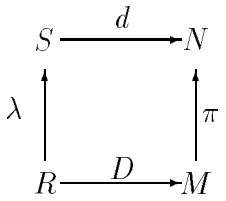
Beispiel 1.13 *Sei P ein beliebiger Körper von Primzahlcharakteristik p, z.B. $P := \mathbb{Z}/(p)$, $R := P[X]$ der Polynomring in X über P und $S := R[y]$ mit $y^p = X$ eine rein inseparable Körpererweiterung von R. Sei ferner* $\mathrm{D} : R \to M$ *eine beliebige Derivation von R mit* $\mathrm{D}X \neq 0$ *(etwa* $\mathrm{D} := \frac{\partial}{\partial X}$ *). Dann läßt sich* D *nicht zu einer Derivation* D' *von S in einen S-Modul N fortsetzen; denn für eine solche Fortsetzung würde gelten:* $\mathrm{D}'X = \mathrm{D}'(y^p) = p \cdot y^{p-1} \cdot \mathrm{D}'(y) = 0 \neq \mathrm{D}X$.

Daher wird der Begriff der Fortsetzung zu dem Begriff der Ausdehnung [Be1] abgeschwächt. Allerdings ist der Begriff der Ausdehnung insofern zu schwach,

als die triviale Derivation des Oberrings stets Ausdehnung jeder Derivation des Unterrings ist. Bedeutung gewinnt er erst durch die zusätzlichen Forderungen, daß die Ausdehnung „universell“, „tensoriell“ oder „Fortsetzung“ ist.

Definitionen und Grundeigenschaften

Definition 1.14 *Seien* $\lambda : R \to S$ *ein Ringhomomorphismus,*
$\mathrm{D} : R \to M$ *eine Derivation von* R*,*
$\mathrm{d} : S \to N$ *eine Derivation von* S*,*
$\pi : M \to N$ *eine* R*-lineare Abbildung. (Man faßt dabei den* S*-Modul* N *vermöge* λ *als* R*-Modul auf.)*
Ein Paar (d, π) *heißt „*λ*-Ausdehnung“ von* D*, wenn gilt*
$\mathrm{d} \circ \lambda = \pi \circ \mathrm{D}$.
D.h., wenn das Diagramm

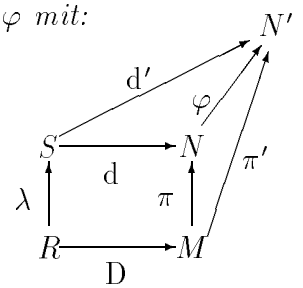


kommutativ ist.
(Wenn klar ist, um welche Abbildungen λ und π es sich handelt, sagen wir auch einfach, daß d Ausdehnung von D ist.)
d *bzw.* (d, π) *heißt (*λ*-) „Fortsetzung“ von* D*, wenn* π *injektiv ist.*

Anmerkung 1.15 *Sei* (d, π) *eine* λ*-Ausdehnung von* D*,*
$\varphi : N \to N'$ *eine* S*-lineare Abbildung, dann ist* $(\varphi \circ \mathrm{d}, \varphi \circ \pi)$ *wieder eine* λ*-Ausdehnung von* D*. („Spezialisierung“ von* (d, π)*.)*

Definition 1.16 *Seien* D*,* d*,* R*,* S*,* M*,* N*,* π*,* λ *wie in Definition 1.14*
(d, π) *heißt „universelle* λ*-Ausdehnung von* D*“, wenn gilt:*

1. (d, π) *ist eine* λ*-Ausdehnung von* D*.*
2. *Ist* (d', π') *eine beliebige* λ*-Ausdehnung von* D*, so existiert* genau eine S*-lineare Abbildung* φ *mit:*
   $\mathrm{d}' = \varphi \circ \mathrm{d}$
   $\pi' = \varphi \circ \pi$.



Anmerkung 1.17 *Ist* $M = R\,\mathrm{D}R$ *und ist* (d', π') *eine* λ*-Ausdehnung von* D*, so folgt aus* $\mathrm{d}' = \varphi \circ \mathrm{d}$ *schon* $\pi' = \varphi \circ \pi$

Beweis: Für alle $x \in R$ gilt: $\varphi \circ \pi(\mathrm{D}x) = \varphi \circ \mathrm{d} \circ \lambda(x) = \mathrm{d}' \circ \lambda(x) = \pi'(\mathrm{D}x)$. Also ist $\varphi \circ \pi = \pi'$, da nach Voraussetzung M als R-Modul von den $\mathrm{D}x$ erzeugt wird und die Abbildungen R-linear sind. q.e.d.

Satz 1.18 *Eine universelle λ-Ausdehnung einer Derivation D ist bis auf natürliche S-Isomorphie eindeutig bestimmt; d.h: Ist auch (d', π') universelle λ-Ausdehnung von D, so ist die Abbildung φ von Definition 1.16 ein Isomorphismus.*

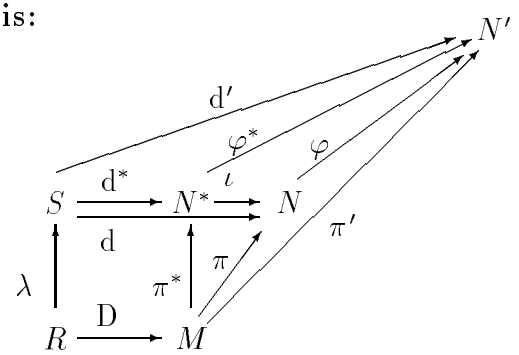
Wir sprechen daher meist von *der* universellen λ-Ausdehnung von D.
Beweis wie üblich bei Definition durch universelle Eigenschaft.

Im Hinblick auf die Berechnung der universellen Ausdehnung ist der folgende Satz von Interesse (vgl. auch Anmerkung 1.17), da er oft das Nachprüfen der eindeutigen Bestimmtheit von φ erspart:

Satz 1.19 *Sei (d, π) mit $\mathrm{d} : S \to N$ eine λ-Ausdehnung einer Derivation $\mathrm{D} : R \to M$. Es gilt:*
(d, π) ist genau dann universelle λ-Ausdehnung von D, wenn gilt:

1. $N = S\langle \mathrm{d}S, \pi(M)\rangle$
2. *Ist (d', π') eine beliebige λ-Ausdehnung von D, so gibt es eine S-lineare Abbildung φ mit $\mathrm{d}' = \varphi \circ \mathrm{d}$ und $\pi' = \varphi \circ \pi$.*

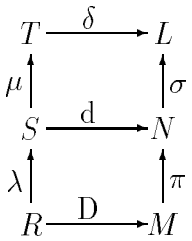
Beweis:



$\underline{\Leftarrow}$: Es ist zu zeigen, daß φ eindeutig durch (d', π') bestimmt ist:
Es ist $\varphi(\mathrm{d}x) = \mathrm{d}'x$ für alle $x \in S$ und $\varphi(\pi(y)) = \pi'(y)$ für alle $y \in M$. Da N nach Voraussetzung als S-Modul von $\mathrm{d}S$ und $\pi(M)$ erzeugt wird und φ eine S-lineare Abbildung ist, ist φ dadurch auf ganz N durch d' und π' festgelegt.
$\underline{\Rightarrow}$: Sei (d, π) universelle und (d', π') eine beliebige λ-Ausdehnung von D, so gilt 2. nach Definition. Bleibt 1. zu zeigen:
Sei $N^* := S\langle \mathrm{d}(S), \pi(M)\rangle$ und $\iota : N^* \hookrightarrow N$ die Inklusionsabbildung.
Seien $\pi^* := \pi \mid (M \to N^*)$
$\mathrm{d}^* := \mathrm{d} \mid (S \to N^*)$
die Einschränkungen der betreffenden Abbildungen. Also
$\mathrm{d} = \iota \circ \mathrm{d}^*$

$\pi = \iota \circ \pi^*$
Dann ist auch (d^*, π^*) universelle λ-Ausdehnung von D:
Da (d, π) universelle λ-Ausdehnung von D ist, existiert eine S-lineare Abbildung $\varphi : N \to N'$ mit $\mathrm{d}' = \varphi \circ \mathrm{d}$ und $\pi' = \varphi \circ \pi$.
Setze $\varphi^* = \varphi \circ \iota$.
$\Rightarrow \varphi^* \circ \mathrm{d}^* = \varphi \circ \iota \circ \mathrm{d}^* = \varphi \circ \mathrm{d} = \mathrm{d}'$ und $\varphi^* \circ \pi^* = \varphi \circ \iota \circ \pi^* = \varphi \circ \pi = \pi'$
Nach $\underline{\Leftarrow}$ folgt, daß φ^* durch diese beiden Eigenschaften auch eindeutig bestimmt ist. Also ist auch (d^*, π^*) universelle λ-Ausdehnung von D. Da (d, π) auch eine λ-Ausdehnung von D ist, gibt es also *genau eine* S-lineare Abbildung $\psi : N^* \to N$ mit
$d = \psi \circ \mathrm{d}^*$ und $\pi = \psi \circ \pi^*$,
und nach Satz 1.18 ist ψ ein Isomorphismus, also insbesondere surjektiv.
Es ist aber auch
$\mathrm{d} = \iota \circ \mathrm{d}^*$ und $\pi = \iota \circ \pi^*$.
Folglich ist $\iota = \psi$ surjektiv, also $N = N^*$ q.e.d.

Satz 1.20 (Transitivität der universellen Ausdehnung) *Seien*
$R \xrightarrow{\lambda} S \xrightarrow{\mu} T$ *Ringhomorphismen,*
D *eine Derivation von* R,
(d, π) *die universelle* λ*-Ausdehnung von* D,
(δ, σ) *die universelle* μ*-Ausdehnung von* d.
Dann ist $(\delta, \sigma \circ \pi)$ *die universelle* $\mu \circ \lambda$*-Ausdehnung von* D.

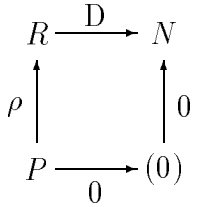


Beweis durch direktes Nachrechnen mit der universellen Eigenschaft unter Verwendung von Satz 1.19.

Der Zusammenhang mit der universellen Derivation (Definition 1.8) von R über P wird durch den folgenden Satz hergestellt:

Satz 1.21 *Sei* $\rho : P \to R$ *ein Ringhomomorphismus,* $\mathrm{d} : R \to M$ *eine Derivation von* R. *Es gilt:*
d *ist genau dann universelle Derivation von* R *über* P, *wenn* $(\mathrm{d}, 0)$ *universelle* ρ*-Ausdehnung der trivialen Derivation von* P *ist.*

Beweis: Nach Definition ist eine Derivation $\mathrm{D} : R \to N$ genau dann eine ρ-Derivation, wenn $\mathrm{D} \circ \rho = 0 = 0 \circ 0$ ist. Das bedeutet aber gerade, daß $(\mathrm{D}, 0)$ eine ρ-Ausdehnung der trivialen Derivation von P ist. Daraus folgt unmittelbar die Behauptung. q.e.d.

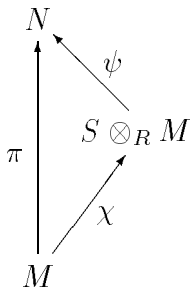


Korollar 1.22 *Sei* $\mathrm{d} : R \to M$ *universelle Derivation von* R *über* P*. Dann gilt:* $M = R\,\mathrm{d}R$

Beweis (vgl. auch Satz 1.12): Nach Satz 1.19 zusammen mit Satz 1.21 ist $M = R\langle \mathrm{d}R, 0(0)\rangle = R\langle \mathrm{d}R\rangle = R\,\mathrm{d}R$. q.e.d.

Neben der universellen Ausdehnung spielt auch der Begriff der „tensoriellen Ausdehnung“ oft eine Rolle. Beispielsweise lassen sich mit seiner Hilfe separable Körpererweiterungen charakterisieren (s. Satz 2.42).

Anmerkung 1.23 *Sei* $\lambda : R \to S$ *ein Ringhomomorphismus,* $\mathrm{D} : R \to M$ *eine Derivation von* R*,* (d, π) *eine* λ*-Ausdehnung von* D*,*
$\mathrm{d} : S \to N$*.*
Ferner sei $\chi : M \to S \otimes_R M$ *die kanonische* R*-lineare Abbildung mit* $m \mapsto 1 \otimes m$*,*
$\pi : M \to N$ *ist eine* R*-lineare Abbildung von* M *in den* S*-Modul* N*.*
Auf Grund der universellen Eigenschaft des Tensorproduktes gibt es genau eine S*-lineare Abbildung*
$\psi : S \otimes_R M \to N$ *mit* $\pi = \psi \circ \chi$



Mit diesen Bezeichnungen definieren wir:

Definition 1.24 (d, π) *heißt „tensorielle Ausdehnung“ von* D*, wenn* ψ *injektiv ist.* (In diesem Falle können wir $S \otimes_R M$ als R-Untermodul von N betrachten.) *Falls* (d, π) universelle *Ausdehnung von* D *ist, bezeichnen wir* $\mathrm{T}(S/\mathrm{D}) := \mathrm{Ker}\ \psi$*.*

Anmerkung 1.25

1. (d, π) *ist tensorielle Ausdehnung von* D $\Leftrightarrow S \otimes_R M \cong S \cdot \pi(M)$ *vermöge* ψ*.*

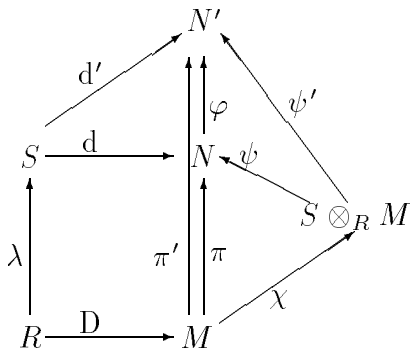
2. *Ist* $\chi : M \to S \otimes_R M$ *injektiv und* (d, π) *tensorielle Ausdehnung von* D*, so ist* π *injektiv, also* (d, π) *Fortsetzung von* D*. Die Voraussetzung, daß* χ *injektiv ist, ist z.B. stets erfüllt, wenn* λ *injektiv und* M *ein freier* R*-Modul ist. Insbesondere ist dies der Fall, wenn* R *ein Körper ist.*

Anmerkung 1.26

1. *Eine tensorielle Ausdehnung existiert im allgemeinen nicht.*

2. *Wenn sie aber existiert, dann ist auch die universelle Ausdehnung tensoriell.*

Beweis: 1) Aus Satz 2.42 folgt, daß bei einer inseparablen Körpererweiterung K/k die absolute universelle Derivation von k keine tensorielle Ausdehnung auf K besitzt. In Beispiel 2.48 wird sogar ein explizites Beispiel einer einfachen Körpererweiterung K/k angegeben, bei der die absolute universelle Derivation von k zwar eine Fortsetzung auf K besitzt, aber nicht tensoriell ausdehnbar ist.



2) Seien (d, π) die universelle und (d', π') eine tensorielle λ-Ausdehnung von D. Dann gibt es nach Anmerkung 1.23 (genau) eine S-lineare Abbildung $\psi : S \otimes_R M \to N$ mit $\pi = \psi \circ \chi$ und *genau eine* S-lineare Abbildung $\psi' : S \otimes_R M \to N'$ mit $\pi' = \psi' \circ \chi$. Ferner existiert nach Definition der universellen Ausdehnung (genau) eine S-lineare Abbildung $\varphi : N \to N'$ mit $\pi' = \varphi \circ \pi$.
Man hat dann $\pi' = \varphi \circ \pi = \varphi \circ (\psi \circ \chi) = (\varphi \circ \psi) \circ \chi$. Da aber ψ' durch die Gleichung $\pi' = \psi' \circ \chi$ eindeutig bestimmt ist, folgt $\varphi \circ \psi = \psi'$. Nach Voraussetzung ist nun (d', π') tensorielle Ausdehnung von D und daher nach Definition ψ' injektiv. Dann ist aber wegen $\psi' = \varphi \circ \psi$ auch ψ injektiv, also (d, π) tensorielle Ausdehnung. q.e.d.

Da, wie im nächsten Abschnitt gezeigt wird, die universelle Ausdehnung immer existiert, ist damit die Frage nach der Existenz einer tensoriellen Ausdehnung im Einzelfall auf die Untersuchung zurückgeführt, ob die universelle Ausdehnung tensoriell ist. Dies läßt sich unter Benutzung der im nächsten Abschnitt angegebenen Konstruktion der universellen Ausdehnung oft einfach entscheiden.

Konstruktion der universellen Ausdehnung

Wir geben im folgenden eine Konstruktion der universellen λ-Ausdehnung an, die zugleich einen Existenzbeweis liefert. Damit hat man wegen Satz 1.21 auch eine Konstruktionsvorschrift und einen zweiten Existenzbeweis für die universelle Derivation von R über P. Wir gehen dabei in drei Schritten vor: Zunächst konstruieren wir die universelle Ausdehnung auf einen Polynomring über R (Satz 1.27) und dann auf einen Faktorring von R (Satz 1.28). Schließlich konstruieren wir durch Zusammenfügen der beiden ersten Schritte eine beliebige λ-Ausdehnung (Satz 1.29). Für den Fall der universellen Ausdehnung auf einen Quotientenring von R geben wir schließlich noch eine spezielle Konstruktion an, die der Situation besser angepaßt ist (Satz 1.30).

