Zahlentheorie ueber Funktionenkoerpern

Anton Deitmar
WS 2013/14

Inhaltsverzeichnis

1 Polynome ueber endlichen Koerpern **1**
- 1.1 Division mit Rest . . . 1
- 1.2 Die Eulersche Φ-Funktion . . . 7

2 Die Zetafunktion **11**
- 2.1 Das Eulerprodukt . . . 11
- 2.2 Der Primzahlsatz . . . 13

3 Das Reziprozitaetsgesetz **19**
- 3.1 Das Restsymbol . . . 19

4 L-Reihen **24**
- 4.1 Dichte . . . 24
- 4.2 Der Dirichletsche Primzahlsatz . . . 26

5 Allgemeine Funktionenkoerper **33**
- 5.1 Primstellen . . . 33
- 5.2 Erweiterungen von Funktionenkoerpern . . . 36
- 5.3 Der Satz von Riemann-Roch . . . 42
- 5.4 Der Beweis des Riemann-Roch-Satzes . . . 47

6 Zetafunktionen allgemeiner Funktionenkoerper **54**
- 6.1 Globale Funktionenkoerper . . . 54
- 6.2 Konvergenz und Fortsetzung . . . 55
- 6.3 Zetafunktionen und Konstantenerweiterungen . . . 57
- 6.4 Die Funktionalgleichung . . . 59

7 Die Riemann-Hypothese **62**
- 7.1 Formulierung der RH . . . 62
- 7.2 Reduktionsschritte . . . 64
- 7.3 Eine obere Schranke . . . 65
- 7.4 Eine untere Schranke . . . 68

1 Polynome ueber endlichen Koerpern

Das Wort **Ring** soll in diesem Skript stets fuer einen kommutativen Ring mit Eins stehen.

1.1 Division mit Rest

Zu jeder Primzahlpotenz $q = p^f$ gibt es bis auf Isomorphie genau einen Koerper $\mathbb{F} = \mathbb{F}_q$ mit q Elementen. Dann ist p die Charakteristik von $\mathbb{F}_q$ und $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ist ein Unterkoerper. Jedes $x \in \mathbb{F}_q$ erfuellt die Gleichung $x^q = x$. Die Gruppe $\mathbb{F}_q^\times$ ist zyklisch der Ordnung $q - 1$. Der Grad der Koerpererweiterung $\mathbb{F}_q/\mathbb{F}_p$ ist f. Der **Frobenius-Homomorphismus**

$$x \mapsto x^p$$

erzeugt die Galois-Gruppe $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, deren Ordnung f ist. Es gilt also insbesondere $(x + y)^p = x^p + y^p$ fuer alle $x, y \in \mathbb{F}_q$.

Sei $A = \mathbb{F}[x]$ der Polynomring ueber $\mathbb{F}$. Dieser Ring ist nullteilerfrei, also ein **Integritaetsring**. Jedes Polynom $f \in A$, $f \neq 0$ laesst sich in eindeutiger Weise schreiben als

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

mit $a_0, \ldots, a_n \in \mathbb{F}$ und $a_n \neq 0$. Die ganze Zahl n heisst dann der **Grad** von f, also $\deg(f) = n$. Das Element $\mathrm{sgn}(f) = a_n \in \mathbb{F}^\times$ wird auch das **Signum** von f genannt. Es gilt dann

$$\deg(fg) = \deg(f) + \deg(g), \quad \mathrm{sgn}(fg) = \mathrm{sgn}(f)\,\mathrm{sgn}(g)$$

und

$$\deg(f + g) \leq \max\left(\deg(f), \deg(g)\right).$$

In der zweiten Zeile gilt Gleichheit, falls $\deg(f) \neq \deg(g)$. Ist $\mathrm{sgn}(f) = 1$, so heisst das Polynom f **normiert**. Wir definieren fuer das Nullpolynom $\mathrm{sgn}(0) = 0$ und $\deg(0) = -\infty$, dann bleiben die obigen Regeln fuer alle Polynome bestehen.

Proposition 1.1.1 (Division mit Rest)**.** *Sind $f, g \in \mathbb{F}[x]$ und ist $g \neq 0$, so gibt es eindeutig bestimmte Polynome $q, r \in \mathbb{F}[x]$ so dass*

$$f = qg + r \qquad \textit{und} \qquad \deg(r) < \deg(g).$$

Beweis. Existenz: Wir geben ein Verfahren zur Berechnung an. Schreibe

$$f(x) = a_n x^n + \cdots + a_0$$
$$g(x) = b_m x^m + \cdots + b_0$$

mit $a_n \neq 0$ und $b_m \neq 0$. Ist $n < m$, so setze $r = f$ und $q = 0$, denn dann ist ja

$$f = qg + r \qquad \text{und} \qquad \deg(r) < \deg(g).$$

Ist hingegen $n \geq m$, so setze $q_1 = \frac{a_n}{b_m} x^{n-m}$ und $f_1 = f - q_1 g$. Dann folgt $\deg(f_1) < \deg(f)$. Ersetze nun f durch f_1 und wiederhole diesen Vorgang bis der Grad kleiner wird als $\deg(g)$.

Nun zur *Eindeutigkeit:* Seien $q', r' \in \mathbb{F}[x]$ zwei weitere Polynome mit $f = q'g + r'$ und $\deg(r) < \deg(g)$. Dann gilt

$$0 = f - f = (q - q')g + (r - r').$$

Also gilt $(q - q')r = (r' - r)$ und damit

$$\begin{aligned} \deg(q - q') + \deg(g) &= \deg(r' - r) \\ &\leq \max(\deg(r'), \deg(r)) < \deg(g). \end{aligned}$$

Daraus folgt $\deg(q - q') < 0$, also $\deg(q - q') = -\infty$ und damit $q = q'$, woraus auch $r = r'$ folgt. □

Erinnerung.

- Ein Element p eines Ringes heisst prim oder **Primelement**, falls aus $p|ab$ folgt $p|a$ oder $p|b$. Ein Element p ist genau dann prim, wenn das Hauptideal $(p) = pR$ ein Primideal ist, also genau dann wenn der Ring R/pR nullteilerfrei ist.
- Ein Element q eines Rings R heisst **irreduzibel**, falls aus $q = ab$ folgt dass $a \in R^\times$ oder $b \in R^\times$. Ist der Ring integer, dann ist jedes Primelement schon irreduzibel.
- Zwei Elemente a, b eines Rings R heissen **assoziiert**, wenn $a = bu$ fuer ein $u \in R^\times$.
- Ein Ring R heisst **faktoriell**, wenn jedes Element $x \neq 0$ eine bis auf Reihenfolge und Assoziiertheit eindeutige Darstellung $x = q_1 \cdots q_n$ als Produkt von Irreduziblen hat. In einem faktoriellen Ring ist jedes irreduzible Element prim, also sind dann prim und irreduzibel das Gleiche. Ein nullteilerfreier Hauptidealring ist faktoriell.

- Ein integrer Ring R heisst **euklidisch**, falls es eine Abbildung $d : R \setminus \{0\} \to \mathbb{N}_0$ gibt so dass fuer je zwei Elemente $f, g \in R$ mit $g \neq 0$ eindeutig bestimmte Elemente $q, r \in R$ gibt, so dass

$$f = qg + r \quad \text{und} \quad d(r) < d(g),$$

  wobei man $d(0) = -\infty$ setzt.
  Jeder euklidische Ring ist ein Hauptidealring, also auch faktoriell.

Nach der proposition ist A ein euklidischer Ring, also insbesondere ein Hauptidealring und faktoriell.

Proposition 1.1.2. *Sei $g \in A$, $g \neq 0$. Dann ist A/gA ein endlicher Ring mit $q^{\deg(g)}$ Elementen.*

Beispiel: $A/xA \cong \mathbb{F}$.

Beweis. Sei $m = \deg(g)$. Mit Hilfe der Proposition 1.1.1 sieht man, dass die Menge aller $f \in A$ mit $\deg(f) < m$ ein vollstaendiges Repraesentantensystem von A/gA ist. □

Definition 1.1.3. Sei $g \in A$. Ist $g \neq 0$, so setze $|g| = q^{\deg(g)}$. Ist $g = 0$, so setze $|g| = 0$.

