Carl-von-Ossietzky-Universität Oldenburg
Studiengang Diplom-Mathematik
Diplomarbeit

Zyklotomische Funktionenkörper

vorgelegt von Roland Auer
am 19. März 1993.
Erstprüfer: Prof. Dr. H.-G. Quebbemann
Zweitprüferin: Prof. Dr. I. Pieper-Seier

Korrigierte und leicht berarbeitete Fassung vom 27. August 2007.

Inhaltsverzeichnis

Einleitung

Zyklotomische Funktionenkörper sind algebraische Funktionenkörper über $\mathbb{F}_q$ (dem endlichen Körper mit q Elementen), die in eigenartiger Analogie zu den klassischen Kreisteilungskörpern gebildet werden. Dabei übernimmt der rationale Funktionenkörper $\mathbb{F}_q(x)$ die Rolle des Körpers $\mathbb{Q}$ der rationalen Zahlen, während die Polynome über $\mathbb{F}_q$, die 'ganzen Funktionen' in $\mathbb{F}_q(x)$, an die Stelle der ganzen Zahlen treten. Hat man klassisch zu jeder (positiven) ganzen Zahl $m \neq 0$ einen m-ten Kreisteilungskörper, so assoziiert man nun zu jedem (normierten) Polynom $M \neq 0$ einen M-ten zyklotomischen Funktionenkörper.
Die Grundlage hierfür legte schon 1939 Leonard Carlitz mit seiner Untersuchung einer 'Klasse von Polynomen', die er mit $W_M(u)$ bezeichnete, und die die Analoga zu den klassischen Kreisteilungspolynomen darstellen. Bei ihm findet sich bereits die Rekursionsformel (in dieser Arbeit 8.6(c)), die er als definierende Gleichung für die $W_M(u)$ einführt, und das Zerlegungsgesetz 9.1, das er ganz elementar beweist.
Im Jahre 1974 greift Hayes die Idee von Carlitz auf und bestimmt in den Paragraphen 3 und 4 seines Artikels [Ha] die unendlichen Primdivisoren sowie das Geschlecht des M-ten zyklotomischen Funktionenkörpers, beides allerdings nur für den Fall, daß M die Potenz eines irreduziblen Polynoms ist.
Ein Ziel dieser Diplomarbeit ist es, Hayes' Untersuchungen auf beliebige Polynome M auszudehnen (Sätze 9.1, 9.3(a)–(b), 9.4 und 10.2(a)) und dabei parallel für einen Teilkörper, der klassisch dem maximalen reellen Teilkörper entspricht, durchzuführen (Sätze 9.3(c)–(d), 9.4(a), 10.2(b)–(c) und 10.4). In der Folge hiervon ist es uns möglich, im letzten Abschnitt eine Aussage über den Klassenzahlfaktor h^-, die Quebbemann [Qb] ebenfalls nur für Potenzen irreduzibler Polynome formuliert hat, für beliebiges M zu zeigen (Satz 11.4).
Dies sind die wesentlichen Inhalte des dritten Teils. Die ersten beiden Teile, d. h. die Abschnitte 1–6, sind als Vorbereitung hierzu zu sehen. In ihnen werden bekannte Tatsachen aus der Bewertungstheorie und der Theorie der algebraischen Funktionenkörper aufbereitet und zusammengestellt. Der/die mit diesen Themen vertraute LeserIn kann daher sofort bei Teil III beginnen. Wir wollen auch über die ersten beiden Teile einen kurzen Überblick geben. Detailliertere Einleitungen finden sich zu Beginn der einzelnen Abschnitte.
In Teil I befassen wir uns mit (diskreten) Bewertungen beliebiger Körper und ihrem Zusammenhang mit Dedekindringen (Abschnitt 1). Wir studieren das Wechselspiel zwischen Galoisgruppe und Bewertungen in einer endlichen Galoiserweiterung (Abschnitt 2) sowie besondere Eigenschaften vollständiger bewerteter Körper (Abschnitt 3).
Abschnitt 4 macht uns mit algebraischen Funktionenkörpern und Begriffen wie Divisor, Differential, Adle und Geschlecht vertraut. Abschnitt 5 beschäftigt sich mit dem Geschlecht in einer separablen Erweiterung von algebraischen Funktionenkörpern. Mit Abschnitt 6, der die Theorie algebraischer Funktionenkörper über endlichem Konstantenkörper entwickelt, nähern wir uns dann den in Teil III untersuchten zyklotomischen Funktionenkörpern.
Vorausgesetzt werden in dieser Arbeit algebraische Kenntnisse bis einschließlich Galoistheorie, wie sie zumeist im Grundstudium vermittelt werden.

An dieser Stelle möchte ich mich bei Herrn Prof. Quebbemann für die Vergabe des Themas, das meinen persönlichen Vorlieben sehr entgegenkam, sowie für die hervorragende und unermüdliche Betreuung recht herzlich bedanken. Durch seine wertvollen Gedankenanstöße und ständig neuen Fragestellungen hat er meine Arbeit wesentlich vorangetrieben.

Notation

Ringe sind in dieser Arbeit stets kommutativ mit 1. Es bezeichnen a, b Elemente und I, J Ideale eines Rings R. Wir verwenden die folgenden Schreibweisen.

R^*	Einheitengruppe von R.
$Ra, aR, (a)$	von a erzeugtes Ideal in R.
$a\|b$	a teilt b in R.
IJ	Produktideal aus I und J.
$I\|J$	I teilt J, d. h. es gibt ein Ideal I' von R mit $II' = J$.
SI, IS	von I erzeugtes Ideal im Oberring S von R.
$\mathrm{Max}(R)$	Menge der maximalen Ideale von R.
$R^{m\times n}$	R-Algebra der $m \times n$-Matrizen über R.
$\mathrm{ann}_R(M)$	Annihilatorideal des R-Moduls M
$\mathrm{ann}_R(x)$	bzw. des Elements $x \in M$.
$\mathrm{Aut}(L/K)$	Automorphismengruppe der Körpererweiterug L/K.
$\mathrm{Fix}(L, G)$	Fixkörper der Untergruppe $G < \mathrm{Aut}(L)$ im Körper L.
$\mathrm{char}(K)$	Charakteristik des Körpers K.
K_1K_2	Kompositum der Körper K_1 und K_2 in einem gemeinsamen Oberkörper L, d. h. der kleinste Unterkörper von L der sowohl K_1 als auch K_2 enthlt.
$\mathrm{Hom}_K(V, W)$	Algebra der K-Vektorraumhomomorphismen von V nach W.
$\mathrm{End}_K(V)$	$= \mathrm{Hom}_K(V, V)$.
$\#A$	Anzahl der Elemente der Menge A.
$B \setminus A$	Differenzmenge der Mengen B und A (B ohne A).
B^A	Menge aller Abbildungen aus der Menge A in die Menge B.
$f\|_A$	Restriktion der Abbildung f auf die Menge A.
δ_{ij}	Kronecker-Symbol.

Teil I
Bewertete Körper

1 Dedekindringe und Bewertungen

Dieser Abschnitt soll die wesentlichen Grundbegriffe der Bewertungstheorie — Ganzheit, Diskriminante, Dedekindringe, Fortsetzung von Bewertungen — in der für diese Arbeit benötigten Form bereitstellen. Die gesamte Theorie, wie sie z. B. bei [Jc] dargestellt ist, ist um einiges allgemeiner angelegt und würde mit ihrer ganzen Herleitung zu viel Raum einnehmen. Wir beschränken uns daher auf die wesentlichen Aussagen und beziehen uns, wo es möglich ist, auf die entsprechende Literatur.

Die Aussagen 1.1 bis 1.4 sowie 1.5(c) und (d) finden sich bei [Nk, pp. 6–13] wieder. Für den Beweis zu 1.5(a) und (b) verweisen wir auf [L2, p. 65].

a. Ganzheit. Das Konzept algebraischer Größen über einem Körper läßt sich auf Ringe wie folgt übertragen.

1.1 Definition und Satz. *Sei C/A eine Ringerweiterung. Ein Element $\beta \in C$ heißt* **ganz über** *A, falls β Nullstelle eines normierten Polynoms $f \in A[X]$ ist. Die Menge $B := \{\beta \in C : \beta \text{ ist ganz über } A\}$ heißt* **der ganze Abschluß von** *A* **in** *C. Falls $A = B$ ist, heißt A* **ganz abgeschlossen in** *C. B ist ein Ring und ganz abgeschlossen in C. Ein Integritätsring heißt* **ganz abgeschlossen**, *wenn er ganz abgeschlossen in seinem Quotientenkörper ist.*

Beispiel. *Jeder faktorielle Ring ist ganz abgeschlossen.*

1.2 Satz. *Sei A ein ganz abgeschlossener Integritätsring mit Quotientenkörper K, L/K eine endliche Körpererweiterung und B der ganze Abschluß von A in L.*

(a) *Jedes $\alpha \in L$ läßt sich in der Form $\alpha = \frac{\beta}{a}$ mit $\beta \in B$ und $a \in A$ schreiben. Insbesondere ist L Quotientenkörper von B und B ganz abgeschlossen.*

(b) *Für $\beta \in B$ ist das Minimalpolynom von β über K in $A[X]$.*

(c) *Für $\sigma \in \mathrm{Aut}(L/K)$ ist $\sigma(B) = B$.*

b. Diskriminante. Wesentliche Bedingung für die meisten Definitionen und Aussagen ist die Separabilität der betrachteten Körpererweiterung. So auch bei den im folgenden eingeführten Begriffen.

1.3 Definition und Satz. *Sei L/K eine separable Körpererweiterung vom Grad n. Die K-Homomorphismen von L in einen gegebenen algebraischen Abschluß seien mit $\sigma_1, \ldots, \sigma_n$ bezeichnet. Sei weiter $(\beta_1, \ldots, \beta_n)$ eine K-Basis von L, $\alpha \in L$ beliebig und β ein primitives Element von L über K. Wir führen die folgenden Bezeichnungen ein:*

(a) *$S_{L/K}(\alpha) := \sum_{i=1}^{n} \sigma_i(\alpha) \in K$ heißt* **Spur von** *α* **in** *L/K.*

(b) *$N_{L/K}(\alpha) := \prod_{i=1}^{n} \sigma_i(\alpha) \in K$ heißt* **Norm von** *α* **in** *L/K.*

(c) $D_{L/K}(\beta_1,\dots,\beta_n) := \det^2(\sigma_i(\beta_j))_{1\le i,j\le n} = \det(S_{L/K}(\beta_i\beta_j))_{1\le i,j\le n} \in K^*$ *heißt* **Diskriminante von** $(\beta_1,\dots,\beta_n)$ **in** L/K.
(d) $D_{L/K}(\beta) := D_{L/K}(1,\beta,\dots,\beta^{n-1})$ *heißt* **Diskriminante von** β **in** L/K.

1.4 Rechenregeln. *Sei L/K eine separable Körpererweiterung vom Grad n, F ein Zwischenkörper, $\alpha,\beta \in L$ und $a \in K$. Desweiteren sei A ein Unterring von K, ganz abgeschlossen in K.*

(a) $S_{L/K}(a) = na$ *und* $N_{L/K}(a) = a^n$.
(b) $S_{L/K}(\beta) = S_{F/K}(S_{L/F}(\beta))$ *und* $N_{L/K}(\beta) = N_{F/K}(N_{L/F}(\beta))$.
(c) *Die Spur ist K-linear, d. h.* $S_{L/K}(\alpha+\beta) = S_{L/K}(\alpha) + S_{L/K}(\beta)$ *und* $S_{L/K}(a\beta) = aS_{L/K}(\beta)$.
(d) *Die Norm ist multiplikativ, d. h.* $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$.
(e) *Ist β ganz über A, so ist* $S_{L/K}(\beta), N_{L/K}(\beta) \in A$.

1.5 Satz. *Sei A ein ganz abgeschlossener Integritätsring mit Quotientenkörper K, L/K eine separable Körpererweiterung vom Grad n und B der ganze Abschluß von A in L. Seien weiter $(\beta_1,\dots,\beta_n)$ und $(\beta'_1,\dots,\beta'_n)$ zwei K-Basen von L mit $M := A\beta_1 \oplus \cdots \oplus A\beta_n \subseteq M' := A\beta'_1 \oplus \cdots \oplus A\beta'_n$.*

(a) $D_{L/K}(\beta_1,\dots,\beta_n) = aD_{L/K}(\beta'_1,\dots,\beta'_n)$ *für ein $a \in A$.*
(b) $M = M'$ *genau dann, wenn* $D_{L/K}(\beta_1,\dots,\beta_n) = \varepsilon D_{L/K}(\beta'_1,\dots,\beta'_n)$ *für ein $\varepsilon \in A^*$.*
(c) *Sind $\beta_1,\dots,\beta_n \in B$, so ist $d := D_{L/K}(\beta_1,\dots,\beta_n) \in A$ und $M \subseteq B \subseteq \frac{1}{d}M$.*
(d) *Ist A ein Hauptidealring, dann gibt es eine K-Basis $(\gamma_1,\dots,\gamma_n)$ von L mit $B = A\gamma_1 \oplus \cdots \oplus A\gamma_n$.*

c. Dedekindringe. Dedekindringe werden in [Nk, pp. 19–24, 47–52] behandelt. Dort sind die Sätze 1.7 bis 1.10 bewiesen.

1.6 Definition. *Ein Integritätsring A heißt* **Dedekindring**, *wenn gilt:*

(a) *A ist noethersch,*
(b) *A ist ganz abgeschlossen und*
(c) *jedes Primideal $\neq 0$ von A ist ein maximales Ideal.*

Beispiel. *Jeder Hauptidealring ist ein Dedekindring.*

1.7 Satz. *Sei A ein Dedekindring mit Quotientenkörper K, L/K endlich und separabel. Dann ist der ganze Abschluß von A in L ein Dedekindring.*

Die wichtigen Eigenschaften eines Dedekindrings beziehen sich auf seine Ideale.

1.8 Satz. *Sei A ein Dedekindring.*

(a) *Jedes Ideal $I \neq 0$ von A hat eine eindeutige Darstellung*

$$I = \prod_{P \in \operatorname{Max}(A)} P^{e_P}$$

mit $e_P \in \mathbb{N}_0$, $e_P = 0$ für fast alle $P \in \operatorname{Max}(A)$.

(b) *Die Ideale von A lassen sich invertieren, d. h. zu jedem Ideal I von A existiert ein Ideal $I' \neq 0$, so daß II' ein Hauptideal ist.*

(c) *Sind $I, J \subseteq A$ Ideale von A, so gilt ('Enthalten heißt Teilen')*

$$I \supseteq J \iff I|J.$$

1.9 Definition. *Für Ideale $I_1, I_2 \neq 0$ eines Integritätsrings A erklären wir die Äquivalenzrelation*

$$I_1 \sim I_2 \ :\Longleftrightarrow\ \exists \alpha_1, \alpha_2 \in A \setminus \{0\} : \alpha_1 I_1 = \alpha_2 I_2$$

und bezeichnen die Äquivalenzklasse eines Ideals $I \neq 0$ mit $[I]$. Wegen der Nullteilerfreiheit von A ist die Multiplikation von Äquivalenzklassen durch $[I][J] := [IJ]$ wohldefiniert und macht die Menge $\{[I] : I \neq 0$ Ideal von $A\}$ zu einem Monoid (mit der Klasse $[A]$ der Hauptideale als Einselement).

Aus 1.8(b) ergibt sich als unmittelbare Folgerung:

1.10 Satz und Definition. *Sei A ein Dedekindring.*

(a) *$\mathcal{C}\ell(A) := \{[I] : I \neq 0$ Ideal von $A\}$ ist eine Gruppe, die* **(Ideal)klassengruppe von** *A.*

(b) *Ihre Ordnung $h(A) := \#\mathcal{C}\ell(A)$ heißt die* **(Ideal)klassenzahl von** *A.*

d. Bewertungen.

1.11 Definition. *Unter einer* **diskreten Bewertung** *eines Körpers K verstehen wir eine surjektive Abbildung $v : K \to \mathbb{Z} \cup \{\infty\}$ mit den Eigenschaften*

(a) $v(a) = \infty \iff a = 0$,

(b) $v(ab) = v(a) + v(b)$, *(d. h. $v|_{K^*}$ ist ein Gruppenhomomorphismus) und*

(c) $v(a+b) \geq \min\{v(a), v(b)\}$,

wobei $a, b \in K$. Dabei gelten für ∞ die üblichen Rechenregeln.

Wie wir in 1.16 sehen werden, erhält man jede diskrete Bewertung in der Form des folgenden Beispiels, wenn man den Ring A geeignet wählt.

1.12 Beispiele.

(a) *Sei A ein faktorieller Ring mit Quotientenkörper K und $p \in A$ ein Primelement. Jedes $a \in K^*$ hat eine Darstellung $a = p^l \frac{r}{s}$ mit $r, s \in A$, $p \nmid rs$ und eindeutig bestimmtem $l \in \mathbb{Z}$. Durch $v_p(a) := l$ (und $v_p(0) := \infty$) wird eine diskrete Bewertung von K definiert. Man nennt v_p die* **p-adische Bewertung von** *K.*

(b) *Sei A ein Dedekindring mit Quotientenkörper K und $P \in \mathrm{Max}(A)$. Jedes $a \in K^*$ hat eine Darstellung $a = \frac{r}{s}$ mit $r, s \in A$. Gemäß 1.8(a) schreiben wir $rA = P^d I$ und $sA = P^e J$ mit Idealen I, J von A, $P \nmid IJ$ und $d, e \in \mathbb{N}_0$. Die Definition $v_P(a) := d - e$ ist von der Wahl von r und s unabhängig und liefert eine diskrete Bewertung von K. Man nennt v_P die* **P-adische Bewertung von** *K.*

(c) *Ein faktorieller Dedekindring ist ein Hauptidealring. Hier fallen die Bezeichnungen zusammen, d. h. für $(p) = P$ ist $v_p = v_P$.*

BEWEIS. **(a)** Die bei [Nk, p. 111f] für $\mathbb{Z}$ durchgeführten Überlegungen lassen sich wie bei [FJ, p. 14] auf einen beliebigen faktoriellen Ring übertragen.
(b) Vgl. [Nk, pp. 71-73].
(c) Aufgrund einfacher Überlegungen mithilfe von 1.8 und den Eigenschaften faktorieller Ringe.

□

Zu 1.13–1.19 vgl. [FJ, pp. 12–14] und [Nk, pp. 70f, 122–127].

1.13 RECHENREGELN. *Sei v eine diskrete Bewertung des Körpers K und $a, b \in K$.*
(a) $v(1) = 0$.
(b) $v(a) = v(-a)$.
(c) *Ist $v(a) \neq v(b)$, so ist $v(a+b) = \min\{v(a), v(b)\}$.*

1.14 DEFINITION UND SATZ. *Ein Ring $R \neq 0$ mit nur einem maximalen Ideal heißt* **lokal**. *Das maximale Ideal eines lokalen Rings R ist $P = R \setminus R^*$.*

1.15 DEFINITION. *Ein echter Unterring R eines Körper K heißt ein* **diskreter Bewertungsring (von K)**, *falls R ein lokaler Hauptidealring mit K als Quotientenkörper ist.*

1.16 SATZ. *Sei K ein Körper. Für eine diskrete Bewertung v von K ist $R_v := \{a \in K : v(a) \geq 0\}$ ein diskreter Bewertungsring von K und $P_v := \{a \in K : v(a) > 0\}$ sein maximales Ideal. Man hat eine Bijektion*

$$\begin{array}{rcl} \{\text{diskrete Bewertungen von } K\} & \leftrightarrow & \{\text{diskrete Bewertungsringe von } K\} \\ v & \mapsto & R_v, \end{array}$$

wobei $v = v_{P_v}$ die P_v-adische Bewertung aus 1.12(b) ist.

Da wir es in dieser Arbeit ausschließlich mit diskreten Bewertungen zu tun haben, wollen wir der Kürze wegen von nun an einfach von **Bewertungen** und **Bewertungsringen** sprechen, auch wenn diese Begriffe üblicherweise allgemeiner gefaßt sind.

1.17 DEFINITION. *Sei v eine Bewertung des Körpers K. Der Ring R_v aus 1.16 heißt der* **Bewertungsring** *und der Körper $k_v := R_v/P_v$ der* **Restklassenkörper zu** *v.*

1.18 LEMMA. *Sei A ein Dedekindring, $P \in \operatorname{Max}(A)$ und $v := v_P$ die P-adische Bewertung auf dem Quotientenkörper von A. Dann ist $P = P_v \cap A$ und die kanonische Einbettung*

$$\begin{array}{rcl} A/P & \hookrightarrow & k_v \\ a + P & \mapsto & a + P_v \end{array}$$

ein Körperisomorphismus.

Der folgende Satz ist in gewissem Sinne eine Verallgemeinerung des chinesischen Restsatzes und findet seine Anwendung auch in ähnlichen Situationen.

1.19 APPROXIMATIONSSATZ. *Seien $v_1, \ldots, v_n$ paarweise verschiedene Bewertungen des Körpers K, $\alpha_1, \ldots, \alpha_n \in K$ und $m_1, \ldots, m_n \in \mathbb{Z}$. Dann gibt es ein $\alpha \in K$ mit*

$$v_i(\alpha - \alpha_i) \geq m_i \quad \forall i = 1, \ldots, n.$$

Mithilfe von 1.13(c) lassen sich sogar Gleichheitszeichen erreichen.

e. Fortsetzungen.

1.20 DEFINITION. *Sei L/K eine Körpererweiterung und v eine Bewertung von K. Eine Bewertung w von L heißt eine* **Fortsetzung von v nach L** *(in Zeichen w/v), wenn ein $e \in \mathbb{N}$ existiert mit $w|_K = ev$. Die Zahl $e_{w/v} := e$ heißt der* **Verzweigungsindex von w über v**. *Die kanonische Injektion $k_v \hookrightarrow k_w, a + P_v \mapsto a + P_w$ fassen wir als Inklusion auf. Dabei heißt $f_{w/v} := [k_w : k_v]$ der* **(relative) Restklassengrad von w über v**.

Die wesentlichen Resultate über Fortsetzung von Bewertungen lassen sich [Ws, pp. 21-27, 54, 67] entnehmen. Es sei versichert, daß auf die dort verwendeten Methoden der Komplettierung, die wir erst in Abschnitt 3 einführen werden, verzichtet werden kann. Eine Anleitung für einen elementaren Beweis des folgenden zusammenfassenden Satzes gibt uns [FJ, pp. 14f, 25].

1.21 SATZ. *Sei L/K eine endliche Körpererweiterung vom Grad n.*

(a) *Jede Bewertung von L setzt genau eine Bewertung von K fort.*

(b) *Jede Bewertung von K hat mindestens eine und nur endlich viele Fortsetzungen nach L.*

(c) *Sind $w_1, \ldots, w_r$ sämtliche Fortsetzungen einer Bewertung v von K nach L, so gilt die* **fundamentale Ungleichung**

$$\sum_{i=1}^{r} e_{w_i/v} f_{w_i/v} \leq n.$$

1.22 DEFINITION. *Sei L/K endlich vom Grad n und v eine Bewertung von K mit Fortsetzung w nach L. w/v heißt*

- **unverzweigt**, *falls $e_{w/v} = 1$ ist.*
- **zahm verzweigt**, *falls k_w/k_v separabel ist und $\mathrm{char}(k_v)$ nicht $e_{w/v}$ teilt.*
- **total verzweigt**, *falls $e_{w/v} = n$ ist.*
- **träge**, *falls $f_{w/v} = n$ ist.*

v heißt **unverzweigt** *bzw.* **zahm verzweigt** *bzw.* **total verzweigt** *bzw.* **träge in L/K**, *falls alle Fortsetzungen von v nach L unverzweigt bzw. zahm verzweigt bzw. total verzweigt bzw. träge über v sind. v heißt* **total zerlegt in L/K**, *falls v genau n Fortsetzungen nach L hat.*

Die im folgenden Satz beschriebene Korrespondenz zwischen den Fortsetzungen einer P-adischen Bewertung und der Zerlegung von P im Erweiterungskörper ist bei [Jc, pp. 614–618] besprochen.

1.23 SATZ. *Sei A ein Dedekindring mit Quotientenkörper K, L/K eine endliche, separable Erweiterung vom Grad n, B der ganze Abschluß von A in L (ein Dedekindring nach 1.7) und $P \in \mathrm{Max}(A)$. Wir schreiben*

$$PB = \prod_{i=1}^{r} Q_i^{e_i}$$

mit $r, e_i \in \mathbb{N}$ und paarweise verschiedenen $Q_i \in \mathrm{Max}(B)$ gemäß 1.8(a). Der Körper $\overline{A} := A/P$ ist auf natürliche Weise in den Körpern $\overline{B}_i := B/Q_i$ enthalten. Wir setzen $f_i := [\overline{B}_i : \overline{A}]$.

(a) *Die Bewertung $v := v_P$ hat genau die r Fortsetzungen $w_i := v_{Q_i}$ nach L mit $e_{w_i/v} = e_i$ und $f_{w_i/v} = f_i$ für $i = 1, \ldots, r$.*

(b) *Es gilt die* **fundamentale Gleichung**

$$\sum_{i=1}^{r} e_i f_i = n.$$

(c) *Ist speziell $A = R_v$, so ist $\mathrm{Max}(B) = \{Q_1, \ldots, Q_r\}$ und $B = \bigcap_{i=1}^{r} R_{w_i}$.*

Der folgende Satz, den wir bei [L2, pp. 27–29] wiederfinden, gibt uns ein Verfahren an die Hand, um das Fortsetzungsverhalten von Primidealen (sprich Bewertungen) in vielen konkreten Situationen explizit zu bestimmen.

1.24 Satz (Explizite Faktorisierung). *In der Situation von 1.23 existiere ein $\beta \in B$ mit $B = A[\beta]$. Sei $\Phi \in A[X]$ das Minimalpolynom von β über K und $\varphi := \overline{\Phi} \in \overline{A}[X]$ das modulo P reduzierte Polynom. Wir schreiben $\varphi = \varphi_1^{m_1} \cdots \varphi_s^{m_s}$ mit $s, m_i \in \mathbb{N}$ und paarweise verschiedenen normierten, irreduziblen $\varphi_i \in \overline{A}[X]$ und wählen $\Phi_i \in A[X]$ mit $\varphi_i = \overline{\Phi_i}$. Dann ist $r = s$ und nach eventueller Umordnung $Q_i = PB + \Phi_i(\beta)B$, $e_i = m_i$ und $f_i = \operatorname{grad} \varphi_i$.*

Wir stellen nun noch einige spezielle Hilfsmittel bereit, die wir im dritten Teil der Arbeit häufiger benötigen werden. Um Diskriminanten zu berechnen, bedient man sich häufig der folgenden Rechenregel.

1.25 Lemma. *Sei L/K eine separable Körpererweiterung vom Grad n mit β als primitivem Element und Φ das Minimalpolynom von β über K. Dann ist*

$$D_{L/K}(\beta) = (-1)^{n(n-1)/2} N_{L/K}(\Phi'(\beta)).$$

Beweis. Seien $\sigma_1, \ldots, \sigma_n$ wie in 1.3. $\left(\sigma_i(\beta^{j-1})\right)_{1 \le i,j \le n}$ ist die Vandermondesche Matrix in $\sigma_1(\beta), \ldots, \sigma_n(\beta)$, also gilt

$$\begin{aligned} D_{L/K}(\beta) &= \det{}^2 \left(\sigma_i(\beta^{j-1})\right)_{1 \le i,j \le n} \\ &= \prod_{i<j} (\sigma_j(\beta) - \sigma_i(\beta))^2 \\ &= (-1)^{n(n-1)/2} \prod_{i \ne j} (\sigma_j(\beta) - \sigma_i(\beta)). \end{aligned}$$

Wir schreiben $\Phi = \prod_{i=1}^{n} (X - \sigma_i(\beta))$, dann ist nach der Produktregel $\Phi'(\beta) = \prod_{\sigma \ne \mathrm{id}_L} (\beta - \sigma(\beta))$, also

$$N_{L/K}(\Phi'(\beta)) = \prod_{j=1}^{n} \sigma_j(\Phi'(\beta)) = \prod_{j=1}^{n} \prod_{\sigma \ne \mathrm{id}_L} (\sigma_j(\beta) - (\sigma_j\sigma)(\beta)) = \prod_{j=1}^{n} \prod_{i \ne j} (\sigma_j(\beta) - \sigma_i(\beta)).$$

□

Als spezielle Anwendung von 1.24 wollen wir eine häufig anzutreffende Situation untersuchen.

1.26 Lemma. *Sei A ein Dedekindring mit Quotientenkörper K, L/K endlich, separabel und B der ganze Abschluß von A in L. Ist $L = K(\beta)$ für ein $\beta \in B$ und $D_{L/K}(\beta) \in A^*$, so ist $B = A[\beta]$ und für alle $P \in \mathrm{Max}(A)$ ist v_P unverzweigt in L/K.*

BEWEIS. $B = A[\beta]$ folgt direkt aus 1.5(c). Sei $\Phi \in A[X]$ das Minimalpolynom von β über K und L' ein Zerfällungskörper von Φ über K, der L enthält (normale Hülle von L/K), dann ist L'/K galoissch und die K-Homomorphismen von L nach L' sind die Abbildungen $\sigma'|_L$ mit $\sigma' \in G' := \mathrm{Aut}(L'/K)$. Sei $P \in \mathrm{Max}(A)$ und w' eine Fortsetzung von $v := v_P$ nach L'. Wir bezeichnen mit $^-$ die kanonische Restklassenabbildung $R_v \to k_v$ bzw. $R_{w'} \to k_{w'}$, die wir auch auf die Polynomringe fortsetzen, und schreiben

$$\Phi = \prod_{\sigma' \in H'} (X - \sigma'(\beta))$$

für eine geeignete Teilmenge H' von G'. Da $\sigma'(\beta)$ für alle $\sigma' \in G'$ ganz über R_v ist, können wir zu Restklassen übergehen und erhalten eine Zerlegung

$$\overline{\Phi} = \prod_{\sigma' \in H'} (X - \overline{\sigma'(\beta)})$$

in Linearfaktoren aus $k_{w'}$. Wegen

$$\pm \prod_{\substack{\sigma', \tau' \in H' \\ \sigma' \neq \tau'}} (\sigma'(\beta) - \tau'(\beta)) = D_{L/K}(\beta) \in A^* \subseteq R_v^* \subseteq R_{w'}^*$$

ist $\sigma'(\beta) - \tau'(\beta) \notin P_{w'}$ für alle $\sigma', \tau' \in H'$ mit $\sigma' \neq \tau'$, d. h. $\overline{\Phi}$ hat in $k_{w'}$ keine mehrfachen Nullstellen. Daher zerfällt $\overline{\Phi}$ in lauter verschiedene irreduzible Faktoren aus $k_v[X]$. Das bedeutet nach 1.24 gerade, daß v unverzweigt in L'/K ist. □

Mithilfe der vorigen beiden Lemmata kann das Fortsetzungsverhalten 'gewisser' Bewertungen in einer Radikalerweiterung bestimmt werden.

1.27 BEISPIEL. *Sei v eine Bewertung des Körpers K und $L = K(\beta)$ mit $\beta^n = a \in K$, $v(a) = 0$ und $\mathrm{char}(k_v) \nmid n$. Dann ist v unverzweigt in L/K.*

BEWEIS. Man beachte, daß $\mathrm{char}(K) = 0$ oder $\mathrm{char}(K) = \mathrm{char}(k_v)$, also $nX^{n-1} \neq 0$ ist. Daher ist L/K separabel. Sei B_v der ganze Abschluß von R_v in L. Da $a \in R_v^*$ ist, sind β und β^{-1} ganz über R_v, also $\beta \in B_v^*$. Sei $\Phi \in R_v[X]$ das Minimalpolynom von β über K. Nach dem Lemma von Gauß existiert ein $\Psi \in R_v[X]$ mit

$$X^n - a = \Phi\Psi.$$

Differenzieren und Einsetzen von β ergibt

$$\Phi'(\beta)\Psi(\beta) = n\beta^{n-1} \in B_v^*,$$

also

$$N_{L/K}(\Phi'(\beta))N_{L/K}(\Psi(\beta)) = N_{L/K}(n\beta^{n-1}) \in B_v^* \cap K = R_v^*.$$

Da sowohl $N_{L/K}(\Phi'(\beta))$ als auch $N_{L/K}(\Psi(\beta)) \in R_v$ ist, folgt $D_{L/K}(\beta) = \pm N_{L/K}(\Phi'(\beta)) \in R_v^*$. □

2 Galoiserweiterungen

In einer endlichen Galoiserweiterung ist das Fortsetzungsverhalten von Bewertungen besonders schön. Darauf wollen wir hier näher eingehen. Die getroffenen Aussagen sind üblicherweiser unter dem Stichwort 'Galoisidealtheorie' bekannt. Wir folgen im wesentlichen [L2, p. 12–18].
In diesem Abschnitt sei L/K eine endliche Körpererweiterung und v eine (feste) Bewertung von K. Mit W wollen wir die Menge der Fortsetzungen von v nach L bezeichnen.

2.1 Bemerkung. *Sei $w \in W$.*

(a) *Ist L/K normal, so auch die Restklassenkörpererweiterung k_w/k_v.*

(b) *Für $\sigma \in \mathrm{Aut}(L/K)$ ist $w^\sigma := w \circ \sigma \in W$ mit $e_{w^\sigma/v} = e_{w/v}$ und $f_{w^\sigma/v} = f_{w/v}$.*

Beweis. **(a)** Sei $\alpha \in k_w$ und $\varphi \in k_v[X]$ das Minimalpolynom von α über k_v. Wir bezeichnen mit $^-$ die kanonische Restklassenabbildung $R_v \to k_v$ bzw. $R_w \to k_w$, die wir uns auch auf die Polynomringe $R_v[X]$ bzw. $R_w[X]$ fortgesetzt denken. Nach 1.23(a) und 1.18 können wir $\alpha = \overline{a} = a + P_w$ schreiben mit einem über R_v ganzen $a \in L$. Sei f das Minimalpolynom von a über K. Da L/K normal ist, zerfällt f in Linearfaktoren aus $L[X]$:

$$f = \prod_i (X - a_i) \text{ mit } a_i \in L.$$

Da f nach 1.2(b) aus $R_v[X]$ ist, sind alle a_i ganz über R_v. Offenbar ist α Nullstelle von $\overline{f} = \prod_i (X - \overline{a_i})$, also gilt $\varphi | \overline{f}$, und φ zerfällt in Linearfaktoren aus $k_w[X]$.

(b) $w^\sigma \in W$ ist klar. Sei $t \in K$ mit $v(t) = 1$, dann ist

$$e_{w^\sigma/v} = w^\sigma(t) = w(\sigma(t)) = w(t) = e_{w/v}.$$

Weiter ist

$$\begin{array}{rcl} R_{w^\sigma} & \to & R_w \\ a & \mapsto & \sigma(a) \end{array}$$

ein Ringisomorphismus mit $\sigma(P_{w^\sigma}) = P_w$ und $\sigma|_{R_v} = \mathrm{id}_{R_v}$, also

$$\begin{array}{rcl} k_{w^\sigma} & \to & k_w \\ a + P_{w^\sigma} & \mapsto & \sigma(a) + P_w \end{array}$$

ein k_v-Isomorphismus und daher $f_{w^\sigma/v} = [k_{w^\sigma} : k_v] = [k_w : k_v] = f_{w/v}$.