Satz 1.27 (Universelle Ausdehnung auf einen Polynomring) *Sei*
$S = R[\{X_\iota \mid \iota \in J\}]$ *der Polynomring über* R *in den Unbestimmten* X_ι, *wobei die* ι *einer beliebigen Indexmenge* J *entstammen,*
$\lambda : R \hookrightarrow S$ *die Inklusionsabbildung,*
$\mathrm{D} : R \to M$ *eine beliebige Derivation von* R.

Dann existiert die universelle λ-Ausdehnung (d,π) von D und man erhält sie folgendermaßen:
Bilde $N := S \otimes_R M \oplus \bigoplus_{\iota\in J} S\cdot\Delta X_\iota$,
wobei die große direkte Summe den freien S-Modul mit Unbestimmten ΔX_ι als Basis bezeichnet.
Für ein Polynom $f = \sum a_{\nu_1\dots\nu_n}\cdot X_{\iota_1}^{\nu_1}\cdots X_{\iota_n}^{\nu_n}$ *sei*
$\delta f := \sum X_{\iota_1}^{\nu_1}\cdots X_{\iota_n}^{\nu_n}\otimes \mathrm{D}(a_{\nu_1\dots\nu_n}) \in S\otimes_R M$,
und $\frac{\partial f}{\partial X_\iota}$ *bezeichne die formale partielle Ableitung nach der Unbestimmten* X_ι.
Definiere:
$d : S \to N$ *durch*
$\mathrm{d}f := \delta f + \sum \frac{\partial f}{\partial X_\iota}\cdot\Delta X_\iota$ *für alle* $f\in S$
und
$\pi : M \to N$ *durch*
$\pi(y) := 1\otimes y + 0$ *für alle* $y\in M$.
Dann ist (d,π) universelle λ-Ausdehnung von D.

Beweis: Zunächst rechnet man sofort nach, daß d eine Derivation und (d,π) eine λ-Ausdehnung von D ist.
Sei (d',π') eine beliebige λ-Ausdehnung von D. Für $f\in S$ gilt auf Grund der Summen- und Produktregel
$\mathrm{d}'(f) = \sum X_{\iota_1}^{\nu_1}\cdots X_{\iota_n}^{\nu_n}\cdot \mathrm{d}'\circ\lambda(a_{\nu_1\dots\nu_n}) + \sum\frac{\partial f}{\partial X_\iota}\cdot \mathrm{d}'X\iota \in N'$.
Sei $\varphi_1 : S\otimes_R M \to N'$ die durch die bilineare Abbildung $S\times M\to N'$ mit $(s,y)\mapsto s\cdot\pi'(y)$ definierte S-lineare Abbildung.
Sei ferner $\varphi_2 : \bigoplus_\iota S\cdot\Delta X_\iota \to N'$ die durch $\Delta X_\iota \mapsto \mathrm{d}'X_\iota$ definierte S-lineare Abbildung.
Dann definiert $\varphi := \varphi_1\oplus\varphi_2 : N\to N'$ eine S-lineare Abbildung und es ist:

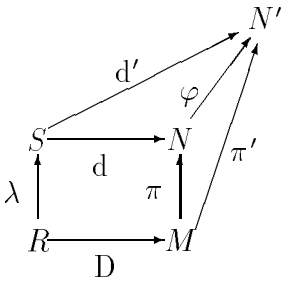
$$\begin{aligned}
\varphi\circ\mathrm{d}(f) &= \sum\varphi_1\left(X_{\iota_1}^{\nu_1}\cdots X_{\iota_n}^{\nu_n}\otimes\mathrm{D}(a_{\nu_1\dots\nu_n})\right) + \sum\frac{\partial f}{\partial X_\iota}\cdot\varphi_2(\Delta X_\iota)\\
&= \sum X_{\iota_1}^{\nu_1}\cdots X_{\iota_n}^{\nu_n}\cdot\underbrace{\pi'\circ\mathrm{D}}_{=\mathrm{d}'\circ\lambda}(a_{\nu_1\dots\nu_n}) + \sum\frac{\partial f}{\partial X_\iota}\cdot\mathrm{d}'X_\iota\\
&= \mathrm{d}'(f)
\end{aligned}$$

Nach Definition gilt auch
$\varphi\circ\pi(y) = \varphi_1(1\otimes y) = \pi'(y)$ für alle $y\in M$.
Da ferner nach Konstruktion $N = \langle \mathrm{d}S, \pi(M)\rangle$ gilt, folgt aus Satz 1.19, daß (d,π) universelle λ-Ausdehnung von D ist. q.e.d.

Satz 1.28 (Universelle Ausdehnung auf einen Faktorring) *Sei*
$\lambda : R\to S$ *ein* surjektiver *Ringhomomorphismus*
$\mathrm{D} : R\to M$ *eine beliebige Derivation von R*
Dann existiert die universelle λ-Ausdehnung (d,π) von D und man erhält sie

folgendermaßen:
Sei $n = \operatorname{Ker}\lambda$, $N := M/\langle n \cdot M, R\,\mathrm{D}n\rangle$.
Sei $\pi : M \to N$ *der Restklassenhomomorphismus und*
$\mathrm{d} : S \to N$ *definiert durch*
$\mathrm{d}(x) := \pi(\mathrm{D}(\lambda^{-1}(x)))$
Dann ist (d, π) *universelle* λ*-Ausdehnung von D.*
Zusatz: *1) Ist* $M = R\mathrm{D}R$, *so ist* $n \cdot M \subseteq R\,\mathrm{D}n$, *also* $N = M/R\,\mathrm{D}n$.
2) Ist $n = (\{f_\kappa \mid \kappa \in K\})$, *so ist* $R\,\mathrm{D}n = R\langle\{\mathrm{D}f_\kappa \mid \kappa \in K\}\rangle + n \cdot \mathrm{D}R$.

Beweis: Zunächst ist d wohldefiniert; denn sind $y_1, y_2 \in \lambda^{-1}(x)$, dann ist $y_2 - y_1 \in n$ also $\mathrm{D}(y_1) - \mathrm{D}(y_2) \in \mathrm{D}n \subseteq \operatorname{Ker}(\pi)$ und daher $\pi(\mathrm{D}(y_1)) = \pi(\mathrm{D}(y_2))$.
Ferner ist N in natürlicher Weise ein S-Modul durch die Definition $x \cdot y := \pi(\lambda^{-1}(x) \cdot \pi^{-1}(y))$ für alle $x \in S$ und $y \in M$. (Wegen $\operatorname{Ker}(\lambda) \cdot M \subseteq \operatorname{Ker}(\pi)$ ist auch diese Definition sinnvoll.)
d ist eine Derivation, und es gilt nach Definition $\mathrm{d} \circ \lambda = \pi \circ \mathrm{D}$, d.h. (d, π) ist eine λ-Ausdehnung von D.
Universelle Ausdehnung:
Sei (d', π') eine beliebige λ-Ausdehnung von D.
N' ist ein S-Modul, dessen R-Modulstruktur durch λ definiert ist. Also ist $n \cdot N' = (0)$, also $n \cdot M \subseteq \operatorname{Ker}(\pi')$
Ferner ist $\pi'(\mathrm{D}n) = \mathrm{d}'(\lambda(n)) = (0)$, also insgesamt:
$\langle n \cdot M, R\mathrm{D}n\rangle \subseteq \operatorname{Ker}(\pi')$. Also induziert π' *genau eine* S-lineare Abbildung $\varphi : N \to N'$ mit $\pi' = \varphi \circ \pi$.



Es ist aber auch $\mathrm{d}' \circ \lambda(x) = \pi' \circ \mathrm{D}(x) = \varphi \circ \pi \circ \mathrm{D}(x) = \varphi \circ \mathrm{d} \circ \lambda(x)$ für alle $x \in R$.
Da λ surjektiv ist, folgt $\mathrm{d}' = \varphi \circ \mathrm{d}$.
Beweis der Zusätze:
1) Sei $M = R\mathrm{D}R$ und sei $x \in n \cdot M$. Dann ist $x = \sum n_i \cdot \mathrm{D}r_i$ mit $n_i \in n$ und $r_i \in R$. $\Rightarrow x = \sum \mathrm{D}(n_i \cdot r_i) - \sum r_i \cdot \mathrm{D}(n_i) \in R\,\mathrm{D}n$.
2) Sei $n = (f_\kappa)$ und $n \in n$. $\Rightarrow n = \sum r_i \cdot f_i$, also
$\mathrm{D}n = \underbrace{\sum r_i \mathrm{D}f_i}_{\in R(\{\mathrm{D}f_\kappa\})} + \underbrace{\sum f_i \cdot \mathrm{D}r_i}_{\in n \cdot \mathrm{D}R} \in R\langle\{\mathrm{D}f_\kappa\}\rangle + n \cdot \mathrm{D}R$.
Umgekehrt ist nach 1) $n\mathrm{D}R \subseteq R\,\mathrm{D}n$ und natürlich auch $R\langle\{\mathrm{D}f_\kappa\}\rangle \subseteq R\,\mathrm{D}n$.
q.e.d.
Aus Satz 1.27 und Satz 1.28 ergibt sich das folgende Rezept zur Berechnung der universellen λ-Ausdehnung im allgemeinen Fall, das im Spezialfall $\mathrm{D} = 0$ und $M = 0$ zugleich einen neuen Existenzbeweis für die universelle λ-Derivation liefert:

Satz 1.29 (Rezept für die universelle Ausdehnung) *Sei*
$\lambda : R \to S$ *ein Ringhomomorphismus,*
$\mathrm{D} : R \to M$ *eine Derivation von R.*
Dann existiert die universelle λ*-Ausdehnung* (d, π) *von D, und man erhält sie*

folgendermaßen:

Wähle ein Erzeugensystem $\{x_\iota \mid \iota \in J\}$, *so daß* $S = \lambda(R)[\{x_\iota\}]$ *ist, und stelle* S *dar als homomorphes Bild des Polynomrings* $S^* := R[\{X_\iota\}]$ *mittels*

$\lambda' : S^* \to S$, *definiert durch*

$\lambda' \mid R := \lambda, \quad \lambda'(X_\iota) := x_\iota$ *für alle* $\iota \in J$.

Wähle ferner für $n := \operatorname{Ker}(\lambda')$ *ein Erzeugendensystem* $\{f_\kappa \mid \kappa \in K\}$ *als* S^*-*Modul:*

$n = S^*\langle\{f_\kappa\}\rangle$.

Für alle $f \in S^*$ *bezeichne*

$\partial f = \delta f|_{X \mapsto x} \in S \otimes_R M$

das Bild des δf *aus Satz 1.27 bei der kanonischen Abbildung*

$\lambda' \otimes \mathrm{id} : S^* \otimes_R M \to S \otimes_R M$

und

$\frac{\partial f}{\partial x_\kappa} := \lambda'\left(\frac{\partial f}{\partial X_\kappa}\right)$.

Bilde

$$N := \left(S \otimes_R M \oplus \bigoplus_\iota S \cdot \Delta X_\iota\right) \Big/ \underbrace{S\left\langle\left\{\partial f_\kappa + \sum_\iota \frac{\partial f_\kappa}{\partial x_\iota} \cdot \Delta X_\iota \mid \kappa \in K\right\}\right\rangle}_{=:N}$$

Definiere dann

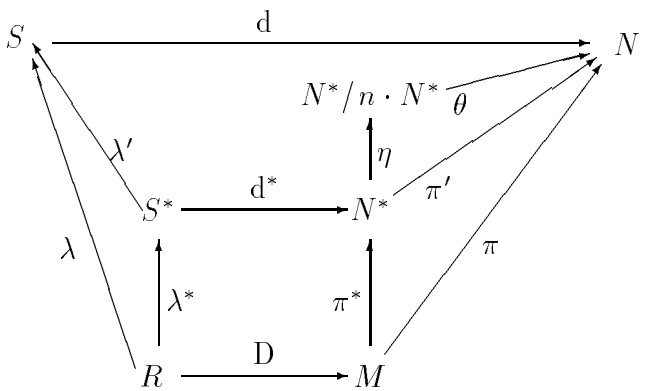
$\mathrm{d} : S \to N$ *und* $\pi : M \to N$ *durch:*

$\mathrm{d}(g(x)) := \left(\partial g + \sum_\iota \frac{\partial g}{\partial x_\iota} \cdot \Delta X\iota\right) \bmod N \qquad$ *für alle* $g(x) \in S$

und

$\pi(m) := (1 \otimes m + 0) \bmod N \qquad$ *für alle* $m \in M$.

Beweis:



Daß $\mathrm{d}(g(x))$ wohldefiniert ist, wird sich im Beweis ergeben. Bilde zunächst nach

Satz 1.27 die universelle λ^*-Ausdehnung (d^*, π^*) von D für die Inklusionsabbildung $\lambda^* : R \hookrightarrow S^*$
$\mathrm{d}^* \to N^* := S^* \otimes_R M \oplus \bigoplus_\iota S^* \cdot \Delta X_\iota$.
Betrachte nun die kanonischen Abbildungen
$N^* \xrightarrow{\eta} N^*/n \cdot N^* = S \otimes_R M \oplus \bigoplus_\iota S \cdot \Delta X_\iota \xrightarrow[\mathrm{mod}\ N]{\theta} N$.
Sei nun (d', π') die universelle λ'-Ausdehnung von d^* nach Satz 1.28. Nach der dort angegebenen Konstruktion ist dann $\pi' = \theta \circ \eta$, also
$\pi' \circ \pi^*(m) = (1 \otimes m) \bmod N = \pi(m)$ für alle $m \in M$ und
$\mathrm{d}'(g(x)) = (\theta \circ \eta) \circ \mathrm{d}^*(g(X)) = \theta\left(\partial g + \sum_\iota \frac{\partial g}{\partial x_\iota} \cdot \mathrm{d}^* X_\iota\right) = \mathrm{d}(g(x))$.
(Da $\mathrm{d}'(g(x))$ wohldefiniert ist, ist damit zugleich gezeigt, daß auch $\mathrm{d}(g(x))$ wohldefiniert ist.)
Nach Satz 1.20 ist aber $(\mathrm{d}', \pi' \circ \pi^*)$ universelle $\lambda' \circ \lambda^* = \lambda$-Ausdehnung von D. Es ist aber, wie eben gezeigt, $\mathrm{d}' = \mathrm{d}$ und $\pi' \circ \pi^* = \pi$. q.e.d.

Die eben angegebene Vorschrift zur Berechnung der universellen Ausdehnung läßt sich zwar prinzipiell immer anwenden, jedoch ist es oft schwer geeignete Erzeugendensysteme für S und n zu finden. Daher ist es günstig, daß man im Falle der universellen Ausdehnung auf einen Quotientenring ein der speziellen Situation besser angepaßtes Verfahren hat, das durch die übliche Quotientenregel der Differentialrechnung angeregt ist:

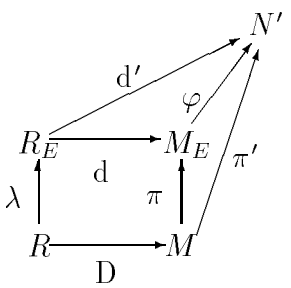
Satz 1.30 (Universelle Ausdehnung auf einen Quotientenring) *Sei E eine multiplikativ abgeschlossene Teilmenge des Ringes R, die die Eins von R enthält, $S = R_E$ der Quotientenring von R bezüglich E und $\lambda : R \to S$ der kanonische Homomorphismus mit $\lambda(r) = \frac{r}{1}$ für alle $r \in R$. Sei ferner $\mathrm{D} : R \to M$ eine Derivation von R.*
Dann erhält man die universelle λ-Ausdehnung (d, π) von D folgendermaßen:
Bilde den Quotientenmodul $M_E = S \otimes_R M$ von M bezüglich E.
$\pi : M \to M_E$ ist der kanonische Homomorphismus mit $\pi(m) = \frac{m}{1} = 1 \otimes m$ für alle $m \in M$.
$\mathrm{d} : S \to M_E$ ist gegeben durch

$$\mathrm{d}\left(\frac{r}{t}\right) := \frac{1}{t^2} \cdot \left(t \cdot \frac{\mathrm{D}r}{1} - r \cdot \frac{\mathrm{D}t}{1}\right)$$

für alle $r \in R$ und alle $t \in E$.

Beweis: Zunächst muß man nachrechnen, daß d wohldefiniert ist, d.h. daß die angegebene Definition nicht von der Darstellung eines Elements von S in der Form r/t abhängt:
Sei also $r/t = r'/t'$ in S. Dann gibt es ein $u \in E$ mit $u \cdot (t' \cdot r - t \cdot r') = 0$ in R.
Wende darauf D an:
$u \cdot ((t' \cdot \mathrm{D}r - r' \cdot \mathrm{D}t) - (t \cdot \mathrm{D}r' - r \cdot \mathrm{D}t')) + (t' \cdot r - t \cdot r') \cdot \mathrm{D}u = 0$.