Ist $g \neq 0$, so gilt $|g| = \#(A/gA)$. Stets gilt $|fg| = |f||g|$, sowie $|f + g| \leq \max(|f|, |g|)$ mit Gleichheit, falls $|f| \neq |g|$.

Proposition 1.1.4. *Die Einheitengruppe $A^\times$ ist genau die multiplikative Gruppe der konstanten Polynome $\neq 0$. Insbesondere ist also $A^\times \cong \mathbb{F}^\times$ eine zyklische Gruppe der Ordnung $q - 1$.*

Beweis. Sei $f \in A^\times$. Dann existiert ein $g \in A \setminus \{0\}$ mit $fg = 1$. Daher ist $0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g)$. Da $\deg(f), \deg(g) \geq 0$, folgt also $\deg(f) = 0$, also ist f konstant. Andersrum liefert jedes konstante Polynom $\neq 0$ ein invertierbares Element des Polynomrings. □

In einem Integritaetsring ist jedes Primelement irreduzibel. Ist der Ring R ausserdem faktoriell, dann gilt auch die Umkehrung, dann sind bedeutet also prim und irreduzibel das Gleiche.

Da jedes Polynom $f \neq 0$ in A sich als Produkt einer Einheit mit einem normierten Polynom schreiben laesst, hat jedes Ideal in A genau einen normierten Erzeuger. Da

der Ring A ausserdem faktoriell ist, laesst sich jedes $f \in A \setminus \{0\}$ in eideutiger Weise in der Form

$$f = \alpha p_1 \cdots, p_n$$

schreiben, wobei α eine Einheit und die $p_1, \ldots, p_n$ normierte irreduzible Polynome sind. Diese Zerlegung nennt man die **Primfaktorzerlegung** von f.

Definition 1.1.5. Zwei Polynome $f, g \in A$ heissen **teilerfremd**, falls das von f und g erzeugte Ideal der ganze Ring ist, also wenn

$$fA + gA = A$$

gilt. Dies ist gleichbedeutend damit, dass in den Primfaktorzerlegungen von f und g keine gemeinsamen irreduziblen Faktoren auftreten. Insbesondere sind also zwei verschiedene normierte irreduzible Polynome teilerfremd.

Zei Elemente f, g eines Rings R heissen **teilerfremd**, wenn

$$Rf + Rg = R,$$

wenn also das von f und g erzeugte Ideal der ganze Ring ist.

Proposition 1.1.6 (Chinesischer Restsatz)**.** *Fuer jeden Ring A gilt: seien $f_1, \ldots, f_k \in A$ paarweise teilerfremd und sei $f = f_1 \cdots f_k$. Sei ϕ_j der natuerliche Ringhomomorphismus $A/fA \to A/f_jA$. Dann ist die Abbildung $\phi : A/fA \to (A/f_1A) \times \cdots \times (A/f_kA)$, gegeben durch*

$$\phi(a) = (\phi_1(a), \ldots, \phi_k(a))$$

ein Isomorphismus von Ringen. Insbesondere folgt fuer die Einheitengruppen

$$(A/fA)^\times \cong (A/f_1A)^\times \times \cdots \times (A/f_kA)^\times.$$

Beweis. Dies ist ein Standardresultat der Algebra, siehe etwa Langs Buch. □

Ist nun wieder $A = \mathbb{F}[x]$ und $f \in A$ mit der Primfaktorzerlegung $f = \alpha P_1^{e_1} \cdots P_k^{e_k}$ gegeben, wobei die P_j jetzt paarweise verschieden sind, dann folgt also

$$(A/fA)^\times \cong (A/P_1^{e_1})^\times \times \cdots \times (A/P_k^{e_k})^\times.$$

Um also de Struktur der Gruppe $(A/fA)^\times$ zu erfassen, reicht es, die Gruppen $(A/P_j^{e_j})^\times$ zu verstehen.

Proposition 1.1.7. *Sei $P \in A$ ein irreduzibles Polynom. Dann ist A/PA ein endlicher Koerper mit $|P|$ Elementen, also ist $(A/PA)^\times$ eine zyklische Gruppe mit $|P| - 1$ Elementen.*

Beweis. Das Ideal PA ist wegen der Primfaktorzerlegung ein maximales Ideal, also ist A/PA ein Koerper. □

Lemma 1.1.8. *Sei*

$$1 \to A \to B \to C \to 1$$

eine exakte Sequenz endlicher abelscher Gruppen. Sind die Gruppenordnungen von A und C teilerfremd, dann spaltet die Sequenz.

Beweis. Nach dem Hauptsatz ueber endliche abelsche Gruppen ist B isomorph zu einem Produkt von Gruppen von Primpotenzordnung, also $B \cong \prod_p B_p$. Seien

$$B_A = \prod_{p|\#A} B_p \quad \text{und} \quad B_C = \prod_{p|\#C} B_p.$$

Da die Gruppenordnung von B das Produkt der beiden aeusseren Gruppenordnungen ist und diese teilerfremd sind, folgt $B \cong B_A \times B_C$. Es ist nur noch zu zeigen, dass B_A der Kern der Abbildung $B \to C$ ist. Da die Gruppenordnungen von B_A und C teilerfremd sind, liegt es im Kern. Schliesslich gilt $\#B_A = \#A$ und damit folgt die Behauptung. □

Proposition 1.1.9. *Seien $P \in A$ ein irreduzibles Polynom und sei $e \in \mathbb{N}$. Die Ordnung der Gruppe $(A/P^eA)^\times$ ist $|P|^{e-1}(|P|-1)$. Die Untergruppe*

$$(A/P^eA)^{(1)} = \ker\left((A/P^eA)^\times \to (A/PA)^\times\right)$$

hat Ordnung $|P|^{e-1}$, ist also eine p-Sylow-Gruppe. Wenn e gegen unendlich geht, waechst auch die minimale Anzahl von Erzeugern der Gruppe $(A/P^eA)^{(1)}$ gegen unendlich. Die exakte Sequenz

$$1 \to (A/P^eA)^{(1)} \to (A/P^eA)^\times \to (A/PA)^\times \to 1.$$

spaltet, es ist also

$$(A/P^eA)^\times \cong (A/P^eA)^{(1)} \times (A/PA)^\times.$$

Proof. Der Ring A/P^eA hat genau ein maximales Ideal $I = PA/P^eA$. Das Komplement dieses maximalen Ideal ist also die Gruppe der Einheiten, also hat $(A/P^eA)^\times$ genau

$$|(A/P^eA) \setminus (PA/P^eA)| = |P|^e - |P|^{e-1} = |P|^{e-1}(|P|-1)$$

Elemente. Da die Abbildung $A/P^eA \to A/PA$ surjektiv ist, folgt die Aussage ueber die Elementezahlen. Es bleibt die Aussage ueber die Erzeuger zu zeigen. Jedes Element von $(A/PA)^{(1)}$ laesst in der Form $1 + bP$ fuer ein $b \in A$ schreiben. Sei s die kleinste natuerliche Zahl so dass $p^s \geq e$. Da $(1+bP)^{p^s} = 1 + (bP)^{p^s} \equiv 1 \mod (P^e)$ folgt $x^{p^s} = 1$

fuer jedes $x \in G = (A/P^eA)^{(1)}$. Nach dem Hauptsatz ueber endliche abelsche Gruppen ist G ein Produkt von zyklischen Gruppen, die alle eine Ordnung $\leq p^s$ haben. Die Ordnung von G ist p^{e-1}, also ist G isomorph zu einem Produkt von mindestens $p^{e-1}/p^s = p^{e-1-s}$ zyklischen Gruppen. Mit e waechst auch diese Zahl gegen unendlich. Schliesslich spaltet die exakte Sequenz nach dem Lemma. □

Erinnerung.

- Eine **diskrete Bewertung** von K ist eine surjektive Abbildung $v : K^\times \twoheadrightarrow \mathbb{Z}$ so dass
  - $v(ab) = v(a) + v(b)$ und
  - $v(a+b) \geq \min(v(a), v(b))$, wobei Gleichheit gilt, wenn $v(a) \neq v(b)$.