□

2.2 Satz und Definition. *Sei L/K galoissch mit Gruppe G, $w \in W$, $e := e_{w/v}$, $f := f_{w/v}$ und $\overline{G}_w := \mathrm{Aut}(k_w/k_v)$.*

(a) *Es gilt $W = \{w^\sigma : \sigma \in G\}$. Daher ist $e_{\tilde{w}/v} = e$ und $f_{\tilde{w}/v} = f$ für alle $\tilde{w} \in W$ und $[L : K] = ef\#W$.*

(b) *$G_w^- := \{\sigma \in G : w = w^\sigma\}$ ist eine Untergruppe von G. Sie heißt die* **Zerlegungsgruppe von w über v** *und der zugehörige Zwischenkörper $L_w^- := \mathrm{Fix}(L, G_w^-)$ der* **Zerlegungskörper von w über v.**

(c) *Ist w^- die Bewertung von L_w^- mit w/w^-, so ist w die einzige Fortsetzung von w^- nach L und $f_{w^-/v} = 1$.*

(d) *Für $\sigma \in G_w^-$ ist*

$$\overline{\sigma}_w : \begin{array}{ccc} k_w & \to & k_w \\ a + P_w & \mapsto & \sigma(a) + P_w \end{array}$$

ein k_v-Automorphismus von k_w.

(e) *Der Gruppenhomomorphismus*

$$\begin{array}{ccc} G_w^- & \to & \overline{G}_w \\ \sigma & \mapsto & \overline{\sigma}_w \end{array}$$

ist surjektiv. Sein Kern G_w^+ wird als die **Trägheitsgruppe** *und $L_w^+ := \mathrm{Fix}(L, G_w^+)$ als der* **Trägheitskörper von w über v** *bezeichnet.*

Beweis. **(a)** Angenommen, es gibt ein $\tilde{w} \in W$ mit $\tilde{w} \neq w^\sigma$ für alle $\sigma \in G$, dann ist auch $\tilde{w}^\tau \neq w^\sigma$ für alle $\sigma, \tau \in G$. Nach 1.19 existiert ein $\alpha \in L$ mit

$$\begin{array}{rcll} w^\sigma(\alpha) & \geq & 1 & \forall \sigma \in G \text{ und} \\ \tilde{w}^\sigma(\alpha - 1) & \geq & 1 & \forall \sigma \in G. \end{array}$$

Für $a := N_{L/K}(\alpha)$ folgt einerseits

$$e_{w/v} v(a) = \sum_{\sigma \in G} w^\sigma(\alpha) > 0,$$

andererseits ist $\tilde{w}^\sigma(\alpha) = 0$ für alle $\sigma \in G$ nach 1.13, also

$$e_{\tilde{w}/v} v(a) = \sum_{\sigma \in G} \tilde{w}^\sigma(\alpha) = 0.$$

Dies ist ein Widerspruch. Der Rest der Behauptung folgt aus 2.1(b) und 1.23(b).

(b) Nur nachrechnen.

(c) Sei $\tilde{w}$ ebenfalls eine Fortsetzung von w^-. Dann existiert, da L/L_w^- galoissch ist, nach (a) ein $\sigma \in \mathrm{Aut}(L/L_w^-)$ mit $\tilde{w} = w^\sigma$. Wegen $\mathrm{Aut}(L/L_w^-) = G_w^-$ ist aber $w^\sigma = w$.
Nun zum zweiten Teil der Behauptung. Sei B^- der ganze Abschluß von R_v in L_w^- (ein Dedekindring nach 1.7) und $Q^- := P_{w^-} \cap B^-$ das maximale Ideal von B^- mit $w^- = v_{Q^-}$ gemäß 1.23(a). Nach 1.18 genügt es, zu zeigen, daß die kanonische Einbettung

$$\begin{array}{rcl} k_v & \hookrightarrow & B^-/Q^- \\ a + P_v & \mapsto & a + Q^- \end{array}$$

surjektiv ist. Sei also $\beta \in B^-$. Für $\sigma \in G$ bezeichne $w^{\sigma -}$ die Bewertung von L_w^- mit $w^\sigma / w^{\sigma -}$. Da w die einzige Fortsetzung von w^- nach L ist, ist $w^{\sigma -} \neq w^-$ für alle $\sigma \in G \setminus G_w^-$. Folglich existiert nach 1.19 und 1.23(c) ein $\alpha \in B^-$ mit

$$\begin{array}{rcll} (1) \quad w^-(\alpha - \beta) & > & 0 & \text{und} \\ (2) \quad w^{\sigma -}(\alpha - 1) & > & 0 & \forall \sigma \in G \setminus G_w^-. \end{array}$$

Dann haben wir $a := N_{L_w^-/K}(\alpha) \in R_v$. Nach Galoistheorie ist $\{\sigma|_{L_w^-} : \sigma \in G\}$ die Menge der K-Homomorphismen von L_w^- nach L und $\sigma|_{L_w^-} = \mathrm{id}_{L_w^-} \iff \sigma \in G_w^-$, daher

$$a = \alpha \prod_{\sigma \in H} \sigma(\alpha) \text{ mit } H \subseteq G \setminus G_w^-.$$

Mit (1) und (2) folgt $a \equiv \beta \pmod{P_w}$, wegen $a, \beta \in B^-$ also $a + Q^- = \beta + Q^-$.

(d) Folgt aus dem Beweis von 2.1(b).

(e) Sei w^- die Bewertung von L_w^- mit w/w^-. Nach (c) ist $\overline{G}_w = \mathrm{Aut}(k_w/k_{w^-})$. Wir bezeichnen mit $^-$ die Restklassenabbildung $R_w \to k_w$ bzw. $R_{w^-} \to k_{w^-}$, die wir auch auf die Polynomringe fortsetzen. Nach dem Satz von Artin ist k_w galoissch über $k' := \mathrm{Fix}(k_w, \overline{G}_w)$ und $k_{w^-} \subseteq k'$. Wir schreiben $k_w = k'(\overline{a})$ mit $a \in R_w$ und das Minimalpolynom f von a über L_w^- in der Form

$$f = \prod_{\sigma \in H} (X - \sigma(a)) \text{ mit } H \subseteq G_w^-.$$

Da nach (c) und 1.23(c) außerdem R_w der ganze Abschluß von R_{w^-} in L ist, gilt

$$f \in R_{w^-}[X]$$

und

$$\sigma(a) \in R_w \quad \forall \sigma \in H.$$

Sei nun $\psi \in \overline{G}_w$ beliebig. Da mit $\overline{a}$ auch $\psi(\overline{a})$ Nullstelle von

$$\overline{f} = \prod_{\sigma \in H} \left(X - \overline{\sigma(a)}\right) = \prod_{\sigma \in H} (X - \overline{\sigma}_w(\overline{a})) \in k_{w^-}[X] \subseteq k'[X]$$

und ψ durch $\psi(\overline{a})$ eindeutig bestimmt ist, folgt $\psi = \overline{\sigma}_w$ für ein $\sigma \in H$.

□

2.3 Definition. *Ist in Teil (e) des vorigen Satzes $\#k_v =: q$ endlich, so wird $\overline{G}_w$ bekanntlich erzeugt von dem Frobeniusautomorphismus $\varphi_{w/v}$ mit $\varphi_{w/v}(\alpha) = \alpha^q$ für alle $\alpha \in k_w$. Jedes $\sigma \in G_w^-$ mit $\overline{\sigma}_w = \varphi_{w/v}$ heißt ein* **Frobeniusautomorphismus von** w **über** v.

Sei im folgenden L/K **abelsch**, d. h. galoissch mit abelscher Galoisgruppe G. Dann vereinfacht sich die Sache noch weiter.

2.4 Bemerkung und Definition. *Für $w, \tilde{w} \in W$ gilt*

(a) $G_{\tilde{w}}^- = G_w^-$,

(b) $G_{\tilde{w}}^+ = G_w^+$.

Wir können also $G^- := G_w^-$ und $G^+ := G_w^+$ für beliebiges $w \in W$ setzen. G^- heißt **Zerlegungs-**, *G^+* **Trägheitsgruppe**, *$L^- := \mathrm{Fix}(L, G^-)$* **Zerlegungs-** *und $L^+ := \mathrm{Fix}(L, G^+)$* **Trägheitskörper von** v **in** L/K.

Beweis. Nach 2.2(a) ist $\tilde{w} = w^\tau$ für ein $\tau \in G$.

(a) $\sigma \in G_w^- \implies w = w^\sigma \implies \tilde{w} = w^\tau = w^{\sigma\tau} = w^{\tau\sigma} = \tilde{w}^\sigma \implies \sigma \in G_{\tilde{w}}^-$. Umgekehrt analog.

(b) Sei $\sigma \in G^- = G_w^- = G_{\tilde{w}}^-$. Nach Beweis von 2.1(b) gilt

$$\begin{aligned}
\overline{\sigma}_{\tilde{w}} = \mathrm{id}_{k_{\tilde{w}}} &\iff \forall \beta \in R_{\tilde{w}} : \beta - \sigma(\beta) \in P_{\tilde{w}} \\
&\iff \forall \beta \in R_{\tilde{w}} : \tau(\beta) - \sigma(\tau(\beta)) = \tau(\beta - \sigma(\beta)) \in P_w \\
&\iff \forall \alpha \in R_w : \alpha - \sigma(\alpha) \in P_w \\
&\iff \overline{\sigma}_w = \mathrm{id}_{k_w},
\end{aligned}$$

also $\sigma \in G_{\tilde{w}}^+ \iff \sigma \in G_w^+$.

□

Die Rechtfertigung der Begriffe 'Zerlegungskörper' und 'Trägheitsköper' liefert der folgende Satz.

2.5 Satz. *Bezeichnet W^- bzw. W^+ die Menge der Fortsetzungen von v nach L^- bzw. L^+, so gilt:*

(a) *$[L^- : K] = \#W^- = \#W$, d. h. v ist total zerlegt in L^-/K und über jedem $w^- \in W^-$ liegt nur ein $w \in W$.*

(b) *Für $w \in W$, $w^+ \in W^+$, $w^- \in W^-$ mit $w/w^+/w^-/v$ ist w^+/w^- träge und w/w^+ total verzweigt.*

Zusammengefaßt: $f_{w/v} = f_{w^+/w^-} = [L^+ : L^-]$ und $e_{w/v} = e_{w/w^+} = [L : L^+] = \#G^+$.

Beweis. **(a)** Wir betrachten für festes $w^- \in W^-$ die Abbildung

$$\begin{array}{rcl} G/G^- & \to & W^- \\ \sigma G^- & \mapsto & w^- \circ \sigma. \end{array}$$

Sie ist wohldefiniert und injektiv, denn für die Fortsetzung $w \in W$ von w^- und $\sigma, \tau \in G$ gilt (unter Beachtung von 2.2(c) bei der dritten Äquivalenz):

$$\begin{array}{ccccc} \sigma G^- = \tau G^- & \iff & \sigma^{-1}\tau \in G^- & \iff & w = w^{\tau\sigma^{-1}} \\ & \iff & w^- = w^- \circ (\tau\sigma^{-1}) & \iff & w^- \circ \sigma = w^- \circ \tau. \end{array}$$

Sie ist surjektiv nach 2.2(a) angewendet auf L^-/K. Also gilt

$$[L^- : K] = \#(G/G^-) = \#W^-.$$

Nach 2.2(c) ist $\#W^- = \#W$.

(b) Nach 2.2(e) ist $\mathrm{Aut}(k_w/k_v) \simeq G^-/G^+$, also

(1) $\quad f_{w/v} = [L^+ : L^-]$.

Wenden wir 2.2(e) auf die Erweiterung L/L^+ an, so ergibt sich, daß der Gruppenhomomorphismus

$$\begin{array}{rcl} G^+ & \to & \mathrm{Aut}(k_w/k_{w^+}) \\ \sigma & \mapsto & \overline{\sigma}_w \end{array}$$

surjektiv ist und den Kern G^+ hat, daher ist

(2) $\quad f_{w/w^+} = 1$.

Aus (a), (1), (2) und 1.23(b) folgt die Behauptung.

□

Zum Schluß wollen wir noch einmal zu der Situation aus 2.3 zurückkehren.

2.6 Bemerkung und Definition. *Sei v unverzweigt in L/K und $\#k_v = q$ endlich. Dann gibt es genau ein $\sigma \in G^-$ mit $\overline{\sigma}_w = \varphi_{w/v}$ für ein und für alle $w \in W$. Dieses σ heißt der* **Artinautomorphismus von v in L/K**. *Desweiteren ist $G^- = \langle\sigma\rangle$ zyklisch und $f_{w/v}$ die Ordnung von σ in G.*

BEWEIS. Seien $w, \tilde{w} \in W$. Nach 2.5 gilt

$$e_{w/v} = 1 \iff G^+ = 1,$$

also existiert nach 2.2(e) ein eindeutig bestimmtes $\sigma \in G^-$ mit $\overline{\sigma}_w = \varphi_{w/v}$. Dieses σ ist unabhängig von der Wahl von w. Wir können nämlich wieder $\tilde{w} = w^\tau$ mit $\tau \in G$ schreiben und wie im Beweis von 2.4(b) folgern, daß

$$\begin{aligned}
\overline{\sigma}_{\tilde{w}} = \varphi_{\tilde{w}/v} &\iff \forall \beta \in R_{\tilde{w}} : \beta^q - \sigma(\beta) \in P_{\tilde{w}} \\
&\iff \forall \beta \in R_{\tilde{w}} : (\tau(\beta))^q - \sigma(\tau(\beta)) = \tau(\beta^q - \sigma(\beta)) \in P_w \\
&\iff \forall \alpha \in R_w : \alpha^q - \sigma(\alpha) \in P_w \\
&\iff \overline{\sigma}_w = \varphi_{w/v}.
\end{aligned}$$

$G^- = \langle \sigma \rangle$ ist klar nach Gruppentheorie. Aus 2.5 folgt

$$f_{w/v} = [L^+ : L^-] = [L : L^-] = \#G^- = \# \langle \sigma \rangle .$$

□

3 Komplettierung

In der Analysis wird der Körper der reellen Zahlen häufig als Vervollständigung des Körpers der rationalen Zahlen bezüglich des gewöhnlichen Absolutbetrages charakterisiert. Dieses Konzept läßt sich verallgemeinern. Die Theorie der sogenannten 'lokalen Körper' ist Anfang dieses Jahrhunderts entwickelt worden. Sie ist entstanden aus dem Versuch, die Laurent-Reihenentwicklung aus der Funktionentheorie zunächst auf die rationalen Zahlen (p-adische Zahlen), dann auf beliebige Körper zu übertragen. Wir wollen hier nur die für diese Arbeit benötigten Hilfsmittel bereitstellen. Eine breitere Darstellung der Theorie findet sich beispielsweise bei [Sr] oder [Cs].

3.1 DEFINITION. *Sei K ein Körper und V ein K-Vektorraum. Ein* **Absolutbetrag auf** *K ist eine Abbildung*

$$|\ | : K \to \mathbb{R}_+$$

mit den Eigenschaften

- $|a| = 0 \iff a = 0$,
- $|a + b| \leq |a| + |b|$ *und*
- $|ab| = |a|\,|b|$

für $a, b \in K$. Ist $|\ |$ ein Absolutbetrag auf K, so nennen wir eine Abbildung

$$\|\ \| : V \to \mathbb{R}_+$$

eine $|\ |$**-Norm auf** *V, wenn für alle $a \in K$ und $x, y \in V$ gilt:*

- $\|x\| = 0 \iff x = 0$,

- $\|x+y\| \le \|x\| + \|y\|$ *und*
- $\|ax\| = |a|\,\|x\|$.

Zwei $|\,|$*-Normen* $\|\ \|$ *und* $\|\ \|'$ *auf* V *heißen* **äquivalent**, *falls* $m, M > 0$ *existieren mit* $m\|x\| \le \|x\|' \le M\|x\|$ *für alle* $x \in V$.

3.2 Bemerkung und Definition. *Sei* K *ein Körper,* V *ein* K*-Vektorraum,* $|\ |$ *ein Absolutbetrag auf* K *und* $\|\ \|$ *eine* $|\,|$*-Norm auf* V.

(a) *Ist* $V = K$, *so ist* $\|\ \| = \lambda|\ |$ *mit* $\lambda > 0$.

(b) *Durch* $d(x,y) := \|x-y\|$ *für* $x, y \in V$ *wird eine Metrik auf* V *erklärt. Die Begriffe* **Nullfolge**, **Cauchy-Folge**, **Konvergenz**, **Vollständigkeit** *werden wie üblich definiert.*

(c) *Ist* v *eine Bewertung von* K *und* $\rho > 1$, *so wird durch* $|a|_v := \rho^{-v(a)}$ *für* $a \in K$ *ein Absolutbetrag auf* K *definiert, der die stärkere Dreiecksungleichung*

$$|a+b|_v \le \max\{|a|_v, |b|_v\}$$

für $a, b \in K$ *erfüllt. Die Konvergenz bezüglich* $|\ |_v$ *ist von* ρ *unabhängig, denn für eine Folge* $(a_n)_{n\in\mathbb{N}}$ *mit* $a_n \in K$ *gilt*

$$|a_n|_v \to 0 \iff v(a_n) \to \infty.$$

Man spricht daher von **Konvergenz**, **Vollständigkeit** *etc.* **bezüglich** v.

(d) *Ist* $\|\ \|'$ *eine weitere* $|\,|$*-Norm auf* V, *die zu* $\|\ \|$ *äquivalent ist, so ist die Menge der* $\|\ \|$*-Nullfolgen gleich der Menge der* $\|\ \|'$*-Nullfolgen, also stimmen die Begriffe aus (b) für beide Normen überein.*

(e) *Hat* V *eine endliche* K*-Basis* $(e_1, \dots, e_r)$, *so wird durch*

$$\left\| \sum_{i=1}^{r} x_i e_i \right\|_1 := \sum_{i=1}^{r} |x_i|,\ x_i \in K,$$

eine $|\,|$*-Norm auf* V *definiert. Ist* $(K, |\ |)$ *vollständig, so auch* $(V, \|\ \|_1)$.

Beweis. **(a)**–**(d)** Einfaches Nachrechnen.

(e) Sei $\left(x^{(n)}\right)_{n\in\mathbb{N}}$ eine Cauchy-Folge in $(V, \|\ \|_1)$. Wir schreiben $x^{(n)} = \sum_{i=1}^{r} x_i^{(n)} e_i$ mit $x_i^{(n)} \in K$, dann ist $\left(x_i^{(n)}\right)_{n\in\mathbb{N}}$ eine Cauchy-Folge in $(K, |\ |)$ für $1 \le i \le r$. Wir setzen nun $x_i := \lim_{n\to\infty} x_i^{(n)}$ und zeigen, daß $\left(x^{(n)}\right)_{n\in\mathbb{N}}$ bezüglich $\|\ \|_1$ gegen $x := \sum_i x_i e_i$ konvergiert. Sei $\varepsilon > 0$. Nach Definition der x_i existiert ein $n_i \in \mathbb{N}$ mit

$$|x_i^{(n)} - x_i| \le \frac{\varepsilon}{r} \quad \forall n \ge n_i.$$

Für $n \ge n_0 := \max\{n_i : 1 \le i \le r\}$ gilt somit

$$\|x^{(n)} - x\|_1 = \sum_{i=1}^{r} |x_i^{(n)} - x_i| \le \varepsilon.$$

□

Der folgende Satz scheint zunächst aus der Analysis bekannt zu sein. Man beachte jedoch, daß wir es mit beliebigen, i. a. nicht geordneten Körpern zu tun haben und der Beweis aus der Analysis daher nicht einfach kopiert werden kann. Wir haben uns hier an [L1, p. 409] orientiert.

3.3 Satz. *Sei $(K,|\ |)$ vollständig und V ein endlich-dimensionaler K-Vektorraum. Dann sind alle $|\ |$-Normen auf V äquivalent.*

Beweis. Sei $(e_1,\dots,e_r)$ eine K-Basis von V, $\|\ \|_1$ wie in 3.2(e) und $\|\ \|$ irgendeine $|\ |$-Norm auf V. Es genügt zu zeigen, daß $\|\ \|$ äquivalent zu $\|\ \|_1$ ist. Wir setzen $M := \max\{\|e_i\| : 1 \le i \le r\}$, dann gilt für beliebiges $x := \sum_i x_i e_i \in V$ mit $x_i \in K$, daß $\|x\| = \|\sum_i x_i e_i\| \le \sum_i |x_i|\,\|e_i\| \le M \sum_i |x_i| = M\|x\|_1$ ist. Also haben wir

(1) $\quad \|\ \| \le M\|\ \|_1$.

Bleibt zu zeigen, daß umgekehrt für jede Folge $\left(x^{(n)}\right)_{n\in\mathbb{N}}$ aus V gilt:

$$\lim_{n\to\infty} \|x^{(n)}\| = 0 \implies \lim_{n\to\infty} \|x^{(n)}\|_1 = 0.$$

Wir beweisen dies durch vollständige Induktion nach r. Für $r = 1$ ist $\|\ \| = \|e_1\|\,\|\ \|_1$, also die Aussage klar. Sei $r > 1$ und $\left(x^{(n)}\right)_{n\in\mathbb{N}}$ Nullfolge bezüglich $\|\ \|$ mit $x^{(n)} = \sum_i x_i^{(n)} e_i$, $x_i^{(n)} \in K$. Angenommen $\left(\|x^{(n)}\|_1\right)_{n\in\mathbb{N}}$ ist keine Nullfolge, dann ist eine Koeffizientenfolge, o. B. d. A. $\left(x_1^{(n)}\right)_{n\in\mathbb{N}}$ keine Nullfolge. Wir können (nach eventuellem Übergang zu einer entsprechenden Teilfolge) schließen, daß $\varepsilon > 0$ existiert mit

$$|x_1^{(n)}| \ge \varepsilon \quad \forall n \in \mathbb{N}.$$

Es folgt $\left\| \frac{x^{(n)}}{x_1^{(n)}} \right\| \to 0$, also gilt für

$$y^{(n)} := \sum_{i=2}^{r} \frac{x_i^{(n)}}{x_1^{(n)}} e_i \in W := \bigoplus_{i=2}^{r} Ke_i \subseteq V,$$

daß

(2) $\quad \lim_{n\to\infty} \|y^{(n)} + e_1\| = 0.$

Insbesondere ist $\left(y^{(n)}\right)_{n\in\mathbb{N}}$ Cauchy-Folge in $(W,\|\ \|)$, also nach Induktionsvoraussetzung Cauchy-Folge in $(W,\|\ \|_1)$. Nach 3.2(e) konvergiert $\left(y^{(n)}\right)_{n\in\mathbb{N}}$ gegen ein $y \in W$ bezüglich $\|\ \|_1$ und nach (1) auch bezüglich $\|\ \|$. Dies ist ein Widerspruch zu (2), da $e_1 \notin W$ ist. □

Der folgende wichtige Satz ist nun eine leichte Folgerung.

3.4 Satz. *Sei L/K endliche Körpererweiterung und K vollständig bezüglich einer Bewertung v. Dann hat v genau eine Fortsetzung w nach L, und L ist vollständig bezüglich w.*

Beweis. Existenz nach 1.21(b). Seien w_1 und w_2 Fortsetzungen von v nach L und $e_i := e_{w_i/v}$. Wir wählen $\rho, \sigma_i > 1$ mit $\rho = \sigma_i^{e_i}$ und setzen $|\ | := |\ |_v := \rho^{-v}$ und $\|\ \|_i := |\ |_{w_i} := \sigma_i^{-w_i}$ gemäß 3.2(c). Dann ist

$$\|ab\|_i = \sigma_i^{-e_i v(a)} \sigma_i^{-w_i(b)} = |a|\,\|b\|_i$$

für alle $a \in K$, $b \in L$, also $\| \ \|_i$ eine $|\ |$-Norm auf L. Da w_i nach 1.16 bestimmt ist durch

$$R_{w_i} = \{b \in L : \left(\|b^{-n}\|_i\right)_{n\in\mathbb{N}} \text{ ist keine Nullfolge}\},$$

folgt nach 3.3 und 3.2(d), daß $w_1 = w_2$ ist. Die zweite Aussage ergibt sich dann mit 3.2(e). □

3.5 Korollar. *Sei L/K endlich, K vollständig bezüglich der Bewertung v und w die Fortsetzung von v nach L. Ist $f \in K[X]$ ein irreduzibles Polynom mit Nullstellen $\alpha, \beta \in L$, so gilt $w(\alpha) = w(\beta)$.*

Beweis. Sei o. B. d. A. L/K normal, dann ist $\beta = \sigma(\alpha)$ für ein $\sigma \in \mathrm{Aut}(L/K)$. Wegen 2.1(b) und dem vorhergehenden Satz ist $w = w^\sigma$, also folgt die Behauptung. □

In den meisten praktischen Anwendungen, wie auch in Teil III dieser Arbeit, sind die betrachteten Körper leider nicht vollständig. Doch dagegen kann man etwas tun.

3.6 Definition. *Sei K ein Körper mit einem Absolutbetrag $|\ |$. Ein Oberkörper $\hat{K}$ von K mit einem Absolutbetrag $\| \ \|$, der auf K mit $|\ |$ übereinstimmt, heißt* **Komplettierung von K (bezüglich $|\ |$)**, *falls gilt:*

(a) *$(\hat{K}, \| \ \|)$ ist vollständig, und*

(b) *K liegt dicht in $\hat{K}$.*

Die Existenz und Eindeutigkeit der Komplettierung wird gesichert durch den folgenden Satz.

3.7 Satz. *Sei $|\ |$ ein Absolutbetrag auf dem Körper K. Die Menge der $|\ |$-Cauchy-Folgen bzw. $|\ |$-Nullfolgen bezeichnen wir mit $\mathcal{C}$ bzw. $\mathcal{N}$.*

(a) *$\mathcal{C}$ ist (bei gliedweiser Addition und Multiplikation von Folgen) ein kommutativer Ring, $\mathcal{N}$ ein maximales Ideal von $\mathcal{C}$.*

(b) *Auf dem Körper $\hat{K} := \mathcal{C}/\mathcal{N}$ wird durch*

$$\left\|(a_n)_{n\in\mathbb{N}} + \mathcal{N}\right\| := \lim_{n\to\infty} |a_n|$$

für $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}$ ein Absolutbetrag auf $\hat{K}$ definiert. Die kanonische Einbettung

$$\begin{array}{rcl} K & \hookrightarrow & \hat{K} \\ a & \mapsto & (a)_{n\in\mathbb{N}} + \mathcal{N} \end{array}$$

fassen wir als Inklusion auf.

(c) *$(\hat{K}, \| \ \|)$ ist vollständig.*

(d) *K liegt dicht in $\hat{K}$.*

(e) *Ist $\tilde{K}$ ebenfalls eine Komplettierung von K, so ist die Abbildung*

$$\begin{array}{rcl} \hat{K} & \to & \tilde{K} \\ (a_n)_{n\in\mathbb{N}} + \mathcal{N} & \mapsto & \lim\limits_{n\to\infty} a_n \end{array}$$

ein K-Isomorphismus.

BEWEIS. **(a)** Ring- und Idealeigenschaften folgen mit den üblichen Abschätzungen bei Summen und Produkten von Folgen. Bleibt zu zeigen, daß $\mathcal{N}$ maximal, d. h. $\mathcal{C}/\mathcal{N}$ ein Körper ist. Sei $(a_n)_{n\in\mathbb{N}} \in \mathcal{C} \setminus \mathcal{N}$. Dann existiert $\varepsilon > 0$ und ein $n_0 \in \mathbb{N}$, so daß $|a_{n_0}| \geq 2\varepsilon$. Wählen wir n_0 dabei genügend groß, so haben wir noch $|a_{n_0} - a_n| \leq \varepsilon$, also $|a_n| = |a_{n_0} - (a_{n_0} - a_n)| \geq |a_{n_0}| - |a_{n_0} - a_n| \geq \varepsilon$ für alle $n \geq n_0$. Setzen wir $b_n := 1/a_n$ für $n \geq n_0$ und $b_n := 0$ für $n < n_0$, so ergibt sich

$$|b_n - b_m| = \left|\frac{a_m - a_n}{a_n a_m}\right| \leq \varepsilon^{-2}|a_n - a_m| \quad \forall m, n \geq n_0,$$

also $(b_n)_{n\in\mathbb{N}} \in \mathcal{C}$, und wegen $a_n b_n = 1$ für alle $n \geq n_0$:

$$(a_n)_{n\in\mathbb{N}}\,(b_n)_{n\in\mathbb{N}} \equiv 1 \pmod{\mathcal{N}}.$$

(b) Man beachte, daß $\mathbb{R}$ vollständig, also $\lim_{n\to\infty} |a_n|$ definiert ist. Die Eigenschaften des Absolutbetrags sind leicht zu verifizieren. Klar ist, daß bei der angegebenen Einbettung $\|\ \|$ auf K mit $|\ |$ übereinstimmt.

(c)–(e) Geht wie bei der Komplettierung von Vektorräumen in der Funktionalanalysis oder bei der Konstruktion von $\mathbb{R}$ aus $\mathbb{Q}$.

□

3.8 DEFINITION UND SATZ. *Mit den Bezeichnungen aus 3.7 sei speziell* $|\ | = |\ |_v = \rho^{-v}$ *mit einer Bewertung* v *von* K *und* $\rho > 1$ *wie in 3.2(c). Dann heißt* $\hat{K}$ *heißt dann die* **Komplettierung von** K **nach** v. *Durch*

$$\hat{v}((a_n)_{n\in\mathbb{N}} + \mathcal{N}) := \lim_{n\to\infty} v(a_n)$$

für $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}$ *wird eine (kanonische) Fortsetzung von* v *nach* $\hat{K}$ *definiert, so daß* $\|\ \| = |\ |_{\hat{v}} = \rho^{-\hat{v}}$ *ist. Ferner gilt*

$$e_{\hat{v}/v} = f_{\hat{v}/v} = 1.$$

BEWEIS. Sei $(a_n)_{n\in\mathbb{N}} \in \mathcal{C}$ und $\alpha := (a_n)_{n\in\mathbb{N}} + \mathcal{N}$. Für $\alpha = 0$ ist $\lim_{n\to\infty} v(a_n) = \infty$. Ist $\alpha \neq 0$, so ist $\lim_{n\to\infty} |a_n| > 0$, und da $\{\rho^{-m} : m \in \mathbb{Z}\}$ in $\mathbb{R}^*$ keinen Häufungspunkt hat, existiert ein $n_0 \in \mathbb{N}$, so daß $v(a_n) = v(a_{n_0})$ ist für alle $n \geq n_0$. Daher ist $\lim_{n\to\infty} v(a_n) = v(a_{n_0}) \in \mathbb{Z}$. Die übrigen Bewertungsaxiome, $\|\ \| = \rho^{-\hat{v}}$ sowie $e_{\hat{v}/v} = 1$ sind klar. Bleibt noch zu zeigen, daß die kanonische Einbettung

$$\begin{aligned} R_v/P_v &\to R_{\hat{v}}/P_{\hat{v}} \\ a + P_v &\mapsto a + P_{\hat{v}} \end{aligned}$$

surjektiv ist. Sei $\alpha = (a_n)_{n\in\mathbb{N}} + \mathcal{N} \in R_{\hat{v}}$. Da $(a_n)_{n\in\mathbb{N}}$ Cauchy-Folge ist, existiert ein $n_1 \in \mathbb{N}$, so daß $|a_n - a_{n_1}| < 1$, d. h. $v(a_n - a_{n_1}) > 0$ für alle $n \geq n_1$ gilt. Nach Definition ist dann

$$\hat{v}\left((a_n - a_{n_1})_{n\in\mathbb{N}} + \mathcal{N}\right) > 0,$$

d. h. $\alpha - a_{n_1} \in P_{\hat{v}}$, und wegen $\alpha \in R_{\hat{v}}$ ist $a_{n_1} \in R_{\hat{v}} \cap K = R_v$. □

3.9 Beispiel. *Sei k ein Körper und t eine Unbestimmte über k. Die Komplettierung des rationalen Funktionenkörpers $k(t)$ nach der t-adischen Bewertung $v := v_t$ wird mit $k((t))$ bezeichnet.*

(a) *Für eine beliebige Koeffizientenfolge $a_0, a_1, \ldots \in k$ ist die Folge $(x_n)_{n\in\mathbb{N}_0}$ der Partialsummen $x_n := \sum_{i=0}^{n} a_i t^i \in k[t]$ eine Cauchy-Folge bezüglich v. Ihr Grenzwert x in $k((t))$ wird mit $\sum_{n=0}^{\infty} a_n t^n$ bezeichnet. Ist $a_n = 0$ für alle $n > n_0$, so ist $x = \sum_{i=0}^{n_0} a_i t^i \in k[t]$. Ferner gilt*

$$x = 0 \iff \forall n \in \mathbb{N}_0 : a_n = 0,$$

also sind die a_n durch x eindeutig bestimmt.

(b) *Die Menge*

$$k[[t]] := \left\{ \sum_{n=0}^{\infty} a_n t^n \,:\, a_n \in k \;\forall n \in \mathbb{N}_0 \right\}$$

ist ein Unterring von $k((t))$ und heißt der **(formale) Potenzreihenring über** *k. Das Produkt zweier (formaler) Potenzreihen ist gleich ihrem Cauchy-Produkt.*

(c) *Es gilt*

$$R_v = \left\{ \frac{f}{g} \in k(t) \,:\, f, g \in k[t],\ g(0) \neq 0 \right\} \subseteq k[[t]].$$

(d) *Für $q \in k$ und $r \in \mathbb{N}$ gilt beispielsweise*

$$\frac{1}{1-(qt)^r} = \sum_{n=0}^{\infty} q^{rn} t^{rn}.$$

Beweis. **(a)** Für $m \leq n$ ist

$$v(x_n - x_m) = v\left(\sum_{i=m+1}^{n} a_i t^i \right) > m,$$

also ist $(x_n)_{n\in\mathbb{N}_0}$ eine Cauchy-Folge bezüglich v. Die zweite Aussage ist offensichtlich. Bei der letzten Behauptung ist nur die Richtung von links nach rechts zu zeigen. Sind nicht alle $a_n = 0$, so wählen wir $n_0 \in \mathbb{N}_0$ minimal mit $a_{n_0} \neq 0$. Dann ist $v(x_n) = n_0$ für alle $n \geq n_0$, also ist $(x_n)_{n\in\mathbb{N}_0}$ keine Nullfolge.

(b) Seien $x = \sum_{n=0}^{\infty} a_n t^n$, $y = \sum_{n=0}^{\infty} b_n t^n \in k[[t]]$ zwei (formale) Potenzreihen und $z := \sum_{n=0}^{\infty} c_n t^n$ mit $c_n := \sum_{i+j=n} a_i b_j$ ihr Cauchy-Produkt. Für die n-ten Partialsummen x_n, y_n und z_n gilt $v(x_n y_n - z_n) > n$, also folgt

$$xy = \lim_{n\to\infty} x_n y_n = \lim_{n\to\infty} z_n = z.$$

Die übrigen Ringeigenschaften sind klar.