Multipliziere diese Gleichung mit $u \cdot t \cdot t'$ und beachte, daß $u \cdot (t' \cdot r - t \cdot r') = 0$, also $u \cdot t' \cdot r = u \cdot t \cdot r'$ gilt. $\Rightarrow$
$u^2 \cdot (t'^2 \cdot (t \cdot \mathrm{D}r - r \cdot \mathrm{D}t) - t^2(t' \cdot \mathrm{D}r' - r' \cdot \mathrm{D}t')) + 0 = 0.$
Dann gilt in M_E nach Konstruktion des Quotientenmoduls:
$\dfrac{(t \cdot \mathrm{D}r - r \cdot \mathrm{D}t)}{t^2} = \dfrac{(t' \cdot \mathrm{D}r' - r' \cdot \mathrm{D}t')}{t'^2}$, also
$\dfrac{1}{t^2} \cdot \left(t \cdot \dfrac{\mathrm{D}r}{1} - r \cdot \dfrac{\mathrm{D}t}{1}\right) = \dfrac{1}{t'^2} \cdot \left(t' \cdot \dfrac{\mathrm{D}r'}{1} - r' \cdot \dfrac{\mathrm{D}t'}{1}\right).$
Man rechnet sofort nach, daß das so definierte d eine Derivation von R_E ist. Ferner gilt nach Definition $\mathrm{d} \circ \lambda(r) = \mathrm{d}(\frac{r}{1}) = \frac{\mathrm{D}r}{1} = \pi \circ \mathrm{D}(r)$ für alle $r \in R$. Also ist (d, π) eine λ-Ausdehnung von D.
Sei nun (d', π') eine beliebige λ-Ausdehnung von D.
$\pi' : M \to N'$ ist eine R-lineare Abbildung von M in einen R_E-Modul. Auf Grund der universellen Eigenschaft von π gibt es dann *genau eine* R_E-lineare Abbildung $\varphi : M_E \to N'$ mit $\pi' = \varphi \circ \pi$. Ferner gilt mit diesem φ (Beachte die Quotientenregel Anmerkung 1.3) :



$$\begin{aligned}
\mathrm{d}'\left(\frac{r}{t}\right) &= \frac{1}{t^2} \cdot \left(\frac{t}{1} \cdot \mathrm{d}'\left(\frac{r}{1}\right) - \frac{r}{1} \cdot \mathrm{d}'\left(\frac{t}{1}\right)\right) \\
&= \frac{1}{t^2} \cdot (\lambda(t) \cdot \mathrm{d}' \circ \lambda(r) - \lambda(r) \cdot \mathrm{d}' \circ \lambda(t)) \\
&= \frac{1}{t^2} \cdot (\lambda(t) \cdot \pi' \circ \mathrm{D}(r) - \lambda(r) \cdot \pi' \circ \mathrm{D}(t)) \\
&= \frac{1}{t^2} \cdot \pi'(t \cdot \mathrm{D}(r) - r \cdot \mathrm{D}(t)) \\
&= \frac{1}{t^2} \cdot \varphi \circ \pi\,(t \cdot \mathrm{D}(r) - r \cdot \mathrm{D}(t)) \\
&= \varphi\left(\frac{1}{t^2} \cdot (t \cdot \pi(\mathrm{D}r) - r \cdot \pi(\mathrm{D}(t))\right) \\
&= \varphi \circ \mathrm{d}\left(\frac{r}{t}\right). \quad \text{q.e.d.}
\end{aligned}$$

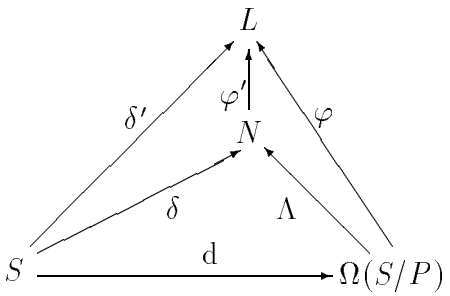
Vergrößerung des Konstantenrings

Manchmal muß man von einem Konstantenring P zu einem größeren übergehen. Das ist auf Grund des folgenden Satzes recht einfach:

Satz 1.31 (Vergrößerung des Konstantenrings) *Seien*
$P \xrightarrow{\rho} R \xrightarrow{\lambda} S$ *Ringhomomorphismen,*
$\mathrm{d} : S \to \Omega(S/P)$ *die universelle Derivation von* S *über* P.

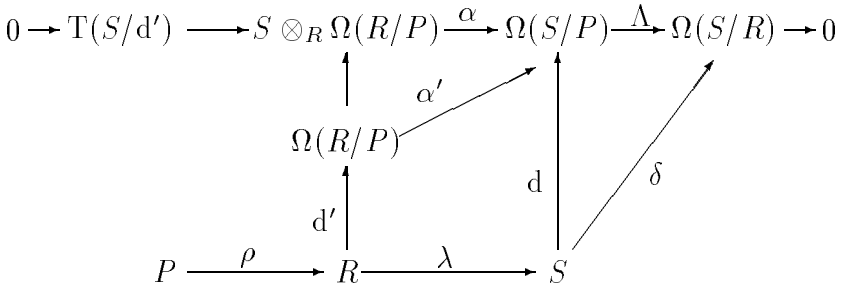
$\Lambda : \Omega(S/P) \to \Omega(S/P)/S \cdot \mathrm{d}(\lambda(R)) =: N$ *kanonisch.*
Dann ist $\delta := \Lambda \circ \mathrm{d}$ *die universelle Derivation von* S *über* R.

Beweis:



Zunächst ist δ eine Derivation, und es ist $\delta \circ \lambda = 0$ nach Definition, also ist δ eine Derivation von S über R.
Sei nun $\delta' : S \to L$ eine beliebige Derivation von S über R. Dann ist δ' auch eine Derivation von S über P. Also existiert genau eine S-lineare Abbildung $\varphi : \Omega(S/P) \to L$ mit $\delta' = \varphi \circ \mathrm{d}$. Es ist
$\varphi\,(S \cdot \mathrm{d}(\lambda(R))) = S \cdot \varphi \circ \mathrm{d} \circ \lambda(R) = \delta' \circ \lambda(R) = 0$, weil δ' eine λ-Derivation ist.
Also existiert genau eine S-lineare Abbildung φ' mit $\varphi' \circ \Lambda = \varphi$. $\Rightarrow \varphi' \circ \delta = \varphi' \circ \Lambda \circ \mathrm{d} = \varphi \circ \mathrm{d} = \delta'$.
Es folgt, daß δ universelle Derivation von S über R ist. q.e.d.

Manchmal ist eine Umformulierung der Aussage von Satz 1.31 nützlich:



Sei d' die universelle Derivation von R/P. Da $\mathrm{d} \circ \lambda : R \to \Omega(S/P)$ eine Derivation von R/P ist, gibt es genau eine R-lineare Abbildung $\alpha' : \Omega(R/P) \to \Omega(S/P)$ mit $\mathrm{d} \circ \lambda = \alpha' \circ \mathrm{d}'$.
Nun ist $\Omega(S/P)$ ein S-Modul. Also gibt es genau eine S-lineare Abbildung $\alpha : S \otimes_R \Omega(R/P) \to \Omega(S/P)$ mit $s \otimes \omega \mapsto s \cdot \alpha'(\omega)$.
Wegen $\Omega(R/P) = R\mathrm{d}'R$ ist $\alpha(S \otimes_R \Omega(R/P)) = S \cdot \alpha'(\Omega(R/P)) = S \cdot \alpha' \circ \mathrm{d}'(R) = S \cdot \mathrm{d}(\lambda(R)) = \mathrm{Ker}\,(\Lambda)$.
Es folgt zusammen mit Satz 1.31 :

Korollar 1.32 *Mit den oben erklärten Bezeichnungen hat man eine exakte Folge*

$$0 \to \mathrm{T}(S/\mathrm{d}') \to S \otimes_R \Omega(R/P) \xrightarrow{\alpha} \Omega(S/P) \xrightarrow{\Lambda} \Omega(S/R) \to 0$$

Kapitel 2

Separable und inseparable Körpererweiterungen

Als erste Anwendung der Differentiale betrachten wir in diesem Kapitel Körpererweiterungen. Dabei wird sich herausstellen, daß man mittels der Differentiale ein Maß für die Inseparabilität einer endlich erzeugten Körpererweiterung definieren kann. (Andere Inseparabilitätsmaße lassen sich mit höheren Differentialen einführen [Be2]). Ferner werden wir nähere Aussagen über die Erzeugendenanzahl einer Körpererweiterung erhalten. Wegen der vollständigen Dualität ist es bei endlich erzeugten Körpererweiterungen K/k im Prinzip egal, ob man mit dem Modul der Derivationen $\mathrm{Der}_k(K,K)$ oder mit dem universellen Differentialmodul $\Omega(K/k)$ arbeitet. Wir werden hier den letzten benutzen, weil in allgemeineren Situationen der universelle Differentialmodul meistens vorzuziehen ist, da er mehr Information als der Modul der Derivationen enthält. Die hier gewählte Darstellung geht in wesentlichen Teilen auf E. Kähler zurück.
In den ersten vier Abschnitten dieses Kapitels setzen wir, soweit nichts anderes angegeben ist, voraus, daß alle Körpererweiterungen endlich erzeugt sind. Den Transzendenzgrad von K/k bezeichnen wir mit $\dim \frac{K}{k}$.

Inseparabilität einer Körpererweiterung

Vorbemerkung: *Ist K/k eine endlich erzeugte Körpererweiterung, dann ist $\Omega(K/k)$ endlich erzeugter K-Vektorraum.*
Genauer:
Sei $K = k(x_1, \ldots, x_n)$, $\mathrm{D} : K \to M$ eine Derivation von K über k. Dann ist $K\,\mathrm{D}K = K\langle \mathrm{D}x_1, \ldots, \mathrm{D}x_n\rangle$.
Beweis: Jedes Element von K ist von der Form $F = f(x)/g(x)$. Zunächst folgt aus Summen- und Produktregel (mit den Bezeichnungen von Satz 1.29) $\mathrm{D}f = \sum\limits_{i=1}^{n} \frac{\partial f(x)}{\partial x_i} \cdot \mathrm{D}x_i \in K\langle \mathrm{D}x_1, \ldots, \mathrm{D}x_n\rangle$ und ebenso $\mathrm{D}g(x) \in K\langle \mathrm{D}x_1, \ldots, \mathrm{D}x_n\rangle$. Auf Grund der Quotientenregel ist dann $\mathrm{D}F = (1/g^2) \cdot (g \cdot \mathrm{D}f - f \cdot \mathrm{D}g) \in$

$K\langle \mathrm{D}x_1, \ldots, \mathrm{D}x_n \rangle$ q.e.d.

Definition 2.1 *Sei K/k eine endlich erzeugte Körpererweiterung.*

$$\mathrm{insep}\frac{K}{k} := \dim_K \Omega(K/k) - \dim \frac{K}{k}$$

heißt die „Inseparabilität" von K über k.

Satz 2.2 *Seien $k \subseteq K_1 \subseteq K = K_1(x)$ Körper, K_1/k endlich erzeugt. Dann gilt:*

$$\mathrm{insep}\frac{K}{k} = \mathrm{insep}\frac{K_1}{k} \qquad \textit{falls } x \textit{ transzendent oder separabel algebraisch über } K_1 \textit{ ist}$$

$$\mathrm{insep}\frac{K_1}{k} \;\leq\; \mathrm{insep}\frac{K}{k} \;\leq\; \mathrm{insep}\frac{K_1}{k} + 1 \qquad \textit{allgemein.}$$

Beweis: Falls x algebraisch über K_1 ist, sei f das Minimalpolynom von x über K_1. Dann gilt nach Satz 1.29
$\Omega(K/k) = (K \otimes_{K_1} \Omega(K_1/k) \oplus K \cdot \Delta X) \,/\, K \cdot (\partial f + f'(x) \cdot \Delta X)$
Falls x transzendent über K_1 ist, setzen wir $f := 0$. Nach Satz 1.27 und Satz 1.30 ergibt sich dann derselbe Ausdruck für $\Omega(K/k)$.
Ferner gilt $\dim_K K \otimes_{K_1} \Omega(K_1/k) = \dim_{K_1} \Omega(K_1/k)$. (Das gilt für jeden Vektorraum!) Also:
$\dim_K \Omega(K/k) = \dim_{K_1} \Omega(K_1/k) + 1 - \dim_K K \cdot (\partial f + f'(x) \cdot \Delta X)$ und
$0 \leq \dim_K K \cdot (\partial f + f'(x) \cdot \Delta X) \leq 1$.

1. Fall: x transzendent über K_1, also $f = 0$.
$\Rightarrow$ $\dim_K \Omega(K/k) = \dim_{K_1} \Omega(K_1/k) + 1$
$\dim \frac{K}{k} = \dim \frac{K_1}{k} + 1$

$\Rightarrow \mathrm{insep}\frac{K}{k} = \mathrm{insep}\frac{K_1}{k}$

2. Fall: x separabel algebraisch über K_1, also $f'(x) \neq 0$.
$\Rightarrow \dim_K K \cdot (\partial f + f'(x) \cdot \Delta X) = 1$
$\Rightarrow$ $\dim_K \Omega(K/k) = \dim_{K_1} \Omega(K_1/k)$
$\dim \frac{K}{k} = \dim \frac{K_1}{k}$

$\Rightarrow \mathrm{insep}\frac{K}{k} = \mathrm{insep}\frac{K_1}{k}$

3. Fall: x inseparabel algebraisch über K_1, also $f'(x) = 0$.
Dagegen kann ∂f Null oder ungleich Null sein.
Man kann also nur sagen:
$\dim_{K_1} \Omega(K_1/k) \leq \dim_K \Omega(K/k) \leq \dim_{K_1} \Omega(K_1/k) + 1$
$\dim \frac{K_1}{k} = \quad \dim \frac{K}{k} \quad = \dim \frac{K_1}{k}$

$\Rightarrow \mathrm{insep}\frac{K_1}{k} \leq \quad \mathrm{insep}\frac{K}{k} \quad \leq \mathrm{insep}\frac{K_1}{k} + 1$ q.e.d.

Korollar 2.3 *Seien $k \subseteq K_0 \subseteq K$ endlich erzeugte Körpererweiterungen. Dann gilt:*

$$\operatorname{insep}\frac{K_0}{k} \leq \operatorname{insep}\frac{K}{k}$$

Insbesondere ist stets

$$\operatorname{insep}\frac{K}{k} \geq 0.$$

Beweis: Bilde eine Körperkette $k \subseteq K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = K$ mit $K_i = K_{i-1}(x_i), \quad i = 1, \ldots, n$. Nach Satz 2.2 folgt dann:
$\operatorname{insep}\frac{K_0}{k} \leq \operatorname{insep}\frac{K_1}{k} \leq \ldots \leq \operatorname{insep}\frac{K}{k}$. Im Spezialfall $k = K_0$ ergibt sich:
$0 = \operatorname{insep}\frac{k}{k} \leq \operatorname{insep}\frac{K}{k}$. q.e.d.

Satz 2.4 *Seien $k \subseteq K_1 \subseteq K$ endlich erzeugte Körpererweiterungen. Dann gilt:*

$$\operatorname{insep}\frac{K}{k} \leq \operatorname{insep}\frac{K_1}{k} + \operatorname{insep}\frac{K}{K_1}$$

Beweis: Nach Satz 1.31 ist $\Omega(K/K_1) = \Omega(K/k)/K\,\mathrm{d}K_1$, wenn d die universelle Derivation von K/k bezeichnet, also
$\dim_K \Omega(K/k) = \dim_K \Omega(K/K_1) + \dim_K K\,\mathrm{d}K_1$.
Die Einschränkung
$\mathrm{d}|(K_1 \to K\mathrm{d}K_1)$ ist eine Derivation von K_1/k in einen K-Modul, der von dem Bild erzeugt wird. Also existiert ein surjektiver K-Homomorphismus
$\varphi : K \otimes_{K_1} \Omega(K_1/k) \to K \cdot \mathrm{d}K_1$; denn nach Definition der universellen Derivation d_1 von K_1/k existiert zunächst ein K_1-Homomorphismus $\varphi_1 : \Omega(K_1/k) \to K \cdot \mathrm{d}K_1$ mit $\mathrm{d} = \varphi_1 \circ \mathrm{d}_1$ auf K_1 und $K \cdot \mathrm{d}K_1$ ist ein K-Vektorraum. (Beachte die universelle Eigenschaft von $K \otimes_{K_1} \bullet$.) Es folgt
$\dim_K K \cdot \mathrm{d}K_1 \leq \dim_K K \otimes_{K_1} \Omega(K_1/k) = \dim_{K_1} \Omega(K_1/k)$. Also

$$\begin{array}{rcl} \dim_K \Omega(K/k) & \leq & \dim_K \Omega(K/K_1) + \dim_{K_1} \Omega(K_1/k) \\ \dim \frac{K}{k} & = & \dim \frac{K}{K_1} + \dim \frac{K_1}{k} \\ \hline \Rightarrow \operatorname{insep}\frac{K}{k} & \leq & \operatorname{insep}\frac{K}{K_1} + \operatorname{insep}\frac{K_1}{k} \end{array}$$

q.e.d.