  Man setzt dann die diskrete Bewertung nach K fort, indem man $v(0) = \infty$ setzt, wobei $\infty > k$ fuer jedes $k \in \mathbb{Z}$. Dann bleiben die obengenannten Eigenschaften der Bewertung erhalten.
- Sei R ein Unterring eines Koerpers K. Ein Element $\alpha \in K$ heisst **ganz** ueber R, wenn es eine Gleichung der Form

  $$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$$

  erfuellt, wobei $a_0, \ldots, a_{n-1} \in R$ sind. Die Menge aller ganzen Elemente ueber R bilden einen Ring $\bar{R} \supset R$, den **ganzen Abschluss** von R in K. Der Ring R heisst **ganz abgeschlossen in** K, wenn $R = \bar{R}$ gilt. Ein Integritaetsring R heisst **ganz abgeschlossen**, wenn er ganz abgeschlossen in seinem Quotientenkoerper ist.
- Ein Integritätsring R, der kein Körper ist, heisst**diskreter Bewertungsring**, falls eine der folgenden äquivalenten Bedingungen erfüllt ist:
  (a) R ist ein lokaler Hauptidealring,
  (b) es existiert eine diskrete Bewertung $v : K^\times \to \mathbb{Z}$, wobei K der Quotientenkoerper ist, so dass $R = \{x \in K : v(x) \geq 0\}$.
- Für einen Integritätsring R sind die folgenden Bedingungen äquivalent:
  (a) Jedes echte Ideal ist ein Produkt von Primidealen,
  (b) R ist noethersch und die Lokalisierung an jedem maximalen Ideal ist ein diskreter Bewertungsring,
  (c) Jedes gebrochene Ideal ist invertierbar,
  (d) R ist noethersch, ganz abgeschlossen und jedes Primieal $\neq 0$ ist maximal.

Einen solchen Ring nennt man **Dedekind-Ring**. In einem Dedekind Ring kann man jedes echte Ideal als Produkt von Primidealen schreiben:

$$I = P_1 \cdots P_k.$$

Diese Darstellung ist bis auf die Reihenfolge eindeutig. (Siehe Neukirch: Algebraische Zahlentheorie).

- Jeder integre faktorielle Hauptidealring ist ein Dedekind-Ring, der ganze Abschluss von $\mathbb{Z}$ in einem Zahlkoerper ist ein Dedekind-Ring.
- Sei R ein Dedekind-Ring und $P \neq 0$ ein Primideal von R. Dann ist die Lokalisierung $R_P = S_P^{-1}R$ mit $S_P = R \setminus P$ von R an P ein diskreter Bewertungsring (=lokaler Hauptidealring) mit Bewertungsideal P.

  Wir beweisen diese Aussage: wegen der Eindeutigkeit der Primidealzerlegung ist $P^2 \neq P$, also gibt es ein $\pi \in P \setminus P^2$. Sei $R\pi = PP_1 \cdots P_k$ die Primidealzerlegung des Hauptideals $R\pi$. Da $\pi \notin P^2$, gilt $P_j \neq P$ fuer jedes $1 \leq j \leq k$. Damit ist insbesondere $P_j \setminus P \neq \emptyset$, also enthaelt P_j eine Einheit der Lokalisierung $S_P^{-1}R = R_P$, also ist das lokalisierte Ideal $S_P^{-1}P_j$ schon der ganze Ring R_P. Also folgt $R_P\pi = S_P^{-1}(R\pi) = S_P^{-1}P =$ das maximale Ideal, welches also ein Hauptideal ist.

Lemma 1.1.10. (a) *Ein endlicher Integritaetsring ist ein Koerper.*

(b) *Der Ring* $\mathbb{F}[x]$ *ist ein Dedekind-Ring.*

Proof. (a) Sei R ein endlicher Integritaetsring, dann ist fuer jedes $a \neq 0$ die Abbildung $x \mapsto ax$ injektiv, da R endlich ist also surjektiv und daher gibt es ein $b \in r$ mit $ab = 1$, d.h., $a \in R^\times$.

(b) Sei P ein Primideal in $\mathbb{F}[x]$. Dann ist $\mathbb{F}[x]/P$ ein endlicher Integritaetsring, also ein Koerper, also ist P ein maximales Ideal. □

1.2 Die Eulersche Φ-Funktion

Fuer $f \in A \setminus \{0\}$ sei $\Phi(f)$ die Anzahl der Elemente von $(A/fA)^\times$.

Proposition 1.2.1. *Es gilt*

$$\Phi(f) = |f| \prod_{P|f} \left(1 - \frac{1}{|P|}\right),$$

wobei das Produkt ueber alle irreduziblen normierten Teiler P von f erstreckt wird.

Proof. Sei $f = \alpha P_1^{e_1} \cdots P_k^{e_k}$ die Primfaktorzerlegung von f. Nach dem chinesischen Restsatz und Proposition 1.1.9 gilt

$$\begin{aligned}\Phi(f) &= \Phi(P_1^{e_1}) \cdots \Phi(P_k^{e_k}) \\ &= \prod_{j=1}^{k} |P_j|^{e_j} \left(1 - \frac{1}{|P_j|}\right) \\ &= |f| \prod_{j=1}^{k} \left(1 - \frac{1}{|P_j|}\right).\end{aligned}$$

□

Proposition 1.2.2. *Sei $f \in A \setminus \{0\}$ und sei $a \in A$ teilerfremd zu f. Dann gilt*

$$a^{\Phi(f)} \equiv 1 \mod (f).$$

Ist insbesondere P ein irreduzibles Polynom, das $a \in A$ nicht teilt, dann gilt

$$a^{|P|-1} \equiv 1 \mod (P).$$

Beweis. Die Aussage, dass a teilerfremd zu f ist, ist aequivalent dazu, dass die Restklasse $a + fA$ in $(A/fA)^\times$ liegt. Diese Gruppe hat die Ordnung $\Phi(f)$ und in einer endlichen Gruppe G gilt $x^{|G|} = 1$ fuer jedes $x \in G$. Ist P irreduzibel, dann ist P genau dann zu a teilerfremd, wenn P das Element a nicht teilt. Ferner ist $\Phi(P) = |P| - 1$, so dass die Behauptung folgt. □

Die letzte Proposition und das Korollar sind die Analoga von Eulers kleinem Satz und Fermats kleinem Satz. Wir kommen nun zum Analogon von Wilsons Satz, der besagt, dass fuer jede Primzahl p gilt

$$(p-1)! \equiv -1 \mod (p).$$

Ist $P \in A$ ein irreduzibles Polynom, dann ist A/PA ein endlicher Koerper. Wir schreiben diesen Koerper auch als $\mathbb{F}_P$. Da dieser Koerper $|P| = q^{\deg(f)}$ Elemente hat, gilt $\mathbb{F}_P = \mathbb{F}_{q^{\deg(f)}}$.

Proposition 1.2.3. (a) *Sei P irreduzibel von Grad d. Sei X eine Unbestimmte, dann gilt im Polynomring $\mathbb{F}_P[X]$,*

$$X^{|P|-1} - 1 = \prod_{0 \neq f \in A/PA} (X - f).$$

(b) *Sei d ein Teiler von $|P| - 1$. Dann hat die Gleichung $X^d = 1$ genau d Loesungen in $\mathbb{F}_P = A/PA$.*

(c) *In* $\mathbb{F}_P = A/PA$ *gilt*

$$\prod_{0 \neq f \in A/PA} f = -1.$$

Beweis. (a) Die beiden Polynome rechts und links des Gleichheitszeichens haben dieselben Nullstellen. Da jede dieser Nullstellen auf der rechten Seite einfach ist und beide Seiten denselben Grad haben, ist auch links der Grad gleich der Anzahl der Nullstellen. Damit sind die beiden normierten Polynome gleich.

(b) Die Gleichung

$$(Y-1)(Y^{k-1} + Y^{k-2} + \cdots + Y + 1) = Y^k - 1$$

zeigt, dass das Polynom $Y - 1$ das Polynom $Y^k - 1$ teilt. Ersetzen wir Y durch X^d folgt dass $X^d - 1$ das Polynom $X^{dk} - 1$ teilt. Da d die Zahl $|P| - 1$ teilt, also $|P| - 1$ in der Form dk geschrieben werden kann, teilt das Polynom $X^d - 1$ auch das Polynom $X^{|P|-1} - 1$. Das letztere ist ein Produkt von verschiedenen Linearfaktoren, damit auch der erstere.