(c) Sei $\frac{f}{g} \in R_v$ mit $f = \sum_{i=0}^{m} f_i t^i$, $g = \sum_{j=0}^{n} g_j t^j \in k[t]$, $f_i, g_j \in k$, dann können wir durch Auskürzen $g_0 \neq 0$ erreichen. Setzen wir außerdem $f_i = 0$ für $i > m$ und $g_j = 0$ für $j > n$, so können wir

$$a_i := \frac{1}{g_0}(f_i - \sum_{j=1}^{i} g_j a_{i-j})$$

für $i = 0, 1, 2, \ldots$ rekursiv berechnen und $x := \sum_{i=0}^{\infty} a_i t^i$ definieren. Wir erhalten $f_i = \sum_{j=0}^{i} g_j a_{i-j}$ für alle $i \in \mathbb{N}_0$, also

$$f = \sum_{i=0}^{\infty} \sum_{j=0}^{i} g_j a_{i-j} t^i = \sum_{j=0}^{m} \sum_{i=j}^{\infty} g_j a_{i-j} t^i = gx.$$

(d) Wegen

$$(1 - (qt)^r) \sum_{n=0}^{\infty} q^{rn} t^{rn} = \sum_{n=0}^{\infty} q^{rn} t^{rn} - \sum_{n=1}^{\infty} q^{rn} t^{rn} = 1.$$

□

Um die Methode der Komplettierung auf eine Erweiterung von nicht vollständigen Körpern anwenden zu können, müssen wir wissen, in welchem Verhältnis sie zur Erweiterung der vervollständigten Körper steht. Den Zusammenhang beschreibt der folgende Satz.

3.10 Satz. *Sei L/K endlich, v eine Bewertung von K und w eine Fortsetzung von v nach L, $\hat{K}$ bzw. $\hat{L}$ die Komplettierung von K bzw. L nach v bzw. w, schließlich $\hat{v}$ bzw. $\hat{w}$ die kanonische Fortsetzung von v bzw. w nach $\hat{K}$ bzw. $\hat{L}$ aus dem vorigen Satz. Dann ist $\hat{K}$ auf natürliche Weise in $\hat{L}$ enthalten. Außerdem gilt:*

(a) *$\hat{w}$ ist die einzige Fortsetzung von $\hat{v}$ nach $\hat{L}$, $e_{\hat{w}/\hat{v}} = e_{w/v}$ und $f_{\hat{w}/\hat{v}} = f_{w/v}$.*

(b) *$\hat{L} = \hat{K}L$.*

Beweis. Wir bezeichnen mit $\mathcal{M}$ bzw. $\mathcal{N}$ die Menge der Nullfolgen aus K bzw. L. Die kanonische Einbettung

$$\begin{array}{rcl} \hat{K} & \to & \hat{L} \\ (a_n)_{n\in\mathbb{N}} + \mathcal{M} & \mapsto & (a_n)_{n\in\mathbb{N}} + \mathcal{N} \end{array}$$

kommutiert mit den Einbettungen $K \hookrightarrow \hat{K}$ und $L \hookrightarrow \hat{L}$ aus 3.7(b) und wird ebenfalls als Inklusion aufgefaßt.

(a) Folgt aus 3.4 und 3.8 durch einfaches Nachrechnen.

(b) Nach 3.4 hat $\hat{v}$ (genau) eine Fortsetzung $\tilde{w}$ nach $\tilde{L} := \hat{K}L$ und $\tilde{L}$ ist vollständig bezüglich $\tilde{w}$. Wegen $L \subseteq \tilde{L} \subseteq \hat{L}$ ist $\tilde{w}$ Fortsetzung von w mit $\hat{w}/\tilde{w}$, so da $\tilde{L} = \hat{L}$ sein mu.

□

Zum Ende dieses Abschnitts möchte ich noch ein sehr nützlches Verfahren vorstellen, um Polynome über vollständigen Körpern in (nicht notwendig irreduzible) Faktoren zu zerlegen. In der Literatur ist es unter dem Stichwort ‘Newtonpolygon’ zu finden.

3.11 Definition. *Sei K ein Körper mit einer Bewertung v und $f = \sum_{j=0}^{n} a_j X^j \in K[X]$ ein Polynom mit $a_0 a_n \neq 0$. Für $i \neq j$ und $a_i a_j \neq 0$ setzen wir*

$$\delta(i, j) := \frac{v(a_j) - v(a_i)}{j - i}.$$

Wir definieren das **Newtonpolygon von f bezüglich** v *als die Menge*

$$\Pi(f) := \{(j, v(a_j)) \,:\, a_j \neq 0, \text{ und für } i < j < k \text{ mit } a_i a_k \neq 0 \text{ gilt } \delta(i,j) < \delta(j,k)\},$$

anschaulich die 'untere konvexe Einhüllende' aller Punkte $(j, v(a_j))$ mit $a_j \neq 0$, und schreiben $\Pi(f) = \{(j_m, v(a_{j_m})) \,:\, 0 \leq m \leq s\}$ mit $0 = j_0 < \cdots < j_s = n$. Für die **Steigungen** $\gamma_m := \delta(j_{m-1}, j_m)$ **der Kanten von** $\Pi(f)$ *gilt offenbar*

$$\gamma_1 < \cdots < \gamma_s.$$

Die folgende Bemerkung ist eine rein geometrische Aussage, die anschaulich leicht einzusehen ist: Steckt ein Teil der Punkte $(j, v(a_j))$ einen konvexen Polygonzug ab und liegen alle übrigen Punkte oberhalb dieses Polygonzuges, so bildet dieser Teil bereits das Newtonpolygon von f. Zuvor wollen wir uns kurz klarmachen, daß

$$(*) \quad \delta(i,j) < \delta(i,k) \iff \delta(i,k) < \delta(j,k) \iff \delta(i,j) < \delta(j,k)$$

ist für $i < j < k$ und $a_i a_j a_k \neq 0$. Die erste Äquivalenz sieht man, indem man in beiden Ungleichungen $v(a_j)$ auf die linke Seite bringt. Die rechten Seiten sind dann gleich. Die zweite Äquivalenz ergibt sich unmittelbar aus der ersten.

3.12 Bemerkung. *Mit den Bezeichnungen von 3.11 sei $0 = h_0 < \cdots < h_t = n$, $a_{h_m} \neq 0$ für $0 \leq m \leq t$,*

(a) *$\delta(h_{m-1}, h_m) < \delta(h_m, h_{m+1})$ für $0 < m < t$ und*

(b) *$\delta(h_{m-1}, j) \geq \delta(j, h_m)$, wenn immer $h_{m-1} < j < h_m$ und $a_j \neq 0$ ist.*

Dann ist $\Pi(f) = \{(h_m, v(a_{h_m})) \,:\, 0 \leq m \leq t\}$.

Beweis. Nach (b) und Definition von $\Pi(f)$ gilt $\Pi(f) \subseteq \{(h_m, v(a_{h_m})) \,:\, 0 \leq m \leq t\}$. Mittels $(*)$ und vollständiger Induktion nach $r - l$ läßt sich (a) verallgemeinern zu

$$(1) \quad l < m < r \implies \delta(h_l, h_m) < \delta(h_m, h_r).$$

Wir zeigen nun per Fallunterscheidung, daß

$$(2) \quad i < h_m, a_i \neq 0 \implies \delta(i, h_m) \leq \delta(h_{m-1}, h_m).$$

Für $h_{m-1} \leq i < h_m$ folgt dies aus (b) und $(*)$, für $i = h_l$ mit $l < m - 1$ aus (1) und $(*)$. Für $h_{l-1} < i < h_l$ mit $l < m$ können wir unter Verwendung von (b), $(*)$ und (1) folgern, daß $\delta(i, h_l) \leq \delta(h_{l-1}, h_l) < \delta(h_l, h_m)$, also $\delta(i, h_m) < \delta(h_l, h_m) \leq \delta(h_{m-1}, h_m)$ ist. Analog läßt sich

$$(3) \quad h_m < k, a_k \neq 0 \implies \delta(h_m, h_{m+1}) \leq \delta(h_m, k)$$

beweisen. Aus (2), (a) und (3) folgt $(h_m, v(a_{h_m})) \in \Pi(f)$. □

Wir kommen jetzt zu dem angestrebten Satz über das Newtonpolygon. Der sehr elegante Beweis stammt aus [Ws, p. 74f].

3.13 SATZ. *Sei K ein Körper, vollständig bezüglich der Bewertung v, L/K endlich und $f = \sum_{j=0}^{n} a_j X^j \in K[X]$ ein Polynom mit $a_0 a_n \neq 0$, dessen sämtliche Nullstellen in L liegen. Ist w die Fortsetzung von v nach L und $e := e_{w/v}$ ihr Verzweigungsindex, so gilt mit den Bezeichnungen aus 3.11 für $1 \leq m \leq s$:*

(a) *f hat, wenn man Vielfachheiten zählt, genau $j_m - j_{m-1}$ Nullstellen $\alpha_{j_{m-1}+1}, \ldots, \alpha_{j_m}$ mit $w(\alpha_i) = -e\gamma_m$ für $j_{m-1} < i \leq j_m$.*

(b) *Das Polynom*

$$f_m := \prod_{j_{m-1} < i \leq j_m} (X - \alpha_i)$$

liegt in $K[X]$ und hat Newtonpolygon $\Pi(f_m) = \{(0, -(j_m - j_{m-1})\gamma_m), (j_m - j_{m-1}, 0)\}$.

BEWEIS. Da sich die γ_m bei Multiplikation von f mit Elementen aus K^* nicht ändern, können wir o. B. d. A. f als normiert annehmen. Wir schreiben $f = \prod_{i=1}^{n}(X - \alpha_i)$ mit $\alpha_i \in L$ und ordnen die α_i nach fallenden Werten für $w(\alpha_i)$, d. h.

$$\lambda_m := w(\alpha_{h_{m-1}+1}) = \cdots = w(\alpha_{h_m}),\ 1 \leq m \leq t,$$

mit $0 = h_0 < \cdots < h_t = n$ und $\lambda_1 > \cdots > \lambda_t$.

(a) Für die Koeffizienten

$$a_j = \pm \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ \#I = n-j}} \prod_{i \in I} \alpha_i$$

von f ergibt sich nach 1.13(c) und 1.11(c)

$$w(a_{h_m}) = w(\alpha_{h_m+1} \cdots \alpha_n) = \sum_{m < r \leq t} (h_r - h_{r-1})\lambda_r$$

und

$$h_{m-1} < j < h_m \implies w(a_j) \geq w(\alpha_{j+1} \cdots \alpha_n) = (h_m - j)\lambda_m + w(a_{h_m}),$$

also gilt für $h_{m-1} < j < h_m$, $a_j \neq 0$:

$$e\delta(j, h_m) = \frac{w(a_{h_m}) - w(a_j)}{h_m - j} \leq -\lambda_m = \frac{w(a_{h_m}) - w(a_{h_{m-1}})}{h_m - h_{m-1}} = e\delta(h_{m-1}, h_m).$$

Mit $(*)$ und 3.12 folgt $\Pi(f) = \{(h_m, v(a_{h_m})) : 0 \leq m \leq t\}$, daher $t = s$ und für $1 \leq m \leq s$: $h_m = j_m$ und $\lambda_m = -e\gamma_m$. Man beachte, daß bis hierhin von der Vollständigkeit kein Gebrauch gemacht wurde.

(b) Wir beweisen $f_m \in K[X]$ durch vollständige Induktion nach $n = \operatorname{grad} f$. Für $n \leq 1$ ist die Aussage trivial. Sei $n > 1$ und φ das Minimalpolynom von α_1 über K. Nach 3.5 ist $f_1 = \varphi g_1$ mit $g_1 \in L[X]$ und $f = \varphi g$ mit $g = g_1 \prod_{m=2}^{s} f_m \in K[X]$. Die Induktionsvoraussetzung angewendet auf g ergibt

$$g_1, f_2, \ldots, f_s \in K[X]$$

und damit auch $f_1 = \varphi g_1 \in K[X]$. Die zweite Aussage ergibt sich, indem wir (a) auf f_m anwenden.

□

Teil II
Algebraische Funktionenkörper

Wir wollen nun die Theorie algebraischer Funktionen in einer Variablen behandeln. Sie weist viele Analogien zur algebraischen Zahlentheorie auf und läßt andererseits eine Reihe geometrischer Interpretationen zu, was uns zur algebraischen Geometrie führen würde. Wir haben uns hier bewußt für einen algebraischen Zugang entschieden, da wir auch später bei den zyklotomischen Funktionenkörpern an eher algebraischen Fragen (Galoisgruppe, Ring ganzer Zahlen, Geschlecht, Klassenzahlen) interessiert sind, während der geometrische Aspekt allenfalls in den Bezeichnungen (abstrakte Kurve, Pol, Differential) durchscheint. Die hiermit verbundene Problematik bespricht Chevalley in der Einleitung zu seinem Buch [Cv], das uns für die Abschnitte 4 und 5 als grober Leitfaden dienen wird. Lassen wir in diesen Abschnitten noch (fast) beliebige Grundkörper zu, so betrachten wir in Abschnitt 6 algebraische Funktionenkörper über endlichem Konstantenkörper. Bei ihnen wird die Analogie zu den algebraischen Zahlkörpern noch enger. Wir werden für sie [FJ, Chapter 3] folgend eine zur Riemannschen Vermutung (vgl. [Nk, p. 452]) analoge Aussage formulieren, die als Satz von Weil bekannt ist.

4 Divisoren und Differentiale

Die algebraischen Funktionenkörper stellen eine besondere Klasse bewerteter Körper dar. Ausgehend von den Bewertungen eines rationalen Funktionenkörpers (Satz 4.3) werden wir die allgemeine Struktur algebraischer Funktionenkörper untersuchen und dafür einige Begriffe (Konstantenkörper, Divisoren, Klassengruppe, Geschlecht, Differentiale) einführen. Als zentrale Aussage dieses Abschnitts ist wohl der Satz von Riemann-Roch anzusehen, den wir in mehreren Varianten kennenlernen werden.

4.1 Definition. *Sei k ein Körper. Ein Oberkörper K von k heißt* **algebraischer Funktionenkörper (in einer Variablen) über** k*, falls K endliche Erweiterung eines rationalen Funktionenkörpers $k(x)$ mit transzendentem x über k ist. Die Elemente von K heißen dann* **(algebraische) Funktionen über** k*.*
Eine Bewertung v von K heißt **Bewertung von** K **über** k*, wenn außer den Bewertungseigenschaften 1.11 noch $v(k^*) = 0$ gilt. Die Menge aller Bewertungen von K über k wird mit $V(K/k)$ bezeichnet und heißt die* **abstrakte Kurve von** K/k*. Ihre Elemente nennt man auch* **Punkte** *oder* **Stellen (von** K/k**)**.
Ein Punkt $v \in V(K/k)$ heißt **Nullstelle** *bzw.* **Pol(stelle)** *einer Funktion $z \in K$* **der Ordnung** m*, falls $v(z) = m > 0$ bzw. $v(z) = -m < 0$ ist.*

Einfachstes Beispiel eines algebraischen Funktionenkörpers über k ist der rationale Funktionenkörper $k(x)$ selbst, dessen abstrakte Kurve wir gleich bestimmen werden. Im folgenden sei K/k stets ein algebraischer Funktionenkörper. Nach Definition hat K über k den Transzendenzgrad 1.

a. Konstantenkörper. Die Forderung $v(k^*) = 0$ bedeutet für endliches k keine Einschränkung, da in diesem Fall $v(k^*)$ als endliche Untergruppe von $\mathbb{Z}$ ohnehin trivial ist. Sie ermöglicht uns jedoch, k in den Restklassenkörper k_v kanonisch einzubetten.

4.2 Definition. *Sei $v \in V(K/k)$. Die kanonische Einbettung*

$$\begin{aligned} k &\hookrightarrow k_v \\ a &\mapsto a + P_v \end{aligned}$$

fassen wir als Inklusion auf. $f_v := [k_v : k]$ heißt der **(absolute Restklassen)grad von** v **(über** k**)**. *Eine Bewertung vom Grad* 1 *heißt ein* **rationaler Punkt von** K/k. *Die Menge aller rationalen Punkte von K/k wird mit $V_1(K/k)$ bezeichnet.*

Wir werden als Korollar des folgenden Satzes erhalten, daß f_v stets endlich ist. Die Aussage (c) dieses Satzes ist das Analogon zum Satz von Ostrowski aus der algebraischen Zahlentheorie.

4.3 Satz. *Sei x transzendent über k und $K = k(x)$.*

(a) *Für $z = \frac{r}{s} \in K$ mit $r, s \in k[x]$ setzen wir $v_\infty(z) := \operatorname{grad} s - \operatorname{grad} r$. Damit ist v_∞ eine Bewertung von K/k. Sie heißt die* **Gradbewertung von** K/k.

(b) *Für jede p-adische Bewertung v_p mit normiertem, irreduziblem $p \in k[x]$ gilt $f_{v_p} = \operatorname{grad} p$, und für die Gradbewertung gilt $f_{v_\infty} = 1$.*

(c) $V(K/k) = \{v_p : p \in k[x] \text{ normiert, irreduzibel}\} \cup \{v_\infty\}$.

(d) $k[x] = \bigcap_{\substack{v \in V(K/k) \\ v \neq v_\infty}} R_v$.

Beweis. **(a)** Die Bewertungseigenschaften lassen sich leicht direkt nachprüfen. Oder man mache sich klar, daß $v_\infty = v_{\frac{1}{x}}$ ist ($\frac{1}{x}$ ist Primelement in $k[\frac{1}{x}]$).

(b) Nach 1.18 ist $k_{v_p} \simeq k[x]/(p)$. Für v_∞ kann man entweder direkt die Surjektivität von $k \hookrightarrow k_{v_\infty}$ nachweisen, oder man führt die Überlegungen aus Teil (a) des Beweises fort.

(c) Sei $v \in V(K/k)$. Wir unterscheiden zwei Fälle.
Ist $k[x] \subseteq R_v$, so können wir ein o. B. d. A. normiertes, irreduzibles $p \in k[x]$ wählen mit minimalem $v(p) > 0$. Für $p \nmid f \in k[x]$ existieren $g, h \in k[x]$ mit $pg + fh = 1$, also gilt

$$0 = v(1) \geq \min\{v(p) + v(g), v(f) + v(h)\},$$

woraus $v(f) = 0$ folgt. Für beliebiges $z \in K$ schreiben wir $z = p^m \frac{r}{s}$ mit $m \in \mathbb{Z}$, $r, s \in k[x]$, $p \nmid rs$ und erhalten $v(z) = mv(p)$. Die Surjektivität von v impliziert $v(p) = 1$, d. h. $v = v_p$.
Im Fall $k[x] \not\subseteq R_v$ existiert $f \in k[x]$ mit $v(f) < 0$. Nach 1.11(c) muß dann auch $v(x) < 0$ sein. Für $z = \frac{r}{s} \in K$ mit $r, s \in k[x]$ folgt $v(z) = (\operatorname{grad} r - \operatorname{grad} s)v(x)$ mithilfe von 1.13(c). Wiederum impliziert die Surjektivität von v, daß $v(x) = -1$, also $v = v_\infty$ ist.

(d) Klar.

□

4.4 Korollar. *Für alle $v \in V(K/k)$ ist $f_v < \infty$.*

Für spätere Zwecke wollen wir noch gleich eine Hilfsaussage festhalten.

4.5 Lemma. *Sei $v \in V(K/k)$ und $a \in R_v$. Dann ist $R_v/(a)$ ein k-Vektorraum der Dimension $v(a)f_v$.*

BEWEIS. $R_v/(a)$ ist ein R_v-Modul, also wegen $k \subseteq R_v$ auch ein k-Vektorraum. Wir wählen $t \in R_v$ mit $v(t) = 1$, dann gilt $R_v/(a) = R_v/(t^{v(a)})$ und daher

$$\dim_k R_v/(a) = \sum_{i=1}^{v(a)} \dim_k (t^{i-1})/(t^i) = v(a) \dim_k R_v/(t) = v(a) f_v.$$

□

Man ist daran interessiert, k möglichst groß zu wählen. Das führt zu dem folgenden Begriff des Konstantenkörpers.

4.6 DEFINITION. *Der algebraische Abschluß*

$$\tilde{k} := \{a \in K : a \text{ ist algebraisch über } k\}$$

von k in K heißt der **Konstantenkörper von** K/k.

Daß man k problemlos durch $\tilde{k}$ ersetzen kann, ersehen wir aus der folgenden Bemerkung.

4.7 BEMERKUNG.

(a) *K ist ein algebraischer Funktionenkörper über $\tilde{k}$ mit $V(K/\tilde{k}) = V(K/k)$.*

(b) *$\tilde{k}$ ist endlich über k.*

(c) *Hat K/k einen rationalen Punkt, so gilt $k = \tilde{k}$.*

BEWEIS. **(a)** Klar, daß $K/\tilde{k}$ algebraischer Funktionenkörper ist. Sei $v \in V(K/k)$ und $a \in K^*$ algebraisch über k. Dann sind a und a^{-1} wegen $k \subseteq R_v$ ganz über R_v, also in R_v. Es folgt $a \in R_v^*$, d. h. $v(a) = 0$.

(b) Folgt aus 4.4, da $k \subseteq \tilde{k} \subseteq k_v$ für eine beliebige Bewertung v von K/k.

(c) Ist $k_v = k$, so muß $k = \tilde{k}$ sein.

□

Daß $\tilde{k}$ wirklich maximal ist mit der Eigenschaft $v(\tilde{k}^*) = 0$ für alle $v \in V(K/k)$, können wir dem folgenden Satz entnehmen.

4.8 SATZ. *Sei $\tilde{k}$ der Konstantenkörper von K/k. Es gilt:*

(a) *$\#V(K/k) = \infty$.*

(b) *Jedes $x \in K \setminus \tilde{k}$ hat mindestens eine und nur endlich viele Nullstellen $v \in V(K/k)$. Gleiches gilt für die Zahl der Pole von x.*

BEWEIS. **(a)** Wir wählen $x \in K$, so daß $K/k(x)$ endlich ist. Die Menge $\{p \in k[x] : p$ normiert, irreduzibel$\}$ ist unendlich, daher folgt die Behauptung mit 1.21(b).

(b) Für $x \in K \setminus \tilde{k}$ ist $K/k(x)$ algebraisch und, da K/k endlich erzeugt ist, auch endlich. Nach 4.3(c) ist v_x die einzige Nullstelle von x in $k(x)/k$, also folgt die Behauptung mit 1.21(b). Die Pole von x sind die Nullstellen von $\frac{1}{x}$.

□

b. Divisoren. Von nun an bis zum Ende dieses Abschnitts sei stets k der Konstantenkörper von K/k. Zur Abkürzung setzen wir $V := V(K/k)$. Eine Verallgemeinerung des Approximationsproblems 1.19 auf unendlich viele Bewertungen führt uns zu den folgenden Begriffsbildungen.

4.9 Definition. *Die freie abelsche Gruppe*

$$\mathcal{D}_K := \mathbb{Z}^{(V)} := \{\mathfrak{d} \in \mathbb{Z}^V \,:\, \mathfrak{d}(v) = 0 \text{ für fast alle } v \in V\}$$

heißt die **Divisorengruppe von** K*, ihre Elemente heißen* **Divisoren**. *Der Divisor* $\mathfrak{o}$ *mit* $\mathfrak{o}(v) = 0$ *für alle* $v \in V$ *heißt* **Nulldivisor**. *Für* $\mathfrak{d}, \mathfrak{d}' \in \mathcal{D}_K$ *schreiben wir* $\mathfrak{d} \geq \mathfrak{d}'$*, falls* $\mathfrak{d}(v) \geq \mathfrak{d}'(v)$ *für alle* $v \in V$ *gilt. Die Elemente der kanonischen Basis* $(\mathfrak{p}_v)_{v\in V}$ *von* $\mathcal{D}_K$ *mit* $\mathfrak{p}_v(v) = 1$ *und* $\mathfrak{p}_v(\tilde{v}) = 0$ *für alle* $\tilde{v} \neq v$ *heißen* **Primdivisoren**. *Für* $\mathfrak{d} = \sum_{v\in V} d_v\mathfrak{p}_v \in \mathcal{D}_K$ *setzen wir* $\operatorname{grad} \mathfrak{d} := \sum_{v\in V} d_v f_v$. *Den Kern des Gruppenhomomorphismus* $\operatorname{grad} : \mathcal{D}_K \to \mathbb{Z}$ *bezeichnen wir mit* $\mathcal{D}_{K,0}$.

Zur Abkürzung setzen wir für den Rest dieses Abschnitts $\mathcal{D} := \mathcal{D}_K$ und $\mathcal{D}_0 := \mathcal{D}_{K,0}$.
Sei $x \in K^*$. Nach 4.8(b) ist $v(x) = 0$ für fast alle $v \in V$. Daher können wir zu x einen Divisor assoziieren.

4.10 Definition. *Für* $x \in K^*$ *heißt*

$$(x) := \sum_{v\in V} v(x)\mathfrak{p}_v \in \mathcal{D}$$

der **Hauptdivisor zu** x.

Die Abbildung $K^* \to \mathcal{D}$, $x \mapsto (x)$ ist offenbar ein Gruppenhomomorphismus mit dem Kern k^*. Daher ist

$$(K^*) := \{(x) \,:\, x \in K^*\}$$

eine Untergruppe von $\mathcal{D}$ und isomorph zu K^*/k^*. Wir werden später sehen, daß (K^*) sogar eine Untergruppe von $\mathcal{D}_0$ ist.

4.11 Definition. *Die* K*-Unteralgebra*

$$\mathcal{A} := \mathcal{A}_K := \{(x_v)_{v\in V} \in K^V \,:\, x_v \in R_v \text{ für fast alle } v \in V\}$$

von K^V *heißt der* **Adlering**, *seine Elemente heißen* **Adle von** K/k. *Die Diagonaleinbettung* $K \hookrightarrow \mathcal{A}$, $x \mapsto (x)_{v\in V}$ *fassen wir als Inklusion auf. Für* $\mathfrak{d} = \sum_{v\in V} d_v\mathfrak{p}_v \in \mathcal{D}$ *definieren wir außerdem die* k*-Vektorräume*

$$\mathcal{A}(\mathfrak{d}) := \mathcal{A}_K(\mathfrak{d}) := \{(x_v)_{v\in V} \in K^V \,:\, v(x_v) \geq -d_v \;\forall v \in V\} \subseteq \mathcal{A}$$

und

$$\mathcal{L}(\mathfrak{d}) := \mathcal{L}_K(\mathfrak{d}) := \{x \in K \,:\, v(x) \geq -d_v \;\forall v \in V\} = \mathcal{A}(\mathfrak{d}) \cap K.$$

Wir wollen einige grundlegende Eigenschaften der gerade eingeführten Räume zusammenfassen.

4.12 Lemma. *Seien $\mathfrak{d}, \mathfrak{d}' \in \mathcal{D}$ mit $\mathfrak{d} \geq \mathfrak{d}'$. Es gilt:*

(a) $\mathcal{L}(\mathfrak{d}) = \{x \in K^* : (x) \geq -\mathfrak{d}\} \cup \{0\}$.

(b) $\mathcal{L}(\mathfrak{o}) = k$, *und* $\mathcal{L}(\mathfrak{d}) = 0$, *falls* $\mathfrak{d} \leq \mathfrak{o}$, $\mathfrak{d} \neq \mathfrak{o}$.

(c) *Für* $x \in K^*$ *ist* $\mathcal{L}(\mathfrak{d} + (x)) \simeq \mathcal{L}(\mathfrak{d})$.

(d) $\mathcal{A}(\mathfrak{d}) \supseteq \mathcal{A}(\mathfrak{d}')$ *und* $\mathcal{L}(\mathfrak{d}) \supseteq \mathcal{L}(\mathfrak{d}')$.

(e) *Die Sequenz der kanonischen k-Vektorraumhomomorphismen*

$$0 \to \mathcal{L}(\mathfrak{d})/\mathcal{L}(\mathfrak{d}') \to \mathcal{A}(\mathfrak{d})/\mathcal{A}(\mathfrak{d}') \to (\mathcal{A}(\mathfrak{d}) + K)/(\mathcal{A}(\mathfrak{d}') + K) \to 0$$

ist exakt.

(f) $\dim_k \mathcal{A}(\mathfrak{d})/\mathcal{A}(\mathfrak{d}') = \operatorname{grad} \mathfrak{d} - \operatorname{grad} \mathfrak{d}'$.

Beweis. **(a)** Nach Definition.

(b) Folgt aus 4.8(b).

(c) Die Abbildung $\mathcal{L}(\mathfrak{d} + (x)) \to \mathcal{L}(\mathfrak{d})$, $y \mapsto xy$ ist offenbar ein k-Vektorraumisomorphismus.

(d) Nach Definition.

(e) Ist eine leichte Übung in linearer Algebra.

(f) Wir schreiben $\mathfrak{d} = \sum_{v \in V} d_v \mathfrak{p}_v$ und $\mathfrak{d}' = \sum_{v \in V} d'_v \mathfrak{p}_v$ und wählen zu jedem $v \in V$ ein $t_v \in K$ mit $v(t_v) = 1$, dann gilt

$$\mathcal{A}(\mathfrak{d})/\mathcal{A}(\mathfrak{d}') = \left(\prod_{v \in V} R_v t_v^{-d_v}\right) / \left(\prod_{v \in V} R_v t_v^{-d'_v}\right) \simeq \prod_{v \in V} R_v / R_v t_v^{d_v - d'_v},$$

also folgt die Behauptung mit 4.5.

□

4.13 Definition. *Wir zerlegen $\mathfrak{d} = \sum_{v \in V} d_v \mathfrak{p}_v \in \mathcal{D}$ in $\mathfrak{d}_+ := \sum_{d_v \geq 0} d_v \mathfrak{p}_v$ und $\mathfrak{d}_- := -\sum_{d_v \leq 0} d_v \mathfrak{p}_v$. (Also $\mathfrak{d} = \mathfrak{d}_+ - \mathfrak{d}_-$.) Für $x \in K^*$ heißt $(x)_+$ der* **Nullstellendivisor** *und $(x)_-$ der* **Polstellendivisor zu** *x.*

4.14 Korollar und Definition. *Sei $\mathfrak{d} \in \mathcal{D}$. $\mathcal{L}(\mathfrak{d})$ ist ein endlich-dimensionaler k-Vektorraum. Wir schreiben fortan kurz $\dim \mathfrak{d}$ statt $\dim_k \mathcal{L}(\mathfrak{d})$.*

Beweis. Es gilt $\mathfrak{d} \geq -\mathfrak{d}_-$ und $-\mathfrak{d}_- \leq \mathfrak{o}$. Nach 4.12(b), (e) und (f) haben wir daher

$$\begin{aligned} \dim_k \mathcal{L}(\mathfrak{d}) &= \dim_k \mathcal{L}(\mathfrak{d})/\mathcal{L}(-\mathfrak{d}_-) + \dim_k \mathcal{L}(-\mathfrak{d}_-) \\ &\leq \operatorname{grad} \mathfrak{d} - \operatorname{grad} \mathfrak{d}_- + 1 \\ &= \operatorname{grad} \mathfrak{d}_+ + 1. \end{aligned}$$

□

c. Klassengruppe. In Analogie zur Produktformel oder Geschlossenheitsrelation (vgl. [Nk, p. 195]) aus der algebraischen Zahlentheorie haben wir für algebraische Funktionenkörper die folgende Aussage:

4.15 Satz. *Für $x \in K \setminus k$ ist*

$$\operatorname{grad}(x)_+ = \operatorname{grad}(x)_- = [K : k(x)].$$

Insbesondere ist also $(K^*) \subseteq \mathcal{D}_0$ und wir können definieren:

4.16 Definition. *Die Faktorgruppe $\mathcal{D}_0/(K^*)$ heißt die* **(Divisoren)klassengruppe von** *K und wird mit $\mathcal{C}\ell_0(K)$ bezeichnet. Ihre Ordnung $h_0 := h_0(K) := \#\mathcal{C}\ell_0(K)$ heißt die* **(Divisoren)klassenzahl von** *K.*

Die Klassengruppe ist von zentraler Bedeutung. Wir werden in Abschnitt 6 sehen, daß für endliches k auch h_0 endlich ist.

Beweis von 4.15. Wegen $(x)_+ = (\frac{1}{x})_-$ und $k(x) = k(\frac{1}{x})$ genügt es,

$$\operatorname{grad}(x)_- = [K : k(x)]$$

zu zeigen. Im Beweis von 4.8(b) haben wir schon gesehen, daß $n := [K : k(x)] < \infty$ ist. Sei v_∞ die Gradbewertung von $k(x)$ und $S \subseteq V$ die Menge ihrer Fortsetzungen nach K. Nach 4.3 und 1.21(c) gilt

$$\operatorname{grad}(x)_- = -\sum_{v\in S} v(x) f_v = \sum_{v\in S} e_{v/v_\infty} f_{v/v_\infty} \leq [K : k(x)].$$

Zum Beweis der umgekehrten Ungleichung wähle man eine Basis $(y_1, \ldots, y_n)$ von K über $k(x)$. Sei $F_i = \sum r_{ij} Y^j$ mit $r_{ij} \in k(x)$ das Minimalpolynom von y_i über $k(x)$. Nach Multiplikation von y_i mit dem Hauptnenner der r_{ij} kann angenommen werden, daß $F_i \in k[x][Y]$, also $v(y_i) \geq 0$ für alle $v \in V \setminus S$ ist. Nach 4.8(b) ist dann

$$c := -\min\{v(y_i) \,:\, v \in S, 1 \leq i \leq n\} \geq 0.$$

Für $d \geq c$ gilt offenbar

$$x^j y_i \in \mathcal{L}(d(x)_-) \quad \forall j \in \{0, \ldots, d-c\} \quad \forall i \in \{1, \ldots, n\}.$$

Man überlegt sich leicht, daß diese $(d-c+1)n$ Funktionen sogar linear unabhängig über k sind, daher folgt

$$\dim d(x)_- \geq (d-c+1)n \quad \forall d \geq c.$$

Nach 4.12(e) und (f) haben wir für $d \in \mathbb{N}$ außerdem

$$\dim d(x)_- - \dim(x)_- \leq \operatorname{grad} d(x)_- - \operatorname{grad}(x)_- = (d-1)\operatorname{grad}(x)_-,$$

also folgt

$$\operatorname{grad}(x)_- \geq \frac{d-c+1}{d-1} n - \frac{\dim(x)_-}{d-1} \quad \forall d > c,$$

woraus wir $\operatorname{grad}(x)_- \geq n$ schließen können. □

Nach 4.12(c) und dem vorhergehenden Satz sind für eine Nebenklasse $\mathfrak{D} \in \mathcal{D}/(K^*)$ von (K^*) in $\mathcal{D}$ die Zahlen $\dim \mathfrak{d}$ und $\operatorname{grad} \mathfrak{d}$ von der Wahl des Repräsentanten $\mathfrak{d} \in \mathfrak{D}$ unabhängig.

4.17 Definition. *Sei $\mathfrak{D} \in \mathcal{D}/(K^*)$. Wir setzen $\dim \mathfrak{D} := \dim \mathfrak{d}$ und $\operatorname{grad} \mathfrak{D} := \operatorname{grad} \mathfrak{d}$ für $\mathfrak{d} \in \mathfrak{D}$ beliebig.*

d. Geschlecht. Nach dem Beweis von 4.15 existiert zu jedem $x \in K \setminus k$ ein $c \geq 0$, so daß

$(*)$ $\quad \operatorname{grad} d(x)_- - \dim d(x)_- \leq (c-1)[K : k(x)] \quad \forall d \geq c.$

Dies veranlaßt uns zu der folgenden Definition.