Satz 2.5 *Seien K_1/k und K_2/k endlich erzeugte Körpererweiterungen und $K = k(K_1, K_2)$ das Körperkompositum. Sei ferner*
$\dim \frac{K}{k} = \dim \frac{K_1}{k} + \dim \frac{K_2}{k}$. *Dann gilt:*

$$\operatorname{insep}\frac{K}{k} \leq \operatorname{insep}\frac{K_1}{k} + \operatorname{insep}\frac{K_2}{k}$$

Beweis: Sei d die universelle Derivation von K/k. Aus $K = k(K_1, K_2)$ folgt $\Omega(K/k) = K\,\mathrm{d}K_1 + K\,\mathrm{d}K_2$. Ferner hat man wie im Beweis von Satz 2.4 surjektive

K-Homomorphismen $K \otimes_{K_i} \Omega(K_i, k) \to K\,\mathrm{d}K_i$, also
$\dim_K K\,\mathrm{d}K_i \leq \dim_{K_i} \Omega(K_i/k)$.
Es folgt:

$$\begin{array}{lrcll} & \dim_K \Omega(K/k) & \leq & \dim_{K_1} \Omega(K_1/k) & + \dim_{K_2} \Omega(K_2/k) \\ \text{und nach Voraussetzung} & \dim \frac{K}{k} & = & \dim \frac{K_1}{k} & + \dim \frac{K_2}{k} \\ \hline & \Rightarrow \ \mathrm{insep}\frac{K}{k} & \leq & \mathrm{insep}\frac{K_1}{k} & + \mathrm{insep}\frac{K_2}{k} \end{array}$$

q.e.d.

Separable Körpererweiterungen

Satz 2.6 *Sei K/k endlich erzeugte Körpererweiterung. Es gilt:*
K/k ist separabel algebraisch $\Longleftrightarrow \Omega(K/k) = 0$.

Anmerkung 2.7 *Für nicht endlich erzeugte Körpererweiterungen ist die Aussage von Satz 2.6 falsch: Sei etwa k ein unvollkommener Körper der Charakteristik p und $K := k^{p^{-\infty}}$ die vollkommene Hülle von k. Dann ist K/k inseparabel algebraisch, aber trotzdem ist $\Omega(K/k) = 0$, weil jedes Element von K eine p-te Potenz ist.*
Die Umkehrung ist trivialerweise richtig: Ist K/k separabel algebraisch, dann ist $\Omega(K/k) = 0$, wie aus dem folgenden Beweis hervorgeht.

Beweis von Satz 2.6: $\underline{\Rightarrow:}$ Sei D eine Derivation von K/k , $y \in K$ beliebig und $f \in k[X]$ das Minimalpolynom für y über k. Da K/k separabel algebraisch ist, gilt $f'(y) \neq 0$. Aus $f(y) = 0$ folgt durch Anwendung von D, daß $0 = \mathrm{D}f(y) = f'(y) \cdot \mathrm{D}y$, also $\mathrm{D}y = 0$ ist. Da $\Omega(K/k) = K\,\mathrm{d}K$ ist, hat man $\Omega(K/k) = 0$.
$\underline{\Leftarrow:}$ Sei $\Omega(K/k) = 0$. $\Rightarrow 0 \leq \mathrm{insep}\frac{K}{k} = \dim_K \Omega(K/k) - \dim \frac{K}{k} = -\dim \frac{K}{k}$.
$\Rightarrow \dim \frac{K}{k} = 0$. Also K/k algebraisch und $\mathrm{insep}\frac{K}{k} = 0$.
Sei nun $y \in K$ beliebig, f das Minimalpolynom für y über k.
Wäre y *inseparabel* über k, so wäre $f'(y) = 0$. Sei nun $K_1 := k(y) \cong k[X]/(f)$.
Nach der Konstruktion von Satz 1.29 erhält man:
$\Omega(K_1/k) = K_1 \cdot \Delta X/K_1 \cdot \underbrace{f'(y)}_{=0} \cdot \Delta X = K_1 \Delta X \neq (0)$.
Andererseits ist auch K_1/k algebraisch, also $\dim \frac{K_1}{k} = 0$.
$\Rightarrow \mathrm{insep}\frac{K_1}{k} = \dim_{K_1} \Omega(K_1/k) - \dim \frac{K_1}{k} = 1 > 0$.
Wegen Korollar 2.3 folgt $\mathrm{insep}\frac{K}{k} \geq \mathrm{insep}\frac{K_1}{k} > 0$ im Widerspruch zu dem oben gezeigten. q.e.d.

Definition 2.8 *Sei K/k eine endlich erzeugte Körpererweiterung.*
K/k heißt „separabel“, wenn es eine Transzendenzbasis $\{x_1, \ldots, x_n\}$ gibt, so daß $K/k(x_1, \ldots, x_n)$ separabel algebraisch ist.
Eine solche Transzendenzbasis heißt „separierende Transzendenzbasis“ der Körpererweiterung.

Anmerkung 2.9 *Bei nicht endlich erzeugten Körpererweiterungen von Primzahlcharakteristik ist dieser Begriff zu stark. Man nennt eine Körpererweiterung K/k, die eine, nicht notwendig endliche, Transzendenzbasis $\{x_\iota\}$ besitzt, so daß $K/k(\{x_\iota\})$ separabel algebraisch ist, „separabel erzeugt". Dagegen heißt K/k „separabel", wenn K^p und k linear disjunkt über k^p sind. ($p := \mathrm{char}(K)$.) Aus „separabel erzeugt" folgt „separabel", aber im allgemeinen nicht umgekehrt. Bei endlich erzeugten Körpererweiterungen stimmen die beiden Begriffe überein. Wir werden im Abschnitt über Separabilität bei nicht endlich erzeugten Körpererweiterungen darauf noch näher eingehen.*

Satz 2.10 *Sei K/k endlich erzeugt. Es gilt:*

K/k separabel $\Longleftrightarrow \mathrm{insep}\frac{K}{k} = 0$
Folgerung: *Sind $k \subseteq K_0 \subseteq K$ Körper und K/k separabel, so ist auch K_0/k separabel*
(Aber im allgemeinen nicht *K/K_0 separabel! Dies ist jedoch der Fall, wenn K/k separabel* algebraisch *ist, da dann jedes Element von K separabel algebraisch über k, also erst recht über K_0 ist.)*

Beweis : $\underline{\Rightarrow:}$ Da K/k endlich erzeugt und separabel ist, gibt es eine endliche separierende Transzendenzbasis $\{x_1, \ldots, x_n\}$. $\Rightarrow K/\underbrace{k(x_1, \ldots, x_n)}_{=:K_1}$ ist eine endliche separabel algebraische Körpererweiterung. Wiederholte Anwendung von Satz 2.2 zeigt, daß $\mathrm{insep}\frac{K}{k} = 0$ ist. q.e.d.
Genauer hat man: Nach Satz 2.6 ist $\Omega(K/K_1) = 0$.
Aber $\Omega(K/K_1) = \Omega(K/k)/K\,\mathrm{d}K_1$ nach Satz 1.31, also
$\Omega(K/k) = K\,\mathrm{d}K_1 = K\mathrm{d}x_1 + \ldots + K\mathrm{d}x_n$.
Wegen $\mathrm{insep}\frac{K}{k} \geq 0$ ist $\dim \Omega(K/k) = n$, also ist $\{\mathrm{d}x_1, \ldots, \mathrm{d}x_n\}$ eine K-Basis von $\Omega(K/k)$.
$\underline{\Leftarrow:}$ Sei $\mathrm{insep}\frac{K}{k} = 0$.
$\Rightarrow \dim_K \Omega(K/k) = \dim \frac{K}{k} =: n$.
$\Rightarrow$ Es existieren $x_1, \ldots, x_n \in K$ so daß $\{\mathrm{d}x_1, \ldots, \mathrm{d}x_n\}$ eine K-Basis von $\Omega(K/k)$ bilden. (Beachte dabei, daß man bei einem Vektorraum aus jedem Erzeugendensystem eine Basis auswählen kann und daß $\Omega(K/k)$ von $\{\mathrm{d}x \mid x \in K\}$ erzeugt wird.)
Sei $K_1 := k(x_1, \ldots x_n)$.
$\Rightarrow \Omega(K/K_1) = \Omega(K/k)/K\,\mathrm{d}K_1 = 0$. Nach Satz 2.6 ist dann $K/k(x_1, \ldots, x_n)$ separabel algebraisch, insbesondere auch $\dim \frac{K_1}{k} = \dim \frac{K}{k} = n$.
$\Rightarrow \{x_1, \ldots, x_n\}$ algebraisch unabhängig über k, bilden also eine separierende Transzendenzbasis von K/k.
$\Rightarrow K/k$ ist separabel. q.e.d.

Beweis der Folgerung: Nach Korollar 2.3 gilt $0 \leq \mathrm{insep}\frac{K_0}{k} \leq \mathrm{insep}\frac{K}{k}$, und nach dem Satz ist $\mathrm{insep}\frac{K}{k} = 0$, weil K/k separabel ist. Also ist auch $\mathrm{insep}\frac{K_0}{k} = 0$ und damit nach dem Satz K_0/k separabel. q.e.d.

Daß aus K/k separabel im allgemeinen nicht folgt, daß auch K/K_0 separabel ist, zeigt das folgende Beispiel:

Beispiel 2.11 *Sei k ein Körper der Charakteristik $p > 0$, x eine Unbestimmte, $K := k(x)$ und $K_0 := K(x^p)$.*
Dann ist K/k separabel, aber K/K_0 ist (rein) inseparabel vom Grad p, denn das Minimalpolynom von x über K_0 ist $f = X^p - x^p$. (siehe Anmerkung 2.20)

Beim Beweis von Satz 2.10 hat sich ergeben:

Korollar 2.12 *Sei K/k endlich erzeugt und separabel,* d *die universelle Derivation von K/k und $x_1, \ldots, x_n \in K$. Es gilt:*
$\{\mathrm{d}x_1, \ldots, \mathrm{d}x_n\}$ ist eine K-Basis von $\Omega(K/k)$
$\iff \{x_1, \ldots, x_n\}$ ist separierende Transzendenzbasis von K/k.

Im Falle der Charakteristik Null ist jede Körpererweiterung separabel. Daher gilt hier:

Korollar 2.13 *Sei K/k eine nicht notwendig endlich erzeugte Körpererweiterung,* $\mathrm{char}(K) = 0$,
d *die universelle Derivation von K/k und*
$\{x_\iota \mid \iota \in J\} \subseteq K$.
Es gilt:
$\{\mathrm{d}x_\iota \mid \iota \in J\}$ linear unabhängig über $K \iff$
$\{x_\iota \mid \iota \in J\}$ algebraisch unabhängig über k
Folgerung: *Ein Element $z \in K$ ist algebraisch abhängig von $\{x_1, \ldots, x_r\} \iff$ dz ist linear abhängig über K von $\{\mathrm{d}x_1, \ldots, \mathrm{d}x_r\}$.*

Beweis:
1. Fall: K/k endlich erzeugt: Dann ist notwendigerweise auch J endlich, also o.B.d.A. $J = \{1, \ldots, r\}$.
$\underline{\Rightarrow:}$ Ergänze $\{\mathrm{d}x_1, \ldots, \mathrm{d}x_r\}$ zu einer K-Basis $\{\mathrm{d}x_1, \ldots, \mathrm{d}x_r, \ldots, \mathrm{d}x_n\}$ von $\Omega(K/k)$. Wegen $\mathrm{char}(K) = 0$ ist K/k separabel, also ist nach Korollar 2.12 $\{x_1, \ldots, x_n\}$ eine (separierende) Transzendenzbasis von K/k.
Insbesondere sind also $\{x_1, \ldots, x_r\}$ algebraisch unabhängig über k.
$\underline{\Leftarrow:}$ Ergänze $\{x_1, \ldots, x_r\}$ zu einer Transzendenzbasis $\{x_1, \ldots, x_r, \ldots, x_n\}$ von K/k. Wegen $\mathrm{char}(K) = 0$ ist das eine separierende Transzendenzbasis, also sind nach Korollar 2.12 $\{\mathrm{d}x_1, \ldots, \mathrm{d}x_n\}$ und damit erst recht $\{\mathrm{d}x_1, \ldots, \mathrm{d}x_r\}$ linear unabhängig über K.
2. Fall: K/k beliebig erzeugt: Wir führen diesen Fall auf den Fall einer endlich erzeugten Körpererweiterung zurück.
$\underline{\Rightarrow:}$ (indirekt) Sei $\{\mathrm{d}x_\iota\}$ linear unabhängig über K. Wäre $\{x_\iota\}$ algebraisch abhängig über k, so gäbe es schon ein endliches Teilsystem, o.B.d.A $\{x_1 \ldots, x_r\}$, das algebraisch abhängig über k wäre. Sei $K_0 = k(\{x_1 \ldots, x_r\})$.
Dann ist $\{x_1 \ldots, x_r\} \subseteq K_0$ und algebraisch abhängig über k. Nach dem 1. Fall

ist dann $\{\mathrm{d}_0x_1, \ldots \mathrm{d}_0x_r\}$ linear abhängig über K_0, wenn d_0 die universelle Derivation von K_0 über k bezeichnet. d ist aber als universelle Derivation von K über k nach Satz 1.20 und Satz 1.21 die universelle Ausdehnung von d_0 auf K. Daher sind die $\mathrm{d}x_i$ K_0-homomorphe Bilder der d_0x_i und wären als solche ebenfalls linear abhängig über K_0 und daher erst recht über K gegen Voraussetzung.
$\underline{\Leftarrow:}$ (indirekt) Sei $\{x_\iota\}$ algebraisch unabhängig über k. Wäre $\{\mathrm{d}x_\iota\}$ linear abhängig über K, so gäbe es ein endliches Teilsystem, o.B.d.A. $\{\mathrm{d}x_1, \ldots, \mathrm{d}x_r\}$, das linear abhängig über K wäre. Auf Grund der Konstruktion der universellen Derivation von K über k nach Satz 1.29 sieht man, daß man nur endlich viele Elemente von K braucht, um eine solche lineare Relation zu erhalten. Daher gäbe es schon einen über k endlich erzeugten Teilkörper K_0 von K, so daß $\{\mathrm{d}_0x_1, \ldots, \mathrm{d}_0x_r\}$ linear abhängig über K_0 wäre, wenn d_0 die universelle Derivation von K_0 über k bezeichnet. Nach dem 1. Fall folgte dann, daß bereits $\{x_1, \ldots, x_m\} \subseteq K_0$ und damit erst recht $\{x_\iota\}$ algebraisch abhängig über k wäre gegen Voraussetzung.
Die Folgerung ist offenbar nur eine äquivalente Umformulierung der Aussage des Korollars. q.e.d.

Korollar 2.14 (Verallgemeinerung der ersten Aussage von Satz 2.2) *Seien $k \subseteq K_1 \subseteq K$ endlich erzeugte Körpererweiterungen. Es gilt:*

$$K/K_1 \text{ separabel } \Longrightarrow \mathrm{insep}\frac{K}{k} = \mathrm{insep}\frac{K_1}{k}$$

Beweis: Es ist nach Satz 2.4 $\mathrm{insep}\frac{K}{k} \leq \mathrm{insep}\frac{K_1}{k} + \mathrm{insep}\frac{K}{K_1} = \mathrm{insep}\frac{K_1}{k}$, weil $\mathrm{insep}\frac{K}{K_1} = 0$ ist wegen Satz 2.10.
Andererseits gilt nach Korollar 2.3 $\mathrm{insep}\frac{K}{k} \geq \mathrm{insep}\frac{K_1}{k}$, also insgesamt „=“.
q.e.d.

Man könnte annehmen, daß ein dem Korollar 2.13 entsprechender Satz auch bei vollkommenem Grundkörper k gilt, weil ja auch in diesem Fall jede endlich erzeugte Körpererweiterung separabel ist, wie wir in Satz 2.16 zeigen werden. Hier gilt aber nur die eine Richtung von Korollar 2.13. (Siehe Satz 2.17.)

Definition 2.15 *Ein Körper k heißt „vollkommen“, wenn entweder* $\mathrm{char}(k) = 0$ *ist oder* $\mathrm{char}(k) = p > 0$ *und $k^p = k$.*
(Dabei bedeutet $k^p = \{x^p \mid x \in k\}$.)

Satz 2.16 *Sei k ein Körper. Es gilt*
k ist vollkommen genau dann, wenn alle endlich erzeugten Körpererweiterungen K/k separabel sind.

Beweis: $\underline{\Leftarrow:}$ Wäre k unvollkommen, so wäre $\mathrm{char}(k) = p > 0$ und es existierte ein $y \in k$ mit $y^{1/p} \notin k$. Sei $K = k(x)$ mit $x^p = y$. Dann wäre K/k eine (rein) inseparable Körpererweiterung von Grad p. Das gibt es nach Voraussetzung aber nicht!

$\underline{\Rightarrow:}$ Sei nun k vollkommen und K/k eine endlich erzeugte Körpererweiterung. Falls $p := \mathrm{char}\,(k) = 0$ ist, ist trivialerweise K/k separabel. Im Falle $p > 0$ sind wegen $k = k^p$ offensichtlich K^p und k linear disjunkt über k^p (s. Satz 2.31), also ist nach Satz 2.35 K/k separabel. q.e.d.

Zusammen mit Korollar 2.12 folgt dann:

Korollar 2.17 *Sei k ein vollkommener Körper, K/k eine endlich erzeugte Körpererweiterung, d die universelle Derivation von K/k und $y_1, \ldots, y_r \in K$. Es gilt:*
$\{y_1, \ldots, y_r\}$ algebraisch abhängig über $k \Rightarrow \{\mathrm{d}y_1, \ldots, \mathrm{d}y_r\}$ linear abhängig über K.