(c) folgt aus (a) indem wir $X = 0$ setzen. □

Sind $a, f \in A$ teilerfremd und $d \in \mathbb{N}$ dann sagen wir: a ist eine d**-te Potenz modulo** f, falls die Gleichung $x^d \equiv a \mod (f)$ eine Loesung in A besitzt. Ist $f = \alpha P_1^{e_1} \cdots P_k^{e_k}$ die Primfaktorzerlegung von f, dann folgt aus dem chinesischen Restsatz, dass a genau dann eine d-te Potenz modulo f ist, wenn es dies modulo $P_i^{e_i}$ fuer jedes $i = 1, \ldots, k$ ist.

Proposition 1.2.4. *Sei $P \in A$ irreduzibel und $a \in A$ sei nicht durch P teilbar. Sei $d \in \mathbb{N}$ ein Teiler von $|P| - 1$. Die Kongruenzgleichung $X^d \equiv a \mod (P^e)$ ist genau dann loesbar, wenn*

$$a^{\frac{|P|-1}{d}} \equiv 1 \mod (P).$$

Es gibt $\frac{\Phi(P^e)}{d}$ verschiedene d-te Potenzen modulo P^e.

Proof. Ist a eine d-te Potenz, also etwa $a \equiv b^d \mod (P^e)$, dann gilt $a^{\frac{|P|-1}{d}} \equiv b^{|P|-1} \mod (P^e)$. Nach Projektion modulo P folgt $a \equiv 1 \mod (P)$, da $|P| - 1$ die Gruppenordnung von $(A/PA)^\times$ ist.

Fuer die Rueckrichtung nimm an, dass $a^{\frac{|P|-1}{d}} \equiv 1 \mod (P)$ gilt. Sei zunaechst $e = 1$. Die Gruppe $(A/PA)^\times$ is zyklisch, sei τ ein Erzeuger, also folgt $a = \tau^k$ fuer ein $k \in \{1, \ldots, |P| - 1\}$. Damit ist $1 \equiv a^{\frac{|P|-1}{d}} \equiv \tau^{k\frac{|P|-1}{d}}$, also ist $k\frac{|P|-1}{d}$ ein Vielfaches von $|P| - 1$ und daher ist k ein Vielfaches von d, also ist a eine d-te Potenz.

Nun zum Fall $e > 1$. Betrachte die exakte Sequenz

$$1 \to (A/P^eA)^{(1)} \to (A/P^eA)^\times \to (A/PA)^\times \to 1.$$

Da die Ordnungen der beiden aeusseren Gruppen teilerfremd sind, ist die mittlere Gruppe ein Produkt der beiden aeusseren, also ist $(A/P^eA)^\times \cong (A/P^eA)^{(1)} \times (A/PA)^\times$. Schreibe entsprechend $a = (b, c)$. Da d teilerfremd zur Ordnung $|P|^{e-1}$ dieser Gruppe ist, ist jedes Element dieser Gruppe eine d-te Potenz, also ist b eine d-te Potenz, wohingegen c nach dem ersten Teil des Beweises ebenfalls eine d-te Potenz ist. □

2 Die Zetafunktion

2.1 Das Eulerprodukt

Sei wieder $A = \mathbb{F}_q[x]$. Die **Zetafunktion** zu A ist

$$\zeta_A(s) = \sum_{\substack{f \in A \\ \text{normiert}}} \frac{1}{|f|^s}.$$

Es gibt genau q^d normierte Polynome vom Grad d, so dass

$$\sum_{\deg(f) \leq d} = 1 + \frac{q}{q^s} + \frac{q^2}{q^{2s}} + \cdots + \frac{q^d}{q^{ds}}.$$

Daher konvergiert die Reihe fuer $\mathrm{Re}(s) > 1$ und liefert dort

$$\zeta_A(s) = \sum_{j=0}^{\infty} q^{j(1-s)} = \frac{1}{1 - q^{1-s}}$$

Proposition 2.1.1. *Es gilt*

$$\zeta_A(s) = \prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1},$$

wobei das Produkt ueber alle normierten Primpolynome in A erstreckt wird. Das Produkt konvergiert absolut fuer $\mathrm{Re}(s) > 1$. *Da die Zetafunktion andererseits einen Pol bei* $s = 1$ *hat, kann man folgern, dass es unendlich viele Primpolynome P in A gibt.*

Beweis. Fuer $\mathrm{Re}(s) > 1$ konvergiert die geometrische Reihe und wir erhalten

$$\left(1 - \frac{1}{|P|^s}\right)^{-1} = \sum_{n=0}^{\infty} |P|^{-ns}.$$

Sei also $k \in \mathbb{N}$ dann ist

$$\prod_{P:|P| \leq k} \left(1 - \frac{1}{|P|^s}\right)^{-1} = \sum_f \frac{1}{|f|^s},$$

wobei die Summe ueber alle f erstreckt wird, in deren Primfaktorzerlegung nur Primpolynome P mit $|P| \leq k$ vorkommen. Laesst man k gegen unendlich gehen, folgt die Behauptung. □

Sei $n = p_1^{n_1} \cdots p_k^{n_k}$ die Primfaktorzerlegung der natuerlichen Zahl n mit verschiedenen Primzahlen $p_1, \ldots, p_k$. Wir nennen n eine **quadratfreie Zahl**, falls $n_j = 1$ fuer jedes

$j = 1, \ldots, k$. Andernfalls sagen wir, dass n ein Quadrat enthaelt.

Fuer eine natuerliche Zahl n sei die **Moebius-Funktion** $\mu(n)$ wie folgt definiert: $\mu(n) = 0$ falls n ein Quadrat enthaelt und fuer $n = p_1 \cdots p_k$ mit verschiedenen Primzahlen ist

$$\mu(n) = (-1)^k.$$

Lemma 2.1.2 (Moebius-Umkehrformel)**.** (a) *Fuer jede natuerliche Zahl $n \geq 3$ gilt*

$$\sum_{d|n} \mu(d) = 0.$$

(b) *Ist a_n eine Folge in einer additiven Gruppe und ist $b_n = \sum_{d|n} a_d$, dann gilt*

$$a_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) b_d.$$

Hierbei wird die Summe jeweils ueber die positiven Teiler erstreckt.

Beweis. Sind m und n teilerfremde natuerliche Zahlen, so gilt $\mu(mn) = \mu(m)\mu(n)$, man sagt auch, die Moebius-Funktion ist **schwach multiplikativ**. Sei $F(n) = \sum_{d|n} \mu(d)$ und seien m, n teilerfremd, so ist

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1)\mu(d_2) = \sum_{d_1|m} \sum_{d_2|n} \mu(d_1)\mu(d_2) = F(m)F(n).$$

Damit reicht es, (a) fuer eine Primpotenz $n = p^k \geq 2$ zu zeigen. Fuer die ist es aber klar, da nur zwei Summanden auftreten.

Wir benutzen (a) und zeigen (b) durch Induktion. Fuer $n = 1$ ist es klar. Sei also $n \in \mathbb{N}$ und (b) gezeigt fuer alle Zahlen $< n$, dann ist

$$\begin{aligned} a_n &= b_n - \sum_{\substack{d|n \\ d<n}} a_d = b_n - \sum_{\substack{d|n \\ d<n}} \sum_{l|d} \mu\left(\frac{d}{l}\right) b_l \\ &= b_n - \sum_{l|n} \left(\sum_{\substack{l|d|n \\ d<n}} \mu\left(\frac{d}{l}\right) \right) b_l = b_n - \sum_{l|n} \left(\sum_{\substack{d|n/l \\ d<n/l}} \mu(d) \right) b_l = b_n + \sum_{\substack{l|n \\ l<n}} b_l \mu\left(\frac{n}{l}\right). \end{aligned}$$

□

Sei wieder $A = \mathbb{F}_q[x]$ und sei a_d die Anzahl der normierten Primpolynome in A vom grad d.