4.18 Definition. *Die Zahl*

$$g := g_K := \max\{\operatorname{grad} \mathfrak{d} - \dim \mathfrak{d} + 1 \,:\, \mathfrak{d} \in \mathcal{D}\}$$

heißt das **Geschlecht von** K.

4.19 Satz. *Es gilt*

(a) $0 \leq g < \infty$ *und*

(b) $\dim \mathfrak{d} \geq \operatorname{grad} \mathfrak{d} + 1 - g$ *für alle* $\mathfrak{d} \in \mathcal{D}$ *(Riemannsche Ungleichung).*

Beweis. **(a)** Wegen $\operatorname{grad} \mathfrak{o} - \dim \mathfrak{o} + 1 = 0 - 1 + 1 = 0$ ist $g \geq 0$. Bleibt $g < \infty$ zu beweisen. Wir wählen $x \in K \setminus k$. Nach $(*)$ genügt es, zu zeigen, daß für einen beliebigen Divisor $\mathfrak{d} = \sum_v d_v \mathfrak{p}_v \in \mathcal{D}$ ein $d \geq 0$ existiert mit

$$\operatorname{grad} \mathfrak{d} - \dim \mathfrak{d} \leq \operatorname{grad} d(x)_- - \dim d(x)_-.$$

Für normiertes, irreduzibles $p \in k[x]$ setzen wir $m_p := \max\{d_v \,:\, v \in V, v/v_p\}$ und definieren

$$y := \prod_{m_p \geq 0} p^{m_p} \in k[x],$$

dann ist $(y) \geq \mathfrak{d} - d(x)_-$ für ein genügend großes $d \in \mathbb{N}_0$. Mit 4.12 und 4.15 folgt

$$\operatorname{grad} \mathfrak{d} - \dim \mathfrak{d} \leq \operatorname{grad}(d(x)_- + (y)) - \dim(d(x)_- + (y)) = \operatorname{grad} d(x)_- - \dim d(x)_-.$$

(b) Folgt sofort aus der Definition von g.

□

4.20 Korollar.

(a) *Für* $K = k(x)$ *ist* $g = 0$.

(b) *Ist* $g = 0$, *so ist* $h_0 = 1$.

Beweis. **(a)** Nach dem vorigen Beweis ist

$$g = \max\{\operatorname{grad} d(x)_- - \dim d(x)_- + 1 \,:\, d \geq 0\}.$$

Wegen 4.3 haben wir für $d \geq 0$, daß $\operatorname{grad} d(x)_- = d$ ist und $\mathcal{L}(d(x)_-) = \{z \in k[x] \,:\, \operatorname{grad} z \leq d\}$ Dimension $d+1$ über k hat.

(b) Sei $g = 0$ und $\mathfrak{d} \in \mathcal{D}_0$. Dann gilt $\dim \mathfrak{d} \geq 0 + 1 - 0 = 1$ nach 4.19(b), also können wir $y \in K^*$ wählen mit $\mathfrak{d} + (y) \geq \mathfrak{o}$. Da andererseits $\operatorname{grad}(\mathfrak{d} + (y)) = 0$ ist, folgt $\mathfrak{d} = (\frac{1}{y}) \in (K^*)$.

□

In die Riemannsche Ungleichung läßt sich ein Korrekturterm einfügen. Wir erhalten den wichtigen

4.21 Satz von Riemann-Roch. *Sei $\mathfrak{d} \in \mathcal{D}$. Dann ist*

$$\dim \mathfrak{d} = \operatorname{grad} \mathfrak{d} + 1 - g + \dim_k \mathcal{A}/(\mathcal{A}(\mathfrak{d}) + K).$$

Beweis. Nach Definition des Geschlechts existiert ein Divisor $\mathfrak{d}_0 \in \mathcal{D}$ mit $g = \operatorname{grad} \mathfrak{d}_0 - \dim \mathfrak{d}_0 + 1$. Für jedes $\mathfrak{a} \in \mathcal{D}$ mit $\mathfrak{a} \geq \mathfrak{d}_0$ folgt mithilfe von 4.12, daß

$$\begin{aligned} \dim_k (\mathcal{A}(\mathfrak{a}) + K)/(\mathcal{A}(\mathfrak{d}_0) + K) &= \operatorname{grad} \mathfrak{a} - \dim \mathfrak{a} - (\operatorname{grad} \mathfrak{d}_0 - \dim \mathfrak{d}_0) \\ &\leq g - 1 - (g - 1) \\ &= 0, \end{aligned}$$

also $\mathcal{A}(\mathfrak{a}) + K = \mathcal{A}(\mathfrak{d}_0) + K$ und $\operatorname{grad} \mathfrak{a} - \dim \mathfrak{a} = g - 1$. Daher gilt

$$\mathcal{A} = \bigcup_{\mathfrak{a} \in \mathcal{D}} \mathcal{A}(\mathfrak{a}) = \bigcup_{\substack{\mathfrak{a} \in \mathcal{D} \\ \mathfrak{a} \geq \mathfrak{d}_0}} \mathcal{A}(\mathfrak{a}) = \mathcal{A}(\mathfrak{d}_0) + K.$$

Wählen wir nun $\mathfrak{d}_1 \in \mathcal{D}$ mit $\mathfrak{d}_1 \geq \mathfrak{d}$ und $\mathfrak{d}_1 \geq \mathfrak{d}_0$, so ist

$$\dim_k \mathcal{A}/(\mathcal{A}(\mathfrak{d}) + K) = \operatorname{grad} \mathfrak{d}_1 - \dim \mathfrak{d}_1 - (\operatorname{grad} \mathfrak{d} - \dim \mathfrak{d}) = g - 1 - \operatorname{grad} \mathfrak{d} + \dim \mathfrak{d}.$$

□

e. Differentiale. Statt der Räume $\mathcal{A}/(\mathcal{A}(\mathfrak{d}) + K)$ betrachten wir lieber ihre Dualräume.

4.22 Definition. *Für $\mathfrak{d} \in \mathcal{D}$ definieren wir den k-Vektorraum*

$$\Omega(\mathfrak{d}) := \Omega_K(\mathfrak{d}) := \{\omega \in \operatorname{Hom}_k(\mathcal{A}, k) \,:\, \omega(\mathcal{A}(\mathfrak{d}) + K) = 0\}.$$

Desweiteren setzen wir

$$\Omega := \Omega_K := \bigcup_{\mathfrak{d} \in \mathcal{D}} \Omega(\mathfrak{d}).$$

Die Elemente von Ω heißen **(Weil-)Differentiale**.

Offenbar gilt $\Omega(\mathfrak{d}) \simeq \operatorname{Hom}_k(\mathcal{A}/(\mathcal{A}(\mathfrak{d}) + K), k) \simeq \mathcal{A}/(\mathcal{A}(\mathfrak{d}) + K)$ als k-Vektorräume. Daher können wir den Satz von Riemann-Roch umformulieren in

$$\dim \mathfrak{d} = \operatorname{grad} \mathfrak{d} + 1 - g + \dim_k \Omega(\mathfrak{d}).$$

Insbesondere gilt $g = \dim_k \Omega(\mathfrak{o})$.

4.23 Bemerkung. *Ω ist ein K-Untervektorraum von $\operatorname{Hom}_k(\mathcal{A}, k)$ bezüglich der Skalarmultiplikation*

$$(y\omega)(\alpha) := \omega(y\alpha)$$

für $y \in K$, $\omega \in \operatorname{Hom}_k(\mathcal{A}, k)$ und $\alpha \in \mathcal{A}$. Für $\mathfrak{a}, \mathfrak{b} \in \mathcal{D}$ gilt

$$\mathcal{L}(\mathfrak{a})\Omega(\mathfrak{b}) \subseteq \Omega(\mathfrak{b} - \mathfrak{a}).$$

BEWEIS. Klar, daß $\mathrm{Hom}_k(\mathcal{A}, k)$ wie angegeben ein K-Vektorraum wird. Die Abgeschlossenheit der Addition in Ω rechnet man ebenfalls leicht nach. Zum Nachweis der Abgeschlossenheit der Skalarmultiplikation schreiben wir $\mathfrak{a} = \sum_v a_v \mathfrak{p}_v$ und $\mathfrak{b} = \sum_v b_v \mathfrak{p}_v$. Sei $y \in \mathcal{L}(\mathfrak{a})$ und $\omega \in \Omega(\mathfrak{b})$. Für $\alpha = (x_v)_v \in \mathcal{A}(\mathfrak{b} - \mathfrak{a})$ gilt dann $v(x_v y) \geq a_v - b_v + v(y) \geq -b_v$ für alle $v \in V$, also $y\alpha \in \mathcal{A}(\mathfrak{b})$, d. h. $(y\omega)(\alpha) = 0$. Da trivialerweise $(y\omega)(K) = 0$ ist, folgt $y\omega \in \Omega(\mathfrak{b} - \mathfrak{a})$. □

Ist $\operatorname{grad} \mathfrak{d}$ genügend groß, so tritt in der Riemannschen Ungleichung das Gleichheitszeichen ein:

4.24 LEMMA. *Sei $\mathfrak{d} \in \mathcal{D}$. Ist $\operatorname{grad} \mathfrak{d} > 2g - 2$, so gilt $\Omega(\mathfrak{d}) = 0$.*

BEWEIS. Angenommen, $\Omega(\mathfrak{d}) \neq 0$. Dann können wir $\omega \in \Omega(\mathfrak{d})$ mit $\omega \neq 0$ wählen und nach der vorigen Bemerkung einen injektiven k-Vektorraumhomomorphismus

$$\begin{array}{ccc} \mathcal{L}(\mathfrak{d}) & \hookrightarrow & \Omega(\mathfrak{o}) \\ y & \mapsto & y\omega \end{array}$$

definieren. Es folgt $\dim \mathfrak{d} \leq \dim_k \Omega(\mathfrak{o}) = g$, also nach dem Satz von Riemann-Roch:

$$\operatorname{grad} \mathfrak{d} = \dim \mathfrak{d} - 1 + g - \dim_k \Omega(\mathfrak{d}) \leq g - 1 + g - 1 = 2g - 2.$$

□

4.25 SATZ. $\dim_K \Omega = 1$.

BEWEIS. Es ist $\Omega \neq 0$, denn für $\mathfrak{d} \in \mathcal{D}$ mit $\operatorname{grad} \mathfrak{d} \leq -2$ hat $\Omega(\mathfrak{d})$ nach dem Satz von Riemann-Roch k-Dimension $\dim \mathfrak{d} - 1 + g - \operatorname{grad} \mathfrak{d} \geq 1$. Angenommen, $\omega_1, \omega_2 \in \Omega$ sind linear unabhängig über K. Wir wählen $\mathfrak{d}_0, \mathfrak{d} \in \mathcal{D}$, so daß $\omega_1, \omega_2 \in \Omega(\mathfrak{d}_0)$, $\mathfrak{d} \geq \mathfrak{d}_0$, $\mathfrak{d} \neq \mathfrak{d}_0$ und

$(*)$ $\quad \operatorname{grad} \mathfrak{d} + \operatorname{grad} \mathfrak{d}_0 > 3g - 3.$

Sei $y_1, \ldots, y_m$ eine k-Basis von $\mathcal{L}(\mathfrak{d})$, dann sind $y_1\omega_1, \ldots, y_m\omega_1, y_1\omega_2, \ldots, y_m\omega_2 \in \Omega(\mathfrak{d}_0 - \mathfrak{d})$ linear unabhängig über k, also gilt

$$2 \dim \mathfrak{d} \leq \dim_k \Omega(\mathfrak{d}_0 - \mathfrak{d}).$$

Mithilfe von 4.19(b) und dem Satz von Riemann-Roch folgt

$$2(\operatorname{grad} \mathfrak{d} + 1 - g) \leq 2 \dim \mathfrak{d} \leq \dim(\mathfrak{d}_0 - \mathfrak{d}) - 1 + g - \operatorname{grad}(\mathfrak{d}_0 - \mathfrak{d}),$$

nach 4.12(b) also $\operatorname{grad} \mathfrak{d} + \operatorname{grad} \mathfrak{d}_0 \leq 3g - 3$ im Widerspruch zu $(*)$. □

4.26 LEMMA UND DEFINITION. *Sei $0 \neq \omega \in \Omega$.*

(a) *Es existiert genau ein Divisor $\mathfrak{c} \in \mathcal{D}$, so daß für alle $\mathfrak{d} \in \mathcal{D}$ gilt:*

$$\omega \in \Omega(\mathfrak{d}) \iff \mathfrak{d} \leq \mathfrak{c}.$$

$(\omega) := \mathfrak{c}$ heißt der **(kanonische) Divisor zu** *ω.*

(b) *Für $y \in K^*$ ist $(y\omega) = (y) + (\omega)$.*

BEWEIS. **(a)** Nach 4.24 existiert ein Divisor $\mathfrak{c} = \sum_v c_v \mathfrak{p}_v \in \mathcal{D}$ von maximalem Grad mit $\omega \in \Omega(\mathfrak{c})$. Für $\mathfrak{d} = \sum_v d_v \mathfrak{p}_v \in \mathcal{D}$ setzen wir $\mathfrak{d}' := \sum_v d'_v \mathfrak{p}_v$ mit $d'_v := \max\{c_v, d_v\}$. Damit haben wir $\mathfrak{c}, \mathfrak{d} \leq \mathfrak{d}'$ und somit $\mathcal{A}(\mathfrak{c}), \mathcal{A}(\mathfrak{d}) \subseteq \mathcal{A}(\mathfrak{d}')$. Man überlegt sich leicht, daß sogar $\mathcal{A}(\mathfrak{d}') = \mathcal{A}(\mathfrak{c}) + \mathcal{A}(\mathfrak{d})$ gilt. Daher haben wir

$$\omega \in \Omega(\mathfrak{d}) \iff \omega \in \Omega(\mathfrak{d}') \iff \mathfrak{d}' = \mathfrak{c} \iff \mathfrak{d} \leq \mathfrak{c}.$$

Die Eindeutigkeit von $\mathfrak{c}$ ist klar.

(b) Nach 4.23 haben wir $y\omega \in \Omega((\omega) + (y))$, also $(y) + (\omega) \leq (y\omega)$. Ebenso $(y\omega) - (y) = (y\omega) + (\frac{1}{y}) \leq (\omega)$.

□

Aus 4.25 und 4.26 folgt, daß $\{(\omega) : 0 \neq \omega \in \Omega\}$ eine Nebenklasse von (K^*) in $\mathcal{D}$ ist.

4.27 DEFINITION. $\mathfrak{C} := \mathfrak{C}_K := \{(\omega) : 0 \neq \omega \in \Omega\}$ *heißt die* **kanonische Klasse (von K)**.

Wir können jetzt den Satz von Riemann-Roch in eine neue Fassung bringen und daraus die Zahlen $\dim \mathfrak{C}$ und $\operatorname{grad} \mathfrak{C}$ berechnen.

4.28 BEMERKUNG. *Sei* $\mathfrak{c} \in \mathfrak{C}$.

(a) *Für alle* $\mathfrak{d} \in \mathcal{D}$ *gilt*

$$\dim \mathfrak{d} = \operatorname{grad} \mathfrak{d} + 1 - g + \dim(\mathfrak{c} - \mathfrak{d}).$$

(b) $\dim \mathfrak{c} = g$.

(c) $\operatorname{grad} \mathfrak{c} = 2g - 2$.

BEWEIS. **(a)** Sei $0 \neq \omega \in \Omega$ mit $\mathfrak{c} = (\omega)$. Für $y \in K^*$ gilt

$$y\omega \in \Omega(\mathfrak{d}) \iff \mathfrak{d} \leq (y\omega) = (y) + (\omega) \iff y \in \mathcal{L}((\omega) - \mathfrak{d}).$$

Daher haben wir einen k-Vektorraumisomorphismus

$$\begin{array}{ccc} \mathcal{L}(\mathfrak{c} - \mathfrak{d}) & \simeq & \Omega(\mathfrak{d}) \\ y & \mapsto & y\omega. \end{array}$$

(b) Folgt aus (a) für $\mathfrak{d} = \mathfrak{o}$.

(c) Folgt aus (a) und (b) mit $\mathfrak{d} = \mathfrak{c}$.

□

f. Konstantenkörpererweiterung. Wir wollen Erweiterungen von K/k betrachten, die allein durch Vergrößern des Konstantenkörpers zustandekommen. Für diese ändert sich, wie wir in 4.32 sehen werden, das Geschlecht nicht.

4.29 DEFINITION. *Ein algebraischer Funktionenkörper K'/k' mit $k \subseteq k'$ und $K \subseteq K'$ heißt* **Konstantenkörpererweiterung von** *K/k, falls k'/k endlich und $K' = Kk'$ ist.*

4.30 LEMMA. *Sei $k' = k(\alpha)$ eine einfache, endliche Erweiterung von k. Dann gilt:*

(a) *Das Minimalpolynom von α über k ist auch irreduzibel über K.*

(b) *Es gibt einen bis auf Isomorphie eindeutig bestimmten Körper K', so daß K'/k' eine Konstantenkörpererweiterung von K/k ist.*

BEWEIS. Sei X transzendent über K und $f \in k[X]$ das Minimalpolynom von α über k.

(a) Angenommen, es ist $f = gh$ mit normierten Polynomen $g, h \in K[X]$. Dann sind die Koeffizienten von g und h als elementarsymmetrische Funktionen in den Nullstellen von f algebraisch über k. Da k algebraisch abgeschlossen ist in K, folgt $g, h \in k[X]$ und damit $g = 1$ oder $h = 1$.

(b) Wir identifizieren k' mit $k[X]/(f)$ und setzen $K' := K[X]/(f)$, wobei wir die kanonischen Einbettungen $k' \hookrightarrow K'$ und $K \hookrightarrow K'$ als Inklusionen auffassen. Dann ist $K' = Kk'$ und $[K' : K] = [k' : k] < \infty$ nach (a), also K'/k' Konstantenkörpererweiterung von K/k. Ist K' irgendein Körper mit $K' = Kk'$, so ist $K' = K(\alpha) \simeq K[X]/(f)$ nach (a).

□

Bei der obigen Konstruktion ist nicht gewährleistet, daß k' auch wieder der Konstantenkörper von K'/k' ist. Dafür brauchen wir in der Tat mehr Voraussetzungen. Im folgenden sei k stets vollkommen und k'/k endlich. Wir können dann $k' = k(\alpha)$ schreiben und haben nach dem vorigen Lemma eine eindeutige Konstantenkörpererweiterung K'/k' von K/k.

4.31 LEMMA. *K'/K ist eine endliche, separable Erweiterung vom Grad $[K' : K] = [k' : k]$, und k' ist der Konstantenkörper von K'/k'.*

BEWEIS. Es ist $K' = K(\alpha)$, also K'/K separabel und $[K' : K] = [k' : k]$ nach dem vorigen Lemma. Sei $\beta \in K'$ algebraisch über k'. Dann ist $k'' := k'(\beta)$ endlich und separabel über k, etwa $k'' = k(\alpha')$, und $K' = Kk'' = K(\alpha')$. Wiederum mit dem vorigen Lemma folgt $[K' : K] = [k'' : k]$, also ist $k'' = k'$ und $\beta \in k'$. □

Wir wollen nun die wesentlichen Eigenschaften von Konstantenkörpererweiterungen in einem abschließenden Satz zusammenfassen. Zur Abkürzung führen wir die Bezeichnungen $V' := V(K'/k') = V(K'/k)$ für die abstrakte Kurve, $\mathcal{D}' := \mathcal{D}_{K'}$ für die Divisorengruppe und $g' := g_{K'}$ für das Geschlecht von K' ein. Zu $\mathfrak{d} = \sum_{v \in V} d_v \mathfrak{p}_v \in \mathcal{D}$ definieren wir $\mathfrak{d}' := \sum_{v \in V} d_v \sum_{v'/v} e_{v'/v} \mathfrak{p}_{v'} \in \mathcal{D}'$.

4.32 SATZ.

(a) *Für $v \in V$ und $v' \in V'$ mit v'/v gilt $e_{v'/v} = 1$ und $k_{v'} = k_v k'$.*

(b) *Für $\mathfrak{d} \in \mathcal{D}$ gilt* $\operatorname{grad} \mathfrak{d}' = \operatorname{grad} \mathfrak{d}$ *und*

(c) $\dim \mathfrak{d}' = \dim \mathfrak{d}$.

(d) $g' = g$.

BEWEIS. Sei $n := [k' : k]$.

(a) Sei B_v der ganze Abschluß von R_v in K'. Wegen $D_{K'/K}(\alpha) = D_{k'/k}(\alpha) \in k^* \subseteq R_v^*$ ist $B_v = R_v[\alpha]$ und v unverzweigt in K'/K nach 1.26. Der Fortsetzung v' von v entspricht ein maximales Ideal $Q_{v'}$ von B_v gemäß 1.23(a), so daß

$$k_{v'} \simeq B_v/Q_{v'} \simeq k_v[\alpha] = k_v k'.$$

(b) Es genügt offenbar, die Behauptung für einen Primdivisor $\mathfrak{d} = \mathfrak{p}_v$ mit $v \in V$ zu zeigen. Mithilfe von 1.23(b) und 4.31 erhalten wir

$$\operatorname{grad} \mathfrak{p}'_v = \sum_{v'/v} [k_{v'} : k'] = \frac{[k_v : k]}{[k' : k]} \sum_{v'/v} f_{v'/v} = [k_v : k] = \operatorname{grad} \mathfrak{p}_v.$$

(c) Sei f das Minimalpolynom von α über k, k'' ein Zerfällungskörper von f über k, der k' enthält, und $K'' := Kk''$, dann ist K''/k'' Konstantenkörpererweiterung von K/k und K''/K galoissch (normale Hülle von K'/K). Wir wählen $\sigma_1, \ldots, \sigma_n \in \operatorname{Aut}(K''/K)$ so, daß $\alpha_1 := \sigma_1(\alpha), \ldots, \alpha_n := \sigma_n(\alpha) \in k''$ die Nullstellen von f sind. Desweiteren setzen wir $\mathfrak{d}'' := \sum_{v \in V} d_v \sum_{v''/v} \mathfrak{p}_{v''} \in \mathcal{D}'' := \mathcal{D}_{K''}$ analog zu den Bezeichnungen von oben, dann haben wir offenbar

$$\mathcal{L}(\mathfrak{d}) = \mathcal{L}(\mathfrak{d}') \cap K = \mathcal{L}(\mathfrak{d}'') \cap K.$$

Sei nun $(y_1, \ldots, y_m)$ eine k-Basis von $\mathcal{L}(\mathfrak{d})$. Wir wollen zeigen, daß diese auch eine k'-Basis von $\mathcal{L}(\mathfrak{d}')$ ist. Es ist leicht zu überprüfen, daß $y_1, \ldots, y_m$ linear unabhängig über k' sind. Bleibt also

$$\mathcal{L}(\mathfrak{d}') \subseteq k'y_1 + \cdots + k'y_m$$

zu zeigen. Sei $z \in \mathcal{L}(\mathfrak{d}') \subseteq \mathcal{L}(\mathfrak{d}'')$, $z = \sum_{j=0}^{n-1} z_j \alpha^j$ mit $z_j \in K$. Nach 2.1(b) ist dann auch $\sigma_i(z) = \sum_{j=0}^{n-1} z_j \alpha_i^j \in \mathcal{L}(\mathfrak{d}'')$ für $1 \le i \le n$. Mithilfe der Cramerschen Regel folgt für $1 \le l \le n$:

$$\begin{aligned} z_l &= (\det(\alpha_i^j)_{i,j})^{-1} \det \begin{pmatrix} 1 & \cdots & \alpha_1^{l-1} & \sigma_1(z) & \alpha_1^{l+1} & \cdots & \alpha_1^n \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 1 & \cdots & \alpha_n^{l-1} & \sigma_n(z) & \alpha_n^{l+1} & \cdots & \alpha_n^n \end{pmatrix} \\ &\in K \cap \sum_{i=1}^{n} k'' \sigma_i(z) \subseteq \mathcal{L}(\mathfrak{d}). \end{aligned}$$

Wir können daher $z_j = \sum_{i=1}^{m} \gamma_{ij} y_i$ schreiben mit $\gamma_{ij} \in k$ für $1 \le i \le m$ und $0 \le j < n$ und erhalten

$$z = \sum_{i=1}^{m} \sum_{j=0}^{n-1} \gamma_{ij} \alpha^j y_i \in k'y_1 + \cdots + k'y_m.$$

(d) Wählen wir $\mathfrak{d} \in \mathcal{D}$ mit $\operatorname{grad} \mathfrak{d} > 2g - 2, 2g' - 2$, so folgt nach (b), (c), 4.24 und dem Satz von Riemann-Roch

$$g = \operatorname{grad} \mathfrak{d} - \dim \mathfrak{d} + 1 = \operatorname{grad} \mathfrak{d}' - \dim \mathfrak{d}' + 1 = g'.$$

□

5 Die Geschlechtsformel von Riemann-Hurwitz

Haben wir zum Schluß des letzten Abschnitts Erweiterungen algebraischer Funktionenkörper betrachtet, die allein auf einer Vergrößerung des Konstantenkörpers beruhten, so wollen wir jetzt den gerade entgegengesetzten Fall untersuchen. Es seien K und L algebraische Funktionenkörper über k, so daß L/K eine endliche, separable Erweiterung vom Grad $n \in \mathbb{N}$ und k der Konstantenkörper von L/k (damit auch von K/k) ist. Unser Ziel ist es, eine Formel

anzugeben, mit der sich das Geschlecht von L aus dem Geschlecht von K berechnen läßt. Wir setzen zur Abkürzung $V := V(K/k)$ und bezeichnen für $v \in V$ mit B_v den ganzen Abschluß des Bewertungsrings R_v in L. Bevor wir unsere Geschlechtsformel hinschreiben, führen wir noch einige Begriffe ein.

5.1 Bemerkung und Definition.

(a) *Sei $v \in V$. B_v und sein* **Komplementärmodul** $B_v^\# := \{y \in L : S_{L/K}(xy) \in R_v \ \forall x \in B_v\}$ *(bezüglich der Spur) sind freie R_v-Moduln vom Rang n. Für Basen $(x_1, \ldots, x_n)$ bzw. $(y_1, \ldots, y_n)$ von B_v bzw. $B_v^\#$ hängt die Zahl*

$$d_{L,v} := v(D_{L/K}(x_1, \ldots, x_n)) = -v(D_{L/K}(y_1, \ldots, y_n)) \in \mathbb{N}_0$$

allein von L und v ab. Ferner gilt $D_{L/K}(x_1, \ldots, x_n)B_v^\# \subseteq B_v \subseteq B_v^\#$.

(b) *Für fast alle $v \in V$ ist $d_{L,v} = 0$.*

Beweis. **(a)** Nach 1.5(d) gibt es eine R_v-Basis $(x_1, \ldots, x_n)$ von B_v, die zugleich eine K-Basis von L ist, und nach 1.5(b) und (c) hängt die Zahl $d_{L,v} := v(D_{L/K}(x_1, \ldots, x_n)) \in \mathbb{N}_0$ nicht von der speziellen Wahl dieser Basis ab. Wegen 1.3(c) und 1.4(c) ist die Abbildung

$$\begin{aligned} L \times L &\to K \\ (x, y) &\mapsto S_{L/K}(xy) \end{aligned}$$

eine nicht-singuläre, symmetrische Bilinearform. Bezüglich ihr existiert eine Komplementärbasis, d. h. eine K-Basis $(x_1', \ldots, x_n')$ von L mit

$$S_{L/K}(x_i x_j') = \delta_{ij} \quad \forall i, j.$$

Für beliebiges $y = \sum a_j x_j' \in L$ gilt offenbar

$$y \in B_v^\# \iff \forall i : a_i = S_{L/K}(x_i y) \in R_v,$$

also ist $(x_1', \ldots, x_n')$ eine R_v-Basis von $B_v^\#$. Wegen 1.4(e) ist $B_v \subseteq B_v^\#$. Daher existieren $a_{ij} \in R_v$ mit

$$x_i = \sum_{j=1}^{n} a_{ij} x_j'.$$

Es ergibt sich $a_{ij} = S_{L/K}(x_i x_j)$, also $D_{L/K}(x_1, \ldots, x_n) = \det(a_{ij})_{i,j}$ nach 1.3(c). Sei $(a_{ij}')_{i,j} := (a_{ij})_{i,j}^{-1} \in K^{n \times n}$ die inverse Matrix. Wegen

$$x_i' = \sum_{j=1}^{n} a_{ij}' x_j$$

ergibt sich analog $D_{L/K}(x_1', \ldots, x_n') = \det(a_{ij}')_{i,j}$, also gilt $v(D_{L/K}(y_1, \ldots, y_n)) = -d_{L,v}$ für jede beliebige R_v-Basis $y_1, \ldots, y_n$ von $B_v^\#$ nach 1.5(b). Ferner gilt nach der Cramerschen Regel $a_{ij}' D_{L/K}(x_1, \ldots, x_n) \in R_v$ für alle i, j, also haben wir $D_{L/K}(x_1, \ldots, x_n)x_i' \in B_v$ für $1 \le i \le n$, woraus die letzte Behauptung folgt.

(b) Wir schreiben $L = K(y)$. Sei $f = \sum_{i=0}^{n} a_i X^i$ das Minimalpolynom von y über K. Nach 4.8(b) gilt für fast alle $v \in V$, daß $a_0, \ldots, a_n \in R_v$ und $D_{L/K}(y) \in R_v^*$, d. h. nach 1.26, daß $d_{L,v} = v(D_{L/K}(y)) = 0$ ist.

□

Wir können nun die zentrale Aussage dieses Abschnitts formulieren.

5.2 Satz von Riemann-Hurwitz. *Für die Geschlechter g_K und g_L von K bzw. L gilt die Beziehung*

$$2g_L - 2 = (2g_K - 2)n + \sum_{v \in V} d_{L,v} f_v.$$

Für den Beweis sind einige Vorbereitungen erforderlich.

5.3 Lemma. *Sei R ein Bewertungsring. Sind M und N freie R-Moduln vom Rang $m \in \mathbb{N}$ mit $M \subseteq N$, so existiert eine R-Basis $(z_1, \ldots, z_m)$ von N und $a_1, \ldots, a_m \in R$, so daß $(a_1 z_1, \ldots, a_m z_m)$ eine R-Basis von M ist.*

Beweis. Sei v die zu R korrespondierende Bewertung auf dem Quotientenkörper von R gemäß 1.16. Seien $(x_1, \ldots, x_m)$ und $(y_1, \ldots, y_m)$ beliebige R-Basen von M bzw. N. Wegen $M \subseteq N$ existiert eine Matrix $A = (a_{ij})_{i,j} \in R^{m \times m}$ mit

$$\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = A \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}.$$

Nach eventueller Umordnung der Basen können wir dabei $v(a_{11}) = \min\{v(a_{ij}) : 1 \leq i, j \leq m\}$, d. h. $\frac{a_{ij}}{a_{11}} \in R$ für alle i, j annehmen. Setzen wir $z_1 := y_1 + \sum_{j=2}^{m} \frac{a_{1j}}{a_{11}} y_j$ und $x_i' := x_i - \frac{a_{i1}}{a_{11}} x_1$ für $2 \leq i \leq m$, so sind $(x_1, x_2', \ldots, x_m')$ und $(z_1, y_2, \ldots, y_m)$ weiterhin R-Basen von M bzw. N und

$$\begin{pmatrix} x_1 \\ x_2' \\ \vdots \\ x_m' \end{pmatrix} = \begin{pmatrix} a_{11} & 0 \cdots 0 \\ 0 & \\ \vdots & A' \\ 0 & \end{pmatrix} \begin{pmatrix} z_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$$

mit $A' = (a_{ij} - \frac{a_{1j}}{a_{11}})_{2 \leq i,j \leq m}$. Die Fortsetzung dieses Verfahrens liefert die Behauptung. □

5.4 Satz. *Sei $v \in V$.*

(a) *Es gibt einen eindeutig bestimmten Divisor $\mathfrak{d}_{L,v} \geq \mathfrak{o}$ von L der Form $\mathfrak{d}_{L,v} = \sum_{w/v} d_{w/v} \mathfrak{p}_w$, so daß*

$$B_v^{\#} = \{y \in L : w(y) \geq -d_{w/v} \, \forall w/v\}.$$

(b) *Für alle w/v gilt $d_{w/v} \geq e_{w/v} - 1$.*

(c) *Ist w/v zahm verzweigt, so gilt sogar $d_{w/v} = e_{w/v} - 1$.*

(d) $\operatorname{grad} \mathfrak{d}_{L,v} = d_{L,v} f_v$.

Beweis. Wir setzen zur Abkürzung $d_v := d_{L,v}$ und $e_w := e_{w/v}$ und wählen $t_v \in R_v$ mit $v(t_v) = 1$. Nach 1.23 ist B_v ein Dedekindring mit den maximalen Idealen $Q_w := B_v \cap P_w$, w/v, also

$$t_v B_v = \prod_{w/v} Q_w^{e_w}.$$

(a) Nach 5.1(a) ist $t_v^{d_v} B_v^{\#}$ ein Ideal von B_v. Wir können daher

$$(1) \quad t_v^{d_v} B_v^{\#} = \prod_{w/v} Q_w^{c_w}$$

mit $c_w \in \mathbb{N}_0$ schreiben. Damit gilt für $y \in L$ nach 1.8(c)

$$(2) \quad y \in B_v^{\#} \iff t_v^{d_v} y \in \prod_{w/v} Q_w^{c_w} \iff \forall w/v : d_v e_w + w(y) \geq c_w.$$

Also ist $\mathfrak{d}_{L,v} := \sum_{w/v} d_{w/v} \mathfrak{p}_w$ mit $d_{w/v} := d_v e_w - c_w$ der gesuchte Divisor. Wegen $t_v^{d_v} B_v \subseteq t_v^{d_v} B_v^{\#}$ ist $d_v e_w \geq c_w$ für alle w/v, also $\mathfrak{d}_{L,v} \geq \mathfrak{o}$. Die Eindeutigkeit von $\mathfrak{d}_{L,v}$ folgt aus (2) und 1.8(a).

Zur Abkürzung setzen wir für den Rest des Beweises $d_w := d_{w/v}$.

(b) Sei L' normale Hülle von L/K, $G' := \mathrm{Aut}(L'/K)$ und $H := \{\sigma'|_L : \sigma' \in G'\}$ die Menge der K-Homomorphismen von L nach L'. Es genügt, für $I := \prod_{w/v} Q_w$ zu zeigen, daß $t_v^{d_v - 1} I \subseteq t_v^{d_v} B_v^{\#}$ ist. Mit (1) und 1.8(c) folgt dann nämlich $(d_v - 1)e_w + 1 \geq c_w$, d. h. $d_w = d_v e_w - c_w \geq e_w - 1$. Sei also $\alpha \in I$ und $x \in B_v$. Dann gilt $w'(\alpha x) > 0$ für alle Bewertungen w' von L' mit w'/v. Nach 2.1(b) folgt

$$w'(S_{L/K}(\alpha x)) \geq \min\{w'(\sigma(\alpha x)) : \sigma \in H\} > 0 \quad \forall w'/v,$$

daher $S_{L/K}(t_v^{-1}\alpha x) = t_v^{-1} S_{L/K}(\alpha x) \in R_v$. Somit ist $t_v^{-1} I \subseteq B_v^{\#}$, d. h. $t_v^{d_v - 1} I \subseteq t_v^{d_v} B_v^{\#}$ gezeigt.