Beweis: Nach Satz 2.16 ist K/k separabel.
Wäre $\{\mathrm{d}\,y_1, \ldots, \mathrm{d}\,y_r\}$ linear unabhängig über K, so ließe sich das System zu einer K-Basis $\{\mathrm{d}\,y_1, \ldots, \mathrm{d}\,y_r, \ldots, \mathrm{d}\,y_n\}$ von $\Omega(K/k)$ ergänzen. Nach Korollar 2.12 wäre dann $\{y_1, \ldots, y_r, \ldots, y_n\}$ eine (separierende) Tranzendenzbasis von K/k, als wäre insbesondere $\{y_1, \ldots, y_r\}$ algebraisch unabhängig über k. q.e.d.

Anmerkung 2.18 *Die Umkehrung von Korollar 2.17 ist im allgemeinen falsch: Sei etwa k ein vollkommener Körper der Charakteristik $p > 0$, x eine Unbestimmte und $K = k(x)$. Dann ist $\mathrm{d}x^p = p \cdot x^{p-1} \cdot \mathrm{d}x = 0$, also $\{\mathrm{d}x^p\}$ linear abhängig über K, aber $\{x^p\}$ algebraisch unabhängig über k.*
Man muß im Fall der Primzahlcharakteristik „algebraisch abhängig“ durch „p-abhängig“ ersetzen, um analoge Aussagen zu erhalten. (Siehe Korollar 2.28).

Beliebige Körpererweiterungen

Definition 2.19 *Eine Körpererweiterung K/k heißt „rein inseparabel“ genau dann, wenn $\mathrm{char}(k) = p > 0$ ist und es zu jedem $x \in K$ eine natürliche Zahl ν gibt mit $x^{p^\nu} \in k$.*

Anmerkung 2.20 *Sei k ein Körper der Charakteristik $p > 0$ und x ein Element eines Oberkörpers von k mit $x^{p^\nu} \in k$. Sei μ die kleinste ganze Zahl ≥ 0 mit $x^{p^\mu} \in k$. Dann ist*

$$f(X) := X^{p^\mu} - x^{p^\mu}$$

das Minimalpolynom von x über k.

Beweis: Sei $f \in k[X]$ das Minimalpolynom von x über k. Wegen $z := x^{p^\mu} \in k$ gilt $f \mid (X^{p^\mu} - z)$ in $k[X]$, also auch im Polynomring über dem Zerfällungskörper dieser Polynome über k. Dort ist $X^{p^\mu} - z = (X - x)^{p^\mu}$, weil die p^μ-te Wurzel eindeutig bestimmt ist. Also ist $f = (X - x)^m$ und $m = \mathrm{Grad}(f) \leq p^\mu$. Das konstante Glied von f ist dann x^m, also gilt $x^m \in k$ weil $f \in k[X]$. Sei $n := \mathrm{ggT}(m, p^\mu) \geq 1$. Dann ist $n = p^\lambda$ mit $\lambda \leq \mu$. Ferner ist wegen $x^m \in k$ und

$x^{p^\mu} \in k$ auch $x^{p^\lambda} \in k$, weil $p^\lambda = n = a \cdot p^\mu + b \cdot m$ mit $a, b \in \mathbb{Z}$ als ggT. Wegen der Minimalität von μ ist dann $\mu = \lambda$, also $m = p^\mu \cdot l$ mit $l \in \mathbb{N}$, und wegen $m \leq p^\mu$ ist $l = 1$, also $f = X^{p^\mu} - x^{p^\mu}$. q.e.d.

Satz 2.21 *Sei K/k eine endlich erzeugte rein inseparable Körpererweiterung,* d *die universelle Derivation von K/k.*

$$\Omega(K/k) = \sum_{i=1}^{m} K \, \mathrm{d}x_i \quad \Longrightarrow \quad K = k(x_1, \ldots, x_m) \; .$$

Beweis: Sei $K_1 := k(x_1, \ldots, x_m) \Rightarrow \Omega(K/k) = K \, \mathrm{d}K_1$, und daher $\Omega(K/K_1) = \Omega(K/k)/K \, \mathrm{d}K_1 = 0$. Also ist nach Satz 2.6 K/K_1 separabel algebraisch.
Sei $y \in K$ beliebig. Da K/k rein inseparabel ist, gibt es ein $\nu \in \mathbb{N}$ mit $y^{p^\nu} \in k \subseteq K_1$. Nach Satz 2.20 hat das Minimalpolynom f von y über K_1 die Form $f = X^{p^\mu} - z, \quad z \in K_1$. Andererseits ist y separabel über K_1, d.h. $f'(y) \neq 0$. $\Rightarrow \mu = 0 \Rightarrow y = z \in K_1 \Rightarrow K = K_1$. q.e.d.

Für das Folgende brauchen wir die Begriffe der p-Abhängigkeit, einer p-Basis und des p-Grades, die bei Differentialen bei Charakteristik p oft dieselbe Rolle spielen wie algebraische Abhängigkeit, die Transzendenzbasis und der Transzendenzgrad bei Charakteristik Null. Wir wiederholen hier nur die Definitionen und setzen die Grundeigenschaften als bekannt voraus. (Siehe etwa [Ku]).

Definition 2.22 (p-Basis) *Sei K/k eine (nicht notwendig endlich erzeugte) Körpererweiterung,*
$\mathrm{char}(K) = p > 0$.

Seien $z, x_1, \ldots, x_m \in K$
z heißt „p-abhängig von $\{x_1, \ldots, x_m\}$ in K/k“, wenn gilt
$z \in k(K^p)[x_1, \ldots, x_m]$.

Ein System $\{z_\iota \mid z_\iota \in K, \iota \in I\}$ heißt „p-unabhängig in K/k“, wenn kein z_λ von endlich vielen der übrigen z_ι p-abhängig ist.

Ein System $\{z_\iota \mid z_\iota \in K, \iota \in I\}$ heißt „p-Basis von K/k“, wenn es ein maximales in K/k p-unabhängiges System ist. Dies ist äquivalent dazu, daß das System
$\left\{ z_{\iota_1}^{\nu_1} \cdots z_{\iota_n}^{\nu_n} \mid 0 \leq \nu_i \leq p-1, n \in \mathbb{N}, i = 1, \ldots, n \right\}$
eine $k(K^p)$-Vektorraum-Basis von K ist.

Falls die p-Basis aus endlich vielen Elementen besteht, heißt die Anzahl m der Elemente einer p-Basis der „ p-Grad von K über k (p-grad$\frac{K}{k}$)“. In diesem Falle ist $[K : k(K^p)] = p^m$.

Die folgende Anmerkung erweist sich oft als nützlich:

Anmerkung 2.23 *Seien*
$K^p \subseteq K_2 \subseteq K_1 \subseteq K$ Körper von Primzahlcharakteristik p,
$\{\alpha_\iota | \iota \in I\}$ eine p-Basis von K/K_1,

$\{\beta_\kappa|\kappa \in J\}$ eine p-Basis von K_1/K_2,
Dann ist $\{\alpha_\iota|\iota \in I\} \cup \{\beta_\kappa|\kappa \in J\}$ eine p-Basis von K/K_2.
Insbesondere ist $p\text{-}grad\frac{K}{K_2} < \infty \Longleftrightarrow p\text{-}grad\frac{K}{K_1} < \infty$ und $p\text{-}grad\frac{K_1}{K_2} < \infty$.
In diesem Fall gilt dann
$p\text{-}grad\frac{K}{K_2} = p\text{-}grad\frac{K}{K_1} + p\text{-}grad\frac{K_1}{K_2}$

Beweis: Wegen $K^p \subseteq K_2 \subseteq K_1$ ist $K_2(K^p) = K_2$, $K_2(K_1^p) = K_2$
und $K_1(K^p) = K_1$.
Nach Voraussetzung ist nun $\{\alpha_{\iota_1}^{\nu_1} \cdots \alpha_{\iota_s}^{\nu_s}|\iota_i \in I, 0 \leq \nu_i < p, s \in \mathbb{N}_0\}$ eine K_1-Vektorraumbasis von K und
$\{\beta_{\kappa_1}^{\mu_1} \cdots \beta_{\kappa_r}^{\mu_r}|\kappa_j \in J, 0 \leq \mu_i < p, r \in \mathbb{N}_0\}$ eine K_2-Vektorraumbasis von K_1.
Daher ist
$\{\alpha_{\iota_1}^{\nu_1} \cdots \alpha_{\iota_s}^{\nu_s} \cdot \beta_{\kappa_1}^{\mu_1} \cdots \beta_{\kappa_r}^{\mu_r}|\iota_i \in I,\ \kappa_j \in J,\ 0 \leq \nu_i, \mu_j < p,\ s, r \in \mathbb{N}_0\}$
eine K_2-Vektorraumbasis von K, d.h. $\{\alpha_\iota|\iota \in I\} \cup \{\beta_\kappa|\kappa \in J\}$ ist eine p-Basis von K/K_2.
Die restlichen Aussagen der Anmerkung im Fall endlicher p-Grade folgen nun unmittelbar. q.e.d.

Satz 2.24 *Sei K/k eine nicht notwendig endlich erzeugte Körpererweiterung,* $\mathrm{char}(K) = p > 0$, $K_0 := k(K^p)$, d *die universelle Derivation von K/k und* $\{z_\iota|\iota \in I\} \subseteq K$.
Es sind äquivalent:

1. *$\{\mathrm{d}z_\iota|\iota \in I\}$ ist eine K-Vektorraumbasis von $\Omega(K/k)$.*

2. *$\{z_\iota|\iota \in I\}$ ist eine p-Basis von K/k.*

Zusatz: *Man hat dann eine Darstellung* $K = K_0[\{Z_\iota|\iota \in I\}]\big/(\{Z_\iota^p - z_\iota^p|\iota \in I\})$.

Beweis: *2. $\Rightarrow$ 1.:* Wir beweisen zunächst den Zusatz:
Nach Definition einer p-Basis ist $K = K_0[\{z_\iota\}]$ und $z_\iota^p \in K^p \subseteq K_0$.
Sei $\varphi : K_0[\{Z_\iota\}] \to K_0[\{z_\iota\}]$ der Einsetzungshomomorphismus $Z_\iota \mapsto z_\iota$ und $n := \mathrm{Ker}\,\varphi$.
Sei ferner $n_1 := (\{Z_\iota^p - z_\iota^p\})$. Wir zeigen, daß $n = n_1$ ist. Daraus folgt der Zusatz.
Zunächst ist klar, daß $\varphi(Z_\iota^p - z_\iota^p) = 0$ ist, also $n_1 \subseteq n$.
Umgekehrt sei $f \in K_0[\{Z_\iota\}]$ beliebig. Modulo n_1 lassen sich in $K_0[\{Z_\iota\}]$ alle Potenzen der endlich vielen Z_ι, die in f vorkommen, auf Potenzen $\leq p-1$ reduzieren, d.h. es gibt $a_{\nu_1,\ldots,\nu_n} \in K_0$ mit $f \equiv \sum_{0 \leq \nu_1,\ldots,\nu_n < p} a_{\nu_1,\ldots,\nu_n} \cdot Z_{\iota_1}^{\nu_1} \cdots Z_{\iota_n}^{\nu_n} \bmod n_1$.
Ist nun $f \in n$, so folgt durch Anwenden von φ daraus:
$0 = \sum_{0 \leq \nu_1,\ldots,\nu_n < p} a_{\nu_1\ldots,\nu_n} \cdot z_{\iota_1}^{\nu_1} \cdots z_{\iota_n}^{\nu_n}$ und daher $a_{\nu_1,\ldots,\nu_n} = 0$ für alle $(\nu_1, \ldots, \nu_n)$, da die Potenzprodukte der z_ι mit Exponenten $< p$ wegen der p-Basiseigenschaft linear unabhängig über K_0 sind. Also ist auch $n \subseteq n_1$, und damit ist der Zusatz

bewiesen.
Ferner gilt offenbar $\mathrm{d}\,(K^p) = 0$, und daher ist nach Satz 1.31 $\Omega(K/k) = \Omega(K/K_0)$. Die Konstruktionsvorschrift von Satz 1.29 liefert:

$$\begin{aligned}\Omega(K/k) &= \Omega(K/K_0)\\ &= \Big(\bigoplus_{\iota\in I} K\cdot\Delta Z_\iota\Big)\Big/K\Big\langle\Big\{\underbrace{\partial(Z_\iota^p - z_\iota^p)}_{=0} + \underbrace{\frac{\partial}{\partial z_\iota}(Z_\iota^p - z_\iota^p)\cdot\Delta Z_\iota}_{=0}\,\Big|\,\iota\in I\Big\}\Big\rangle\\ &= \bigoplus_{\iota\in I} K\cdot\mathrm{d}\,z_\iota\ ,\end{aligned}$$

d.h. $\{\mathrm{d}\,z_\iota|\iota\in I\}$ ist eine K-Basis von $\Omega(K/k)$. q.e.d.
1. $\Rightarrow$ 2.: Sei $K_1 := K_0[\{z_\iota|\iota\in I\}]$.
Dann ist $\Omega(K/K_1) = \Omega(K/k)/K\langle\{\mathrm{d}\,z_\iota|\iota\in I\}\rangle = (0)$
Die Differentiale einer p-Basis von K/K_1 sind nach dem oben gezeigten eine K-Basis von $\Omega(K/K_1)$. Da aber $\Omega(K/K_1) = (0)$ ist, muß $K = K_1[K^p]$ sein.
Andererseits ist $K^p \subseteq K_0 \subseteq K_1$, also ist $K = K_1$.
Das System $\{z_\iota|\iota\in I\}$ ist p-unabhängig in K/k;
denn wäre etwa $z_\lambda \in k(K^p)[z_{\iota_1},\ldots,z_{\iota_n}]$, so folgte $\mathrm{d}\,z_\lambda \in \sum_{i=1}^{n} K\cdot\mathrm{d}\,z_{\iota_i}$. Wegen der linearen Unabhängigkeit der $\{z_\iota\}$ wäre dann $\lambda\in\{\iota_1,\ldots,\iota_n\}$.
Andererseits ist $K = k(K^p)[\{z_\iota|\iota\in I\}]$, also ist $\{z_\iota|\iota\in I\}$ eine p-Basis von K/k.
q.e.d.

Aus Satz 2.24 folgen sofort drei Korollare:

Korollar 2.25 *Sei K/k eine endlich erzeugte Körpererweiterung, $\mathrm{char}(K) = p > 0$. Es gilt:*

$$\dim_K \Omega(K/k) = p\text{-}grad\frac{K}{k}\ .$$

Korollar 2.26 *Sei K/k eine endlich erzeugte Körpererweiterung, $\mathrm{char}(K) = p > 0$. Es gilt:*

$$\mathrm{insep}\frac{K}{k} = p\text{-}grad\frac{K}{k} - \dim\frac{K}{k}\ .$$

Korollar 2.27 *Sei K/k eine endlich erzeugte Körpererweiterung, $\mathrm{char}(K) = p > 0$. Es gilt:*

$$K/k \text{ separabel} \iff p\text{-}grad\frac{K}{k} = \dim\frac{K}{k}\ .$$

Nun können wir auch das Analogon bei Primzahlcharakteristik zu Korollar 2.13 zeigen.

Korollar 2.28 *Sei K/k eine nicht notwendig endlich erzeugte Körpererweiterung,* $\mathrm{char}(K) = p > 0$,
d *die universelle Derivation von K/k und*
$\{x_\iota \mid \iota \in J\} \subseteq K$.
Es gilt:
$\{\mathrm{d}x_\iota \mid \iota \in J\}$ *linear unabhängig über* $K \iff$
$\{x_\iota \mid \iota \in J\}$ *p-unabhängig in* K/k
Folgerung: *Ein Element z ist p-abhängig von $\{x_1, \ldots, x_r\}$ in $K/k \iff$*
$\mathrm{d}z$ *ist linear abhängig über K von* $\{\mathrm{d}x_1, \ldots, \mathrm{d}x_r\}$.

Beweis:
$\underline{\Rightarrow:}$ Ergänze $\{\mathrm{d}x_1, \ldots, \mathrm{d}x_r\}$ zu einer K-Basis $\{\mathrm{d}\,x_\iota | \iota \in I\}$ von $\Omega(K/k)$.
Nach Satz 2.24 ist dann $\{x_\iota | \iota \in I\}$ eine p-Basis von K/k. Insbesondere ist dann $\{x_1, \ldots, x_r\}$ p-unabhängig in K/k.
$\underline{\Leftarrow:}$ Ergänze $\{x_1, \ldots, x_r\}$ zu einer p-Basis $\{x_\iota | \iota \in I\}$ von K/k. Nach Satz 2.24 ist dann $\{\mathrm{d}\,x_\iota | \iota \in I\}$ eine K-Basis von $\Omega(K/k)$. Also ist inbesondere $\{\mathrm{d}\,x_1, \ldots, \mathrm{d}\,x_r\}$ linear unabhängig über K.
Die Folgerung ist wiederum nur eine äquivalente Umformulierung des Korollars.
q.e.d.