Proposition 2.1.3. (a) *Fuer jede natuerliche Zahl n gilt*

$$\sum_{d|n} da_d = q^n.$$

(b) *Es ist*

$$a_n = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

Beweis. Nach Definition haben wir

$$\zeta_A(s) = \prod_{d=1}^{\infty} \left(1 - q^{-ds}\right)^{-a_d}.$$

Wir erinnern uns, dass $\zeta_A(s) = 1/(1 - q^{1-s})$ und substituieren $u = q^{-s}$. Wir erhalten

$$\frac{1}{1 - qu} = \prod_{d=1}^{\infty} (1 - u^d)^{-a_d}.$$

Wir nehmen auf beiden Seiten den Logarithmus, erinnern uns dass $\log(ab) = \log(a) + \log(b)$ und $\log\left(\frac{1}{1-x}\right) = \sum_{n=1}^{\infty} \frac{x^n}{n}$ und erhalten

$$\sum_{n=1}^{\infty} \frac{u^n}{n} q^n = \sum_{d=1}^{\infty} a_d \sum_{m=1}^{\infty} \frac{u^{dm}}{m} = \sum_{n=1}^{\infty} \frac{u^n}{n} \sum_{d|n} da_d.$$

Koeffizientenvergleich liefert (a). Teil (b) folgt dann mit der Umkehrformel. □

2.2 Der Primzahlsatz

Satz 2.2.1 (Primzahlsatz fuer Polynome)**.** *Sei $A(n)$ die Anzahl der normierten Primpolynome ueber $\mathbb{F}_q$ von Grad n. Dann ist*

$$A(n) = \frac{q^n}{n} + O\left(\frac{q^{\frac{n}{2}}}{n}\right).$$

Setzt man $x = q^n$, so ist die rechte Seite $\frac{x}{\log_q x} + O\left(\sqrt{x}/\log_q(x)\right)$, was im Fall $\mathbb{Z}$ der Riemann-Hypothese entspricht.

Beweis. Wir muessen zeigen, dass es eine Konstante C_q gibt, so dass

$|A(n) - \frac{q^n}{n}| \leq C_q q^{\frac{n}{2}}/n$ fuer jedes n gilt. Wir haben

$$\left|A(n) - \frac{q^n}{n}\right| = \left|\frac{1}{n}\sum_{2\leq d|n} \mu(d) q^{n/d}\right| \leq \frac{1}{n}\sum_{2\leq d|n} |\mu(d)| q^{n/d} \leq \frac{1}{n}\left(q^{n/2} + q^{n/3}2^t\right),$$

wobei t die Anzahl der Primfaktoren von n ist. Es gilt $2^t \leq p_1 \cdots p_t \leq n$, so dass wir

$$\left|A(n) - \frac{q^n}{n}\right| \leq \left(\frac{q^{n/2}}{n} + q^{n/3}\right)$$

erhalten, woraus die Behauptung folgt. □

Proposition 2.2.2. *Sei b_n die Anzahl der quadratfreien normierten Polynome von Grad n. Dann gilt $b_1 = q$ und fuer $n \geq 2$ gilt*

$$b_n = q^n(1 - q^{-1}).$$

Beweis. Betrachte das Produkt

$$\prod_P \left(1 + \frac{1}{|P|^s}\right) = \sum_f \frac{\delta(f)}{|f|^s}.$$

wobei die Summe ueber alle normierten Polynome laeuft. Dann ist $\delta(f)$ gleich der Anzahl der Primfaktoren, falls f quadratfrei und ist Null sonst. Substituieren wir wieder $u = q^{-s}$, dann ist die rechte Seite gleich $\sum_{n=1}^{\infty} b_n u^n$. Wir benutzen die Gleichung $(1 + w) = (1 - w^2)/(1 - w)$ fuer $w = 1/|P|^s$ und sehen, dass die rechte Seite der Gleichung $\zeta_A(s)/\zeta_A(2s)$ ist. Wir haben also

$$\sum_{n=1}^{\infty} b_n u^n = \frac{1 - qu^2}{1 - qu} = (1 - qu^2)\sum_{n=0}^{\infty} q^n u^n = \sum_{n=0}^{\infty} q^n u^n - \sum_{n=2}^{\infty} q^{n-1} u^n.$$

Koeffizientenvergleich liefert die Behauptung. □

Fuer $f \in A$ sei $\mu(f) = (-1)^k$ falls f das Produkt von k verschiedenen normierten Primpolynomen ist (mal einer Einheit) und sei $\mu(f) = 0$, falls f nicht quadratfrei. Dies ist die Polynomversion der Moebius-Funktion.

Sei $d(f)$ gleich der Anzahl der normierten Teiler von f und sei $\sigma(f)$ die **Teilerbetragsumme**, also

$$\sigma(f) = \sum_{g|f} |g|,$$

wobei die Summe ueber alle normierten Teiler von f laeuft.

Proposition 2.2.3. *Die Funktionen Φ, d, σ sind schwach multiplikativ. Ist $f = \alpha P_1^{e_1} \cdots P_k^{e_k}$ die Primfaktorzerlegung von f, so gilt*

$$\begin{aligned}\Phi(f) &= |f| \prod_{P|f} (1 - |P|^{-1}),\\ d(f) &= (e_1 + 1) \cdots (e_k + 1),\\ \sigma(f) &= \frac{|P_1|^{e_1+1} - 1}{|P_1| - 1} \cdots \frac{|P_k|^{e_k+1} - 1}{|P_k| - 1}.\end{aligned}$$

Insbesondere folgt $d(f) \leq |f|$.

Beweis. Die Multiplikativitaet ist klar. Daher sind die Formeln jeweils nur fuer den Fall eines Primpolynoms P zu zeigen. Die erste Formel ist bereits in Proposition 1.2.1 bewiesen worden. Ist P ein Primpolynom, so sind die normierten Teiler von P^e genau die Polynome $1, P, P^2, \ldots, P^e$, also $e + 1$ an der Zahl. Damit folgt die zweite Formel. Hieraus folgt auch, dass $\sigma(P) = 1 + |P| + \cdots + |P|^e = (|P|^{e+1} - 1)/(|P| - 1)$.

Fuer die letzte Aussage $d(f) \leq |f|$ beachte, dass fuer $x \geq 1$ gilt $q^x \geq x + 1$. Daher ist

$$\begin{aligned}|f| &= |P_1|^{e_1} \cdots |P_k|^{e_k}\\ &= q^{e_1 \deg(P_1)} \cdots q^{e_k \deg(P_k)}\\ &\geq q^{e_1} \cdots q^{e_k}\\ &\geq (e_1 + 1) \cdots (e_k + 1) = d(f).\end{aligned}$$

□

Sei $\mathcal{N}$ die Menge aller normierten Polynome in A. Sei $\alpha : \mathcal{N} \to \mathbb{C}$. Wir sagen, dass α ein **moderates Wachstum** hat, wenn es ein $T > 0$ gibt, so dass $\alpha(f) = O(|f|^T)$ ist. Ist dies der Fall, dann konvergiert die zugehoerige **Dirichlet-Reihe**

$$D_\alpha(s) = \sum_{f \text{ normiert}} \frac{\alpha(f)}{|f|^s} = \sum_{n=0}^{\infty} \frac{\alpha^\Sigma(n)}{q^{ns}}$$

fuer $\mathrm{Re}(s) > T + 1$ absolut. Hierbei ist $\alpha^\Sigma(n) = \sum_{\substack{f \text{ normiert} \\ \deg(f)=n}} \alpha(f)$. Beachte, dass die Zuordnung $\alpha \mapsto D_\alpha$ nicht injektiv ist, da D_α nur von α^Σ abhaengt und man kann leicht Funktionen α herstellen, die $\alpha \neq 0$ aber $\alpha^\Sigma = 0$ erfuellen.

Wir nennen α (schwach) **multiplikativ**, falls

$$\mathrm{ggT}(f, g) = 1 \quad \Rightarrow \quad \alpha(fg) = \alpha(f)\alpha(g)$$

und **stark multiplikativ**, falls $\alpha(fg) = \alpha(f)\alpha(g)$ fuer alle normierten f, g gilt.

Lemma 2.2.4. *Sei α eine Funktion von moderatem Wachstum. Dann gilt*

$$\alpha \text{ ist multiplikativ} \Rightarrow D_\alpha(s) = \prod_P \sum_{n=0}^{\infty} \frac{\alpha(P^n)}{|P|^{ns}},$$
$$\alpha \text{ ist stark multiplikativ} \Rightarrow D_\alpha(s) = \prod_P \frac{1}{1 - \frac{\alpha(P)}{|P|^s}},$$

wobei die Produkte jeweils absolut konvergieren, falls $\mathrm{Re}(s) > T + 1$ *und* $\alpha(f) = O(|f|^T)$.

Die Umkehrungen gelten jeweils nicht, da D_α nur von α^Σ anhaengt.