(c) Für unsere späteren Zwecke benötigen wir diese Aussage nur im Fall, daß L/K galoissch ist. Es soll daher reichen, sie hier für diesen Fall zu zeigen. Einen allgemeinen Beweis, der allerdings nicht ohne Komplettierungsmethoden auskommt, findet der/die LeserIn in [Cv, p. 69f].

Sei $G := \mathrm{Aut}(L/K)$ und w/v zahm verzweigt. Für $I_w := \prod_{\substack{\tilde{w}/v \\ \tilde{w} \neq w}} Q_{\tilde{w}}$ gilt nach 1.8(c) und Teil (b) dieses Beweises

$$d_w \geq e_w \iff (d_v - 1)e_w \geq c_w \iff t_v^{d_v - 1} I_w \subseteq t_v^{d_v} B_v^{\#}.$$

Es genügt also zu zeigen, daß ein $\alpha \in I_w$ existiert mit $t_v^{-1}\alpha \notin B_v^{\#}$. Wir identifizieren wie üblich k_w mit B_v/Q_w und bezeichnen mit $^-$ die Restklassenabbildung $B_v \to k_w$ bzw. $R_v \to k_v$. Nach Voraussetzung und 2.1(a) ist k_w/k_v galoissch, und nach dem Lemma von Dedekind existiert ein $x \in B_v$ mit $S_{k_w/k_v}(\overline{x}) \neq 0$. Wie in 2.2 sei $\overline{G}_w := \mathrm{Aut}(k_w/k_v)$, G_w^- die Zerlegungs- und G_w^+ die Trägheitsgruppe von w/v, weiter w^- die Bewertung des Zerlegungskörpers $L_w^- := \mathrm{Fix}(L, G_w^-)$ mit w/w^-. Nach 2.2(c) ist dann $\#G_w^+ = [L : L_w^-]/[k_w : k_v] = e_{w/w^-}$ ein Teiler von e_w, also gilt nach Voraussetzung

$$(3) \quad 0 \neq e_{w/w^-} S_{k_w/k_v}(\overline{x}) = \#G_w^+ \sum_{\psi \in \overline{G}_w} \psi(\overline{x}) = \sum_{\sigma \in G_w^-} \overline{\sigma(x)}.$$

Nach 1.19 existiert ein $\alpha \in L$ mit

$$\begin{aligned} w(\alpha - 1) &> 0 \quad \text{und} \\ \tilde{w}(\alpha) &> 0 \quad \forall \tilde{w}/v,\ \tilde{w} \neq w. \end{aligned}$$

Damit ist offenbar $\alpha \in I_w$. Angenommen, daß $t_v^{-1}\alpha \in B_v^{\#}$ ist, dann gilt $S_{L/K}(t_v^{-1}\alpha x) \in R_v$. Da außerdem $w^\sigma(\alpha x) > 0$ ist für alle $\sigma \in G \setminus G_w^-$, folgt

$$\sum_{\sigma\in G_w^-} \sigma(\alpha x) = S_{L/K}(\alpha x) - \sum_{\sigma\in G\setminus G_w^-} \sigma(\alpha x) \in P_w \cap B_v = Q_w,$$

wegen $\overline{\alpha} = 1$ also

$$0 = \sum_{\sigma\in G_w^-} \overline{\sigma(\alpha x)} = \sum_{\sigma\in G_w^-} \overline{\sigma(x)}$$

im Widerspruch zu (3).

(d) Zu w/v wählen wir $t_w \in L$ mit $w(t_w) = 1$. Nach (a) haben wir einen R_v-Modulhomomorphismus

$$\begin{aligned} B_v^{\#}/B_v &\to \prod_{w/v} R_w t_w^{-d_w}/R_w \\ y + B_v &\mapsto (y + R_w)_{w/v}, \end{aligned}$$

der nach 1.23(c) injektiv ist. Er ist auch surjektiv, denn zu $(y_w + R_w)_{w/v} \in \prod_{w/v} R_w t_w^{-d_w}/R_w$ existiert nach 1.19 ein $y \in L$ mit $w(y - y_w) \geq 0$, also $w(y) \geq -d_w$ und $y + R_w = y_w + R_w$ für alle w/v. Mithilfe von 4.5 erhalten wir

$$\dim_k B_v^{\#}/B_v = \sum_{w/v} \dim_k R_w/R_w t_w^{d_w} = \sum_{w/v} d_w f_w = \operatorname{grad} \mathfrak{d}_{L,v}.$$

Es bleibt $\dim_k B_v^{\#}/B_v = d_v f_v$ zu zeigen. Nach 5.3 existiert eine R_v-Basis $(z_1, \ldots, z_n)$ von $B_v^{\#}$ und $a_1, \ldots, a_n \in R_v$, so daß $(a_1 z_1, \ldots, a_n z_n)$ eine R_v-Basis von B_v ist. Daher ist $B_v^{\#}/B_v \simeq \bigoplus_{i=1}^n R_v/R_v a_i$ als k-Vektorraum, und wegen $D_{L/K}(a_1 z_1, \ldots, a_n z_n) = (a_1 \cdots a_n)^2 D_{L/K}(z_1, \ldots, z_n)$ und 5.1(a) hat man $d_v = v(a_1 \cdots a_n)$. Mithilfe von 4.5 folgt

$$\dim_k B_v/B_v^{\#} = \sum_{i=1}^n v(a_i) f_v = d_v f_v.$$

□

Aus den Aussagen (b)–(d) läßt sich eine Formel ablesen, um die $d_{L,v}$ direkt zu berechnen.

5.5 Korollar. *Für $v \in V$ ist*

(a) $d_{L,v} \geq \sum_{w/v} (e_{w/v} - 1) f_{w/v}$.

(b) *Ist v zahm verzweigt in L/K, so gilt in (a) das Gleichheitszeichen.*

Beweis. Es gilt

$$d_{L,v} f_v = \operatorname{grad} \mathfrak{d}_{L,v} = \sum_{w/v} d_{w/v} f_w = \sum_{w/v} d_{w/v} f_{w/v} f_v,$$

also folgt

(a) aus 5.4(b) und

(b) aus 5.4(c).

□

Nach 5.1(b) und 5.4 ist $\mathfrak{d}_{L,v} = \mathfrak{o}$ für fast alle $v \in V$. Daher ist die folgende Definition sinnvoll.

5.6 DEFINITION. *Der Divisor $\mathfrak{d}_{L,v} \in \mathcal{D}_L$ aus 5.4(a) heißt die* **(lokale) Differente von** v **in** L/K. *Setzt man alle lokalen Differenten zusammen, so erhält man den Divisor $\mathfrak{d}_{L/K} := \sum_{v\in V} \mathfrak{d}_{L,v}$ von L, den wir die* **(globale) Differente von** L/K *nennen wollen.*

Wir sehen jetzt, daß $\operatorname{grad} \mathfrak{d}_{L/K} = \sum_{v\in V} d_{L,v} f_v$ der 'Korrekturterm' in der Formel 5.2 ist. Die Zahlen $2g_K - 2$ und $2g_L - 2$ legen nahe, die Grade der kanonischen Divisoren von K und L miteinander zu vergleichen. Dafür müssen wir erklären, wie wir Divisoren und Differentiale von K nach L 'liften'.

5.7 DEFINITION. *Sei $\mathfrak{a} = \sum_v a_v \mathfrak{p}_v \in \mathcal{D}_K$ und $\mathfrak{b} = \sum_w b_w \mathfrak{p}_w \in \mathcal{D}_L$. Wir setzen $\mathfrak{a}_L := \sum_{v\in V} a_v \sum_{w/v} e_{w/v} \mathfrak{p}_w \in \mathcal{D}_L$. Desweiteren definieren wir kleinere Adleräume $\mathcal{A}_{L/K} := \{(y_w)_w \in \mathcal{A}_L : y_w = y_{\tilde{w}}$, falls w und $\tilde{w}$ dasselbe $v \in V$ fortsetzen$\}$ und $\mathcal{A}_{L/K}(\mathfrak{b}) := \mathcal{A}_L(\mathfrak{b}) \cap \mathcal{A}_{L/K}$. Dann läßt sich die Spur in L/K durch*

$$\begin{array}{rcl} \mathcal{A}_{L/K} & \to & \mathcal{A}_K \\ (y_w)_w & \mapsto & (x_v)_v \text{ mit } x_v := S_{L/K}(y_w) \text{ für } w/v \end{array}$$

auf die Adleringe fortsetzen und wird dort ebenfalls mit $S_{L/K}$ bezeichnet.

5.8 LEMMA. *Sei $0 \neq \omega \in \Omega_K$ und $\mathfrak{c} := (\omega)_L + \mathfrak{d}_{L/K} \in \mathcal{D}_L$.*

(a) *Für $\mathfrak{a} \in \mathcal{D}_K$ ist $\operatorname{grad} \mathfrak{a}_L = n \operatorname{grad} \mathfrak{a}$.*

(b) *Für $\mathfrak{b} \in \mathcal{D}_L$ ist die kanonische Einbettung*

$$\begin{array}{rcl} \mathcal{A}_{L/K}/(\mathcal{A}_{L/K}(\mathfrak{b}) + L) & \to & \mathcal{A}_L/(\mathcal{A}_L(\mathfrak{b}) + L) \\ \alpha + (\mathcal{A}_{L/K}(\mathfrak{b}) + L) & \mapsto & \alpha + (\mathcal{A}_L(\mathfrak{b}) + L) \end{array}$$

ein k-Vektorraumisomorphismus.

(c) *Für $\omega_L := \omega \circ S_{L/K} \in \operatorname{Hom}_k(\mathcal{A}_{L/K}, k)$ gilt $\omega_L(\mathcal{A}_{L/K}(\mathfrak{c}) + L) = 0$, also definiert ω_L nach (b) ein Differential von L.*

(d) *$(\omega_L) = \mathfrak{c}$.*

BEWEIS. **(a)** Folgt direkt mit 1.23(b).

(b) Zu zeigen ist die Surjektivität. Wir schreiben $\mathfrak{b} := \sum_w b_w \mathfrak{p}_w$. Zu $\beta = (z_w)_w \in \mathcal{A}_L$ existiert nach 1.19 für jedes $v \in V$ ein $y_v \in L$, so daß $w(y_v - z_w) \geq -b_w$ für alle w/v. Für $\alpha := (y_w)_w$ mit $y_w := y_v$ für w/v gilt dann $\alpha \in \mathcal{A}_{L/K}$ und $\alpha - \beta \in \mathcal{A}_L(\mathfrak{b})$.

(c) Offensichtlich ist $\omega_L(L) = \omega(S_{L/K}(L)) \subseteq \omega(K) = 0$. Schreiben wir $(\omega) = \sum_v m_v \mathfrak{p}_v$ und $\mathfrak{c} = \sum_w c_w \mathfrak{p}_w$, so ist

$$c_w = e_{w/v} m_v + d_{w/v} \quad \forall v \in V,\ w/v.$$

Zu $v \in V$ wählen wir wieder $t_v \in K$ mit $v(t_v) = 1$. Sei $\alpha = (y_w)_w \in \mathcal{A}_{L/K}(\mathfrak{c})$, dann gilt

$$\begin{array}{rrcll} & w(y_w) & \geq & -c_w & \forall v \in V,\ w/v \\ \Longrightarrow & w(t_v^{m_v} y_w) & \geq & -d_{w/v} & \forall v \in V,\ w/v \\ \Longrightarrow & t_v^{m_v} y_w & \in & B_v^{\#} & \forall v \in V,\ w/v \\ \Longrightarrow & t_v^{m_v} S_{L/K}(y_w) & \in & R_v & \forall v \in V,\ w/v \\ \Longrightarrow & v(S_{L/K}(y_w)) & \geq & -m_v & \forall v \in V,\ w/v \\ \Longrightarrow & S_{L/K}(\alpha) & \in & \mathcal{A}_{L/K}((\omega)) & \\ \Longrightarrow & \omega_L(\alpha) & = & \omega(S_{L/K}(\alpha)) \quad = \quad 0. & \end{array}$$

(d) Nach (c) ist schon $\mathfrak{c} \leq (\omega_L)$ bewiesen. Sei $v \in V$ und w/v fest. Zu zeigen ist, daß ein $\alpha \in \mathcal{A}_{L/K}(\mathfrak{c} + \mathfrak{p}_w)$ existiert, so daß $\omega_L(\alpha) \neq 0$ ist. Nach 1.19 existiert ein $t_w \in L$ mit

$$\begin{array}{rcll} w(t_w) & = & 1, & \\ \tilde{w}(t_w) & = & 0 & \forall \tilde{w}/v,\ \tilde{w} \neq w, \end{array}$$

und ein $y \in L$ mit

$$(*) \qquad \begin{array}{rcll} w(y) & = & -d_{w/v} - 1, & \\ \tilde{w}(y) & \geq & -d_{\tilde{w}/v} & \forall \tilde{w}/v,\ \tilde{w} \neq w. \end{array}$$

Damit ist $y \notin B_v^{\#}$. Folglich existiert ein $x \in B_v$ mit $S_{L/K}(xy) \notin R_v$. Dabei muß $w(x) = 0$ sein, denn sonst wäre $t_w^{-1} x \in B_v$, also $t_w y \notin B_v^{\#}$ im Widerspruch zu $(*)$. Nach Ersetzen von y durch xy können wir daher $v(S_{L/K}(y)) < 0$ annehmen. Wählen wir $z \in K$ mit $v(z) = -m_v - 1$, also $v(z/S_{L/K}(y)) \geq -m_v$, und setzen $\alpha := (y_{\tilde{w}})_{\tilde{w}}$ mit

$$y_{\tilde{w}} := \begin{cases} \frac{z}{S_{L/K}(y)} y & \text{für } \tilde{w}/v \\ 0 & \text{falls } \tilde{w} \text{ nicht } v \text{ fortsetzt,} \end{cases}$$

so ist $\alpha \in \mathcal{A}_{L/K}(\mathfrak{c} + \mathfrak{p}_w)$ und $\omega_L(\alpha) = \omega(S_{L/K}(\alpha)) \neq 0$.

□

Beweis der Geschlechtsformel 5.2. Wir wählen $\omega \in \Omega_K$, $\omega \neq 0$. Mit 4.28(c) und dem vorangehenden Lemma können wir folgern, daß

$$2g_L - 2 = \operatorname{grad}(\omega)_L = \operatorname{grad}((\omega_L) + \mathfrak{d}_{L/K}) = (2g_K - 2)n + \sum_{v \in V} d_{L,v} f_v.$$

□

6 Der Satz von Weil

Den algebraischen Zahlkörpern noch ähnlicher werden algebraische Funktionenkörper, wenn sie endlichen Konstantenkörper besitzen. Man subsumiert daher diese beiden Klassen von Körpern häufig unter dem Begriff 'globale Körper'. Gemeinsam ist ihnen z. B. die Endlichkeit der Klassenzahl und der Restklassenkörper.
Es sei K ein algebraischer Funktionenkörper über dem endlichen Körper $k := \mathbb{F}_q$ mit q Elementen (q eine Primpotenz), so daß k der Konstantenkörper von K/k ist. Im Mittelpunkt

unseres Interesses steht in diesem Abschnitt die von F. K. Schmidt [Sm] eingeführte Zetafunktion, die analog zur Dedekindschen Zetafunktion, oder genauer: zur vollständigen Zetafunktion eines algebraischen Zahlkörpers (vgl. [Nk, pp. 478, 487]), gebildet wird und deren Untersuchung uns weitere Informationen über K liefert. Wir halten uns im wesentlichen an [FJ, Chapter 3], mit dem Unterschied, daß wir die Zetafunktion rein algebraisch als formale Potenzreihe über $\mathbb{C}$ einführen und behandeln.
Es sei $V := V(K/k)$ die abstrakte Kurve, $N := \#V_1(K/k)$ die Anzahl der rationalen Punkte, $\mathcal{D} := \mathcal{D}_K$ die Divisorengruppe und $g := g_K$ das Geschlecht von K. Für $n \in \mathbb{Z}$ bezeichne $\mathcal{C}\ell_n := \{\mathfrak{A} \in \mathcal{D}/(K^*) : \operatorname{grad}\mathfrak{A} = n\}$ die Menge der Divisorenklassen vom Grad n und $h_0 := h_0(K) = \#\mathcal{C}\ell_0$ die Divisorenklassenzahl von K.
Wir wissen nicht, ob es zu jedem $n \in \mathbb{Z}$ auch einen Divisor $\mathfrak{d} \in \mathcal{D}$ mit $\operatorname{grad}\mathfrak{d} = n$ gibt, zumindest aber ist das Bild der Gradabbildung $\operatorname{grad} : \mathcal{D} \to \mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$. Wir definieren $\delta \in \mathbb{N}$ durch

$$\operatorname{grad}(\mathcal{D}) = \delta\mathbb{Z}.$$

Wir werden später sehen, daß tatsächlich $\delta = 1$ ist, zunächst können wir jedoch nur $\delta | 2g-2$ aus 4.28(c) folgern.

6.1 Satz.

(a) *Für $n \in \mathbb{N}_0$ ist die Menge*

$$\{\mathfrak{a} \in \mathcal{D} : \mathfrak{a} \geq \mathfrak{o}, \operatorname{grad}\mathfrak{a} = n\}$$

endlich.

(b) *Die Klassengruppe $\mathcal{C}\ell_0$ ist endlich.*

Beweis. **(a)** Es genügt offenbar, zu zeigen, daß $\#\{v \in V : f_v \leq n\} < \infty$ ist. Dies folgt mithilfe von 4.3 und 1.21(b), da es für $x \in K \setminus k$ nur endlich viele normierte, irreduzible Polynome $p \in k[x]$ mit $\operatorname{grad} p \leq n$ gibt.

(b) Wir wählen $n \geq g$, so daß $\mathcal{C}\ell_n \neq \emptyset$ ist. Für festes $\mathfrak{A}_1 \in \mathcal{C}\ell_n$ haben wir offenbar eine Bijektion

$$\begin{array}{ccc} \mathcal{C}\ell_0 & \leftrightarrow & \mathcal{C}\ell_n \\ \mathfrak{D} & \mapsto & \mathfrak{D} + \mathfrak{A}_1. \end{array}$$

Nach (a) genügt es, zu zeigen, daß es in jeder Klasse $\mathfrak{A} \in \mathcal{C}\ell_n$ einen Divisor $\mathfrak{a} \geq \mathfrak{o}$ gibt. Sei $\mathfrak{A} \in \mathcal{C}\ell_n$, dann haben wir für irgendein $\mathfrak{d} \in \mathfrak{A}$ nach 4.19(b), daß $\dim\mathfrak{d} \geq n+1-g \geq 1$ ist, also $y \in K^*$ existiert mit $\mathfrak{a} := \mathfrak{d} + (y) \geq \mathfrak{o}$.

□

6.2 Definition. *Wir setzen $A_n := \#\{\mathfrak{a} \in \mathcal{D} : \mathfrak{a} \geq \mathfrak{o}, \operatorname{grad}\mathfrak{a} = n\}$ und definieren die* **Zetareihe** *oder* **Zetafunktion von** *K als die (formale) Potenzreihe*

$$Z(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]],$$

wobei t transzendent über $\mathbb{C}$ ist.

Wir wollen die Koeffizienten der Zetareihe ausrechnen. Offenbar ist $A_0 = 1$, $A_1 = N$ und $A_n = 0$ für $\delta \nmid n$.

6.3 Lemma.

(a) *Für $\mathfrak{A} \in \mathcal{D}/(K^*)$ ist*

$$\#\{\mathfrak{a} \in \mathfrak{A} : \mathfrak{a} \geq \mathfrak{o}\} = \frac{q^{\dim \mathfrak{A}} - 1}{q - 1}.$$

(b) *Sei $n > 2g - 2$ mit $\delta | n$, dann ist*

$$A_n = \frac{q^{n+1-g} - 1}{q - 1} h_0.$$

Beweis. **(a)** Wir wählen einen Divisor $\mathfrak{d} \in \mathfrak{A}$. Offenbar gilt

$$\mathfrak{a} \in \mathfrak{A}, \mathfrak{a} \geq \mathfrak{o} \iff \mathfrak{a} = \mathfrak{d} + (y) \text{ für ein } y \in \mathcal{L}(\mathfrak{d}) \setminus \{0\}.$$

Dabei ist $(y_1) = (y_2) \iff \frac{y_1}{y_2} \in k^*$, also

$$\#\{\mathfrak{a} \in \mathfrak{A} : \mathfrak{a} \geq \mathfrak{o}\} = \frac{\#\mathcal{L}(\mathfrak{d}) - 1}{\#k^*} = \frac{q^{\dim \mathfrak{A}} - 1}{q - 1}.$$

(b) Nach Beweis von 6.1(b) ist $\#\mathcal{C}\ell_n = h_0$, also folgt die Formel aus (a), 4.24 und dem Satz von Riemann-Roch.

□

Nun können wir mithilfe der Rechenregeln aus 3.9 leicht zeigen, daß $Z(t)$ eine rationale Funktion ist.

6.4 Satz. *Es gilt*

$$Z(t) = \frac{P(t)}{Q(t)}$$

mit teilerfremden Polynomen $P(t), Q(t) \in \mathbb{C}[t]$, $\operatorname{grad} P(t) \leq 2(g - 1 + \delta)$ und $Q(t) = (1 - t^\delta)(1 - (qt)^\delta)$.

Beweis. Für $g = 0$ gilt nach 4.20(b) und Teil (b) des vorigen Lemmas

$$Z(t) = \frac{1}{q-1} \sum_{m=0}^{\infty} (q^{m\delta+1} - 1) t^{m\delta} = \frac{1}{q-1} \left(\frac{q}{1 - (qt)^\delta} - \frac{1}{1 - t^\delta} \right) = \frac{P(t)}{Q(t)}$$

mit

$$P(t) = \frac{q^\delta - q}{q - 1} t^\delta + 1$$

und $Q(t)$ wie behauptet. Für $g > 0$ setzen wir $F(t) := \sum_{n=0}^{2g-2} A_n t^n$ und $r := 1 + (2g-2)/\delta$ und erhalten nach 6.3(b)

$$\begin{aligned} Z(t) - F(t) &= \sum_{m=r}^{\infty} A_{m\delta} t^{m\delta} \\ &= \frac{h_0}{q-1} \sum_{m=r}^{\infty} (q^{m\delta+1-g} - 1) t^{m\delta} \\ &= \frac{h_0}{q-1} t^{r\delta} \left(q^{r\delta+1-g} \sum_{m=0}^{\infty} (qt)^{m\delta} - \sum_{m=0}^{\infty} t^{m\delta} \right) \\ &= \frac{h_0}{q-1} t^{2g-2+\delta} \left(\frac{q^{g-1+\delta}}{1-(qt)^\delta} - \frac{1}{1-t^\delta} \right), \end{aligned}$$

also wiederum

$$Z(t) = \frac{P(t)}{Q(t)}$$

mit $Q(t)$ wie oben und

$$P(t) = F(t)Q(t) + \frac{h_0}{q-1} t^{2g-2+\delta} (q^{g-1+\delta}(1-t^\delta) - (1-(qt)^\delta)).$$

In beiden Fällen ist damit $\operatorname{grad} P(t) \le 2g - 2 + 2\delta$. Außerdem gilt für jede Nullstelle $\lambda \in \mathbb{C}$ von $Q(t)$ entweder $\lambda^\delta = 1$, also $P(\lambda) = \frac{h_0}{q-1}(q^\delta - 1) \neq 0$, oder $(q\lambda)^\delta = 1$, woraus $P(\lambda) = \frac{h_0}{q-1} q^{1-g}(1 - q^{-\delta}) \neq 0$ folgt. Daher sind $P(t)$ und $Q(t)$ teilerfremd. □

6.5 Satz. *$Z(t)$ hat eine Darstellung als* **Euler-Produkt**

$$Z(t) = \prod_{v \in V} \frac{1}{1 - t^{f_v}}.$$

Das soll heißen, für jede aufsteigende Folge $S_1 \subseteq S_2 \subseteq \ldots$ von endlichen Teilmengen von V mit $\bigcup_{m\in\mathbb{N}} S_m = V$ (z. B. $S_m = \{v \in V : f_v \le m\}$) konvergiert die Folge

$$\left(\prod_{v \in S_m} \frac{1}{1 - t^{f_v}} \right)_{m \in \mathbb{N}}$$

in $\mathbb{C}((t))$ gegen $Z(t)$.

Beweis. Für jede endliche Teilmenge S von V ist

$$\prod_{v \in S} \frac{1}{1 - t^{f_v}} = \prod_{v \in S} \sum_{n=0}^{\infty} t^{f_v n} = \sum_{n=0}^{\infty} A_n(S) t^n$$

mit

$$A_n(S) := \#\{(n_v)_{v\in S} \in \mathbb{N}_0^S : \sum_{v \in S} f_v n_v = n\} = \#\{\mathfrak{a} \in \sum_{v \in S} \mathbb{N}_0 \mathfrak{p}_v : \operatorname{grad} \mathfrak{a} = n\} \le A_n.$$

Dabei ist offenbar $A_n(S) = A_n$, falls $f(S) := \min\{f_v : v \in V \setminus S\} > n$ ist. Für eine Folge $(S_m)_{m\in\mathbb{N}}$ endlicher Teilmengen $S_m \subseteq V$ mit den geforderten Eigenschaften gilt $\lim_{m\to\infty} f(S_m) = \infty$ nach Beweis von 6.1(a), und daher konvergiert

$$Z(t) - \prod_{v\in S_m} \frac{1}{1-t^{f_v}} = \sum_{n=f(S_m)}^{\infty} (A_n - A_n(S_m))t^n$$

in $\mathbb{C}((t))$ gegen 0 für $m \to \infty$. □

Um mehr herauszufinden, betrachten wir die Konstantenkörpererweiterungen von K/k.

6.6 Definition. *Für $r \in \mathbb{N}$ bezeichne k_r den endlichen Oberkörper $\mathbb{F}_{q^r}$ von k mit $[k_r : k] = r$, K_r/k_r die zugehörige Konstantenkörpererweiterung und $Z_r(t)$ ihre Zetafunktion.*

6.7 Satz. *Sei $r \in \mathbb{N}$.*

(a) *Jede Bewertung $v \in V$ hat genau $d_v := \mathrm{ggT}(f_v, r)$ Fortsetzungen w nach K_r. Für diese gilt $e_{w/v} = 1$ und $f_{w/v} = r/d_v$.*

(b) *Für die Zetafunktionen gilt die Beziehung*

$$Z_r(t^r) = \prod_{\substack{\lambda\in\mathbb{C}\\ \lambda^r=1}} Z(\lambda t).$$

Beweis. **(a)** Sei w eine Fortsetzung von $v \in V$ nach K_r. Aus 4.32(a) wissen wir, daß $e_{w/v} = 1$ und $k_w = k_v k_r$ ist. Nach Galoistheorie existiert genau ein Zwischenkörper k' von k_w/k mit $[k' : k] = m_v := \mathrm{kgV}(f_v, r)$ und dieser enthält k_v und k_r. Daher ist $k_w = k'$ und $f_{w/v} = m_v/f_v = r/d_v =: s_v$. Das Übrige folgt mit 1.23(b).

(b) Zunächst sei $v \in V$ fest. Während λ die r-ten Einheitswurzeln durchläuft, durchläuft λ^{f_v} die s_v-ten Einheitswurzeln, und zwar jede d_v-mal, daher gilt

$$\prod_{\lambda^r=1} (1-(\lambda t)^{f_v}) = \left(\prod_{\mu^{s_v}=1} (1-\mu t^{f_v})\right)^{d_v} = (1-t^{m_v})^{d_v}.$$

Mit (a) und dem Euler-Produkt 6.5 folgt

$$Z_r(t^r) = \prod_{v\in V}\prod_{w/v} \frac{1}{1-t^{m_v}} = \prod_{v\in V}\prod_{\lambda^r=1} \frac{1}{1-(\lambda t)^{f_v}} = \prod_{\lambda^r=1} Z(\lambda t).$$

□

6.8 Korollar. $\delta = 1$.

Beweis. Sei $\delta' \in \mathbb{N}_0$ die Zahl mit $\mathrm{grad}\,(\mathcal{D}_{K_\delta}) = \delta'\mathbb{Z}$. Wir schreiben

$$Z(t) = \frac{P(t)}{Q(t)} \quad \text{und} \quad Z_\delta(t) = \frac{P_\delta(t)}{Q_\delta(t)}$$

mit $P(t), Q(t), P_\delta(t), Q_\delta(t) \in \mathbb{Q}[t]$, $Q(t) = (1-t^\delta)(1-(qt)^\delta)$ und $Q_\delta(t) = (1-t^{\delta'})(1-(q^\delta t)^{\delta'})$ gemäß 6.4. Wegen $Z(t) = \sum_{m=0}^{\infty} A_{m\delta} t^{m\delta} = Z(\lambda t)$ für jede δ-te Einheitswurzel $\lambda \in \mathbb{C}$ gilt nach Teil (b) des vorigen Satzes

$$\frac{P_\delta(t^\delta)}{Q_\delta(t^\delta)} = Z_\delta(t^\delta) = \prod_{\lambda^\delta = 1} Z(\lambda t) = Z(t)^\delta = \frac{P(t)^\delta}{Q(t)^\delta}.$$

Da $P(t)$ zu $Q(t)$ und $P_\delta(t^\delta)$ zu $Q_\delta(t^\delta)$ teilerfremd ist, folgt für die Bewertung $v := v_{t-1}$ von $\mathbb{C}(t)$:

$$-1 = v(Z_\delta(t^\delta)) = \delta v(Z(t)) = -\delta.$$

□

In Umkehrung zu 4.20(a) erhalten wir außerdem:

6.9 Korollar. *Ist $g = 0$, so ist $K = k(x)$ für ein $x \in K$.*

Beweis. Nach dem vorigen Korollar existiert $\mathfrak{d} \in \mathcal{D}$ mit $\operatorname{grad} \mathfrak{d} = 1$, also $\dim \mathfrak{d} \geq 1+1-0 = 2$ nach 4.19(b). Daher gibt es ein $y \in K^*$ mit $\mathfrak{a} := \mathfrak{d} + (y) \geq \mathfrak{o}$. Da außerdem $\operatorname{grad} \mathfrak{a} = 1$ ist, muß $\mathfrak{a} = \mathfrak{p}_v$ ein Primdivisor sein für ein $v \in V$. Auch für diesen gilt $\dim \mathfrak{p}_v \geq 2$, wir haben also erneut ein $x \in K \setminus k$ mit $(x) + \mathfrak{p}_v \geq \mathfrak{o}$. Es folgt, daß $\mathfrak{p}_v$ der Polstellendivisor von x ist und daher $[K : k(x)] = 1$ nach 4.15. □

Fortan sei $P(t) = \sum p_n t^n := (1-t)(1-qt)Z(t) \in \mathbb{Q}[t]$ das Polynom vom Grad $\leq 2g$ gemäß 6.4. Die folgenden Eigenschaften von $P(t)$ lassen sich leicht nachprüfen.

6.10 Bemerkung.

(a) *$p_0 = 1$, $p_1 = N - (q+1)$ und $p_n = A_n - (q+1)A_{n-1} + qA_{n-2}$ für $n \geq 2$.*
(b) *$P(1) = h_0$.*

Beweis. **(a)** Da

$$\begin{aligned} P(t) &= (1 - (q+1)t + qt^2)Z(t) \\ &= A_0 + (A_1 - (q+1)A_0)t + \sum_{n=2}^{\infty} (A_n - (q+1)A_{n-1} + qA_{n-2})t^n \end{aligned}$$

ist, ergibt sich die Behauptung durch Koeffizientenvergleich.

(b) Für $g = 0$ folgt die Behauptung aus (a) und 4.20(b). Ist $g > 0$, so haben wir nach (a) und 6.3(b)

$$\begin{aligned} P(1) &= \sum_{n=0}^{2g} p_n \\ &= \sum_{n=0}^{2g} A_n - (q+1) \sum_{n=0}^{2g-1} A_n + q \sum_{n=0}^{2g-2} A_n \\ &= A_{2g} - qA_{2g-1} \\ &= \frac{q^{g+1} - 1 - q(q^g - 1)}{q-1} h_0 \\ &= h_0. \end{aligned}$$

□

Mithilfe der folgenden Funktionalgleichung läßt sich $P(t)$ genauer analysieren.

6.11 Satz.

(a) *$Z(t)$ erfüllt die Funktionalgleichung*

$$Z(t) = (\sqrt{q}t)^{2g-2} Z(\frac{1}{qt}).$$

(b) *$P(t)$ erfüllt die Funktionalgleichung*

$$P(t) = q^g t^{2g} P(\frac{1}{qt}).$$

Beweis. **(a)** Für $g = 0$ ist

$$Z(t) = Z_0(t) := \frac{1}{(1-t)(1-qt)},$$

und die Funktionalgleichung läßt sich direkt nachrechnen. Für $g > 0$ können wir nach 6.3 schreiben:

$$\begin{aligned} Z(t) &= \frac{1}{q-1} \left(\sum_{\substack{\mathfrak{A} \in \mathcal{D}/(K^*) \\ 0 \le \operatorname{grad} \mathfrak{A} \le 2g-2}} (q^{\dim \mathfrak{A}} - 1) t^{\operatorname{grad} \mathfrak{A}} + h_0 \sum_{n=2g-1}^{\infty} (q^{n+1-g} - 1) t^n \right) \\ &= \frac{F(t) + G(t)}{q-1} \end{aligned}$$

mit

$$F(t) := \sum_{0 \le \operatorname{grad} \mathfrak{A} \le 2g-2} q^{\dim \mathfrak{A}} t^{\operatorname{grad} \mathfrak{A}}$$

und

$$G(t) := h_0 \left(\sum_{n=2g-1}^{\infty} q^{n+1-g} t^n - \sum_{n=0}^{\infty} t^n \right) = h_0 \left(\frac{q^g t^{2g-1}}{1-qt} - \frac{1}{1-t} \right).$$

Man rechnet direkt nach, daß

$$G(t) = (\sqrt{q}t)^{2g-2} G(\frac{1}{qt})$$

ist. Sei $\mathfrak{C} := \mathfrak{C}_K$ die kanonische Klasse von K. Um zu zeigen, daß $F(t)$ ebenfalls die Funktionalgleichung erfüllt, benutzen wir den Satz von Riemann-Roch in der Version 4.28(a) und die Tatsache, daß mit $\mathfrak{A}$ auch $\mathfrak{C} - \mathfrak{A}$ die Menge $\bigcup_{n=0}^{2g-2} \mathcal{C}\ell_n$ durchläuft:

$$\begin{aligned} F(t) &= \sum_{0 \le \operatorname{grad} \mathfrak{A} \le 2g-2} q^{\dim(\mathfrak{C}-\mathfrak{A}) + \operatorname{grad} \mathfrak{A} + 1 - g} t^{\operatorname{grad} \mathfrak{A}} \\ &= \sum_{0 \le \operatorname{grad} \mathfrak{B} \le 2g-2} q^{\dim \mathfrak{B}} q^{g-1-\operatorname{grad} \mathfrak{B}} t^{2g-2-\operatorname{grad} \mathfrak{B}} \\ &= (\sqrt{q}t)^{2g-2} F(\frac{1}{qt}). \end{aligned}$$

(b) Ist $Z_0(t)$ wie oben die Zetafunktion des rationalen Funktionenkörpers, so können wir mithilfe von (a) folgern, daß

$$P(t) = \frac{Z(t)}{Z_0(t)} = \frac{(\sqrt{q}t)^{2g-2} Z(\frac{1}{qt})}{(\sqrt{q}t)^{-2} Z_0(\frac{1}{qt})} = q^g t^{2g} P(\frac{1}{qt}).$$

□

6.12 Korollar. *Für $0 \le n \le 2g$ gilt $p_n = q^{n-g} p_{2g-n}$. Insbesondere ist* $\operatorname{grad} P(t) = 2g$.

Beweis. Aus der Identität

$$\sum_{n=0}^{2g} p_n t^n = q^g t^{2g} P(\frac{1}{qt}) = \sum_{n=0}^{2g} q^{g-n} p_n t^{2g-n} = \sum_{n=0}^{2g} q^{n-g} p_{2g-n} t^n$$

folgt die behauptete Formel durch Koeffizientenvergleich. Insbesondere ist $p_{2g} = q^g$. □

6.13 Definition. *Wir schreiben*

$$P(t) = \prod_{i=1}^{2g} (1 - \omega_i t),$$

wobei $\omega_1, \ldots, \omega_{2g} \in \mathbb{C}$ die **Weil-Zahlen von** *K genannt werden.*

Da $P(t) \in \mathbb{R}[t]$ ist, treten die nicht-reellen Weil-Zahlen in konjugiert komplexen Paaren auf. Da außerdem $\prod_{i=1}^{2g} \omega_i = q^g > 0$ ist, ist die Anzahl sowohl der positiven als auch der negativen reellen Weil-Zahlen gerade.
Die folgende Aussage über die 'Größe' der Weilzahlen kann als das Analogon zur (bisher unbewiesenen) Riemannschen Vermutung aus der algebraischen Zahlentheorie angesehen werden.