Der Hauptsatz

Wir sind nun in der Lage, den Hauptsatz über die Erzeugendenzahl einer Körpererweiterung zu beweisen:

Satz 2.29 (Hauptsatz) *Sei K/k eine endlich erzeugte Körpererweiterung,*
$n = \dim \frac{K}{k}$, $i = \mathrm{insep}\frac{K}{k}$.
Es gilt:

1. *Fall $i = 0$: K läßt sich aus k durch Adjunktion von $n+1$ Elementen erzeugen. Man braucht mindestens n Elemente.*
2. *Fall $i > 0$: K läßt sich aus k durch Adjunktion von $n+i$ Elementen erzeugen. Man braucht auch mindestens $n+i$ Elemente.*

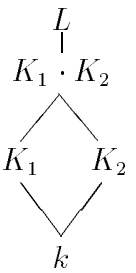
Beweis: 1. Fall: $\mathrm{insep}\frac{K}{k} = 0$. $\Rightarrow \dim_K \Omega(K/k) = n$, also $\Omega(K/k) = K \cdot \mathrm{d}x_1 + \ldots + K \cdot \mathrm{d}x_n$ und K/k separabel nach Satz 2.10. Nach Korollar 2.12 ist ferner $\{x_1, \ldots, x_n\}$ eine separierende Transzendenzbasis von K/k.
Daher ist $K/k(x_1, \ldots, x_n)$ separabel algebraisch. Nach dem Satz vom primitiven Element existiert dann ein $z \in K$ mit $K = k(x_1, \ldots, x_n, z)$, also kann man K aus k durch Adjunktion von $n+1$ Elementen erzeugen.
Falls $K = k(y_1, \ldots, y_m)$ ist, folgt $\Omega(K/k) = K \cdot \mathrm{d}y_1 + \ldots + K \cdot \mathrm{d}y_m$, also $m \geq n$.
$\Rightarrow$ Man braucht mindestens n Elemente um K aus k zu erzeugen. q.e.d.
2. Fall: $\mathrm{insep}\frac{K}{k} = i > 0 \Rightarrow \dim_K \Omega(K/k) = n + i$,
also $\Omega(K/k) = K \cdot \mathrm{d}x_1 + \ldots + K \cdot \mathrm{d}x_{n+i}$.

$\Rightarrow \Omega\left(K/k(x_1,\ldots,x_{n+i})\right) = \Omega(K/k)/(K\cdot \mathrm{d}x_1 + \ldots + K\cdot \mathrm{d}x_{n+i}) = 0.$
Nach Satz 2.6 ist $K/k(x_1,\ldots,x_{n+i})$ (separabel) algebraisch und daher
$\dim \frac{k(x_1,\ldots,x_{n+i})}{k} = \dim \frac{K}{k} = n.$
Wir können also o.B.d.A. annehmen, daß $\{x_1,\ldots,x_n\}$ algebraisch unabhängig über k ist. Sei $K_0 := k(x_1,\ldots,x_n)$. $\Rightarrow K/K_0$ endlich algebraisch. Sei ferner K_1:=separabler Abschluß von K_0 in K. Dann ist K_1/K_0 endlich separabel algebraisch und K/K_1 rein inseparabel endlich algebraisch.
Es ist $\Omega(K/K_1) = K\cdot \mathrm{d}'x_{n+1} + \ldots + K\cdot \mathrm{d}'x_{n+i}$ mit $\mathrm{d}' = \mathrm{d}_{\frac{K}{K_1}}$.
Da K/K_1 endlich erzeugt und rein inseparabel ist, folgt aus Satz 2.21
$K = K_1(x_{n+1},\ldots,x_{n+i})$.
Sei $K_2 = K_1(x_{n+1})$. Da K_1/K_0 endlich separabel algebraisch ist, folgt nach dem verallgemeinerten Satz vom primitiven Element, daß es ein $y \in K_2$ gibt mit $K_2 = K_0(y)$ (siehe etwa [Wae1] § 46).
$\Rightarrow K = \overbrace{\underbrace{k(x_1,\ldots,x_n}_{K_0},y}^{K_2}, x_{n+2},\ldots x_{n+i})$, also kann man K aus k durch Adjunktion von $n+i$ Elementen erzeugen.
Wegen $\dim_K \Omega(K/k) = n+i$ braucht man auch mindestens $n+i$ Elemente, um K aus k zu erzeugen. q.e.d.

Separabilität und lineare Disjunktheit

In diesem Abschnitt behandeln wir den von S. MacLane [ML] (s.a. [Dieu] eingeführten Separabilitätsbegriff, der dann bei nicht endlich erzeugten Körpererweiterungen die „richtigen“ Eigenschaften hat und zeigen, wie er mit dem Separabilitätsbegriff für endlich erzeugte Körpererweiterungen nach Definition 2.8 zusammenhängt. Wir brauchen diesen Separabilitätsbegriff für den Abschnitt über die tensorielle Ausdehnung bei Körpererweiterungen.
Zunächst behandeln wir zur Vorbereitung die Definition und einige Eigenschaften von „linear disjunkt“.

Definition 2.30 *Seien k, K_1, K_2, L Körper, $k \subseteq K_1 \subseteq L$, $k \subseteq K_2 \subseteq L$.*
K_1 und K_2 heißen „linear disjunkt über k“, wenn der kanonische k-Algebra-Homomorphismus
$K_1 \otimes_k K_2 \to K_1 \cdot K_2$ mit $x \otimes y \mapsto x \cdot y$
ein Isomorphismus ist.
Dabei bezeichnet $K_1 \cdot K_2$ den Unterring $k[K_1, K_2]$ von L.

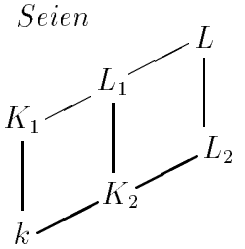


Eine andere Charakterisierung linear disjunkter Körpererweiterungen liefert der folgende Satz:

Satz 2.31 *Seien k, K_1, K_2 wie in Definition 2.30. Es gilt:*
K_1und K_2 sind linear disjunkt über k . $\Longleftrightarrow$
Jedes System von Elementen aus K_1, das über k linear unabhängig ist, ist auch über K_2 linear unabhängig. $\Longleftrightarrow$
Jedes System von Elementen aus K_2, das über k linear unabhängig ist, ist auch über K_1 linear unabhängig.

Beweis : Da das Tensorprodukt symmetrisch in K_1 und K_2 ist, genügt es, die Äquivalenz der beiden ersten Aussagen zu zeigen.
Vorbemerkung: Ist $\{x_\iota\}$ eine k-Basis von K_1 und $\{y_\lambda\}$ eine k-Basis von K_2, so ist $\{x_\iota \otimes y_\lambda\}$ eine k-Basis von $K_1 \otimes_k K_2$.
Ferner sind $\{1 \otimes y_\lambda\}$ eine $(K_1 \otimes 1)$-Basis und $\{x_\iota \otimes 1\}$ eine $(1 \otimes K_2)$-Basis von $K_1 \otimes_k K_2$.
Nimmt man die Eins in eine Basis von K_2 auf, so sieht man, daß die Abbildung $K_1 \ni x \mapsto x \otimes 1 \in K_1 \otimes_k K_2$ injektiv ist, also einen Isomorphismus $K_1 \cong K_1 \otimes 1 \subseteq K_1 \otimes_k K_2$ darstellt. Die kanonische Abbildung $\Phi : K_1 \otimes_k K_2 \to K_1 \cdot K_2$ mit $x \otimes y \mapsto x \cdot y$ induziert auf $K_1 \otimes 1$ die Umkehrabbildung. Analoges gilt für K_2 anstelle von K_1.
$\underline{\Rightarrow:}$ Sei $\{x_\iota \mid \iota \in J\}$ ein System von Elementen von K_1, das linear unabhängig über k ist. Dann läßt es sich zu einer Basis von K_1 über k ergänzen.
$\{x_\iota \otimes 1 \mid \iota \in J\}$ ist dann Teil einer Basis von $K_1 \otimes_k K_2$ über $1 \otimes K_2$, also linear unabhängig über $1 \otimes K_2$. Die Anwendung des kanonischen Isomorphismus $\Phi : K_1 \otimes_k K_2 \to K_1 \cdot K_2$ zeigt, daß $\{x_\iota\} = \{\Phi(x_\iota \otimes 1)\}$ linear unabhängig über $\Phi(1 \otimes K_2) = K_2$ ist.
$\underline{\Leftarrow:}$ Sei $\{x_\iota\}$ eine k-Basis von K_1. Nach Voraussetzung ist dann $\{x_\iota\}$ auch linear unabhängig über K_2, also eine K_2-Basis von $K_2[K_1] = K_1 \cdot K_2$. Andererseits ist nach der Vorbemerkung $\{x_\iota \otimes 1\}$ eine $(1 \otimes K_2)$-Basis von $K_1 \otimes_k K_2$. Vermöge Φ ist aber $1 \otimes K_2 \cong K_2$ und die $(1 \otimes K_2)$-Basis $\{x_\iota \otimes 1\}$ wird durch Φ auf die K_2-Basis $\{x_\iota\}$ abgebildet. $\Rightarrow K_1 \otimes_k K_2 \cong K_1 \cdot K_2$ vermöge Φ, d.h. K_1 und K_2 sind linear disjunkt über k. q.e.d.

Anmerkung 2.32 (Transitivität von „linear disjunkt“) *Seien k, K_1, K_2, L_1, L_2 Unterkörper eines Körpers L, so daß $k \subseteq K_1 \subseteq L_1$, $k \subseteq K_2 \subseteq L_2$ und $K_2 \subseteq L_1$ ist.*
Ferner seien
K_1 und K_2 linear disjunkt über k,
L_1 und L_2 linear disjunkt über K_2.
Dann sind auch K_1 und L_2 linear disjunkt über k.



Beweis: Wende Satz 2.31 an: Seien $x_\iota \in K_1$ linear unbhängig über k, dann sind sie nach Voraussetzung linear unabhängig über K_2. Da die x_ι aber auch zu L_1 gehören, sind sie nach Voraussetzung linear unabhängig über L_2. Nach Satz 2.31 folgt die Behauptung. q.e.d.
Wir stellen nun den Bezug zu den separablen Körpererweiterungen her. Dazu betrachten wir zunächst einige Spezialfälle:

Hilfssatz 2.33 *Sei K/k eine rein transzendente Körpererweiterung, $\mathrm{char}(K) = p > 0$. Dann sind K^p und k linear disjunkt über k^p.*

Beweis: Es ist $K = k(\{x_\iota \mid \iota \in J\})$ mit über k algebraisch unabhängigen Elementen x_ι. Seien nun $z_1, \ldots, z_s \in k$ linear unabhängig über k^p. Es ist zu zeigen, daß die z_i auch über $K^p = k^p(\{x_\iota^p\})$ linear unabhängig sind: Sei $\sum f_i \cdot z_i = 0$ mit $f_i \in K^p$. Wir können o.B.d.A. annehmen, daß schon $f_i \in k^p[\{x_\iota^p\}]$ für alle i gilt. Also ist $f_i = \sum\limits_{\nu_1,\ldots,\nu_r} a^p_{i,\nu_1\ldots\nu_r} \cdot x_{\iota_1}^{p\cdot\nu_1} \cdots x_{\iota_r}^{p\cdot\nu_r}$ mit $a_{i,\nu_1\ldots\nu_r} \in k$ für alle i. $\Rightarrow$

$$0 = \sum_{i,\,\nu_1,\ldots,\nu_r} a^p_{i,\nu_1,\ldots\nu_r} \cdot x_{\iota_1}^{p\cdot\nu_1} \cdots x_{\iota_r}^{p\cdot\nu_r} \cdot z_i = \sum_{\nu_1,\ldots,\nu_r} \left(\sum_i a^p_{i,\nu_1,\ldots\nu_r} \cdot z_i \right) \cdot x_{\iota_1}^{p\cdot\nu_1} \cdots x_{\iota_r}^{p\cdot\nu_r}.$$

Da die $x_{\iota_1}, \ldots, x_{\iota_r}$ algebraisch unabhängig über k sind, folgt:
$\sum\limits_i a^p_{i,\nu_1,\ldots\nu_r} \cdot z_i = 0$ für alle $(\nu_1, \ldots, \nu_r)$. Nach Voraussetzung sind aber die $z_1, \ldots, z_s$ linear unabhängig über k^p. $\Rightarrow a^p_{i,\nu_1,\ldots\nu_r} = 0$ für alle $(i, \nu_1, \ldots, \nu_r)$. $\Rightarrow f_i = 0$ für alle $i = 1, \ldots, s$. $\Rightarrow z_1, \ldots, z_s$ linear unabhängig über K^p. q.e.d.

Hilfssatz 2.34 *Sei $K = k(y)$ eine separabel algebraische Körpererweiterung von k, $\mathrm{char}(K) = p > 0$. Dann ist $K = k(y^p)$.*
Folgerung: *K^p und k sind linear disjunkt über k^p.*

Beweis: Da K/k separabel algebraisch ist, ist K auch separabel algebraisch über jedem Zwischenkörper von K/k. Insbesondere ist also $K = k(y^p)(y)$ separabel algebraisch über $k(y^p)$. Andererseits ist wegen $y^p \in k(y^p)$ nach Satz 2.20 das Minimalpolynom von y über $k(y^p)$ von der Form $f = X^{p^\mu} - y^{p^\mu}$ mit $\mu \in \{0, 1\}$. Aber $\mu = 1$ kommt nicht in Frage, weil dann K inseparabel über $k(y^p)$ wäre, also ist $\mu = 0$ und daher $y \in k(y^p)$. q.e.d.
Beweis der Folgerung: Sei $[K : k] = m$. Dann ist $\{1, y, \ldots, y^{m-1}\}$ eine k-Basis von K. Die Potenzierung mit p induziert einen Isomorphismus von K/k auf K^p/k^p. Also ist $\{1, y^p, (y^p)^2 \ldots, (y^p)^{m-1}\}$ eine k^p-Basis von $K^p = k^p(y^p)$. Andererseits bilden wegen $K = k(y^p)$ diese Elemente auch eine k-Basis von K, sind

also linear unabhängig über k.
Wenn aber eine spezielle k^p-Basis von K^p über k linear unabhängig ist, dann ist klar, daß jedes über k^p linear unabhängige System von Elementen von K^p über k linear unabhängig ist (lineare Algebra!). Damit ist gezeigt, daß K^p und k linear disjunkt über k^p sind nach Satz 2.31. q.e.d.
Nun können wir den bisherigen Kriterien für Separabilität einen weiteren Punkt hinzufügen:

Satz 2.35 *Sei K/k eine endlich erzeugte Körpererweiterung,* $\mathrm{char}(k) = p > 0$. *Es sind äquivalent:*

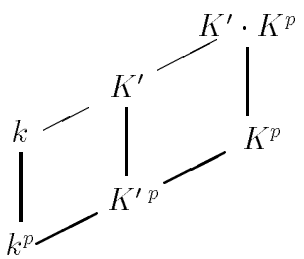
1. *K ist separabel über k.*
2. $\mathrm{insep}\frac{K}{k} = 0$
3. *Jeder über k endlich erzeugte Zwischenkörper K' mit $k \subseteq K' \subseteq K$ ist separabel über k.*
4. *k und K^p sind linear disjunkt über k^p.*

Beweis: *1. $\Leftrightarrow$ 2.:* Gilt nach Satz 2.10.

3. $\Rightarrow$ 1.: Trivial mit $K' = K$.

1. $\Rightarrow$ 3.: Gilt nach der Folgerung zu Satz 2.10.

1. $\Rightarrow$ 4.: Sei $\{x_1, \ldots, x_n\}$ eine separierende Transzendenzbasis von K/k und $K' := k(x_1, \ldots, x_n)$. Dann ist $K = K'(y)$ mit y separabel algebraisch über K'. Betrachte:



K' ist rein transzendent über k, nach Hilfssatz 2.33 sind also k und K'^p linear disjunkt über k^p.
Ferner ist K/K' einfach separabel algebraisch, also sind nach Hilfssatz 2.34 auch K' und K^p linear disjunkt über K'^p.
Nach dem Satz 2.32 (Transitivität) sind dann auch k und K^p linear disjunkt über k^p.