Beweis. Klar. □

Proposition 2.2.5. *Es gilt $D_d(s) = \zeta_A(s)^2 = (1 - qu)^{-2}$. Also ist $d^\Sigma(n) = (n + 1)q^n$.*

Beweis. Wir rechnen

$$\begin{aligned}\zeta_A(s)^2 &= \left(\sum_f \frac{1}{|f|^s}\right)\left(\sum_g \frac{1}{|g|^s}\right) = \sum_{f,g} \frac{1}{|fg|^s} \\ &= \sum_h \underbrace{\left(\sum_{fg=h} 1\right)}_{=d(h)} \frac{1}{|h|^s} = D_d(s).\end{aligned}$$

Damit ist die erste Aussage bewiesen. Fuer die zweite beachte

$$\sum_{n=0}^{\infty} d^\Sigma(n)u^n = D_d(s) = (1 - qu)^{-2} = \sum_{n=0}^{\infty}(n + 1)q^n u^n.$$ □

Seien $\alpha, \beta : \mathcal{N} \to \mathbb{C}$ gegeben. Wir definieren ihre **Dirchlet-Faltung** als

$$\alpha * \beta(f) = \sum_{hg=f} \alpha(h)\beta(g).$$

Proposition 2.2.6. *Sind $\alpha(f), \beta(f) = O(|f|^T)$, dann gilt $\alpha * \beta(f) = O\left(|f|^{T+1}\right)$ und fuer* $\mathrm{Re}(s) > T + 2$ *gilt $D_{\alpha*\beta}(s) = D_\alpha(s)D_\beta(s)$.*

Beweis. Sei $|\alpha(f)|, |\beta(f)| \leq C|f|^T$, dann ist

$$\begin{aligned}|\alpha * \beta(f)| &= \left|\sum_{gh=f} \alpha(h)\beta(g)\right| \\ &\leq \sum_{gh=f} |\alpha(g)||\beta(h)| \\ &\leq C^2 \sum_{gh=f} |gh|^T = C^2|f|^T d(f).\end{aligned}$$

Die erste Behauptung folgt dann aus $|d(f)| \leq |f|$, siehe Proposition 2.2.3. Fuer $\mathrm{Re}(s) > T + 2$ rechnen wir

$$\begin{aligned}D_\alpha(s)D_\beta(s) &= \sum_g \frac{\alpha(g)}{|g|^s} \sum_h \frac{\beta(h)}{|h|^s} \\ &= \sum_f \frac{1}{|f|^s} \sum_{gh=f} \alpha(g)\beta(h) = D_{\alpha*\beta}(s).\end{aligned}$$

□

Proposition 2.2.7. *Wir haben*

$$D_\Phi(s) = \frac{\zeta_A(s-1)}{\zeta_A(s)},$$

oder, aequivalent:

$$\Phi^\Sigma(n) = q^{2n}(1 - q^{-1}) \quad \textit{fuer } n \geq 1.$$

Beweis. Nach Proposition 1.2.1 gilt

$$\begin{aligned}\phi(f) &= |f| \prod_{P|f} (1 - |P|^{-1}) \\ &= \sum_{g|f} \mu(g)|f/g| = (\mu * \lambda)(f),\end{aligned}$$

wobei $\lambda(f) = |f|$. Daher $D_\Phi(s) = D_\mu(s)D_\lambda(s) = \zeta_A(s)^{-1}\zeta_A(s-1) = \frac{1-q^{1-s}}{1-q^{2-s}}$. Mit der Substitution $u = q^{-s}$ wird daraus

$$\begin{aligned}\sum_{n=0}^\infty \Phi^\Sigma(n)u^n &= \frac{1-qu}{1-q^2u} = (1-qu)\sum_{m=0}^\infty q^{2m}u^m \\ &= \sum_{m=0}^\infty q^{2m}u^m - \sum_{m=1}^\infty q^{2m-1}u^m.\end{aligned}$$

□

Sei $\mathbf{1}$ die konstante Funktion mit Wert 1 und $\lambda(f) = |f|$, dann ist

$$\mathbf{1} * \lambda(f) = \sum_{g|f} |g| = \sigma(f).$$

Proposition 2.2.8. *Es ist*

$$D_\sigma(s) = \zeta_A(s)\zeta_A(s-1),$$

also

$$\sigma^\Sigma(n) = q^{2n}\frac{1-q^{-n-1}}{1-q^{-1}}.$$

Beweis. Es gilt

$$D_\sigma(s) = D_{\mathbf{1}*\lambda}(s) = D_{\mathbf{1}}(s)D_\lambda(s) = \zeta_A(s)\zeta_A(s-1) = \frac{1}{(1-q^{1-s})(1-q^{2-s})}. \qquad \square$$

3 Das Reziprozitaetsgesetz

Ist p eine ungerade Primzahl und $a \in \mathbb{Z}$, dann ist das **Legendre-Symbol** wie folgt definiert

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \ (p), \\ 1 & a \not\equiv 0 \ (p) \text{ und } a = x^2 \text{ ist loesbar} \mod (p), \\ -1 & a = x^2 \text{ ist nicht loesbar} \mod (p). \end{cases}$$

Beispiel 3.0.1. Ist $p = 5$, so sieht man an der Tabelle:

x	0	1	2	3	4
x^2	0	1	4	4	1

dass das Legendre Symbol $\left(\frac{a}{5}\right)$ genau dann gleich 1 ist, wenn $a \equiv 1$ oder $a \equiv 4 \mod (5)$ ist.

Es gilt $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, so dass es reicht, das Legendre-Symbol fuer Primzahlen a auszurechnen. Da $p \mod 8$ nur die Werte $1, 3, 5, 7$ annehmen kann, ist $p^2 \mod (8)$ gleich 1, also $p^2 - 1$ durch 8 teilbar. Die Formel

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv 1, 7 \mod (8), \\ -1 & p \equiv 3, 5 \mod (8). \end{cases}$$

reduziert das Problem der Berechnung auf den Fall, dass $a = q$ eine ungerade Primzahl ist. In diesem Fall gilt das **quadratische Reziprozitaetsgesetz**:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

das schliesslich die vollstaendige Berechnung erlaubt.

(Beweis das Reziprozitaetsgesetzes etwa in Schmidt, A.: Einfuehrung in der algebraische Zahlentheorie)

3.1 Das Restsymbol

Zurueck zum Polynomring $A = \mathbb{F}_q[x]$. Sei $P \in A$ ein irreduzibles Polynom und sei d ein Teiler von $q - 1$. Ist $a \in A$ teilerfremd zu P, dann ist nach Proposition 1.2.4 die Kongruenz $x^d \equiv a \mod (P)$ genau dann loesbar, wenn

$$a^{\frac{|P|-1}{d}} \equiv 1 \mod (P)$$

ist. Fuer jedes $a \in A$ definiere

$$\left(\frac{a}{P}\right)_d = a^{\frac{|P|-1}{d}} \in (A/PA)^\times = \mathbb{F}_{|P|}^\times.$$

Die Abbildung $a \mapsto \left(\frac{a}{P}\right)_d$ heisst das d-Potenz **Restsymbol**. Das Element a ist genau dann eine d-te Potenz modulo P, wenn $\left(\frac{a}{P}\right)_d = 1$.