6.14 Satz von Weil. *Es gilt $|\omega_i| = \sqrt{q}$ für $1 \le i \le 2g$.*

Ich möchte diesen sehr wichtigen Satz hier aus Zeitgründen nicht zeigen und verweise den/die LeserIn daher auf den mit modernen Methoden geführten Beweis in [FJ, p. 35ff]. Wir wollen jedoch noch einige Konsequenzen des Satzes von Weil festhalten.

6.15 Korollar.

(a) *Für die Anzahl der rationalen Punkte von K/k gilt die Abschätzung*

$$|N - (q+1)| \le 2g\sqrt{q}.$$

(b) *Für die Klassenzahl von K läßt sich durch*

$$(\sqrt{q} - 1)^{2g} \le h_0 \le (\sqrt{q} + 1)^{2g}$$

eine Größenordnung angeben.

(c) *Die Weilzahlen lassen sich so ordnen, daß $\omega_{g+i} = \overline{\omega_i}$ ist für $1 \le i \le g$.*

Beweis. **(a)** Wegen 6.10(a) und $|\sum_i \omega_i| \le \sum_i |\omega_i|$.

(b) Wegen 6.10(b) und $|\omega_i| - 1 \le |1 - \omega_i| \le |\omega_i| + 1$.

(c) Nach den Überlegungen vor dem Satz von Weil.

□

Dem nächsten Lemma zufolge gilt der Satz von Weil genau dann für K/k, wenn er für eine Konstantenkörpererweiterung K_r/k_r gilt.

6.16 Lemma. *Sei $r \in \mathbb{N}$. Für $P_r(t) := (1-t)(1-q^r t)Z_r(t)$ gilt*

$$P_r(t) = \prod_{i=1}^{2g}(1-\omega_i^r t).$$

Beweis. Mithilfe von 6.7(b) erhalten wir

$$\begin{aligned} P_r(t^r) &= (1-t^r)(1-(qt)^r)Z_r(t^r) \\ &= \prod_{\lambda^r=1}(1-\lambda t)(1-\lambda qt)Z(\lambda t) \\ &= \prod_{\lambda^r=1} P(\lambda t) \\ &= \prod_{i=1}^{2g}\prod_{\lambda^r=1}(1-\lambda\omega_i t) \\ &= \prod_{i=1}^{2g}(1-(\omega_i t)^r) \end{aligned}$$

und daher auch

$$P_r(t) = \prod_{i=1}^{2g}(1-\omega_i^r t).$$

□

Teil III
Zyklotomische Funktionenkörper

Wir kommen nun zum eigentlichen Thema dieser Arbeit. Ausgehend von dem rationalen Funktionenkörper $\mathbb{F}_q(x)$ konstruieren wir zu den klassischen Kreisteilungskörpern analoge Erweiterungen, die zyklotomischen Funktionenkörper. Dabei folgen wir in den Abschnitten 7 bis 10 zunächst Hayes [Ha], der selbst nach einer ursprünglich von Carlitz [Ca] stammenden Idee vorgeht, und verallgemeinern seine Resultate über Bewertungen, Ring ganzer Funktionen und Geschlecht der zyklotomischen Funktionenkörper unter ergänzender Hinzuziehung der beiden Arbeiten [GR1] und [GR2] von Galovich und Rosen. Abschließend greifen wir in Abschnitt 11 die von Quebbemann [Qb] durchgeführte asymptotische Untersuchung der Klassenzahlen zyklotomischer Funktionenkörper auf, die wir in gleicher Weise verallgemeinern.
Fortan bezeichne K den rationalen Funktionenkörper in einer Variablen über dem endlichen Körper $k := \mathbb{F}_q$ mit q Elementen, x eine Unbestimmte über k, so daß $K = k(x)$ ist, und $R = k[x]$ den zugehörigen Polynomring. Sei außerdem u eine Unbestimmte über K.

7 Carlitz-Moduln

In der klassischen Theorie hatte man für $m \in \mathbb{N}$ an $\mathbb{Q}$ die Gruppe der m-ten Einheitswurzeln adjungiert. Diese kann aufgefaßt werden als der Torsionsuntermodul des $\mathbb{Z}$-Moduls $\mathbb{C}^*$ unter der Skalarmultiplikation $z \mapsto z^m$. In ähnlicher Weise lassen wir nun die Elemente von R auf dem algebraischen Abschluß $\overline{K}$ von K, und zwar diesmal auf der additiven Gruppe $(\overline{K}, +)$, linear operieren. So erhalten wir zu jedem $M \in R$ einen — wie in der klassischen Theorie — endlichen, zyklischen Torsionsuntermodul Λ_M des R-Moduls $\overline{K}$, dessen Erzeugende den primitiven m-ten Einheitswurzeln entsprechen.

Der Frobeniusautomorphismus φ mit $\varphi(z) = z^q$ und die Abbildung χ mit $\chi(z) = xz$ sind k-Vektorraumendomorphismen auf $(\overline{K}, +)$. Wir fassen k in üblicher Weise als Teilmenge der k-Algebra $\mathrm{End}_k(\overline{K})$ auf und betrachten den Einsetzungshomomorphismus

$$\begin{aligned} R &\to \mathrm{End}_k(\overline{K}) \\ M &\mapsto M(\varphi + \chi). \end{aligned}$$

Er ist, wie wir gleich sehen werden, injektiv. Sein Bild $k[\varphi + \chi]$ ist eine k-Unteralgebra von $\mathrm{End}_k(\overline{K})$, die wiederum k enthält. Offenbar wird also $\overline{K}$ zu einem R-Modul mit der Skalarmultiplikation

$$\begin{aligned} R \times \overline{K} &\to \overline{K} \\ (M, z) &\mapsto M \circ z := (M(\varphi + \chi))(z). \end{aligned}$$

Man beachte, daß für $\alpha \in k$ hierbei $\alpha \circ z = \alpha z$ gilt.

7.1 Satz. *Für $M \in R$ mit $\operatorname{grad} M = d$ existieren Polynome $\begin{bmatrix} M \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} M \\ d \end{bmatrix} \in R$ mit $\operatorname{grad} \begin{bmatrix} M \\ i \end{bmatrix} = (d-i)q^i$ für $0 \le i \le d$, $\begin{bmatrix} M \\ 0 \end{bmatrix} = M$, $\begin{bmatrix} M \\ d \end{bmatrix}$ = Leitkoeffiezient von M und*

$$M \circ z = \sum_{i=0}^{d} \begin{bmatrix} M \\ i \end{bmatrix} z^{q^i} \quad \forall z \in \overline{K}.$$

Für unsere Unbestimmte u setzen wir ebenfalls $M \circ u := \sum_{i=0}^{d} \begin{bmatrix} M \\ i \end{bmatrix} u^{q^i} \in R[u]$. Die Injektivität des Einsetzungshomomorphismus oben folgt sofort aus dem Satz: Ist $M(\varphi + \chi) = 0$, so ist $\overline{K}$ die Nullstellenmenge des Polynoms $M \circ u$. Wegen $\#\overline{K} = \infty$ muß $M \circ u = 0$, insbesondere $M = \begin{bmatrix} M \\ 0 \end{bmatrix} = 0$ sein.

Beweis von 7.1. Es genügt, die Behauptung für $M = x^d$ zu zeigen. Für beliebiges M ergibt sie sich dann aus der Implikation

$$M = \sum_{j=0}^{d} \alpha_j x^j, \alpha_j \in k \implies M \circ z = \sum_{j=0}^{d} \alpha_j \sum_{i=0}^{j} \begin{bmatrix} x^j \\ i \end{bmatrix} z^{q^i} = \sum_{i=0}^{d} \left(\sum_{j=i}^{d} \alpha_j \begin{bmatrix} x^j \\ i \end{bmatrix} \right) z^{q^i}.$$

Im Fall $M = x^d$ führen wir vollständige Induktion über d. Die Behauptung ist klar für $d \leq 1$. Für $d > 1$ ergibt sie sich aus dem Induktionsschluß

$$\begin{aligned} x^d \circ z &= x \circ (x^{d-1} \circ z) \\ &= \sum_{i=0}^{d-1} \begin{bmatrix} x^{d-1} \\ i \end{bmatrix}^q z^{q^{i+1}} + \sum_{i=0}^{d-1} x \begin{bmatrix} x^{d-1} \\ i \end{bmatrix} z^{q^i} \\ &= x^d z + \sum_{i=1}^{d-1} \left(\begin{bmatrix} x^{d-1} \\ i-1 \end{bmatrix}^q + x \begin{bmatrix} x^{d-1} \\ i \end{bmatrix} \right) z^{q^i} + z^{q^d}. \end{aligned}$$

□

7.2 Korollar. *Sei $0 \neq M \in R$. Das Polynom $M \circ u \in R[u]$ ist separabel. Der Torsions-R-Modul*

$$\Lambda_M := \{z \in \overline{K} \,:\, M \circ z = 0\}$$

hat $q^{\operatorname{grad} M}$ Elemente.

Beweis. Wegen $(M \circ u)' = \begin{bmatrix} M \\ 0 \end{bmatrix} = M \neq 0$ hat $M \circ u$ keine mehrfachen, also genau $q^{\operatorname{grad} M}$ verschiedene Nullstellen. □

7.3 Definition. *Für $0 \neq M \in R$ heißt der R-Modul Λ_M aus dem vorhergehenden Korollar der* **Carlitz-Modul von** *M. Wir wollen außerdem $\Lambda_M^* := \{\lambda \in \Lambda_M \,:\, \Lambda_M = R \circ \lambda\}$ für die Menge seiner Erzeugenden schreiben.*

Man beachte, daß $\Lambda_\alpha = \Lambda_\alpha^* = \{0\}$ ist für $\alpha \in k^*$. Ist $M \in R$ ein lineares Polynom, so hat man $\Lambda_M = k\lambda$ für $0 \neq \lambda \in \Lambda_M$ nach 7.2, also wiederum $\Lambda_M^* = \Lambda_M \setminus \{0\} \neq \emptyset$. Wir werden gleich sehen, daß allgemein Λ_M^* für $0 \neq M \in R$ nicht leer, d. h. Λ_M ein zyklischer R-Modul ist. Dazu zunächst ein Lemma.

7.4 Lemma. *Seien $0 \neq M, N, Q \in R$ mit $M = NQ$.*

(a) *Der R-Modulhomomorphismus*

$$\begin{aligned} \Lambda_M &\to \Lambda_N \\ \mu &\mapsto Q \circ \mu \end{aligned}$$

ist surjektiv und hat den Kern Λ_Q.

(b) *Ist* $\lambda \in \Lambda_M^*$, *so ist* $Q \circ \lambda \in \Lambda_N^*$.

BEWEIS. **(a)** Zu zeigen ist die Surjektivität. Sie folgt aus

$$\#\left(\Lambda_M/\Lambda_Q\right) = \frac{q^{\operatorname{grad} M}}{q^{\operatorname{grad} Q}} = q^{\operatorname{grad} N} = \#\Lambda_N.$$

(b) Sei $\lambda \in \Lambda_M^*$, also $\Lambda_M = R \circ \lambda$, und $\nu \in \Lambda_N$ beliebig. Nach (a) existiert ein $A \in R$ mit $\nu = Q \circ (A \circ \lambda) = A \circ (Q \circ \lambda) \in R \circ (Q \circ \lambda)$.

□

7.5 SATZ. *Sei* $0 \neq M \in R$.

(a) *Schreiben wir* $M = \alpha \prod_{i=1}^r P_i^{n_i}$ *mit* $\alpha \in k^*$, $r \in \mathbb{N}_0$, $n_i \in \mathbb{N}$ *und paarweise verschiedenen normierten, irreduziblen* $P_i \in R$, *so ist*

$$\Lambda_M = \bigoplus_{i=1}^r \Lambda_{P_i^{n_i}}.$$

(b) Λ_M *ist ein zyklischer* R*-Modul.*

BEWEIS. **(a)** Sei $N_i := M/P_i^{n_i}$. Wegen $P_i^{n_i} | M$ ist $\Lambda_{P_i^{n_i}} \subseteq \Lambda_M$. Sei umgekehrt $\mu \in \Lambda_M$, also $M \circ \mu = 0$. Wegen $\operatorname{ggT}(N_1, \ldots, N_r) = 1$ existieren $B_1, \ldots, B_r \in R$ mit $\sum_{i=1}^r B_i N_i = 1$. Setzen wir $\mu_i := (B_i N_i) \circ \mu$, so ist $\sum_{i=1}^r \mu_i = \mu$ und $P_i^{n_i} \circ \mu_i = B_i \circ (M \circ \mu) = 0$, also $\mu \in \sum_{i=1}^r \Lambda_{P_i^{n_i}}$. Die Direktheit der Summe zeigen wir durch vollständige Induktion nach r. Für $r = 1$ ist nichts zu zeigen. Sei $r > 1$ und $\mu_i \in \Lambda_{P_i^{n_i}}$ beliebig mit $\sum_{i=1}^r \mu_i = 0$. Nach Induktionsvoraussetzung ist

$$\Lambda_{N_1} = \bigoplus_{i=2}^r \Lambda_{P_i^{n_i}}.$$

Wegen $\operatorname{ggT}(P_1^{n_1}, N_1) = 1$ existieren $A, B \in R$ mit $AP_1^{n_1} + BN_1 = 1$, und wegen $\mu_1 = -\sum_{i=2}^r \mu_i \in \Lambda_{P_1^{n_1}} \cap \Lambda_{N_1}$ folgt also $\mu_1 = A \circ (P_1^{n_1} \circ \mu_1) + B \circ (N_1 \circ \mu_1) = 0$ und damit nach Induktionsvoraussetzung auch $\mu_2 = \cdots = \mu_r = 0$.

(b) Wir beweisen die Aussage in zwei Schritten. Sei zunächst $M = P^n$ mit $n \in \mathbb{N}$, $P \in R$ normiert, irreduzibel, und $d := \operatorname{grad} P$. Wir führen Induktion über n. Für $n = 1$ ist $\Lambda_M = \Lambda_P$ in natürlicher Weise ein (R/RP)-Vektorraum, der wegen $\#\Lambda_P = q^d = \#(R/RP)$ die Dimension 1 hat, also ein zyklischer (R/RP)-Modul und damit erst recht ein zyklischer R-Modul. Für $n > 1$ ist der R-Modulhomomorphismus

$$\begin{aligned} \Lambda_{P^n} &\to \Lambda_{P^{n-1}} \\ \mu &\mapsto P \circ \mu \end{aligned}$$

surjektiv nach Teil (a) des vorangegangenen Lemmas, also existiert nach Induktionsvoraussetzung ein $\lambda \in \Lambda_{P^n}$ mit

$$P \circ \lambda \in \Lambda_{P^{n-1}}^*.$$

Unser Ziel ist, $\Lambda_{P^n} = R \circ \lambda$ zu zeigen. Sei $\mu \in \Lambda_{P^n}$ beliebig. Wegen $P \circ \mu \in \Lambda_{P^{n-1}}$ existiert ein $A \in R$ mit $P \circ \mu = A \circ (P \circ \lambda)$, d. h. $\mu - A \circ \lambda \in \Lambda_P$. Da nach Teil (b) des Lemmas außerdem $P^{n-1} \circ \lambda = P^{n-2} \circ (P \circ \lambda) \in \Lambda_P^*$ ist, existiert ein $B \in R$ mit $\mu - A \circ \lambda = B \circ (P^{n-1} \circ \lambda)$, und wir erhalten $\mu = (A + BP^{n-1}) \circ \lambda \in R \circ \lambda$, womit gezeigt ist, daß Λ_{P^n} zyklisch ist.

Im allgemeinen Fall schreiben wir M wie in (a). Nach dem ersten Beweisschritt sind die $\Lambda_{P_i^{n_i}}$ zyklisch, etwa $\Lambda_{P_i^{n_i}} = R \circ \lambda_i$. Wegen $P_i^{n_i} \in J_i := \operatorname{ann}_R(\lambda_i) = \operatorname{ann}_R(\Lambda_{P_i^{n_i}})$ ist $J_i + J_j = R$ für $1 \le i < j \le r$, also nach dem chinesischen Restsatz

$$\begin{array}{rcccl} R/\bigcap_{i=1}^{r} J_i & \simeq & \prod_{i=1}^{r} R/J_i & \simeq & \bigoplus_{i=1}^{r} \Lambda_{P_i^{n_i}} \qquad \text{mit den Isomorphismen} \\ A + \bigcap_{i=1}^{r} J_i & \mapsto & (A+J_i)_{1\le i\le r} & & \\ & & (A_i+J_i)_{1\le i\le r} & \mapsto & \sum_{i=1}^{r} A_i \circ \lambda_i. \end{array}$$

Nach (a) ist folglich $\Lambda_M = R \circ \lambda$ mit $\lambda = \sum_{i=1}^{r} \lambda_i$.

□

Für $0 \neq M \in R$ sei $\lambda \in \Lambda_M^*$ und $J := \operatorname{ann}_R(\lambda) = \operatorname{ann}_R(\Lambda_M)$. Wie schon im vorangegangenen Beweis für die $P_i^{n_i}$ benutzt, ist die Abbildung

$$\begin{array}{rcl} R/J & \to & \Lambda_M \\ A+J & \mapsto & A \circ \lambda \end{array}$$

bekanntlich ein R-Modulisomorphismus, wobei $A \circ \lambda \in \Lambda_M^* \iff A+J \in (R/J)^*$ gilt. Wegen $M \in J$ und $\#(R/J) = \#\Lambda_M = q^{\operatorname{grad} M} = \#(R/RM)$ muß $J = RM$ sein. Es drängt sich eine aus der algebraischen Zahlentheorie bekannte Definition auf.

7.6 Definition. *Für $0 \neq M \in R$ heißt $\phi(M) := \#(R/RM)^* = \#\Lambda_M^*$ die* **Eulerfunktion von** M.

Im weiteren Verlauf werden wir noch einige Eigenschaften der Carlitz-Moduln benutzen, die wir hier kurz zusammenfassen wollen.

7.7 Lemma.

(a) *Sind $0 \neq M, N \in R$ teilerfremd, so gilt $\phi(MN) = \phi(M)\phi(N)$.*

(b) *Für $n \in \mathbb{N}$ und irreduzibles $P \in R$ mit $d := \operatorname{grad} P$ ist $\phi(P^n) = (q^d - 1)q^{(n-1)d}$ und $\Lambda_{P^n}^* = \Lambda_{P^n} \setminus \Lambda_{P^{n-1}}$.*

(c) *Für $0 \neq M \in R$ hat man eine disjunkte Vereinigung*

$$\Lambda_M = \bigcup_{\substack{N \in R \text{ normiert} \\ N|M}} \Lambda_N^*.$$

Beweis. **(a)** Nach dem chinesischen Restsatz ist $(R/RMN)^* \simeq (R/RM)^* \times (R/RN)^*$.

(b) Wegen $A+RP^n \notin (R/RP^n)^* \iff P|A$ ist $(R/RP^n)^* = (R/RP^n) \setminus (RP/RP^n)$, außerdem ist $(RP/RP^n) \simeq (R/RP^{n-1})$ als R-Modul, also $\phi(P^n) = q^{nd} - q^{(n-1)d}$. Der zweite Teil der Aussage folgt wegen $\Lambda_{P^n}^* \subseteq \Lambda_{P^n} \setminus \Lambda_{P^{n-1}}$ und aus Anzahlgründen.

(c) Für $0 \neq N, N' \in R$ normiert mit $N \neq N'$ ist $\Lambda_N^* \cap \Lambda_{N'}^* = \emptyset$, denn $\lambda \in \Lambda_N^* \cap \Lambda_{N'}^*$ würde $\Lambda_N = R \circ \lambda = \Lambda_{N'}$ und damit $N \circ u = \prod_{\mu \in \Lambda_N}(u - \mu) = N' \circ u$, insbesondere $N = \begin{bmatrix} N \\ 0 \end{bmatrix} = \begin{bmatrix} N' \\ 0 \end{bmatrix} = N'$ implizieren. Also ist die Vereinigung disjunkt. Aus $N|M$ folgt $\Lambda_M \supseteq \Lambda_N$, also ist

$$\Lambda_M \supseteq \bigcup_{\substack{N \in R \text{ normiert} \\ N|M}} \Lambda_N^*$$

klar. Sei umgekehrt $\mu \in \Lambda_M$. Da R Hauptidealring ist, existiert ein normiertes Polynom $N \in R$ mit $\operatorname{ann}_R(\mu) = RN$. Es folgt $RM = \operatorname{ann}_R(\Lambda_M) \subseteq \operatorname{ann}_R(\mu) = RN$, also $N|M$, und wegen $R/RN \simeq R \circ \mu \subseteq \Lambda_N \simeq R/RN$ ist $\Lambda_N = R \circ \mu$, also $\mu \in \Lambda_N^*$.

□

8 Die Galoisgruppe

Analog zu den klassischen Kreisteilungskörpern konstruieren wir nun aus K durch Adjunktion des im vorigen Abschnitt besprochenen Carlitzmoduls Λ_M den M-ten zyklotomischen Funktionenkörper über K. Wir werden sehen, daß es dabei schon genügt, nur irgendein $\lambda \in \Lambda_M^*$ zu adjungieren, daß $K(\lambda)/K$ galoissch und daß die Galoisgruppe zu $(R/RM)^*$ isomorph ist, daß also alles so ist, wie wir es von der klassischen Theorie her kennen.
Es sei im folgenden stets $0 \neq M \in R$.

8.1 Definition. *Der Körper $K_M := K(\Lambda_M)$ soll als M-***ter zyklotomischer Funktionenkörper (über K)** *bezeichnet werden. Wir setzen $G_M := \operatorname{Aut}(K_M/K)$.*

8.2 Satz. *Sei $\lambda \in \Lambda_M^*$. K_M/K ist eine endliche Galoiserweiterung mit $K_M = K(\lambda)$. G_M ist isomorph zu einer Untergruppe von $(R/RM)^*$, also abelsch.*

Beweis. K_M/K ist als Zerfällungskörper des separablen Polynoms $M \circ u$ eine endliche Galoiserweiterung. Sei $\sigma \in G_M$. Wegen $\Lambda_M = R \circ \lambda \subseteq R[\lambda] \subseteq K(\lambda)$ ist $K_M = K(\lambda)$, also ist σ eindeutig durch $\sigma(\lambda)$ bestimmt. Mit λ ist auch $\sigma(\lambda)$ Nullstelle von $M \circ u$, also

$$\sigma(\lambda) = A_\sigma \circ \lambda \text{ mit } A_\sigma \in R,$$

und A_σ ist modulo M eindeutig bestimmt. A_σ ist unabhängig von der Wahl von λ, denn für $\mu = B \circ \lambda$ ist

$$\sigma(\mu) = \sigma(B \circ \lambda) = B \circ \sigma(\lambda) = B \circ (A_\sigma \circ \lambda) = A_\sigma \circ \mu.$$

$A_\sigma + RM$ ist eine Einheit in R/RM, denn es ist $\lambda = \sigma(\sigma^{-1}(\lambda)) = A_\sigma \circ (A_{\sigma^{-1}} \circ \lambda) = (A_\sigma A_{\sigma^{-1}}) \circ \lambda$, also $A_\sigma A_{\sigma^{-1}} - 1 \in \operatorname{ann}_R(\lambda) = RM$. □

Unser Ziel ist, zu zeigen, daß wie im klassischen Fall $G_M \simeq (R/RM)^*$, also $[K_M : K] = \phi(M)$ ist. Hierfür beweisen wir zunächst zwei Lemmata.

8.3 Lemma. *Sei $L := K_M$, $\lambda \in \Lambda_M^*$, $P \in R$ normiert, irreduzibel mit $P \nmid M$ und $v := v_P$, dann gilt:*

(a) *$D_{L/K}(\lambda) \in R \setminus PR$.*
(b) *$R_v[\lambda]$ ist der ganze Abschluß des Bewertungsrings R_v in L.*
(c) *v ist unverzweigt in L/K.*

Beweis. **(a)** λ ist ganz über R nach 7.1. Sei $\Phi \in R[u]$ das Minimalpolynom von λ über K und $m := \operatorname{grad} \Phi = [L : K]$. Nach dem Lemma von Gauß existiert ein $\Psi \in R[u]$ mit $M \circ u = \Phi\Psi$. Nach 7.1 und 1.4(a) gilt damit

$$M^m = N_{L/K}((M \circ u)'(\lambda)) = N_{L/K}(\Phi'(\lambda)) N_{L/K}(\Psi(\lambda)).$$

Wegen $N_{L/K}(\Phi'(\lambda)), N_{L/K}(\Psi(\lambda)) \in R$ folgt $P \nmid N_{L/K}(\Phi'(\lambda))$, also mithilfe von 1.25 die Behauptung.

(b)–(c) Nach (a) und 1.26.

□

8.4 Lemma. *Sei $M = P^n$ mit $P \in R$ normiert, irreduzibel und $n \in \mathbb{N}$, w eine Fortsetzung von $v := v_P$ nach $L := K_M$ und $\lambda \in \Lambda_M^*$. Dann ist $w(\lambda) = 1$ und $e_{w/v} = \phi(M) = [L : K]$.*

Beweis. Sei B der ganze Abschluß von R in L. Es ist $M \circ u = P \circ (P^{n-1} \circ u) = (P^{n-1} \circ u)\Phi$ mit $\Phi = \sum_{i=0}^{\operatorname{grad} P} \begin{bmatrix} P \\ i \end{bmatrix} (P^{n-1} \circ u)^{q^i - 1}$. Nach 7.7(b) ist Λ_M^* die Nullstellenmenge von Φ, folglich

$$(*) \quad P = \begin{bmatrix} P \\ 0 \end{bmatrix} = \Phi(0) = \pm \prod_{\mu \in \Lambda_M^*} \mu.$$

Für $A \in R$ gilt $u | A \circ u$ in $R[u]$, also auch $\mu | A \circ \mu$ in $R[\mu] \subseteq B$ für alle $\mu \in \Lambda_M$. Daher sind die Elemente von Λ_M^* zueinander assoziiert in B, und wir können $(*)$ reduzieren auf

$$P = \varepsilon \lambda^{\phi(M)} \text{ mit } \varepsilon \in B^*.$$

Wegen $w(\varepsilon) = 0$ ist

$$\phi(M) w(\lambda) = w(P) = e_{w/v} \leq [L : K].$$

Zusammen mit 8.2 folgt die Behauptung. □

8.5 Satz.

(a) $[K_M : K] = \phi(M)$.

(b) *Die Abbildung*

$$\begin{array}{rcl} (R/RM)^* & \to & G_M \\ A + RM & \mapsto & \sigma_A \end{array}$$

mit $\sigma_A(\lambda) := A \circ \lambda$ für $\lambda \in \Lambda_M^*$ ist wohldefiniert und ein Gruppenisomorphismus.

Beweis. **(a)** Durch vollständige Induktion nach $d := \operatorname{grad} M$. Für $d = 0$ ist $K = K_M$ und $\phi(M) = 1$, also die Behauptung trivial. (Für $d = 1$ folgt sie aus dem letzten Lemma.) Sei $d \geq 1$ und $P \in R$ ein normierter, irreduzibler Teiler von M. Wir schreiben $M = P^n N$ mit $P \nmid N \in R$ und $n \in \mathbb{N}$. Nach dem letzten Lemma ist v_P total verzweigt in K_{P^n} und nach 8.3(c) unverzweigt in K_N/K, folglich total verzweigt mit Verzweigungsindex 1 in $(K_{P^n} \cap K_N)/K$, d. h. nach 1.23(b):

$$(*) \quad K_{P^n} \cap K_N = K.$$

Nach 7.5(a) ist $\Lambda_M = \Lambda_{P^n} + \Lambda_N$, also $K_M = K_{P^n} K_N$. Daher ist der Gruppenhomomorphismus

$$\begin{array}{rcl} \operatorname{Aut}(K_M/K_{P^n}) & \to & \operatorname{Aut}(K_N/K) \\ \sigma & \mapsto & \sigma|_{K_N} \end{array}$$

injektiv. Sei H sein Bild, dann ist $\operatorname{Fix}(K_N, H) = K$ wegen $(*)$, also $H = \operatorname{Aut}(K_N/K)$ und $[K_M : K_{P^n}] = [K_N : K]$. Nach Induktionsvoraussetzung und 7.7(a) folgt nun

$$[K_M : K] = [K_{P^n} : K][K_N : K] = \phi(P^n)\phi(N) = \phi(M).$$

(b) Folgt aus (a) und dem Beweis von 8.2.

□

Wie in der klassischen Theorie können wir 'Kreisteilungspolynome' definieren. Es gilt auch die von dort bekannte Rekursionsformel.

8.6 Korollar und Definition.

(a) $\Phi_M := \prod_{\lambda \in \Lambda_M^*}(u - \lambda) \in R[u]$ *ist irreduzibel in* $K[u]$ *und heißt* M**-tes zyklotomisches Polynom über** K.

(b) *Für* $P \in R$ *normiert, irreduzibel und* $n \in \mathbb{N}$ *ist* $P^n \circ u = (P^{n-1} \circ u)\Phi_{P^n}$ *und* Φ_{P^n} *ein Eisensteinpolynom über* R *bezüglich* P.

(c) *Ist* M *normiert, so gilt*

$$M \circ u = \prod_{\substack{N \in R \text{ normiert} \\ N \mid M}} \Phi_N.$$

Beweis. **(a)** Sei $\lambda \in \Lambda_M^*$ und $\Phi \in R[u]$ das Minimalpolynom von λ über K. Nach 8.5(b) ist $\Lambda_M^* = \{A \circ \lambda : A + RM \in (R/RM)^*\} = \{\sigma(\lambda) : \sigma \in G_M\}$ die Nullstellenmenge von Φ, also $\Phi = \Phi_M$.

(b) Die erste Aussage folgt aus (a) und 7.7(b). Zum Beweis der zweiten Aussage schreiben wir $\Phi_{P^n} = \sum_{i=0}^{m} F_i u^i$ mit $m := \phi(P^n)$ und $F_i \in R$. Nach 8.4 gilt für die Fortsetzung w von v_P nach K_{P^n}:

$$w(\lambda) = 1 \quad \forall \lambda \in \Lambda_{P^n}^*.$$

Nach Definition von Φ_{P^n} folgt $w(F_i) > 0$, also $P | F_i$ für $0 \le i < m$, und nach der ersten Aussage und 7.1 ist $F_0 = P$.

(c) Folgt aus 7.7(c).

□

Von wesentlicher Bedeutung für die nächsten Abschnitte ist noch ein Zwischenkörper von K_M/K, der dem maximalen reellen Teilkörper in der klassischen Theorie entspricht.

8.7 Definition. *Sei* $M \in R \setminus k$. *Nach 8.5(b) können wir dann* k^* *als Teilmenge von* G_M *auffassen. Wir wollen* $K_M^+ := \mathrm{Fix}(K_M, k^*)$ *als den* **reellen Teilkörper von** K_M *bezeichnen.*

Die Übereinstimmung in der Schreibweise mit dem in Abschnitt 2 eingeführten Trägheitskörper ist nicht ganz zufällig. Man kann sich in der Tat mithilfe der Ergebnisse des folgenden Abschnitts 9 leicht überlegen, daß K_M^+ der Trägheits- (und Zerlegungs)körper der Gradbewertung v_∞ in K_M/K ist (vgl. [GR1, p. 366]).

8.8 Lemma. *Sei* $M \in R \setminus k$ *und* $\lambda \in \Lambda_M^*$. *Es gilt:*

(a) $[K_M : K_M^+] = q - 1$.

(b) $K_M^+ = K(\lambda^{q-1})$.

(c) *Ist* $z \in K_M^*$ *mit* $\sigma(z)/z \in K_M^+$ *für alle* $\sigma \in \mathrm{Aut}(K_M/K_M^+)$, *so hat* z *eine (eindeutige) Darstellung*

$$z = z^+ \lambda^i$$

mit $z^+ \in K_M^+$ *und* $0 \le i < q - 1$.

BEWEIS. **(a)** Nach Galoistheorie.

(b) Wegen $\sigma_\alpha(\lambda^{q-1}) = (\alpha\lambda)^{q-1} = \lambda^{q-1}$ für alle $\alpha \in k^*$ ist $\lambda^{q-1} \in K_M^+$, also

$$K(\lambda^{q-1}) \subseteq K_M^+.$$

Andererseits ist $K_M = K(\lambda^{q-1})(\lambda)$ und λ Nullstelle von $u^{q-1} - \lambda^{q-1} \in K(\lambda^{q-1})[u]$, damit

$$[K_M : K(\lambda^{q-1})] \leq q - 1.$$

Also ist $K_M^+ = K(\lambda^{q-1})$ nach (a).

(c) Sei $\alpha \in k$ mit $k^* = \langle\alpha\rangle$ und $\sigma := \sigma_\alpha$. Nach Voraussetzung ist $\varepsilon := \sigma(z)/z \in K_M^+$. Gemäß (a) und (b) hat z eine eindeutige Darstellung $z = \sum_{i=0}^{q-2} y_i\lambda^i$ mit $y_0, \ldots, y_{q-2} \in K_M^+$, und wir erhalten wegen $\sigma(\lambda) = \alpha\lambda$:

$$\sum_{i=0}^{q-2} \varepsilon y_i\lambda^i = \varepsilon z = \sigma(z) = \sum_{i=0}^{q-2} y_i\sigma(\lambda^i) = \sum_{i=0}^{q-2} \alpha^i y_i\lambda^i.$$

Durch Koeffizientenvergleich ergibt sich für $0 \leq i < q - 1$:

$$\varepsilon = \alpha^i \text{ oder } y_i = 0.$$

Nach Wahl von α muß $y_i = 0$ für alle bis auf ein i sein.

□

8.9 BEISPIEL. Ist M ein normiertes, lineares Polynom, so ist $\Phi_M = u^{q-1} + M$, also sowohl $K_M^+ = K$ als auch $K_M = K(\sqrt[q-1]{-M}) = k(\sqrt[q-1]{-M})$ ein rationaler Funktionenkörper.