4. $\Rightarrow$ 2.: Sei $r = \dim_K \Omega(K/k)$ und $\{\mathrm{d}y_1, \ldots, \mathrm{d}y_r\}$ eine K-Basis von $\Omega(K/k)$.
Wir zeigen: $\{y_1, \ldots, y_r\}$ algebraisch unabhängig über k.
($\Rightarrow \dim \frac{K}{k} \geq r. \Rightarrow \mathrm{insep}\frac{K}{k} \leq 0. \Rightarrow \mathrm{insep}\frac{K}{k} = 0.$ q.e.d.)
Beweis(indirekt): Wären $y_1, \ldots, y_r$ algebraisch abhängig über k, so existierte ein Polynom
$f \in k[Y_1, \ldots, Y_r]$ von minimalem Gesamtgrad mit $f \neq 0$ und $f(y_1, \ldots, y_r) = 0$.
Die Anwendung von d liefert:
$\sum_{i=1}^{r} f_{y_i} \cdot \mathrm{d}y_i = 0$, wobei $f_{y_i} := f_{Y_i}(y_1, \ldots, y_n)$ ist.
Weil die $\mathrm{d}y_i$ linear unabhängig sind, wäre $f_{y_i} = 0$ für alle $i = 1, \ldots, r$. Aus

$f_{y_i} = 0$ folgt aber $f_{Y_i} = 0$, weil sonst f_{Y_i} ein Polynom $\neq 0$ von niedrigerem Gesamtgrad als f wäre, das $(y_1, \ldots, y_r)$ zur Nullstelle hat. Daher kommt in diesem Falle Y_i in f nur als Y_i^p vor.
Da das für alle $i = 1, \ldots, r$ gälte, wäre f von der Form
$f = \sum a_{i_1 \ldots i_r} \cdot (Y_1^p)^{i_1} \cdots (Y_r^p)^{i_r}$ mit $a_{i_1 \ldots i_r} \in k$, nicht alle $a_{i_1 \ldots i_r} = 0$.
$\Rightarrow \left\{(y_1^p)^{i_1} \cdots (y_r^p)^{i_r}\right\}$ wäre also ein System von Elementen von K^p, die linear abhängig über k sind. Nach Voraussetzung *4.* wären diese Elemente dann auch linear abhängig über k^p.
D.h. es gäbe Elemente $b_{i_1 \ldots i_r} \in k$, nicht alle $= 0$ mit $\sum b^p_{i_1 \ldots i_r} \cdot (y_1^p)^{i_1} \cdots (y_r^p)^{i_r} = 0$.
Sei $g := \sum b_{i_1 \ldots i_r} \cdot Y_1^{i_1} \cdots Y_r^{i_r}$. Dann wäre $g \neq 0$ und
(Gesamtgrad von g) $\leq (1/p) \cdot$ (Gesamtgrad von f) $<$ Gesamtgrad von f.
Ferner $g(y_1, \ldots, y_r)^p = \sum b^p_{i_1, \ldots, i_r} \cdot (y_1^p)^{i_1} \cdots (y_r^p)^{i_r} = 0$ und daher auch
$g(y_1, \ldots, y_r) = 0$ im Widerspruch zur Wahl von f als Polynom $\neq 0$ mit minimalem Gesamtgrad mit dieser Eigenschaft. q.e.d.

Separabilität bei nicht endlich erzeugten Körpererweiterungen

Bei nicht endlich erzeugten Körpererweiterungen ist die Forderung der Existenz einer separierenden Transzendenzbasis im allgemeinen zu stark. Im Hinblick auf die im Falle endlich erzeugter Körpererweiterungen äquivalenten Aussagen von Satz 2.35 kann man aber, ohne mit früheren Bezeichnungen in Widerspruch zu geraten, definieren:

Definition 2.36 *Eine Körpererweiterung K/k heißt „separabel", wenn jeder über k endlich erzeugte Zwischenkörper K^*, $k \subseteq K^* \subseteq K$, separabel über k ist im Sinne von Definition 2.8.*
(D.h. K^* besitzt eine separierende Transzendenzbasis über k.)

Auch die Aussage über die lineare Disjunktheit von Satz 2.35 läßt sich übertragen:

Satz 2.37 *Sei K/k eine Körpererweiterung,* $\mathrm{char}(K) = p > 0$. *Es sind äquivalent:*
1) K ist separabel über k.
2) k und K^p sind linear disjunkt über k^p.

Beweis: *1) $\Rightarrow$ 2):* Seien $z_1^p, \ldots, z_r^p \in K^p$ linear unabhängig über k^p. $\overset{!}{\Rightarrow}$ $z_1^p, \ldots, z_r^p$ sind auch linear unabhängig über k.
Beweis: Sei $K^* = k(z_1, \ldots, z_r) \Rightarrow k \subseteq K^* \subseteq K$ und K^*/k endlich erzeugt. $\overset{1)}{\Rightarrow}$ K^*/k separabel in Sinne von Definition 2.8. Ferner sind $z_1^p, \ldots, z_r^p \in (K^*)^p$, also folgt aus Satz 2.35, daß die $z_1^p, \ldots, z_r^p$ auch linear unabhängig über k sind. q.e.d.

2) $\Rightarrow$ 1): Sei $k \subseteq K^* \subseteq K$ und K^* endlich erzeugt über k. Da nach Voraussetzung k und K^p linear disjunkt über k^p sind, folgt wegen $K^* \subseteq K$, daß Elemente von $(K^*)^p$, die linear unabhängig über k^p sind, auch linear unabhängig über k sind. Also sind auch k und $(K^*)^p$ linear disjunkt über k^p. Da zudem K^*/k endlich erzeugt ist, folgt aus Satz 2.35, daß K^*/k separabel im Sinne von Definition 2.8 ist. Also ist K/k separabel im Sinne von Definition 2.36. q.e.d.

Definition 2.38 *Eine Körpererweiterung K/k heißt „separabel erzeugt", wenn es eine separierende Transzendenzbasis von K/k gibt.*
(D.h. es existieren Elemente $x_\iota \in K$, so daß das System $\{x_\iota\}$ algebraisch unabhängig über k ist und die Körpererweiterung $K/k(\{x_\iota\})$ separabel algebraisch ist.

Anmerkung 2.39 *Ist K/k* endlich erzeugt*, so gilt offenbar:*
K/k separabel $\Longleftrightarrow$ K/k separabel erzeugt.

Allgemein ist das nicht richtig. Es gilt nur:

Satz 2.40 *K/k separabel erzeugt $\Longrightarrow$ K/k separabel.*

Beweis: Sei K/k separabel erzeugt, $k \subseteq K^* \subseteq K$ und $K^* = k(y_1, \ldots, y_r)$ endlich erzeugt über k. Es ist zu zeigen, daß K^*/k separabel ist:
Nach Voraussetzung existiert eine separierende Transzendenzbasis $\{x_\iota\}$ von K/k, also sind die $y_1, \ldots, y_r$ separabel algebraisch über $k(\{x_\iota\})$. Sei für $i = 1, \ldots, r$ $f_i(Y) \in k(\{x_\iota\})[Y]$ das Minimalpolynom von y_i über $k(\{x_\iota\})$. Dann ist f_i irreduzibel in $k(\{x_\iota\})[Y]$, $f_i(y_i) = 0$ und $f_i'(y_i) \neq 0$.
In den endlich vielen Koeffizienten der $f_1, \ldots, f_r$ kommen nur endlich viele der x_ι vor, etwa $x_{\iota_1}, \ldots, x_{\iota_m}$. Sei $K_0 := k(x_{\iota_1}, \ldots, x_{\iota_m})$. Dann gilt also $f_i \in K_0[Y]$ für alle i, und die f_i sind natürlich erst recht irreduzibel in $K_0[Y]$. Also ist f_i für alle i das Minimalpolynom von y_i über K_0, und wegen $f_i'(y_i) \neq 0$ sind alle y_i separabel algebraisch über K_0. Dann ist $K_1 := K_0(y_1, \ldots, y_r)$ endlich erzeugt und separabel über k, also $\mathrm{insep}_k^{K_1} = 0$. Andererseits ist $k \subseteq K^* \subseteq K_1$, also nach der Folgerung zu Satz 2.10 auch K^*/k separabel. q.e.d.

Kriterien für die Existenz einer separierenden Transzendenzbasis bei einer separablen Körpererweiterung findet man z.B. in [Dieu]. Wir zeigen noch an einem Beispiel, daß im allgemeinen aus „separabel" nicht „separabel erzeugt" folgt:

Beispiel 2.41 (Separabel, aber nicht separabel erzeugt) *Sei k ein Körper der Charakteristik $p > 0$, x eine Unbestimmte. Bilde den Oberkörper*
$K := k(x, x^{\frac{1}{p}}, x^{\frac{1}{p^2}}, \ldots, x^{\frac{1}{p^n}}, \ldots)$
Dann ist K/k separabel, aber nicht separabel erzeugt.

Beweis: *K/k ist separabel:* Sei $k \subseteq K^* \subseteq K$ und K^*/k endlich erzeugt. Dann gibt es eine natürliche Zahl m, so daß die endlich vielen Erzeugenden von K^*/k in $k(x, x^{\frac{1}{p}}, x^{\frac{1}{p^2}}, \ldots, x^{\frac{1}{p^m}}) = k(x^{\frac{1}{p^m}}) =: K_m$ liegen, also auch $K^* \subseteq K_m$. Es ist

aber K_m/k separabel nach Satz 2.2 als einfache transzendente Erweiterung von k. Also ist nach der Folgerung zu Satz 2.10 auch K^*/k separabel und daher K/k separabel.
K/k ist nicht separabel erzeugt: Angenommen es gäbe eine separierende Transzendenzbasis von K/k, so bestünde sie aus einem einzigen Element $y \in K$; denn $\{x\}$ ist offenbar eine maximale über k algebraisch unabhängige Teilmenge von K, also $\dim \frac{K}{k} = 1$. Dann gäbe es eine natürliche Zahl m mit $y \in K_m := k(x^{\frac{1}{p^m}})$. Also wäre $k \subseteq k(y) \subseteq K_m \subset K$ und $K/k(y)$ separabel algebraisch. Dann wäre aber auch K/K_m separabel algebraisch, was falsch ist, da z.B. $x^{\frac{1}{p^{m+1}}}$ inseparabel algebraisch über K_m ist. q.e.d.

Tensorielle Ausdehnung und Separabilität

Endlich erzeugte Körpererweiterungen K/k sind nach Satz 2.10 genau dann separabel, wenn $\mathrm{insep}\frac{K}{k} = 0$ ist. Mittels der tensoriellen Ausdehnung kann man auch nicht notwendig endlich erzeugte separable Körpererweiterungen charakterisieren:

Satz 2.42 *Sei*
K/k eine Körpererweiterung,
$\mathrm{D} : k \to \Omega(k)$ *die absolute universelle Derivation von k,*
(d, π) *die universelle Ausdehnung von* D *auf K.*
Es gilt:
K/k separabel $\iff$ (d, π) *ist tensorielle Ausdehnung von* D.

Beweis:
Vorbemerkung: Nach Satz 1.21 ist zunächst D die universelle Ausdehnung der trivialen Derivation des Primkörpers von k, also ist nach Satz 1.19 $\Omega(k) = k\,\mathrm{D}k$. Daß (d, π) tensorielle Ausdehnung von D ist, bedeutet nach Anmerkung 1.25: $K \otimes_k k\,\mathrm{D}k \cong K\,\mathrm{d}k$ vermöge der kanonischen Abbildung
$\psi : K \otimes_k k\,\mathrm{D}k \to K \cdot \pi(k\,\mathrm{D}\,k) = K\,\mathrm{d}k$ mit $y \otimes \mathrm{D}x \mapsto y \cdot \pi(\mathrm{D}x) = y \cdot \mathrm{d}x$ für alle $y \in K$ und $x \in k$. Da $k\,\mathrm{D}k$ ein k-Vektorraum ist, der von $\mathrm{D}k$ erzeugt wird, besitzt $k\,\mathrm{D}k$ eine k-Basis der Form $\{\mathrm{D}x_\iota\}$. Das System $\{1 \otimes \mathrm{D}x_\iota\}$ ist dann eine K-Basis von $K \otimes_k k\,\mathrm{D}k$, die unter ψ auf das System $\{\mathrm{d}x_\iota\}$ abgebildet wird. Offenbar erzeugen diese Elemente den K-Vektorraum $K\,\mathrm{d}k$. Daß ψ den oben genannten Isomorphismus induziert, bedeutet dann, daß das System $\{\mathrm{d}x_\iota\}$ sogar eine K-Basis von $K\,\mathrm{d}\,k$ ist, d.h., daß die $\mathrm{d}x_\iota$ linear unabhängig über K sind. Dabei kommt es jeweils nur auf endlich viele der x_ι an.

Wir behandeln zuerst den *Fall der Charakteristik $p > 0$:*

$\underline{\Rightarrow:}$ Sei K/k separabel und seien $x_1, \ldots, x_m \in k$, so daß die $\mathrm{D}x_1, \ldots, \mathrm{D}x_m$ linear unabhängig über k (also Teil einer k-Basis) sind. Wir zeigen, daß dann $\mathrm{d}x_1, \ldots, \mathrm{d}x_m$ linear unabhängig über K sind. (Nach der Vorbemerkung folgt daraus, daß (d, π) tensorielle Ausdehnung von D ist.)

Wegen Korollar 2.28 ist $\{x_1, \ldots, x_m\}$ p-unabhängig in k/k^p, d.h.
$\{x_1^{\nu_1} \cdots x_m^{\nu_m} \mid 0 \leq \nu_i \leq p-1,\ i = 1, \ldots m\}$ ist linear unabhängig über $k^p(k^p) = k^p$:
Da aber K/k als separabel vorausgesetzt ist, folgt aus Satz 2.37, daß k und K^p linear disjunkt über k^p sind. Also sind diese Elemente auch linear unabhängig über $K^p = k^p(K^p)$, d.h. $\{x_1, \ldots, x_m\}$ ist p-unabhängig in K/k^p.
Aber $\Omega(K) = \Omega(K/k^p)$.
Wiederum nach Korollar 2.28 folgt dann, daß
$\{\mathrm{d}x_1, \ldots, \mathrm{d}x_m\}$ linear unabhängig über K ist.
$\underline{\Leftarrow}$: Sei $\{x_\iota\}$ eine p-Basis von k/k^p, d.h
$\{x_{\iota_1}^{\nu_1} \cdots x_{\iota_n}^{\nu_n} \mid 0 \leq \nu_i \leq p-1,\ i = 1, \ldots, n;\quad n \in \mathbb{N}\}$ ist eine Basis von k als k^p-Vektorraum.
Wir zeigen, daß diese Elemente auch linear unabhängig über K^p sind.
($\Rightarrow$ k und K^p sind linear disjunkt über k^p. Aus Satz 2.37 folgt dann, daß K/k separabel ist.)
Nach Korollar 2.28 folgt zunächst, daß $\{\mathrm{D}x_\iota\}$ linear unabhängig über k sind. Da nach Voraussetzung d tensorielle Ausdehnung von D ist, folgt nach der Vorbemerkung, daß auch $\{\mathrm{d}x_\iota\}$ linear unabhängig über K ist. Wiederum nach Korollar 2.28 bedeutet das, daß $\{x_\iota\}$ p-unabhängig in K/k^p sind, d.h. daß
$\{x_{\iota_1}^{\nu_1} \cdots x_{\iota_n}^{\nu_n} \mid 0 \leq \nu_i \leq p-1,\ i = 1, \ldots, n;\quad n \in \mathbb{N}\}$ linear unabhängig über $k^p(K^p) = K^p$ ist. q.e.d.
Fall der Charakteristik Null: Da in diesem Fall jede Körpererweiterung separabel ist, bleibt nur die Richtung „$\Rightarrow$“ zu zeigen:
Seien $x_1, \ldots, x_m \in k$, so daß die $\mathrm{D}x_1, \ldots, \mathrm{D}x_m$ linear unabhängig über k sind. Wir zeigen, daß dann $\mathrm{d}x_1, \ldots, \mathrm{d}x_m$ linear unabhängig über K sind. (Nach der Vorbemerkung folgt daraus, daß (d, π) tensorielle Ausdehnung von D ist.)
Sei k_0 der Primkörper von k. Nach Korollar 2.13 ist dann $\{x_1, \ldots, x_m\}$ algebraisch unabhängig über k_0. Ebenfalls nach Korollar 2.13 folgt daraus dann, daß auch $\{\mathrm{d}x_1, \ldots, \mathrm{d}x_m\}$ linear unabhängig über K ist. q.e.d.
Als wesentlicher Teil des Beweises von Satz 2.42 wurde gezeigt:

Korollar 2.43 *Mit den Bezeichnungen von Satz 2.42 gilt:*
K/k separabel $\Longleftrightarrow$
Für jedes endliche System $\{x_1, \ldots, x_m\}$ von Elementen von k, für das $\{\mathrm{D}x_1, \ldots, \mathrm{D}x_m\}$ linear unabhängig über k ist, ist auch $\{\mathrm{d}x_1, \ldots, \mathrm{d}x_m\}$ linear unabhängig über K.

Anmerkung 2.44 *Im Fall der Charakteristik Null kann man statt der absoluten universellen Derivation von k die universelle Derivation über einem beliebigen Unterkörper k_0 von k nehmen.* (Das geht unmittelbar aus dem Beweis hervor.)