Proposition 3.1.1. (a) *Fuer alle $a, b \in A$, die zu P teilerfremd sind, gilt*

$$\left(\frac{ab}{P}\right)_d = \left(\frac{a}{P}\right)_d \left(\frac{b}{P}\right)_d.$$

(b) $\left(\frac{a}{P}\right)_d = 1$ *gilt genau dann, wenn* $x^d \equiv a \mod (P)$ *loesbar ist.*

(c) *Sei $\zeta \in \mathbb{F}_q^\times$ von Ordnung d. Dann existiert ein $a \in A$ mit $\left(\frac{a}{P}\right)_d = \zeta$.*

Beweis. Die erste Aussage folgt direkt aus der Definition. Die zweite ist Proposition 1.2.4. Zu Teil (c) beachte, dass die Abbildung $a \mapsto \left(\frac{a}{P}\right)_d$ ein Homomorphismus $\mathbb{F}_{|P|}^\times \to \mathbb{F}_{|P|}^\times$ ist, dessen Kern genau die d-ten Potenzen sind. Da die Gruppe $\mathbb{F}_{|P|}^\times$ zyklisch ist, hat das Bild die Ordnung d. □

Proposition 3.1.2. *Fuer eine Konstante $\alpha \in \mathbb{F}_q$ gilt*

$$\left(\frac{\alpha}{P}\right)_d = \alpha^{\frac{q-1}{d}\deg P}.$$

Beweis. Sei $\delta = \deg(P)$. Dann ist

$$\frac{|P|-1}{d} = \frac{q^\delta - 1}{d} = (1 + q + q^2 + \cdots + q^{\delta-1})\frac{q-1}{d}.$$

Das Ergebnis folgt nun, da $\alpha^q = \alpha$ fuer jedes $\alpha \in \mathbb{F}_q$ gilt. □

Satz 3.1.3 (Reziprozitaetsgesetz)**.** *Seien P und Q teilerfremde irreduzible normierte Polynome vom Grad δ bzw. ν. Dann gilt*

$$\left(\frac{Q}{P}\right)_d = (-1)^{\frac{q-1}{d}\delta\nu}\left(\frac{P}{Q}\right)_d.$$

Beweis. Sei $\left(\frac{a}{P}\right) = \left(\frac{a}{P}\right)_{q-1}$. Dann ist $\left(\frac{a}{P}\right)_d = \left(\frac{a}{P}\right)^{\frac{q-1}{d}}$. Der allgemeine Satz folgt also, wenn wir

$$\left(\frac{Q}{P}\right) = (-1)^{\delta\nu}\left(\frac{P}{Q}\right)$$

zeigen koennen. Sei $\mathbb{F}'$ eine endliche Koerpererweiterung von $\mathbb{F}$, die eine Nullstelle α von P und eine Nullstelle β von Q enthaelt. Aus der Theorie endlicher Koerper folgt

$$P(T) = (T-\alpha)(T-\alpha^q)\cdots(T-\alpha^{q^{\delta-1}})$$

und

$$Q(T) = (T-\alpha)(T-\beta^q)\cdots(T-\beta^{q^{\nu-1}}).$$

Wir betrachten nun Kongruenzen im Ring $A' = \mathbb{F}'[T]$. Beachte, dass fuer $f(T) \in A'$ gilt $f(T) \equiv f(\alpha) \mod (T-\alpha)$. Ferner gilt fuer $g \in A$, dass $g(T)^q = g(T^q)$, da die Koeffizienten von g in $\mathbb{F}$ liegen. Daher ist $\left(\frac{Q}{P}\right)$ kongruent zu

$$\begin{aligned} Q(T)^{1+q+\cdots+q^{\delta-1}} &\equiv Q(T)Q(T^q)\cdots Q(T^{q^{\delta-1}}) \\ &\equiv Q(\alpha)Q(\alpha^q)\cdots Q(\alpha^{q^{\delta-1}}) \mod (T-\alpha). \end{aligned}$$

Wir können denselben Schluss mit jeder Nullstelle $\beta = \alpha^{q^k}$ machen und daher gilt die Kongruenz auch modulo $T - \alpha^{q^k}$ fuer jedes k und nach dem chinesischen Restsatz gilt sie dann modulo P. Setzt man dann $Q(T) = (T-\alpha)(T-\beta^q)\cdots(T-\beta^{q^{\nu-1}})$ ein, findet man

$$\left(\frac{Q}{P}\right) \equiv \prod_{i=0}^{\delta-1}\prod_{j=0}^{\nu-1}(\alpha^{q^i} - \beta^{q^j}) \mod (P).$$

Daher ist

$$\left(\frac{Q}{P}\right) = \prod_{i=0}^{\delta-1}\prod_{j=0}^{\nu-1}(\alpha^{q^i} - \beta^{q^j}) = (-1)^{\delta\nu}\prod_{j=0}^{\nu-1}\prod_{i=0}^{\delta-1}(\beta^{q^j} - \alpha^{q^i})) = (-1)^{\delta\nu}\left(\frac{P}{Q}\right). \qquad \square$$

Sei $0 \neq b \in A$ mit Primfaktorzerlegung $b = \beta Q_1^{f_1}Q_2^{f_2}\cdots Q_s^{f_s}$. Definiere

$$\left(\frac{a}{b}\right)_d = \prod_{j=1}^{s}\left(\frac{a}{Q_j}\right)_d^{f_j} \mod (b).$$

Proposition 3.1.4. (a) $\left(\frac{a_1a_2}{b}\right)_d = \left(\frac{a_1}{b}\right)_d\left(\frac{a_2}{b}\right)_d$

(b) $\left(\frac{a}{b_1b_2}\right)_d = \left(\frac{a}{b_1}\right)_d\left(\frac{a}{b_2}\right)_d$

(c) $\left(\frac{a}{b}\right)_d \neq 0 \Leftrightarrow \mathrm{ggT}(a,b) = 1$

(d) *Sind a und b teilerfremd und hat $x^d \equiv a \mod (b)$ eine Loesung, dann ist $\left(\frac{a}{b}\right)_d = 1$.*

Beweis. Klar. □

Beispiel 3.1.5. Die Umkehrung von (d) in der letzten Proposition gilt nicht. Sei zum Beispiel Q irreduzibel, teilerfremd zu a und sei $b = Q^d$.

Erinnere: Fuer $0 \neq f \in A$ ist $\mathrm{sgn}(f)$ der fuehrende Koeffizient.

Satz 3.1.6 (Allgemeines Reziprozitaetsgesetz)**.** *Seien $a, b \in A$ teilerfremd. Dann gilt*

$$\left(\frac{a}{b}\right)_d \left(\frac{b}{a}\right)_d^{-1} = (-1)^{\frac{q-1}{d}\deg(a)\deg(b)} \mathrm{sgn}(a)^{\frac{q-1}{d}\deg(b)} \mathrm{sgn}(b)^{\frac{q-1}{d}\deg(a)}.$$

Beweis. Uebungsaufgabe. □

Proposition 3.1.7. *Sei $m \in A$ normiert*

(a) *Ist $\deg(m)$ gerade, oder ist $(q-1)/d$ gerade, oder ist $p = \mathrm{char}(\mathbb{F}) = 2$, dann*

$$\left(\frac{m}{P}\right)_d = \left(\frac{P}{m}\right)_d.$$

(b) *Ist $\deg(m)$ ungerade, $(q-1)/d$ ungerade, und p ungerade, dann ist*

$$\left(\frac{m}{P}\right)_d = 1 \quad \Leftrightarrow \quad \left\{ \begin{array}{c} \deg(P) \text{ gerade und } \left(\frac{P}{m}\right)_d = 1 \\ \text{oder} \\ \deg(P) \text{ ungerade und } \left(\frac{P}{m}\right)_d = -1. \end{array} \right\}$$

Beweis. Nach Satz 3.1.6 gilt

$$\left(\frac{m}{P}\right)_d = (-1)^{\frac{q-1}{d}\deg(m)\deg(P)} \left(\frac{P}{m}\right)_d.$$

Damit folgen beide Aussagen. □

Satz 3.1.8. *Sei $m \in A$ ein nichtkonstantes Polynom und sei d ein Teiler von $q-1$. Ist $x^d \equiv m$ loesbar fuer fast alle irreduziblen P, dann ist m eine d-te Potenz in A, d.h., es existiert ein $f \in A$ mit $f^d = m$.*

Beweis. Sei $m = \mu Q_1^{e_1} \cdots Q_t^{e_t}$ die Primfaktorzerlegung von m. Wir zeigen zunaechst dass, wenn eines der e_i nicht durch d teilbar ist, dann existieren unendlich viele Primelemente P mit $\left(\frac{m}{P}\right)_d \neq 1$. Sei also e_1 nicht durch d teilbar.