9 Die Bewertungen

Sei weiterhin $0 \neq M \in R$. Wir wollen in diesem Abschnitt das Fortsetzungsverhalten der Bewertungen von K nach K_M untersuchen. Für die endlichen Stellen haben wir den folgenden, aus der klassischen Theorie vertrauten Sachverhalt (vgl. [Nk, p. 64]).

9.1 SATZ. *Sei $P \in R$ normiert, irreduzibel und w eine Fortsetzung von $v := v_P$ nach K_M. Schreiben wir $M = P^n N$ mit $n \in \mathbb{N}_0$ und $P \nmid N$, so ist $e_{w/v} = \phi(P^n)$ und $f_{w/v}$ die Ordnung von $P + RN$ in $(R/RN)^*$.*

BEWEIS. Sei v' die Fortsetzung von v nach K_N mit w/v'. Nach 8.3(c), 8.4 und Beweis von 8.5 ist

$$e_{w/v} = e_{w/v'} = [K_{P^n} : K] = \phi(P^n) = [K_M : K_N].$$

und

$$f_{w/v} = f_{v'/v}.$$

Sei $\sigma \in G_N$ der Artinautomorphismus von v in K_N/K gemäß 2.6, dann ist $f_{v'/v} = \#\langle\sigma\rangle$, und nach 8.5(b) ist nur noch $\sigma = \sigma_P$ zu zeigen. Sei $d := \operatorname{grad} P$, also $\#k_v = q^d$, und $\nu \in \Lambda_N^*$. Nach Definition ist $\sigma(\nu) - \nu^{q^d} \in P_{v'}$ und nach 8.6(b) ebenfalls $P \circ \nu - \nu^{q^d} \in P_{v'}$, daher

$$\sigma(\nu) - P \circ \nu \in P_{v'}.$$

Wegen $N \circ u = \prod_{\mu \in \Lambda_N}(u - \mu)$ und $P \nmid N$ gilt andererseits

$$\prod_{\substack{\mu \in \Lambda_N \\ \mu \neq \sigma(\nu)}} (\sigma(\nu) - \mu) = (N \circ u)'(\sigma(\nu)) = N \notin P_{v'}.$$

Daher muß $\sigma_P(\nu) = P \circ \nu = \sigma(\nu)$ sein. □

9.2 Bemerkung.

(a) Mit den Bezeichnungen des Satzes gilt $N | P^{f_{w/v}} - 1$, also

$$f_w = \operatorname{grad}(P^{f_{w/v}} - 1) \geq \operatorname{grad} N.$$

(Außerdem ist noch $f_{w/v} | \phi(N)$ zu beachten.) Ist insbesondere M irreduzibel, so hat K_M außer den Fortsetzungen der Gradbewertung v_∞ (die sich als rationale Punkte von K_M herausstellen werden) keine Bewertung vom Grad $< \operatorname{grad} M$.

(b) Im Fall $q = 2$ läßt sich (a) noch verschärfen. Ist nämlich $N(0) = N(1) = 1$, so gilt für nicht-lineares P wegen $x^2 + x | P^{f_{w/v}} - 1$ sogar

$$f_w \geq \operatorname{grad} N + 2.$$

Insbesondere ist für irreduzibles M vom Grad $d \geq 2$ die Fortsetzung von v_M nach K_M die einzige Bewertung von K_M vom Grad d. Gilt überdies $d + 1 \nmid 2^d - 1$, so hat K_M keine Bewertung vom Grad $d + 1$.

Auch der Ring der über R ganzen Funktionen von K_M bzw. K_M^+ hat die von den klassischen Kreisteilungskörpern her zu erwartende Form (vgl. [Wh, pp. 11, 16]).

9.3 Satz. *Sei $M \in R \setminus k$, $P \in R$ normiert, irreduzibel, $v := v_P$, B_v bzw. B der ganze Abschluß von R_v bzw. R in K_M und B_v^+ bzw. B^+ der ganze Abschluß von R_v bzw. R in K_M^+. Für $\lambda \in \Lambda_M^*$ und $\lambda^+ := \lambda^{q-1}$ gilt:*

(a) $B_v = R_v[\lambda]$.

(b) $B = R[\lambda]$.

(c) $B_v^+ = R_v[\lambda^+]$.

(d) $B^+ = R[\lambda^+]$.

Beweis. **(a)** Wir schreiben wieder $M = P^n N$ mit $n \in \mathbb{N}_0$ und $P \nmid N$. Seien $v_1, \ldots, v_r$ die Fortsetzungen von v nach K_N. Aus dem Beweis des vorangegangenen Satzes geht hervor, daß v_i total verzweigt in K_M / K_N ist. Sei also w_i die Fortsetzung von v_i nach K_M und w die Fortsetzung von v nach K_{P^n}, dann ist

(1) $\quad e_{w_i/v_i} = m := \phi(P^n) = [K_M : K_N]$

und

(2) $\quad e_{w_i/w} = 1.$

Wir wählen $\pi \in \Lambda_{P^n}^*$ und $\nu \in \Lambda_N^*$. Nach 8.3(b) ist $A_v := R_v[\nu]$ der ganze Abschluß von R_v in K_N. Wegen $\lambda \in \Lambda_M = \Lambda_{P^n} + \Lambda_N \subseteq R[\pi, \nu] \subseteq R[\lambda]$ gilt weiter:

(3) $\quad A_v[\pi] = R_v[\pi, \nu] = R_v[\lambda]$

und

(4) $K_N(\pi) = K(\pi,\nu) = K(\lambda) = K_M$.

Sei $z \in K_M$ ganz über R_v. Wegen (4) und (1) können wir $z = \sum_{j=0}^{m-1} a_j\pi^j$ mit $a_j \in K_N$ schreiben. Da $w_i(\pi) = w(\pi) = 1$ nach (2) und 8.4 sowie $w_i(a_j) = mv_i(a_j) \in m\mathbb{Z}$ für $0 \le j < m$ aufgrund von (1) gilt, ist

$$0 \le w_i(z) = \min\{w_i(a_j\pi^j) \,:\, 0 \le j < m\}$$

nach 1.13(c), also $0 \le w_i(a_j) = mv_i(a_j)$ für $0 \le j < m$. Somit haben wir $a_j \in \bigcap_{i=1}^r R_{v_i} = A_v$ für $0 \le j < m$, also (3) zufolge $z \in A_v[\pi] = R_v[\lambda]$ gezeigt.

(b) Für $z \in K_M$ gilt nach 4.3(d) und (a):

$$z \in B \iff z \text{ ganz über } R = \bigcap_{v\ne v_\infty} R_v \iff z \in \bigcap_{v\ne v_\infty} R_v[\lambda] = R[\lambda].$$

(c) Sei $z \in K_M^+$. Nach 8.8(b) können wir $z = \sum_j a_j(\lambda^+)^j$ mit $a_j \in K$ schreiben, und nach (a) gilt

$$z \in B_v^+ \iff z \in B_v \iff \forall j : a_j \in R_v.$$

(d) Geht wie (c).

□

Es bleibt noch die Gradbewertung v_∞ bezüglich x von K zu untersuchen. Der folgende Satz verallgemeinert [Ha, Theorem 3.2] für ein beliebiges Polynom $M \in R \setminus k$ und berücksichtigt zugleich den reellen Teilkörper. Der Beweis ist unter stärkerer Ausnutzung des Newtonpolygonverfahrens gegenüber dem von Hayes angegebenen wesentlich vereinfacht (vgl. [Ha, pp. 83–85]).

9.4 Satz. *Sei $M \in R \setminus k$ und w bzw. w^+ eine Fortsetzung von $v := v_\infty$ nach $L := K_M$ bzw. $L^+ := K_M^+$ mit w/w^+. Dann gilt*

(a) *$e_{w^+/v} = f_{w^+/v} = 1$, d. h. v ist total zerlegt in L^+/K, und*

(b) *$e_{w/w^+} = q-1 = [L : L^+]$, d. h. w^+ ist total verzweigt in L/L^+.*

Beweis. Sei $\hat K$ bzw. $\hat L$ bzw. $\hat{L^+}$ die Komplettierung von K bzw. L bzw. L^+ nach v bzw. w bzw. w^+ und seien $\hat v$ und $\hat w$ die kanonischen Fortsetzungen gemäß 3.8.

(a) Für $N \in R \setminus \{0\}$ setzen wir $\Psi_N := \sum_{i=0}^{\operatorname{grad} N} \begin{bmatrix} N \\ i \end{bmatrix} u^{\frac{q^i-1}{q-1}}$. Damit ist $N \circ u = u\Psi_N(u^{q-1})$, also

(∗) $\Omega_N = \{\lambda^{q-1} \,:\, 0 \ne \lambda \in \Lambda_N\}$

die Nullstellenmenge von Ψ_N. Sei $d := \operatorname{grad} M$. Nach 7.1 und 3.12 ist

$$\Pi(\Psi_M) = \left\{ \left(\frac{q^i-1}{q-1}, -(d-i)q^i \right) \,:\, 0 \le i \le d \right\}$$

das Newtonpolygon von Ψ_M, und

$$\gamma_i := \frac{(d-i+1)q^{i-1} - (d-i)q^i}{q^{i-1}} = 1 - (d-i)(q-1),\ 1 \le i \le d,$$

sind die Steigungen seiner Kanten, da diese streng monoton zunehmen. Aus 3.13 ergibt sich, daß Ψ_M eine Nullstelle λ^+ in $\hat{K}$ hat mit

$$\hat{v}(\lambda^+) = -\gamma_1 = (d-1)(q-1) - 1.$$

Nach $(*)$ existiert ein $\lambda \in \Lambda_M$ mit $\lambda^+ = \lambda^{q-1}$. Für $N \in R$ mit $\operatorname{grad} N < d$ haben alle Nullstellen $\nu \in \hat{K}$ von Ψ_N nach den gleichen Überlegungen wie für Ψ_M Bewertung $\hat{v}(\nu) \leq (\operatorname{grad} N - 1)(q-1) - 1 < \hat{v}(\lambda^+)$. Daher ist $\lambda^+ \notin \Omega_N$, also $\lambda \notin \Lambda_N$ für alle echten Teiler N von M. Mit 7.7(c) folgt $\lambda \in \Lambda_M^*$ und mit 8.8(b) dann $L^+ = K(\lambda^+)$. Nach 3.10(b) muß also $\hat{L^+} = \hat{K}$ sein, woraus nach 3.10(a) und 1.23(b) die Behauptung folgt.

(b) Nach (a) und 3.10(a) ist $e_{\hat{w}/\hat{v}} = e_{w/w^+}$. Mit λ und λ^+ wie in (a) ist daher $(q-1)\hat{w}(\lambda) = e_{w/w^+}\hat{v}(\lambda^+)$. Wegen $\operatorname{ggT}(q-1, \hat{v}(\lambda^+)) = 1$ muß $q-1 | e_{w/w^+}$ gelten, also

$$q - 1 \leq e_{w/w^+} \leq [L : L^+] = q - 1.$$

□

9.5 Korollar. *k ist der Konstantenkörper von K_M/k.*

Beweis. Folgt nach 4.7(c) direkt aus dem vorhergehenden Satz. □

Für irreduzibles M läßt sich ein Beweis von 9.4 ohne Komplettierungsmethoden angeben. Er ist jedoch etwas technisch und wird den Rest dieses Abschnitts füllen. Wir benötigen zwei Lemmata. Durch Verschärfung der Abschätzungen bei [GR1, p. 372] gelangt man zu der folgenden Aussage.

9.6 Lemma. *Sei $M \in R \setminus k$, S^+ die Menge der Fortsetzungen von $v := v_\infty$ nach K_M^+, $\lambda \in \Lambda_M^*$ und $\lambda^+ := \lambda^{q-1}$. Für $w^+ \in S^+$ gilt entweder $w^+(\lambda^+) \geq 0$ oder $w^+(\lambda^+) = -e_{w^+/v}$.*

Beweis. Sei o. B. d. A. M normiert. Wir setzen $e := e_{w^+/v}$ und $d := \operatorname{grad} M$. Für $d = 1$ ist $M \circ u = u^q + Mu$, also $\lambda^+ = -M$ und damit $w^+(\lambda^+) = -e$. Sei also von nun an $d \geq 2$. Aus 7.1 ergibt sich $0 = \sum_{i=0}^{d} \begin{bmatrix} M \\ i \end{bmatrix} \lambda^{q^i - 1}$. Nach Division durch $x^{\frac{q^d-1}{q-1}}$ erhält man

$$(1) \quad 0 = \sum_{i=0}^{d} F_i \cdot (\lambda^+/x)^{\frac{q^i-1}{q-1}}$$

mit $F_i = x^{-\frac{q^d - q^i}{q-1}} \begin{bmatrix} M \\ i \end{bmatrix}$, also $F_d = 1$,

$$(2) \quad v(F_i) = \frac{q^d - q^i}{q-1} - q^i(d-i) = q^i \left[\frac{q^{d-i} - 1}{q-1} - d + i \right] \geq 0, \text{ speziell}$$

$$(3) \quad v(F_{d-1}) = 0 \quad \text{und}$$

$$(4) \quad v(F_{d-2}) = q^{d-2}(q-1).$$

Aus (1) und (2) folgt außerdem, daß λ^+/x ganz über R_v ist, daher

$$(5) \quad w^+(\lambda^+/x) \geq 0.$$

Weiter gilt für $0 \le i < d$:

$$\begin{aligned} v(F_i) - v(F_{i+1}) &= q^i \left[\frac{q^{d-i}-1}{q-1} - d + i\right] - q^{i+1}\left[\frac{q^{d-i-1}-1}{q-1} - d + i + 1\right] \\ &= q^i \left[\frac{q^{d-i}-1}{q-1} - \frac{q^{d-i}-q}{q-1} + (q-1)(d-i) - q\right] \\ &= q^i(q-1)(d-i-1) \ge 0, \end{aligned}$$

also

(6) $\quad v(F_i) \ge v(F_{i+1})$.

Wir unterscheiden nun zwei Fälle.

(a) $d = 2$ oder $q > 2$: Aus (1) ergibt sich

$$-\left[(\lambda^+/x)^{q^{d-1}} + F_{d-1}\right](\lambda^+/x)^{\frac{q^{d-1}-1}{q-1}} = \sum_{i=0}^{d-2} F_i \cdot (\lambda^+/x)^{\frac{q^i-1}{q-1}},$$

also nach (5), (6) und (4)

$$\begin{aligned} & w^+\left((\lambda^+/x)^{q^{d-1}} + F_{d-1}\right) + \frac{q^{d-1}-1}{q-1} w^+(\lambda^+/x) \\ &\ge \min\{w^+(F_i) + \frac{q^i-1}{q-1} w^+(\lambda^+/x) \,:\, 0 \le i \le d-2\} \\ &\ge \min\{w^+(F_i) \,:\, 0 \le i \le d-2\} \\ &= q^{d-2}(q-1)e. \end{aligned}$$

Mit (3) und (5) folgt, daß $w^+(\lambda^+/x) = 0$ oder

$$w^+(\lambda^+/x) \ge q^{d-2}\frac{(q-1)^2}{q^{d-1}-1}e = \left[q - 2 + \frac{q^{d-2}+q-2}{q^{d-1}-1}\right]e \ge e$$

ist, und somit haben wir $w^+(\lambda^+) = -e$ oder $w^+(\lambda^+) \ge 0$.

(b) $d > 2$ und $q = 2$: Wir zerlegen (1) in

$$\left[(\lambda^+/x)^{2^d-2^{d-2}} + F_{d-1}\cdot(\lambda^+/x)^{2^{d-2}} + F_{d-2}\right](\lambda^+/x)^{2^{d-2}-1} = \sum_{i=0}^{d-3} F_i \cdot (\lambda^+/x)^{q^i-1}.$$

Wie oben folgt mithilfe von (5), (6) und (2):

$$\begin{aligned} & w^+\left((\lambda^+/x)^{3\cdot 2^{d-2}} + F_{d-1}\cdot(\lambda^+/x)^{2^{d-2}} + F_{d-2}\right) + (2^{d-2}-1)w^+(\lambda^+/x) \\ (7) \quad &\ge w(F_{d-3}) \\ &= 2^{d-1}e. \end{aligned}$$

Nach (3) und (4) folgt aus $0 < w^+(\lambda^+/x) < e$, daß

$$w^+\left(F_{d-1}\cdot(\lambda^+/x)^{2^{d-2}}\right) < \min\left\{w^+\left((\lambda^+/x)^{3\cdot 2^{d-2}}\right), w^+(F_{d-2})\right\},$$

also mit (7), daß $2^{d-2}w^+(\lambda^+/x) + (2^{d-2}-1)w^+(\lambda^+/x) \ge 2^{d-1}e$ ist, und daraus $w^+(\lambda^+/x) > e$, ein Widerspruch. Daher ist $w^+(\lambda^+/x) = 0$ oder $w^+(\lambda^+/x) \ge e$, woraus wie im Fall (a) die Behauptung folgt.

□

Das zweite unserer beiden Lemmata, das sich bei [GR2, p. 367] wiederfindet, beruht auf der Idee, K_M als Erweiterung des rationalen Funktionenkörpers $k(\lambda)$ für $\lambda \in \Lambda_M^*$ aufzufassen. Wir führen die Überlegungen hier zusätzlich parallel für den reellen Teilkörper K_M^+ durch.

9.7 Lemma. *Sei $M = P^n$ mit irreduziblem $P \in R$ und $n \in \mathbb{N}$, $d := \operatorname{grad} P$, $\lambda \in \Lambda_M^*$ und $\lambda^+ := \lambda^{q-1}$. Dann ist*

$$[K_M : k(\lambda)] = [K_M^+ : k(\lambda^+)] = \begin{cases} q^{d-1} & \text{falls } n = 1 \\ q^{(n-1)d-1}(q^d - 1) & \text{falls } n \geq 2. \end{cases}$$

Beweis. Φ_M ist irreduzibel in $K[u]$ und normiert in u, also irreduzibel in $R[u] = k[u][x]$. Außerdem ist $\Phi_M \notin k[u]$, also irreduzibel in $k(u)[x]$. Gleiches gilt für das Minimalpolynom Φ_M^+ von λ^+ über K. Wegen $\Phi_M = \Phi_M^+(u^{q-1})$ ist daher

$$[K_M : k(\lambda)] = \operatorname{grad}_x \Phi_M = \operatorname{grad}_x \Phi_M^+ = [K_M^+ : k(\lambda^+)].$$

Nach 7.1 ist $\operatorname{grad}_x (P^m \circ u) = \operatorname{grad}_x \begin{bmatrix} P^m \\ md-1 \end{bmatrix} = q^{md-1}$ für alle $m \in \mathbb{N}$. Mithilfe von 8.6(b) erhalten wir hieraus

$$\operatorname{grad}_x \Phi_P = \operatorname{grad}_x (P \circ u) = q^{d-1}$$

und

$$\operatorname{grad}_x \Phi_{P^n} = \operatorname{grad}_x (P^n \circ u) - \operatorname{grad}_x (P^{n-1} \circ u) = q^{(n-1)d-1}(q^d - 1)$$

für $n \geq 2$. □

Durch Kombination der beiden Lemmata erhalten wir wie versprochen den weiteren

Beweis von 9.4 für irreduzibles M. Sei $\lambda \in \Lambda_M^*$, $\lambda^+ := \lambda^{q-1}$ und S^+ die Menge der Fortsetzungen von v nach L^+. Nach 8.4 und 4.7(c) ist k der Konstantenkörper von L^+/k.

(a) Wir setzen $d := \operatorname{grad} M$, $e := e_{w^+/v}$ und $f := f_{w^+/v}$. Da λ ganz über R ist, ist

$$(\lambda^+)_- = \sum_{\substack{v^+ \in S^+ \\ v^+(\lambda^+) = -e}} e\, \mathfrak{p}_{v^+}$$

nach 9.6 der Polstellendivisor von λ^+ in L^+. Mit 4.15 und 9.7 folgt

$$ef\#\{v^+ \in S^+ \,:\, v^+(\lambda^+) = -e\} = \operatorname{grad} (\lambda^+)_- = [L^+ : k(\lambda^+)] = q^{d-1}.$$

Daher ist ef eine Potenz von $p := \operatorname{char}(k)$. Da andererseits

$$ef\#S^+ = [L^+ : K] = \frac{q^d - 1}{q - 1} \equiv 1 \pmod{p}$$

gilt, folgt $ef = 1$.

An dem vorangehenden Lemma läßt sich ebenfalls erkennen, warum sich dieser Beweis nicht auf den Fall $M = P^n$ mit irreduziblem $P \in R$ und $n \geq 2$ übertragen läßt.

(b) Nach Teil (a) des Beweises existiert ein $\tilde{w}^+ \in S^+$ mit

$$\tilde{w}^+(\lambda^+) = -1.$$

Für eine Fortsetzung $\tilde{w}$ von $\tilde{w}^+$ nach L ist

$$(q-1)\tilde{w}(\lambda) = e_{\tilde{w}/\tilde{w}^+}\tilde{w}^+(\lambda^+) = -e_{\tilde{w}/\tilde{w}^+},$$

also $(q-1) \leq e_{\tilde{w}/\tilde{w}^+} \leq [L : L^+] = q-1$, woraus nach 2.2(a) die Behauptung folgt.

□

10 Das Geschlecht

Wir wollen nun die von [Ha, p. 85] für K_{P^n} mit irreduziblem $P \in R$ angegebene Geschlechtsformel auf beliebige zyklotomische Funktionenkörper K_M und ihre reellen Teilkörper erweitern. Abschließend werden wir uns in diesem Abschnitt dann mit dem asymptotischen Verhalten der Geschlechter für $\operatorname{grad} M \to \infty$ befassen und damit die asymptotische Untersuchung der Klassenzahlen vorbereiten.
Fortan sei $M \in R \setminus k$ normiert. Wir schreiben

$$M = \prod_{i=1}^{r} P_i^{n_i}$$

mit $r, n_i \in \mathbb{N}$ und verschiedenen normierten, irreduziblen $P_i \in R$ und setzen $f_i := \operatorname{grad} P_i$, $m_i := \phi(P_i) = q^{f_i} - 1$, $m := \phi(M) = \prod_{i=1}^{r} q^{(n_i-1)f_i} m_i$ sowie $d := \operatorname{grad} M = \sum_{i=1}^{r} n_i f_i$. Desweiteren bezeichne g bzw. g^+ das Geschlecht von $L := K_M$ bzw. $L^+ := K_M^+$. All diese Bezeichnungen sollen bis zum Schluß der Arbeit gelten.
Zunächst müssen wir Diskriminanten berechnen.

10.1 Lemma. *Sei $\lambda \in \Lambda_M^*$ und $\lambda^+ := \lambda^{q-1}$.*

(a) *Für $r = 1$ ist $\Phi_M(0) = P_1$.*

(b) *Ist $r \geq 2$, so ist $\Phi_M(0) = 1$ und λ^{-1} ganz über R.*

(c) *λ hat Diskriminante*

$$D_{L/K}(\lambda) = \pm \prod_{i=1}^{r} P_i^{n_i m - m/m_i}.$$

(d) *Ist $r \geq 2$, so ist*

$$D_{L^+/K}(\lambda^+) = \alpha \prod_{i=1}^{r} P_i^{\frac{n_i m - m/m_i}{q-1}}$$

mit $\alpha \in k^*$.

Beweis. **(a)** Wie im Beweis von 8.6(b).

(b) Folgt mithilfe von (a) und 8.6(c) durch Induktion nach d (Die Induktionsvoraussetzung geht beim dritten Gleichheitszeichen ein.):

$$M = \left(\frac{M \circ u}{u}\right)(0) = \prod_{\substack{N \in R \text{ normiert} \\ 1 \neq N \mid M}} \Phi_N(0) = \Phi_M(0) \prod_{i=1}^{r} \prod_{l_i=1}^{n_i} \Phi_{P_i^{l_i}}(0) = \Phi_M(0) M.$$

Ferner ist λ^{-1} als Nullstelle von $u^m\Phi_M(u^{-1}) \in R[u]$ ganz über R.

(c) Für $1 \le i \le r$ setzen wir $M_i := M/P_i$, $N_i := M/P_i^{n_i}$ und $L_i := K_{P_i^{n_i}}$. Nach Definition von Φ_M ist $M \circ u = \Phi_M\Psi$ mit

$$\Psi = \prod_{\mu\in\Lambda_M\setminus\Lambda_M^*} (u-\mu) \in R[u].$$

Mithilfe der Kettenregel und 1.26 folgt

$$(1)\quad M^m = N_{L/K}(\Phi_M'(\lambda)\Psi(\lambda)) = \pm D_{L/K}(\lambda) \prod_{\mu\in\Lambda_M\setminus\Lambda_M^*} N_{L/K}(\lambda-\mu).$$

Für $\mu \in \Lambda_M$ gilt nach (b)

$$(2)\quad \lambda-\mu \in \bigcup_{i=1}^{r} \Lambda_{P_i^{n_i}} \quad \text{oder} \quad N_{L/K}(\lambda-\mu) = \pm 1.$$

Wir betrachten daher $\mu \in \Lambda_M \setminus \Lambda_M^*$ mit $\lambda-\mu \in \Lambda_{P_i^{n_i}}$, $i \in \{1,\dots,r\}$ fest. Nach 7.7(c) muß $\mu \in \Lambda_{M_j}$ sein für ein $j \in \{1,\dots,r\}$. Wäre $j \ne i$, so wäre $P_i^{n_i} \circ \mu \in \Lambda_{N_i/P_j} \subsetneq \Lambda_{N_i}$, im Widerspruch dazu, daß $P_i^{n_i} \circ \mu = P_i^{n_i} \circ \lambda \in \Lambda_{N_i}^*$ ist nach 7.4(b). Also ist

$$(3)\quad \mu \in \Lambda_{M_i}.$$

Außerdem muß schon

$$(4)\quad \lambda-\mu \in \Lambda^*_{P_i^{n_i}}$$

gelten, denn aus $\lambda-\mu \in \Lambda_{P_i^{n_i-1}}$ würde $P_i^{n_i-1}\circ\mu = P_i^{n_i-1}\circ\lambda \in \Lambda^*_{N_iP_i}$ folgen, im Widerspruch zu $P_i^{n_i-1}\circ\mu \in \Lambda_{N_i} \subsetneq \Lambda_{N_iP_i}$.
Wir wollen nun $s_i := \#\{\mu \in \Lambda_M \setminus \Lambda_M^* \,:\, \lambda-\mu \in \Lambda_{P_i^{n_i}}\}$ bestimmen. Nach 7.5(a) gilt

$$(5)\quad \Lambda_{N_i} \cap \Lambda_{P_i} = 0,$$

also ist die Abbildung

$$\begin{array}{rcl} \Lambda_{N_i} & \to & \Lambda_{N_i} \\ \nu & \mapsto & P_i \circ \nu \end{array}$$

ein Isomorphismus von R-Moduln. Wir können demnach ein $\nu \in \Lambda_{N_i}$ finden, so daß $P_i\circ\nu = P_i^{n_i}\circ\lambda$ ist. Für $\mu \in \Lambda_M \setminus \Lambda_M^*$ haben wir damit wegen (3) und (5)

$$\lambda-\mu \in \Lambda_{P_i^{n_i}} \iff P_i\circ(P_i^{n_i-1}\circ\mu-\nu) = 0 \iff P_i^{n_i-1}\circ\mu = \nu.$$

Nach 7.4(a) ist $\Lambda_{P_i^{n_i-1}}$ der Kern bei $\Lambda_{M_i} \to \Lambda_{N_i}$, $\mu \mapsto P_i^{n_i-1}\circ\mu$. Daher ist

$$s_i = \#\Lambda_{P_i^{n_i-1}} = \phi(P_i^{n_i})/m_i.$$

Mit (2), (4) und (a) folgt

$$\prod_{\mu\in\Lambda_M\setminus\Lambda_M^*} N_{L/K}(\lambda-\mu) = \pm\prod_{i=1}^{r}\left(\Phi_{P_i^{n_i}}(0)\right)^{s_i[L:L_i]} = \pm\prod_{i=1}^{r} P_i^{m/m_i},$$

und man erhält die Behauptung durch Einsetzen in (1).

(d) Sei Φ_M^+ das Minimalpolynom von λ^+ über K. Es ist $\Phi_M = \Phi_M^+(u^{q-1})$, also nach Kettenregel

$$\Phi_M' = -u^{q-2}(\Phi_M^+)'(u^{q-1}).$$

Mit 1.26 und (b) folgt

$$\begin{aligned} D_{L/K}(\lambda) &= \pm N_{L/K}(\Phi_M'(\lambda)) \\ &= \pm(N_{L/K}(\lambda))^{q-2} N_{L/K}((\Phi_M^+)'(\lambda^+)) \\ &= \pm(\Phi_M(0))^{q-2}(N_{L^+/K}((\Phi_M^+)'(\lambda^+)))^{q-1} \\ &= \pm(D_{L^+/K}(\lambda^+))^{q-1}. \end{aligned}$$

Da R faktoriell ist, ergibt sich hieraus und aus (c) die Behauptung.

□

Wir können nun die allgemeinen Geschlechtsformeln für zyklotomische Funktionenkörper und ihre reellen Teilkörper hinschreiben.

10.2 Satz. *Für die Geschlechter gelten die Formeln:*

(a) $2g-2 = (d-2)m + (q-2)\frac{m}{q-1} - \sum_{i=1}^r \frac{m}{m_i} f_i$.

(b) *Für* $r=1$ *ist* $2g-2 = (q-1)(2g^+-2) + (q-2)(\frac{m}{q-1} + f_1)$.

(c) *Für* $r \geq 2$ *ist* $2g-2 = (q-1)(2g^+-2) + (q-2)\frac{m}{q-1}$.

Beweis. Sei v_∞ die Gradbewertung von K bezüglich x und $v_i := v_{P_i}$. Nach 4.3(b) ist $f_{v_i} = f_i$.

(a) Wir berechnen die in 5.1(a) eingeführten Zahlen $d_{L,v}$ für $v \in V(K/k)$. Nach 9.3(a) und 10.1(c) ist

$$d_{L,v_i} = v_i(D_{L/K}(\lambda)) = n_i m - m/m_i,$$

und nach 5.5(b) und 9.4 gilt

$$d_{L,v_\infty} = \sum_{w/v_\infty} (e_{w/v_\infty} - 1) f_{w/v_\infty} = (q-2)\frac{m}{q-1}.$$

Für $v \neq v_i, v_\infty$ ist offenbar $d_{L,v} = 0$. Einsetzen in 5.2 ergibt

$$2g-2 = -2m + d_{L,v_\infty} f_{v_\infty} + \sum_{i=1}^r d_{L,v_i} f_i = -2m + (q-2)\frac{m}{q-1} + dm - \sum_{i=1}^r \frac{m}{m_i} f_i.$$

(b) Hier wenden wir den Satz von Riemann-Hurwitz auf L/L^+ an. Nach 8.4 ist v_1 total verzweigt in L/K, daher gilt für die einzige Fortsetzung w_1^+ von v_1 nach L^+, daß $f_{w_1^+} = f_1$, und wegen 5.5(b), daß $d_{L,w_1^+} = q-2$ ist. Für die $\frac{m}{q-1}$ Fortsetzungen w^+/v_∞ ist $f_{w^+} = 1$ und $d_{L,w^+} = q-2$ nach 9.4 und 5.5(b). Wiederum gilt für alle anderen Bewertungen $\tilde{w}^+$ von L^+ nach 8.3(c) und 5.5(b), daß $d_{L,\tilde{w}^+} = 0$ ist. Die Formel ergibt sich hieraus durch Einsetzen.

(c) Diesmal wenden wir 5.2 auf L^+/K an. Nach 9.3(c) und 10.1(d) gilt

$$d_{L^+,v_i} = v_i(D_{L^+/K}(\lambda^+)) = \frac{n_i m - m/m_i}{q-1}$$

und nach 5.5(b) und 9.4(a):

$$d_{L^+,v_\infty} = 0.$$

Einsetzen unter Beachtung von (a) ergibt

$$\begin{aligned}(q-1)(2g^+-2) &= -2m + \sum_{i=1}^{r}(n_i m - m/m_i)f_i \\ &= (d-2)m - \sum_{i=1}^{r}\frac{m}{m_i}f_i \\ &= 2g-2-(q-2)\frac{m}{q-1}.\end{aligned}$$

□

10.3 Korollar. *Sei $r \geq 2$ und S^+ die Menge der Fortsetzungen der Gradbewertung v_∞ von K nach L^+. Dann sind alle Bewertungen $w^+ \notin S^+$ von L^+ unverzweigt in L/L^+.*

Beweis. Aus 5.2 ergibt sich wie im Beweis von Teil (b) des vorigen Satzes

$$2g-2 = (q-1)(2g^+-2) + (q-2)\frac{m}{q-1} + \sum_{w^+\notin S^+} d_{L,w^+}f_{w^+}.$$

Bei Vergleich mit 10.2(c) erkennt man, daß $d_{L,w^+} = 0$ sein muß für alle $w^+ \notin S^+$, woraus mit 5.5(a) die Behauptung folgt. □

10.4 Korollar. *Für normiertes, irreduzibles $P \in R$ schreiben wir wieder $M = P^n N$ mit $n \in \mathbb{N}_0$ und $P \nmid N$. Ist $N \neq 1$ und w^+ eine Fortsetzung von $v := v_P$ nach L^+, so gilt $e_{w^+/v} = \phi(P^n)$, und $f_{w^+/v}$ ist die Ordnung von $(P+RN)k^*$ in $(R/RN)^*/k^*$.*

Beweis. Nach dem Beweis von 9.1 ist $\sigma_P \in G_N$ der Artinautomorphismus von v in K_N/K, also ist $\sigma_P|_{K_N^+}$ der Artinautomorphismus von v in K_N^+/K, und die Behauptung folgt mit 10.3 und 8.3(c). □

Aus den Geschlechtsformeln 10.2 läßt sich wegen 4.20(a) leicht ablesen, wann ein zyklotomischer Funktionenkörper bzw. sein reeller Teilkörper ein rationaler Funktionenkörper $k(z)$ ist. Die konkrete Bestimmung eines geeigneten z wäre eventuell etwas schwieriger.

10.5 Beispiele. Wir wollen sämtliche Polynome M bestimmen, für die L bzw. L^+ ein rationaler Funktionenkörper wird. Für solche Polynome muß nach 9.4

$(*)$ $\quad m \leq q^2-1$

sein. Andererseits ist offenbar $(q-1)^d \leq m$, wobei das Gleichheitszeichen nur für $r = d$ eintritt. Aus $d \geq 3$ und $(*)$ folgt $(q-1)^3 < q^2-1$, d. h. $q < 3$ im Fall $r < d$, und $q \leq 3$ im Fall $r = d$. Wegen 8.9 sind daher nur noch die Fälle

(a) $d = 2$,
(b) $r = d = 3 = q$ und
(c) $q = 2$, $d \geq 3$

zu prüfen.

(a) Für $d = 2$ sind drei verschiedene Formen von M zu unterscheiden. Durch Einsetzen in 10.2(a) ergibt sich

- $g = (q-2)(q-3)/2$ für $r = 2$ (M zerfällt in zwei verschiedene Linearfaktoren).
- $g = (q-1)(q-2)/2$ für $r = 1$, $f_1 = 1$ (M ist das Quadrat eines linearen Polynoms).
- $g = (q+1)(q-2)/2$ für $r = 1$, $f_1 = 2$ (M ist irreduzibel).