Satz 2.45 *Genauere Aussagen erhält man im Falle einer endlich erzeugten Körpererweiterung K/k durch die Ungleichung von Cartier:*

1. *Sei* $\mathrm{char}\,(K) = p > 0$ *und* $\delta : k \to k\delta k$ *eine Derivation von* k*. Dann gilt:*

$$\dim_K \mathrm{T}(K/\delta) \leq \mathrm{insep}\frac{K}{k}.$$

2. *Falls* $\delta = \mathrm{D}$ *die absolute Derivation von* k *ist, gilt in 1. das Gleichheitszeichen.*

Zum Beweis der Ungleichung siehe [Ku], Theorem 5.12. Wir beweisen hier nur die Gleichung 2. im Fall der absoluten Derivation. Dazu brauchen wir als Vorbereitung:

Hilfssatz 2.46 *Sei* K/k *eine endlich erzeugte Körpererweiterung,* $\dim \frac{K}{k} = r$ *und* $\{\alpha_\iota | \iota \in I\}$ *eine* p*-Basis von* k/k^p*. Dann existiert eine* p*-Basis von* K/K^p *folgender Art:*
Sie entsteht aus $\{\alpha_\iota | \iota \in I\}$ *durch Austausch von endlich vielen Elementen und Hinzufügen von weiteren* r *über* k *algebraisch unabhängigen Elementen aus* K*.*

Beweis: Es genügt offenbar, den Fall einer einfachen Erweiterung $K = k(x)$ zu betrachten.
1) x *transzendent über* k*:* In diesem Fall ist $\{\alpha_\iota | \iota \in I\} \cup \{x\}$ eine p-Basis von K/K^p.

$$\begin{array}{c} K = k(x) \\ | \\ k(x^p) \\ | \\ K^p = k^p(x^p) \end{array}$$

Beweis: Es ist K/k separabel, also k und $K^p = k^p(x^p)$ linear disjunkt über k^p. Eine Linearbasis von k/k^p ist also auch linear unabhängig über K^p. Daher ist $\{\alpha_\iota | \iota \in I\}$ auch eine p-Basis von $k(x^p)/K^p$. Ferner ist $\{1, x, \ldots, x^{p-1}\}$ eine Linearbasis von $K/k(x^p)$.
Also ist $\{\alpha_{\iota_1}^{\nu_1} \cdots \alpha_{\iota_s}^{\nu_s} \cdot x^\nu | s \in \mathbb{N}_0, 0 \leq \nu_j, \nu \leq p-1\}$ eine Linearbasis von K/K^p, d.h. $\{\alpha_\iota | \iota \in I\} \cup \{x\}$ ist eine p-Basis von K/K^p. q.e.d.

2) x *separabel algebraisch über* k*:* In diesem Falle ist $\{\alpha_\iota | \iota \in I\}$ auch eine p-Basis von K/K^p.
Beweis: Nach Hilfssatz 2.34 ist zunächst $K = k(x^p) = K^p(k) = K^p(\{\alpha_\iota | \iota \in I\})$. Ferner sind wegen der Separabilität K^p und k linear disjunkt über k^p, also sind die $\{\alpha_{\iota_1}^{\nu_1} \cdots \alpha_{\iota_s}^{\nu_s} | s \in \mathbb{N}_0, 0 \leq \nu_j \leq p-1\}$ auch linear unabhängig über K^p. Daher ist $\{\alpha_\iota | \iota \in I\}$ auch eine p-Basis von K/K^p. q.e.d.

3) x *inseparabel algebraisch über* k*:* Indem man zunächst den maximalen separablen Zwischenkörper nach 2) behandelt, kann man o.B.d.A. annehmen, daß K/k rein inseparabel algebraisch ist, also x ein Minimalpolynom der Form $X^{p^e} - x^{p^e} \in k[X]$ hat. Dann kann man eine Körperkette zwischen k und K von e Zwischenkörpern legen, von denen jeder rein inseparabel vom Grad p über dem vorhergehenden ist. Also kann man o.B.d.A. annehmen, daß $x \notin k$ aber $x^p \in k$ gilt.
Wegen $x \notin k$ ist $x^p \notin k^p$, also p-unabhängig in k/k^p, also kann man nach Steinitz eines der α_ι, etwa α_{ι_0} gegen x^p austauschen, und $\{\alpha_\iota | \iota \in I'\} \cup \{x^p\}$ mit $I' := I \setminus \{\iota_0\}$ ist immer noch eine p-Basis von k/k^p.

Insbesondere ist dann $\{\alpha_\iota|\iota \in I'\}$ auch p-unabhängig in K/K^p; denn $K^p = k^p[x^p]$, und wären die $\{\alpha_\iota|\iota \in I'\}$ p-abhängig in K/K^p, dann wäre für ein $\iota_1 \in I'$ $\alpha_{\iota_1} \in k^p[x^p, \{\alpha_\iota|\iota \in I' \setminus \iota_1\}]$, was der p-Unabhängigkeit von $\{\alpha_\iota|\iota \in I'\} \cup \{x^p\}$ in k/k^p widerspräche.
Nun ist $K = k(x)$ mit $x^p \in k$. $\Rightarrow K = \underbrace{k^p(\{\alpha_\iota|\iota \in I'\}, x^p)}_{=k}[x] = \underbrace{K^p(\{\alpha_\iota|\iota \in I'\})}_{=k}[x]$
und $\{\alpha_\iota|\iota \in I'\} \cup \{x\}$ ist auch p-unabhängig in K/K^p; denn andernfalls wäre schon eine endliche Teilmenge p-abhängig in K/K^p. Diese müßte x enthalten, weil die $\{\alpha_\iota|\iota \in I'\}$, wie oben gezeigt, p-unabhängig in K/K^p sind. Da diese Familie erst durch Hinzunahme von x abhängig würde, folgte aus den allgemeinen Eigenschaften von Abhängigkeiten, daß x von $\{\alpha_\iota|\iota \in I'\}$ in K/K^p p-abhängig wäre, d.h. $x \in K^p[\{\alpha_\iota|\iota \in I'\}] = k$ im Widerspruch zu der Voraussetzung $x \notin k$. Also ist $\{\alpha_\iota|\iota \in I'\} \cup \{x\}$ eine p-Basis von K/K^p, und diese ist durch Austauschen eines Elementes aus der p-Basis $\{\alpha_\iota|\iota \in I\}$ von k/k^p entstanden. q.e.d.

Beweis von Satz 2.45 , 2. : Sei K/k eine endlich erzeugte Körpererweiterung, $r := \dim \frac{K}{k}$ und $\{\alpha_\iota|\iota \in I\}$ eine p-Basis von k/k^p. Nach Hilfssatz 2.46 gibt es eine endliche Teilmenge $\{\iota_1, \ldots, \iota_s\} \subseteq I$ und $s+r$ Elemente $\beta_1, \ldots, \beta_{s+r} \in K$, so daß $\{\alpha_\iota|\iota \in I'\} \cup \{\beta_1, \ldots, \beta_{s+r}\}$ mit $I' := I \setminus \{\iota_1, \ldots, \iota_s\}$ eine p-Basis von K/K^p bildet.
Man hat also eine Darstellung $k = k^p[\{Z_\iota|\iota \in I\}]/(\{Z_\iota^p - \alpha_\iota^p|\iota \in I\})$. Mit Satz 1.29 folgt daraus
$\Omega(k) = \Omega(k/k^p) = \bigoplus\limits_{\iota \in I'} k \cdot \mathrm{D}\,\alpha_\iota \oplus \bigoplus\limits_{i=1}^{s} k \cdot \mathrm{D}\,\alpha_{\iota_i}$ mit $\mathrm{D} = \mathrm{d}_k$
und daraus
$K \otimes_k \Omega(k) = \bigoplus\limits_{\iota \in I'} K \cdot (1 \otimes \mathrm{D}\,\alpha_\iota) \oplus \bigoplus\limits_{i=1}^{s} K \cdot (1 \otimes \mathrm{D}\,\alpha_{\iota_i})$
Analog:
$\Omega(K) = \Omega(K/K^p) = \bigoplus\limits_{\iota \in I'} K \cdot \mathrm{d}\,\alpha_\iota \oplus \bigoplus\limits_{j=1}^{s+r} K \cdot \mathrm{d}\,\beta_j$ mit $\mathrm{d} := \mathrm{d}_K$.
In der exakten Folge von Korollar 1.32

$$0 \to \mathrm{T}(K/\mathrm{D}) \to K \otimes_k \Omega(k) \to \Omega(K) \to \Omega(K/k) \to 0$$

hat man eine exakte „Unterfolge“

$$0 \to 0 \to \bigoplus_{\iota \in I'} K \cdot (1 \otimes \mathrm{D}\,\alpha_\iota) \to \bigoplus_{\iota \in I'} K \cdot \mathrm{d}\,\alpha_\iota \to 0 \to 0\,,$$

da die K-linear unabhängigen Elemente $\{1 \otimes \mathrm{D}\,\alpha_\iota|\iota \in I'\}$ für alle $\iota \in I'$ jeweils auf die K-linear unabhängigen Elemente $\{\mathrm{d}\,\alpha_\iota|\iota \in I'\}$ abgebildet werden. Faktorisiert man diese Folge aus, so erhält man eine exakte Folge

$$0 \to \mathrm{T}(K/\mathrm{D}) \to \bigoplus_{i=1}^{s} K \cdot (1 \otimes \mathrm{D}\,\alpha_{\iota_i}) \to \bigoplus_{j=1}^{s+r} K \cdot \mathrm{d}\,\beta_j \to \Omega(K/k) \to 0$$

Für die Dimensionen der K-Vektorräume bedeutet das:

$$\begin{aligned}\dim_K \mathrm{T}(K/\mathrm{D}) &= \dim_K \bigoplus_{i=1}^{s} K \cdot (1 \otimes \mathrm{D}\,\alpha_{\iota_i}) - \dim_K \bigoplus_{j=1}^{s+r} K \cdot \mathrm{d}\,\beta_j + \dim_K \Omega(K/k) \\ &= s - (s+r) + p\text{-grad}\tfrac{K}{k} \\ &= p\text{-grad}\tfrac{K}{k} - \dim \tfrac{K}{k} \\ &= \mathrm{insep}\tfrac{K}{k} \qquad \text{q.e.d.}\end{aligned}$$

Anmerkung 2.47 *Aus der tensoriellen Ausdehnbarkeit von* D *auf* K *folgt nach Anmerkung 1.25 insbesondere, daß* D *auf* K *fortsetzbar ist. Die Fortsetzbarkeit allein reicht aber nicht für Separabilität, sie muß tensoriell sein, wie das folgende Beispiel zeigt:*

Beispiel 2.48 (Fortsetzung, aber nicht tensorielle Ausdehnung) *Sei* $p \neq 2$ *eine Primzahl,* k_0 *der Primkörper der Charakteristik* p *und* $k = k_0(x,y)$ *der Quotientenkörper des Polynomrings in* x *und* y *über* k_0.
Ferner sei $f(Z) := Z^{2p} + x \cdot Z^p + y \in k[Z]$,
z *eine Nullstelle von* f *in einem Oberkörper von* k *und* $K = k(z)$.
Es bezeichne D *die (absolute) universelle Derivation von* k *und*
d *die universelle Ausdehnung von* D *auf* K.
(Dann ist d die absolute universelle Derivation von K).
Wir zeigen:
d *ist Fortsetzung, aber nicht tensorielle Fortsetzung von* D *auf* K.

Beweis: 1) d ist nicht tensorielle Ausdehnung von D:
Da k_0 Primkörper ist und x, y algebraisch unabhängig über k_0 sind, hat der absolute universelle Differentialmodul $\Omega(k)$ von k nach Satz 1.29 eine Basis, bestehend aus $\mathrm{D}x$ und $\mathrm{D}y$:
$\Omega(k) = k \cdot \mathrm{D}x \oplus k \cdot \mathrm{D}y$
Daher ist
$K \otimes_k \Omega(k) = K \cdot (1 \otimes \mathrm{D}x) \oplus K \cdot (1 \otimes \mathrm{D}y)$
und $1 \otimes \mathrm{D}x$, $1 \otimes \mathrm{D}y$ bilden eine K-Basis von $K \otimes_k \Omega(k)$.
$\psi : K \otimes_k \Omega(k) \to \Omega(K)$ bezeichne die kanonische K-lineare Abbildung mit
$1 \otimes \mathrm{D}w \mapsto \mathrm{d}w$ für alle $w \in k$. Es ist zu zeigen, daß ψ nicht injektiv ist:
Das ist klar:
In $K \otimes_k \Omega(k)$ ist $\theta := z^p \cdot (1 \otimes \mathrm{D}x) + (1 \otimes \mathrm{D}y) \neq 0$, weil $1 \otimes \mathrm{D}x$ und $1 \otimes \mathrm{D}y$ Basiselemente sind, aber
$\psi(\theta) = z^p \cdot \mathrm{d}x + \mathrm{d}y = \mathrm{d}(f(z)) = 0$. q.e.d.

2) Aus 1) folgt nach Satz 2.42, daß K/k inseparabel ist.

3) $[K : k] = 2p$ und folglich ist f das Minimalpolynom von z über k:
Sei $g(U) := U^2 + x \cdot U + y \in k[U]$ und $u := z^p$. Dann ist $f(Z) = g(Z^p)$ und folglich $g(u) = 0$. Betrachte die Körperkette
$k \subseteq k(u) \subseteq K = k(u)(z)$

$g(U)$ ist irreduzibel über k; denn andernfalls hätte es eine Nullstelle $-\frac{1}{2}x + \sqrt{\frac{x^2}{4} - y}$ in k. Dann wäre $\frac{x^2}{4} - y$ ein Quadrat im Polynomring $k = k_0(x)[y]$. Das ist aber unmöglich, weil dies ein lineares Polynom in y und folglich prim ist.
Also ist $[k(u) : k] = 2$ und daher $2 \Big| [K : k]$.
Insbesondere ist dann $K \neq k$. Da andererseits K/k nach 2) inseparabel ist, gilt auch $p \Big| [K : k]$. Da aber p eine Primzahl $\neq 2$ ist, gilt insgesamt $2p \Big| [K : k]$ und daher $[K : k] = 2p$, weil f ein Polynom vom Grad $2p$ ist. q.e.d.

4) d ist Fortsetzung von D:
Sei $\pi : \Omega(k) \to \Omega(K)$ kanonisch. Es ist zu zeigen, daß π injektiv ist:
Da $f = Z^{2p} + x \cdot Z^p + y$ das Minimalpolynom von z über k ist, gilt nach dem Rezept Satz 1.29
$\Omega(K) = (K \otimes_k \Omega(k) \oplus K \cdot \Delta z) / K \cdot \underbrace{(z^p \cdot (1 \otimes \mathrm{D}x) + 1 \otimes \mathrm{D}y)}_{=\Delta f}$ mit einer Unbestimmten ΔZ, deren Restklasse mod $K \cdot \Delta f$ das dz ist.
Für jedes $\omega \in \Omega(k)$ ist dann $\pi(\omega) = 1 \otimes \omega + K \cdot \Delta f$. Sei nun $\omega := a \cdot Dx + b \cdot Dy$ mit $a, b \in k$ ein beliebiges Element von $\Omega(k)$. Nach der oben angegebenen Konstruktion sieht man, daß $\omega \in \mathrm{Ker}\,(\pi)$ genau dann, wenn $1 \otimes \omega \in K \cdot \Delta f$, d.h., wenn es ein $c \in K$ gibt, so daß $a \cdot (1 \otimes Dx) + b \cdot (1 \otimes Dy) = c \cdot (z^p \cdot (1 \otimes Dx) + 1 \otimes Dy)$. Da $1 \otimes Dx$ und $1 \otimes Dy$ Basiselemente von $K \otimes_k \Omega(K)$ sind, bedeutet das: $b = c$ und $a = c \cdot z^p$. Wäre $c \neq 0$, so folgte $z^p = a/b \in k$ und folglich $[K : k] \leq p$ im Widerspruch zu 3). Also ist $c = 0$, folglich $a = 0$ und $b = 0$ und damit auch $\omega = 0$. q.e.d.

Literaturverzeichnis

[Be1] Berger, R., Ausdehnung von Derivationen und Schachtelung der Differente, Math. Z. **78**, 97–115 (1962).

[Be2] Berger, R., Differentiale höherer Ordnung und Körpererweiterungen bei Primzahlcharakteristik, Sitz. Ber. Heidelberger Akad.Wiss., 3. Abh., 143–202 (1966).

[Dieu] Dieudonné, J., Sur les Extensions Transcendantes Séparables, Sum.Bras.Math **2**,1–20 (1947).

[Kä] Kähler, E., Algebra und Differentialrechnung, Bericht über die Mathematikertagung in Berlin 1953.

[Ku] Kunz, E., Kähler Differentials, Vieweg Advanced Lectures in Mathematics, 1986.

[ML] MacLane, S., Modular fields, I, Separating transcendence bases, Duke Math. J. **5**, 372–393 (1939).

[Wae1] van der Waerden, B.L., Algebra Erster Teil, Heidelberger Taschenbücher 12, Springer 1966.

Index

Differentialmodul
  universeller, 2

Ausdehnung, 5, 6
  tensorielle, 9
  universelle
    Faktorring, 11
    Polynomring, 10
    Quotientenring, 14
    Rezept, 12

Cartiers Ungleichung, 36

Derivation, 1
  Spezialisierung, 3
  triviale, 2
  universelle, 2
    Konstantenring, 15
    Konstruktion, 5
  universelle zweiseitige
    Konstruktion, 4
  zweiseitige, 4
Derivationenmodul, 2
Differentialmodul
  universeller
    Konstantenring, 15
    Konstruktion, 5

Erzeugendenzahl, 28

Fortsetzung, 5, 6, 9
  keine tensorielle Ausdehnung, 39

Hauptsatz, 28

Kähler, 2

linear disjunkt, 30

p-abhängig, 25
p-Basis, 25, 26
p-Grad, 25

Quotientenregel, 1

rein inseparabel, 24, 25

separabel, 20
  beliebige Erweiterung, 33
  Charakterisierungen, 32, 33
  tensorielle Ausdehnung, 35
separabel algebraisch, 20
separabel erzeugt, 21, 34
  Gegenbeispiel, 34

tensorielle Ausdehnung
  Separabilität, 35
Transzendenzbasis
  separierende, 20

vollkommener Körper, 23