In allen drei Fällen ist $g^+ = 0$ (nachrechnen).

(b) Für $r = d = 3 = q$ ist $g = 1$ und $g^+ = 0$.

(c) Unter Beachtung von $(*)$ bleiben bei $q = 2$, $d \geq 3$ nur noch die Fälle

$$M \in \{x(x^2+x+1), (x+1)(x^2+x+1), x^2(x+1), x(x+1)^2, x(x+1)(x^2+x+1)\}$$

übrig, für die sämtlich $g = g^+ = 0$ ist.

Beispiel. Es sei $P \in R$ ein lineares Polynom mit $P \nmid M$ und $\tilde{M} := PM$. Desweiteren bezeichne $\tilde{g}$ bzw. $\tilde{g}^+$ das Geschlecht von $\tilde{L} := K_{\tilde{M}}$ bzw. $\tilde{L}^+ := K^+_{\tilde{M}}$. Offenbar ist $[\tilde{L} : L] = q - 1 = [\tilde{L} : \tilde{L}^+]$, und nach 10.2(a) und (c) haben wir für die Geschlechter

$$\begin{aligned}
&(q-1)(2\tilde{g}^+ - 2) + (q-2)m \\
&\quad = \quad 2\tilde{g} - 2 \\
&\quad = \quad (d-1)(q-1)m + (q-2)m - \sum_{i=1}^{r} \frac{(q-1)m}{m_i} f_i - m \\
&\quad = \quad (q-1)(2g-2) + (q-1)m - m,
\end{aligned}$$

also $g = \tilde{g}^+$. Trotzdem ist $L \neq \tilde{L}^+$ für $q \neq 2$, denn jede Fortsetzung von v_P nach L ist nach dem Beweis von 9.1 total verzweigt in $\tilde{L}/L$, während die Fortsetzungen von v_P nach $\tilde{L}^+$ wegen 10.3 in $\tilde{L}/\tilde{L}^+$ unverzweigt sind.

Wir wollen nun noch das asymptotische Verhalten der Geschlechter für $d = \operatorname{grad} M \to \infty$ untersuchen. Dafür führen wir zunächst die folgenden Notationen ein. Für von M abhängige Zahlen $F, G \in \mathbb{C}$ schreiben wir

- $F \prec G$ (in Worten: F ist **von kleinerer Ordnung als** G), falls zu jedem $\varepsilon > 0$ ein $d_0 \in \mathbb{N}$ existiert, so daß $d \geq d_0$ stets $|F| < \varepsilon|G|$ impliziert.
- $F \sim G$ (in Worten: F ist **asymptotisch gleich** G), falls zu jedem $\varepsilon > 0$ ein $d_1 \in \mathbb{N}$ existiert, so daß $d \geq d_1$ stets $|F - G| \leq \varepsilon|F + G|$ impliziert.

Offenbar ist $\prec$ transitiv und $\sim$ eine Äquivalenzrelation. Nehmen wir $G \neq 0$ an, so läßt sich $F \prec G$ bzw. $F \sim G$ in die bekanntere Form $\lim_{d\to\infty} F/G = 0$ bzw. $\lim_{d\to\infty} F/G = 1$ bringen. Desweiteren gelten die Eigenschaften:

- Ist $F \sim G \prec H$ oder $F \prec G \sim H$, so gilt $F \prec H$.
- Mit $F \sim G$ hat man auch $FH \sim GH$.
- Aus $F \prec G$ folgt $G \sim F + G$.

Wir schätzen zuerst den etwas schwierigen Term in der Geschlechtsformel 10.2 ab.

10.6 Lemma. *Es gilt* $\sum_{i=1}^{r} \frac{f_i}{m_i} \le (1+\log_q r)^2$.

Beweis. Für $n \in \mathbb{N}$ setzen wir

$$\mathcal{M}_n := \{N \in R \text{ normiert} : N \neq 1 \text{ und } \operatorname{grad} N \le n\},$$

dann ist offenbar $\#\mathcal{M}_n = q^n - 1$. Wählen wir nun $s \in \mathbb{N}$ minimal mit $s > \log_q r$, so haben wir $\#\mathcal{M}_s \ge r$ und $s \le 1 + \log_q r$. Da außerdem die Folge $\left(\frac{n}{q^n-1}\right)_{n\in\mathbb{N}}$ monoton fallend ist, ergibt sich

$$\sum_{i=1}^{r} \frac{f_i}{m_i} = \sum_{i=1}^{r} \frac{f_i}{q^{f_i}-1} \le \sum_{N\in\mathcal{M}_s} \frac{\operatorname{grad} N}{q^{\operatorname{grad} N}-1} = \sum_{n=1}^{s} (q^n - q^{n-1}) \frac{n}{q^n-1} \le \sum_{n=1}^{s} n \le s^2.$$

□

10.7 Satz. *Für die Geschlechter haben wir das asymptotische Verhalten*

$$g \sim \frac{md}{2} \sim (q-1)g^+.$$

Beweis. Nach dem vorigen Lemma ist $\sum_{i=1}^{r} \frac{f_i}{m_i} \prec r \le d$, also haben wir mithilfe von 10.2(a), daß

$$\frac{2g-2}{m} = d - 2 + \frac{q-2}{q-1} - \sum_{i=1}^{r} \frac{f_i}{m_i} \sim d$$

und daher $g \sim md/2$ ist. Insbesondere gilt $f_1 \le m \prec g$, so daß sich $g \sim (q-1)g^+$ aus 10.2(b) und (c) ergibt. □

11 Klassenzahlen

Die Betrachtungen von Quebbemann [Qb] aufgreifend untersuchen wir in diesem Abschnitt das Verhalten der zyklotomischen Klassenzahlen für $d = \operatorname{grad} M \to \infty$. Für die erforderlichen Resultate über Einheitengruppe und Idealklassengruppe des Rings ganzer Funktionen in L bzw. L^+ stützen wir uns soweit wie möglich auf [GR1] und [GR2].
Für die Divisorenklassenzahlen $h_0 := h_0(L)$ und $h_0^+ := h_0(L^+)$ gelten nach 6.15(b) die Abschätzungen

$$\begin{aligned} 2g\log_q(\sqrt{q}-1) \le \log_q h_0 \le 2g\log_q(\sqrt{q}+1), \\ 2g^+\log_q(\sqrt{q}-1) \le \log_q h_0^+ \le 2g^+\log_q(\sqrt{q}+1). \end{aligned}$$

Diese lassen sich durch den folgenden, auch in allgemeineren Situationen gültigen Satz (vgl. [Qb, p. 84]) für $d \to \infty$ noch verschärfen. Wir verwenden die im letzten Abschnitt eingeführten Relationen $\sim$ und $\prec$.

11.1 Satz. *Es gilt*

(a) $\log_q h_0 \sim g$ *und*
(b) $\log_q h_0^+ \sim g^+$.

BEWEIS. **(a)** Für $j \in \mathbb{N}$ bezeichne $k_j := \mathbb{F}_{q^j}$ den Erweiterungskörper vom Grad j über $k = \mathbb{F}_q$ und K_j/k_j bzw. L_j/k_j die zugehörige Konstantenkörpererweiterung von K/k bzw. L/k. Für die Anzahl N_j der rationalen Punkte von L_j/k_j haben wir nach 4.3 und 1.21(c) die Abschätzung

$$N_j \le m(q^j + 1). \tag{1}$$

Aus 6.10(a), 6.16 und der Definition der Weil-Zahlen $\omega_1, \ldots, \omega_{2g}$ von L ergibt sich für jedes $j \in \mathbb{N}$ die Identität

$$-\sum_{i=1}^{2g} \omega_i^j = N_j - (q^j + 1), \tag{2}$$

woraus wir nach dem Satz von Weil analog zu 6.15(a) die weitere Abschätzung

$$|N_j - (q^j + 1)| \le 2gq^{j/2} \tag{3}$$

ableiten können. Ordnen wir wie in 6.15(c) die Weil-Zahlen so an, daß $\omega_i\omega_{g+i} = q$ ist für $1 \le i \le g$, so können wir mithilfe von 6.10(b) schließen, daß

$$\begin{aligned} h_0 &= \prod_{i=1}^{2g}(1 - \omega_i) \\ &= \prod_{i=1}^{g} \omega_i\omega_{g+i}(1 - \omega_i^{-1})(1 - \omega_{g+i}^{-1}) \\ &= q^g \prod_{i=1}^{g}(1 - q^{-1}\omega_{g+i})(1 - q^{-1}\omega_i) \\ &= q^g \prod_{i=1}^{2g}(1 - q^{-1}\omega_i) \end{aligned}$$

ist. Mithilfe der Reihenentwicklung $\ln(1-z) = -\sum_{j=1}^{\infty} \frac{z^j}{j}$ für $z \in \mathbb{C}$, $|z| < 1$ und (2) erhalten wir hieraus

$$\ln h_0 - g \ln q = \sum_{i=1}^{2g} \ln(1 - q^{-1}\omega_i) = -\sum_{j=1}^{\infty} \frac{1}{jq^j} \sum_{i=1}^{2g} \omega_i^j = \sum_{j=1}^{\infty} \frac{1}{jq^j}(N_j - (q^j + 1)). \tag{4}$$

Wählen wir nun $s \in \mathbb{N}$ abhängig von M mit $s \sim g/m$, so haben wir sowohl

$$\left|\sum_{j=1}^{s} \frac{1}{jq^j}(N_j - (q^j + 1))\right| \le \left|\sum_{j=1}^{s} \frac{N_j}{jq^j}\right| + \left|\sum_{j=1}^{s} \frac{q^j + 1}{jq^j}\right| \le (m+1) \sum_{j=1}^{s} \left(\frac{1}{j} + \frac{1}{jq^j}\right) \prec ms \sim g$$

wegen (1) als auch

$$\left|\sum_{j=s+1}^{\infty} \frac{1}{jq^j}(N_j - (q^j + 1))\right| \le 2g \sum_{j=s+1}^{\infty} \frac{1}{jq^{j/2}} \prec g$$

wegen (3) und 10.7. Daher folgt aus (4), daß $\ln h_0 \sim g \ln q$ ist.

(b) Geht ganz analog.

□

Wir wollen nun auch die Asymptotik der Idealklassenzahlen $h := h(B)$ und $h^+ := h(B^+)$ der ganzen Abschlüsse B bzw. B^+ von R in L bzw. L^+ untersuchen. Zunächst bestimmen wir das Verhältnis der Einheitengruppen dieser beiden Ringe. Vgl. hierzu [GR1, p. 366] und [GR2, p. 166].

11.2 Satz. *Für die Einheitengruppen $U := B^*$ und $U^+ := (B^+)^*$ gilt:*

(a) *Bei $r = 1$ ist $U = U^+$.*

(b) *Bei $r \geq 2$ ist $(U : U^+) = q - 1$.*

Beweis. Die Anfänge der Beweise von (a) und (b) sind identisch. Sei $z \in U$.

Die Menge der Fortsetzungen der Gradbewertung v_∞ von K nach L bezeichnen wir mit S und zu $\sigma \in G_0 := \mathrm{Aut}(L/L^+)$ definieren wir $\varepsilon_\sigma := \sigma(z)/z$. Für jedes $w \in S$ und $\sigma \in G_0$ ist $w^\sigma = w$ nach 9.4(b) und 2.1(b), also gilt

$$w(\varepsilon_\sigma) = 0 \quad \forall \sigma \in G_0.$$

Da außerdem $\varepsilon_\sigma \in U = \bigcap_{w \notin S} R_w^*$ ist für alle $\sigma \in G_0$, ergibt sich nach 4.8(b) und 9.5, daß

$$(*) \quad \varepsilon_\sigma \in k^* \quad \forall \sigma \in G_0.$$

(a) Sei w^+ eine Fortsetzung von v_{P_1} nach L^+ und $L' := L^+(z)$. Aus $(*)$ folgt $\sigma(z^{q-1}) = z^{q-1}$ für alle $\sigma \in G_0$, d. h. $z^{q-1} \in U \cap L^+ = U^+ \subseteq R_{w^+}^*$. Daher ist $w^+(z^{q-1}) = 0$, und mit 1.27 folgt, daß w^+ unverzweigt in L'/L^+ ist. Da nach 8.4 andererseits w^+ total verzweigt in L/L^+ ist, muß $L' = L^+$, also $z \in U \cap L^+ = U^+$ sein.

(b) Sei $\lambda \in \Lambda_M^*$. Nach $(*)$ und 8.8(c) können wir $z = z^+\lambda^i$ mit $z^+ \in L^+$ und $0 \leq i < q - 1$ schreiben. Wegen 10.1(b) ist $\lambda \in U$, also $z^+ \in U \cap L^+ = U^+$ und $z \in \lambda^i U^+$. Damit haben wir

$$U/U^+ = \{\lambda^i U^+ \,:\, 0 \leq i < q - 1\}$$

gezeigt. Wegen $\lambda^i \notin L^+$ für $1 \leq i < q - 1$ ist $\lambda^i U^+ \neq \lambda^j U^+$ für $0 \leq i < j < q - 1$, also tatsächlich $(U : U^+) = q - 1$.

□

Der folgende wichtige Satz, der uns garantiert, daß wie in der klassischen Theorie h^+ ein Teiler von h ist (vgl. [Wh, p. 40]), ist für den Fall $r = 1$ (mit etwas anderen Methoden) bei [GR1, p. 366f] bewiesen.

11.3 Satz. *Der natürliche Klassengruppenhomomorphismus*

$$\begin{array}{rcl} \mathcal{C}\ell(B^+) & \to & \mathcal{C}\ell(B) \\ [I^+] & \mapsto & [BI^+] \end{array}$$

ist injektiv.

BEWEIS. Sei I^+ ein Ideal von B^+, so daß BI^+ ein Hauptideal von B ist, etwa $BI^+ = Bz$ für ein $z \in B$. Zu zeigen ist, daß I^+ Hauptideal von B^+ ist. Für $\sigma \in G_0 := \mathrm{Aut}(L/L^+)$ setzen wir wieder $\varepsilon_\sigma := \sigma(z)/z$. Nach 1.2(c) ist $B\sigma(z) = \sigma(Bz) = \sigma(BI^+) = BI^+ = Bz$ für alle $\sigma \in G_0$, also

$$\varepsilon_\sigma \in B^* \quad \forall \sigma \in G_0.$$

Dem vorhergehenden Satz zufolge ist auf jeden Fall $\varepsilon_\sigma^{q-1} \in (B^+)^*$ für alle $\sigma \in G_0$. Man sieht leicht, daß dann die Abbildung

$$\begin{array}{rcl} G_0 & \to & (B^+)^* \\ \sigma & \mapsto & \varepsilon_\sigma^{q-1} \end{array}$$

ein Gruppenhomomorphismus ist. Daher liegt ε_σ^{q-1} als Nullstelle von $u^{q-1}-1$ für jedes $\sigma \in G_0$ in k^*. Da k in L algebraisch abgeschlossen ist, folgt schließlich

$$(*) \quad \varepsilon_\sigma \in k^* \quad \forall \sigma \in G_0.$$

Wir unterscheiden nun wieder die Fälle $r = 1$ und $r \geq 2$.

(a) Sei $r = 1$ und w^+ eine Fortsetzung von v_{P_1} nach L^+. Nach 1.23(a) ist $w^+ = v_{Q^+}$ für ein $Q^+ \in \mathrm{Max}(B^+)$. Wir schreiben

$$I^+ = (Q^+)^s J^+$$

mit $s \in \mathbb{N}_0$ und einem Ideal J^+ von B^+, das von Q^+ nicht geteilt wird. Aus $(*)$ folgt $\sigma(z^{q-1}) = z^{q-1}$ für alle $\sigma \in G_0$, d. h. $z^{q-1} \in B \cap L^+ = B^+$. Also ist $(I^+)^{q-1} = B^+ z^{q-1}$ Hauptideal von B^+ und $w^+(z^{q-1}) = (q-1)s$. Wählen wir $\lambda^+ \in L^+$ mit $w^+(\lambda^+) = 1$ und setzen $\beta := z/(\lambda^+)^s$ und $L' := L^+(z) = L^+(\beta)$, so ist $w^+(\beta^{q-1}) = w^+(z^{q-1}) - w^+((\lambda^+)^{(q-1)s}) = 0$, also w^+ nach 1.27 unverzweigt in L'/L^+. Da w^+ nach 8.4 andererseits total verzweigt in L/L^+ ist, folgt $L' = L^+$ und $z \in B \cap L^+ = B^+$, also ist $I^+ = B^+ z$ Hauptideal von B^+.

(b) Sei $r \geq 2$ und $\lambda \in \Lambda_M^*$. Wegen $(*)$ und 8.8(c) können wir wieder

$$z = z^+ \lambda^i$$

mit $z^+ \in L^+$ und $0 \leq i < q-1$ schreiben. Nach 10.1(b) ist $z^+ \in B \cap L^+ = B^+$ und $BI^+ = Bz^+$, also $I^+ = B^+ z^+$ Hauptideal von B^+.

□

Die Idealklassengruppen bezeichnen wir nun zur Abkürzung durch $\mathcal{C}\ell := \mathcal{C}\ell(B)$ und $\mathcal{C}\ell^+ := \mathcal{C}\ell(B^+)$. Desweiteren setzen wir $W := V(L/k)$ bzw. $W^+ := V(L^+/k)$ für die abstrakte Kurve von L/k bzw. L^+/k, $S := \{w \in W : w/v_\infty\}$ bzw. $S^+ := \{w^+ \in W^+ : w^+/v_\infty\}$ für die Menge der Fortsetzungen der Gradbewertung v_∞ von K nach L bzw. L^+, $\mathcal{D} := \mathcal{D}_L$, $\mathcal{D}^+ := \mathcal{D}_{L^+}$, $\mathcal{D}_0 := \mathcal{D}_{L,0}$ und $\mathcal{D}_0^+ := \mathcal{D}_{L^+,0}$ für die Divisorengruppen und $\mathcal{C}\ell_0 := \mathcal{C}\ell_0(L)$ bzw. $\mathcal{C}\ell_0^+ := \mathcal{C}\ell_0(L^+)$ für die Divisorenklassengruppen von L bzw. L^+. Die kanonische Einbettung

$$\begin{array}{rcl} \mathcal{D}^+ & \to & \mathcal{D} \\ \displaystyle\sum_{w^+ \in W^+} d_{w^+} \mathfrak{p}_{w^+} & \mapsto & \displaystyle\sum_{w^+ \in W^+} d_{w^+} \sum_{w/w^+} e_{w/w^+} \mathfrak{p}_w \end{array}$$

fassen wir der Einfachheit halber als Inklusion auf. Wir wollen die Divisorenklassengruppen mit den Idealklassengruppen in Zusammenhang bringen und definieren hierfür die Gruppen

$$\mathcal{E} := \bigoplus_{w\in S} \mathbb{Z}\mathfrak{p}_w \subseteq \mathcal{D},$$

$$\mathcal{E}^+ := \bigoplus_{w^+\in S^+} \mathbb{Z}\mathfrak{p}_{w^+} \subseteq \mathcal{D}^+$$

der Divisoren von L bzw. L^+ mit Träger in S bzw. S^+. Man überlegt sich leicht, daß die Abbildung

$$\begin{array}{rcl} \mathcal{C}\ell & \to & \mathcal{D}/(\mathcal{E}+(L^*)) \\ \left[\prod_{Q\in\mathrm{Max}(B)} Q^{d_Q}\right] & \mapsto & \displaystyle\sum_{Q\in\mathrm{Max}(B)} d_Q\mathfrak{p}_{v_Q} + (\mathcal{E}+(L^*)) \end{array}$$

ein Gruppenisomorphismus ist. In gleicher Weise ist auch $\mathcal{C}\ell^+ \simeq \mathcal{D}^+/(\mathcal{E}^+ + ((L^+)^*))$. Dabei kommutiert der Klassengruppenhomomorphismus aus dem vorigen Satz mit der kanonischen Einbettung

$$\mathcal{D}^+/(\mathcal{E}^+ + ((L^+)^*)) \hookrightarrow \mathcal{D}/(\mathcal{E}+(L^*)),$$

die sich aus der Inklusion $\mathcal{D}^+ \subseteq \mathcal{D}$ von oben ergibt. Wir definieren noch $\mathcal{E}_0 := \mathcal{E} \cap \mathcal{D}_0$ und $\mathcal{E}_0^+ := \mathcal{E}^+ \cap \mathcal{D}_0^+$ und betrachten die Sequenzen der kanonischen Gruppenhomomorphismen

$$0 \to \mathcal{E}_0/(\mathcal{E}_0\cap(L^*)) \to \mathcal{C}\ell_0 \to \mathcal{D}/(\mathcal{E}+(L^*)) \to 0,$$

$$0 \to \mathcal{E}_0^+/(\mathcal{E}_0^+\cap((L^+)^*)) \to \mathcal{C}\ell_0^+ \to \mathcal{D}^+/(\mathcal{E}^+ + ((L^+)^*)) \to 0.$$

Sie sind offenbar exakt (Die Surjektivität der hinteren Abbildungen gilt, da S und S^+ rationale Punkte enthalten). Daher ist $h_0 = \rho h$ und $h_0^+ = \rho^+ h^+$, wobei $\rho := (\mathcal{E}_0 : \mathcal{E}_0 \cap (L^*))$ bzw. $\rho^+ := (\mathcal{E}_0^+ : \mathcal{E}_0^+ \cap ((L^+)^*))$ der **Regulator von** L bzw. L^+ genannt wird. Der nächste Satz behandelt in Verallgemeinerung von [Qb, Theorem 3.3] für $d \to \infty$ das asymptotische Verhalten des Quotienten

$$h^- := \frac{h}{h^+},$$

der nach dem vorigen Satz eine natürliche Zahl ist. Für $q = 2$ ist $L^+ = L$, also $h^- = 1$.

11.4 Satz. *Für $q \neq 2$ haben wir*

$$\log_q h^- \sim \frac{q-2}{q-1}\frac{md}{2}.$$

Beweis. Sei $N := \#S = \#S^+ = m/(q-1)$. Offenbar sind $\mathcal{E}_0$ und $\mathcal{E}_0^+$ freie abelsche Gruppen, beide vom Rang $N-1$, und da nach 9.4(b) mit der Inklusion von oben $\mathcal{E}_0^+ = (q-1)\mathcal{E}_0$ ist, folgt

$$(\mathcal{E}_0 : \mathcal{E}_0^+) = (q-1)^{N-1}.$$

Desweiteren ist offenbar $\mathcal{E}_0 \cap (L^*) = (B^*) \simeq B^*/k^*$, ebenso $\mathcal{E}_0^+ \cap ((L^+)^*) = ((B^+)^*) \simeq (B^+)^*/k^*$ und daher

$$(\mathcal{E}_0 \cap (L^*) : \mathcal{E}_0^+ \cap ((L^+)^*)) = (B^* : (B^+)^*) = s := \begin{cases} 1 & \text{für } r = 1 \\ q-1 & \text{für } r \geq 2 \end{cases}$$

nach 11.2. Insgesamt ergibt sich $\rho/\rho^+ = (q-1)^{N-1}/s$, also $\log_q(\rho^+/\rho) \sim -\frac{\ln(q-1)}{(q-1)\ln q} m \prec g$. Zusammen mit 11.1 und 10.7 erhalten wir

$$\log_q h^- = \log_q \frac{\rho^+}{\rho} + \log_q h_0 - \log_q h_0^+ \sim (1 - \frac{1}{q-1})g \sim \frac{q-2}{q-1}\frac{md}{2}.$$

□

Aus diesem Satz ergibt sich insbesondere, daß $h \to \infty$ für $d \to \infty$ und $q \neq 2$. Im Fall $q = 2$ können wir keine Aussage machen. Es stellt sich die Frage, ob es hier überhaupt Beispiele mit $h \neq 1$ gibt (Ich kann keines angeben).
Zur nun folgenden Berechnung von Klassenzahlen für konkrete Polynome M führen wir einige Notationen ein. Wir bezeichnen mit W_n bzw. W_n^+ die Menge der Bewertungen von L bzw. L^+ vom Grad n und definieren für $N \in \mathbb{N}$, $n \in \mathbb{N}_0$ das Symbol

$$\begin{bmatrix} N \\ n \end{bmatrix} := \#\{(a_1, \ldots, a_N) \in \mathbb{N}_0^N \,:\, a_1 + \cdots + a_N = n\}.$$

Mithilfe vollständiger Induktion überlegt man sich leicht, daß $\begin{bmatrix} N \\ n \end{bmatrix} = \binom{N-1+n}{n}$ ist. Desweiteren seien wie in Abschnitt 6 eingeführt $A_0, A_1, \ldots$ bzw. $A_0^+, A_1^+, \ldots$ die Koeffizienten und $P(t)$ bzw. $P^+(t)$ das Zählerpolynom der Zetafunktion von L bzw. L^+.
Für Divisorenklassenzahlen haben Galovich und Rosen in [GR1] und [GR2] Formeln unter Verwendung von L-Reihen angegeben, nach denen Ireland und Small [IS] mithilfe eines Computerprogramms Klassenzahlen ausgerechnet haben. Aber auch aus unseren Sätzen können wir ein konkretes Verfahren zur Berechnung von h_0 und h_0^+ ableiten: Zunächst bestimme man mithilfe von 9.1 bzw. 10.4 sämtliche Bewertungen mit Grad $\leq g$ bzw. $\leq g^+$ von L bzw. L^+. Für die Fortsetzungen der Bewertungen v_P mit $P \nmid M$ ergeben sie sich dabei aus der Zerlegung aller Polynome $AM+1$ für $A \in R$ normiert mit $\operatorname{grad} A \leq g-d$ bzw. aller Polynome $AM + \alpha$ für $\alpha \in k^*$ und $A \in R$ normiert mit $\operatorname{grad} A \leq g^+ - d$. Aus $\#W_1, \ldots, \#W_g$ bzw. $\#W_1^+, \ldots, \#W_{g^+}^+$ lassen sich dann mithilfe kombinatorischer Überlegungen $A_0, \ldots, A_g$ bzw. $A_0^+, \ldots, A_{g^+}^+$ und mit 6.10 und 6.12 schließlich $P(t)$ und h_0 bzw. $P^+(t)$ und h_0^+ gewinnen.
Die Bestimmung der Idealklassenzahlen bereitet i. a. mehr Schwierigkeiten. Wir wollen hier lediglich zwei Lemmata angeben, die man ausnutzen kann, um zu zeigen, daß die Idealklassenzahl 'klein' ist.

11.5 Lemma. *Jede Klasse $\mathfrak{A} \in \mathcal{D}/(\mathcal{E} + (L^*))$ enthält einen Divisor $\mathfrak{a} \geq \mathfrak{o}$ vom Grad g. Für L^+ gilt das hierzu Analoge.*

Beweis. Sei $\mathfrak{A} \in \mathcal{D}/(\mathcal{E} + (L^*))$. Da S rationale Punkte enthält, können wir einen Divisor $\mathfrak{d} \in \mathfrak{A}$ mit $\operatorname{grad} \mathfrak{d} = g$ wählen. Nach 4.19(b) ist $\dim \mathfrak{d} \geq 1$, also existiert ein $y \in L^*$ mit $\mathfrak{a} := \mathfrak{d} + (y) \geq \mathfrak{o}$. □

11.6 Lemma. *Sei $r = 1$ und w bzw. w^+ die Fortsetzung von v_{P_1} nach L bzw. L^+. Dann ist*

(a) $\mathfrak{p}_w \in \mathcal{E} + (L^*)$ *und*

(b) $\mathfrak{p}_{w^+} \in \mathcal{E}^+ + ((L^+)^*)$.

Beweis. Sei $\lambda \in \Lambda_M^*$. Nach dem Beweis von 8.4 ist $w(\lambda) = w^+(\lambda^{q-1}) = 1$ und $\tilde{w}(\lambda) = \tilde{w}^+(\lambda^{q-1}) = 0$ für alle $\tilde{w} \in W \setminus (S \cup \{w\})$ und $\tilde{w}^+ \in W^+ \setminus (S^+ \cup \{w^+\})$. □

Beispiele. Wir wollen die Klassenzahlen für $q = 2$, $d = 3$ bestimmen. Für die in 10.5(c) behandelten Fälle ist $g = 0$, also $h_0 = h = 1$. Es bleibt

(a) $M = (x + \alpha)^3$, $\alpha \in \mathbb{F}_2$, und

(b) M irreduzibel

zu untersuchen.

(a) Es ist $m = 4$ und $g = 1$. Wegen 9.2 ist $W_1 = S \cup \{w\}$, wo w die Fortsetzung von $v_{x+\alpha}$ nach L ist, so daß sich aus 11.5, 11.6 und 6.3(b) sofort $h = 1$ und $h_0 = A_1 = \#W_1 = 5$ ergibt.

(b) Hier ist $m = 7$ und $g = 3$. Es sind also die Bewertungen von L bis zum Grad 3 zu bestimmen. Sei w die Fortsetzung von v_M nach L. Nach 9.2 ist $W_1 = S$, $W_2 = \emptyset$ und $W_3 = \{w\}$, also erhalten wir

$$A_1 = 7,\ A_2 = \begin{bmatrix} 7 \\ 2 \end{bmatrix} = 28,\ A_3 = \begin{bmatrix} 7 \\ 3 \end{bmatrix} + 1 = 85,$$

woraus sich nach 6.10 und 6.12

$$\begin{aligned} P(t) &= 1 + 4t + 9t^2 + 15t^3 + 18t^4 + 16t^5 + 8t^6, \\ h_0 &= 71 \end{aligned}$$

ergibt. Wiederum enthält wegen 11.5 und 11.6 jede Klasse $\mathfrak{A} \in \mathcal{D}/(\mathcal{E} + (L^*))$ einen Divisor $\mathfrak{a} \in \mathcal{E} + \mathbb{Z}\mathfrak{p}_w \subseteq \mathcal{E} + (L^*)$, also ist $h = 1$.

Beispiele. In den Fällen aus 10.5(a) und (b) ist $g^+ = 0$, also $h_0^+ = \rho^+ h^+ = 1$. Wir kennen daher den Regulator ρ aus dem Beweis von 11.4.

(a) Sei $q = 4$ und $M = (x + \alpha)(x + \beta)$ mit $\alpha, \beta \in k$, $\alpha \neq \beta$, dann ist $m = 9$, $g = 1$ und $\rho = 3$.

- Ist $\alpha + \beta = 1$, so ist $x + \alpha \equiv 1 \pmod{x + \beta}$ und umgekehrt. Nach 9.1 haben daher $v_{x+\alpha}$ und $v_{x+\beta}$ je 3 Fortsetzungen vom Grad 1 nach L und es ergibt sich
$$h_0 = \#W_1 = \#S + 6 = 9,\ h = h_0/\rho = 3.$$
- Ist $\alpha + \beta \neq 1$, so ist $W_1 = S$, also $h_0 = 3$ und $h = 1$.

(b) Für Polynome der Form $M = (x + \alpha)^2$ mit $\alpha \in k$ ist $m = q(q-1)$, $g = (q-1)(q-2)/2$ und $\rho = (q-1)^{q-1}$. Wir können o. B. d. A. $\alpha = 0$ annehmen und wollen die Fälle $q = 3$ und $q = 4$ untersuchen.

- Ist $q = 3$, also $g = 1$, so haben wir $h = 1$ nach 9.2, 11.5 und 11.6, also $h_0 = \rho h = 4$.

- Sei $q = 4$, also $m = 12$, $g = 3$ und $\rho = 27$. Wieder haben wir $W_1 = S \cup \{w\}$, wo w die Fortsetzung von v_x nach L ist. Desweiteren ist $M + 1 = (x + 1)^2$, d. h. W_2 besteht aus den $m/2 = 6$ Fortsetzungen von v_{x+1}. Da $\beta^3 = 1$ ist für alle $\beta \in k^*$, ist $(x + \gamma)M + 1 = x^3 + \gamma x + 1$ irreduzibel für alle $\gamma \in k^*$ und $\#W_3 = 3m = 36$. Es ergibt sich

$$A_1 = \#W_1 = 5,\ A_2 = \begin{bmatrix} 5 \\ 2 \end{bmatrix} + 6 = 21,\ A_3 = \begin{bmatrix} 5 \\ 3 \end{bmatrix} + 6A_1 + 36 = 101,$$

  also

$$P(t) = 1 + 16t^3 + 64t^6,$$

  $h_0 = P(1) = 81$ und $h = h_0/\rho = 3$.

(c) Sei $q = 3$ und M irreduzibel vom Grad 2. Es ist $g = 2$ und $\rho = 8$. Man rechnet schnell nach, daß $M + 1 = (x + \alpha)(x + \beta)$ mit $\alpha, \beta \in k$, $\alpha \neq \beta$ ist. Nach 9.2, 11.5 und 11.6 ist daher $h = 1$ und $h_0 = \rho h = 8$.

(d) Sei $r = d = 3 = q$, also $M = x(x + 1)(x + 2)$. Wir haben $m = 8$, $g = 1$ und $W_1 = S$ nach 9.2, also $h_0 = \#S = 4$ und $h = 1$.

Literatur

[Ca] L. Carlitz. *A Class of Polynomials*. Trans. Amer. Math. Soc. **43** (1938) 167–182.

[Cs] J. W. S. Cassels. *Local Fields*. London Math. Soc. Student Texts 3, Cambridge University Press, 1986.

[Cv] Claude Chevalley. *Introduction to the Theory of Algebraic Functions of One Variable*. Amer. Math. Soc., 1951/1979.

[De] Max Deuring. *Lectures on the Theory of Algebraic Functions of One Variable*. Lecture Notes in Mathematics 314, Springer, Berlin, 1973.

[FJ] M. D. Fried, M. Jarden. *Field Arithmetic*. Springer, Berlin, 1986.

[GR1] S. Galovich, M. Rosen. *The Class Number of Cyclotomic Function Fields*. J. Number Theory **13** (1981) 363–375.

[GR2] S. Galovich, M. Rosen. *Units and Class Groups in Cyclotomic Function Fields*. J. Number Theory **14** (1982) 156–184.

[Ha] D. R. Hayes. *Explicit Class Field Theory for Rational Function Fields*. Trans. Amer. Math. Soc. **189** (1974) 77–91.

[IS] K. F. Ireland and R. D. Small. *Class Numbers of Cyclotomic Function Fields*. Mathematics of Computation **46**/173 (Jan. 1986) 337–340.

[Jc] Nathan Jacobson. *Basic Algebra II*. W. H. Freeman and Company, 1980.

[L1] Serge Lang. *Algebra*. Addison-Wesley, 2. ed. 1984.

[L2] Serge Lang. *Algebraic Number Theory*. Springer, New York, 1986.

[L3] Serge Lang. *Cyclotomic Fields I and II*. Springer, New York, 1990.

[Ma] Daniel A. Marcus. *Number Fields*. Springer, New York, 1977.

[Nk] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer, Berlin, 1991.

[Qb] H.-G. Quebbemann. *Estimates of Regulators and Class Numbers in Function Fields*. J. reine angew. Math. **419** (1991) 79–87.

[Sm] F. K. Schmidt. *Analytische Zahlentheorie in Körpern der Charakteristik p*. Math. Z. **33** (1931) 1–32.

[Sr] Jean-Pierre Serre. *Local Fields*. Springer, New York, 1979.

[Wh] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer, New York, 1982.

[Ws] Edwin Weiss. *Algebraic Number Theory*. Chelsea Publishing Company, New York, 1976.