Seien $P_1, \ldots, P_s$ verschiedene irreduzible, die m nicht teilen mit $\left(\frac{m}{P_j}\right)_d \neq 1$ fuer alle $1 \leq j \leq s$. Fuer jedes $a \in A$ gilt

$$\left(\frac{a}{m}\right)_d = \prod_{i=1}^{t} \left(\frac{a}{Q_i}\right)_d^{e_i}. \tag{*}$$

Nach Proposition 3.1.1 existiert ein $c \in A$ so dass $\left(\frac{c}{Q_1}\right)_d = \zeta$ eine primitive d-te Wurzel der Eins ist. Nach dem chinesischen Restsatz gibt es ein $a \in A$ so dass $a \equiv c \mod (Q_1)$ und $a \equiv 1 \mod (Q_i)$ fuer $i \geq 2$ und $a \equiv 1 \mod (P_i)$ fuer alle i. Wir koennen zu a beliebige Vielfache von $Q_1 \cdots Q_t P_1 \cdots P_s$ addieren ohne diese Eigenschaften zu aendern. Also koennen wir annehmen, dass a normiert ist und dass der Grad von a ein Vielfaches von $2d$ ist. Dieses a setzen wir in Gleichung (*) ein und erhalten

$$\left(\frac{a}{m}\right)_d = \zeta^{e_1} \neq 1.$$

Da der Grad von a ein Vielfaches von $2d$ ist, folgt nach dem Reziprozitaetssatz

$$\left(\frac{m}{a}\right)_d = \left(\frac{a}{m}\right)_d \neq 1.$$

Damit folgt, dass es ein irreduzibles $P|a$ gibt mit $\left(\frac{m}{P}\right)_d \neq 1$. Damit ist P von $P_1, \ldots, P_s$ verschieden, also gibt es unendlich viele P mit $\left(\frac{m}{P}\right)_d \neq 1$, was unserer Voraussetzung widerspricht, damit ist also jedes e_i ein Vielfaches von d. Es folgt, dass $m = \mu f^d$ fuer ein normiertes f und $\mu \in \mathbb{F}^\times$. Fuer beliebiges P ist

$$\left(\frac{m}{P}\right)_d = \left(\frac{\mu}{P}\right)_d = \mu^{\frac{q-1}{d} \deg(P)}.$$

Nach Satz 2.2.1 gibt es irreduzible P von jedem Grad. Da es nur endlich viele P gibt mit $\left(\frac{m}{P}\right)_d \neq 1$, gibt es also ein P mit zu d teilerfremden Grad und $\left(\frac{m}{P}\right)_d = 1$. Dann folgt aber $\mu^{\frac{q-1}{d} \deg(P)} = 1$ und da $\deg(p)$ teilerfremd zu d also $\mu^{\frac{q-1}{d}} = 1$, so dass μ eine d-te Potenz sein muss. □

4 L-Reihen

Fuer $T > 0$ sei

$$\pi(T) = |\{p \leq T\}|$$

die Anzahl der Primzahlen $\leq T$. Der **Primzahlsatz** besagt, dass

$$\pi(T) \sim \frac{T}{\log T}$$

wenn $T \to \infty$, wobei $f(T) \sim g(T)$ bedeutet, dass der Quotient $\frac{f(T)}{g(T)}$ gegen 1 geht falls $T \to \infty$. Es geht aber noch genauer. Sei $m \in \mathbb{N}$ beliebig. Dann sind fast alle Primzahlen p teilerfremd zu m. Sei $\Phi(m)$ die Ordnung der Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ und fuer ein gegebenes $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ sei

$$\pi_a(T) = |\{p \equiv a \mod (m), p \leq T\}|$$

die Anzahl aller Primzahlen kongruent zu a modulo m und $\leq T$. Der **Primzahlsatz von Dirichlet** besagt, dass

$$\pi_a(T) \sim \frac{1}{\Phi(m)} \frac{T}{\log T}.$$

4.1 Dichte

Seien f und g Funktionen definiert in einem Intervall $(1, b)$ fuer ein $b > 1$. Wir schreiben $f \approx g$, wenn die Differenz $f(s) - g(s)$ der Funktionen beschraenkt bleibt wenn $s \to 1$.

Proposition 4.1.1. *Es gilt*

$$\log \zeta_A(s) \approx \log\left(\frac{1}{s-1}\right) \approx \sum_P |P|^{-s},$$

wobei die Summe ueber alle irreduziblen normierten Polynome laeuft.

Beweis. Da $\zeta_A(s) = \frac{1}{1-q^{1-s}}$ gilt $\lim_{s\to 1}(s-1)\zeta_A(s) = \frac{1}{\log q}$. Also ist $\log \zeta_A(s) - \log(s-1)^{-1} = \log\left((s-1)\zeta_A(s)\right)$ beschraenkt fuer $s \to 1$. Fuer die zweite Aussage betrachte das Euler-Produkt von ζ_A und erhalte

$$\log \zeta_A(s) = -\sum_P \log(1 - |P|^{-s}) = \sum_P \sum_{k=1}^{\infty} \frac{|P|^{-ks}}{k} = \sum_P |P|^{-s} + \sum_P \sum_{k=2}^{\infty} \frac{|P|^{-ks}}{k}.$$

Wir haben $\sum_{k\geq 2} \frac{|P|^{-ks}}{k} < \sum_{k\geq 2} |P|^{-ks} = |P|^{-2s}(1-|P|)^{-s}) < 2|P|^{-2s}$. Damit ist die letzte Doppelsumme durch $2\zeta_A(2)$ beschraenkt fuer $s \to 1$ und die Behauptung folgt. □

Sei S eine Menge von Primpolynomen. Die **Dichte** von S ist definiert als

$$\delta(S) = \lim_{k\to\infty} \frac{\#\{P \in S : \deg P \leq k\}}{\#\{P : \deg P \leq k\}},$$

falls der Limes existiert.

Die **Dirichlet-Dichte** ist definiert als

$$\delta_D(S) = \lim_{s\to s} \frac{\sum_{P\in S} |P|^{-s}}{\sum_P |P|^{-s}},$$

falls der Limes existiert.

Proposition 4.1.2. *Sei S eine Menge von Primpolynomen. Existiert die Dichte, dann auch die Dirichlet-Dichte und die beiden sind gleich.*

Beweis. Sei S eine Menge von Primpolynomen, die eine Dichte δ hat. Sei $N(k)$ die Anzahl aller Primpolynome von Grad $\leq k$ und sei $N_S(k)$ die Anzahl aller Primpolynome in S vom Grad $\leq k$. Dann ist $\delta = \delta(S) = \lim_{k\to\infty} \frac{N_S(k)}{N(k)}$. Sei $A(n)$ die Anzahl aller Primpolynome, die Grad n haben und sei $A_S(n)$ die Anzahl aller Primpolynome in S, die Grad n haben. Es sei

$$Z(s) = \sum_P |P|^{-s} = \sum_{k=1}^{\infty} A(k)q^{-ks}$$

und ebenso $Z_S(s) = \sum_{P\in S} |P|^{-s} = \sum_{k=1}^{\infty} A_S(k)q^{-ks}$. Wir muessen zeigen, dass $\frac{Z_S(s)}{Z(s)}$ fuer $s \to 1$ gegen δ geht. Es ist

$$\begin{aligned} Z(s) &= \sum_k \left(N(k) - N(k-1)\right) q^{-ks} \\ &= \sum_{k=1}^{\infty} N(k)q^{-ks} - \sum_{k=1}^{\infty} N(k)q^{-ks}q^{-s} \\ &= \sum_{k=1}^{\infty} N(k)q^{-ks}\left(1-q^{-s}\right) \end{aligned}$$

und analog fuer $Z_S(s)$. Daher ist

$$\frac{Z_S(s)}{Z(s)} = \frac{\sum_{k=1}^{\infty} N_S(k)q^{-ks}}{\sum_{k=1}^{\infty} N(k)q^{-ks}}.$$

Sei nun $\varepsilon > 0$ und sei $k_0 \in \mathbb{N}$ so gross, dass fuer jedes $k \geq k_0$ gilt $\left|\frac{N_S(k)}{N(k)} - \delta\right| < \varepsilon/2$, oder $|N_S(k) - \delta N(k)| < \varepsilon N(k)/2$. Dann ist

$$\begin{aligned}
\left|\frac{Z_S(s)}{Z(s)} - \delta\right| &= \left|\frac{\sum_k (N_S(k) - \delta N(k))\, q^{-ks}}{\sum_k N(k) q^{-ks}}\right| \\
&\leq \left|\frac{\sum_{k<k_0} (N_S(k) - \delta N(k))\, q^{-ks}}{\sum_k N(k) q^{-ks}}\right| + \left|\frac{\sum_{k\geq k_0} \overbrace{(N_S(k) - \delta N(k))}^{<\varepsilon N(k)/2}\, q^{-ks}}{\sum_k N(k) q^{-ks}}\right| \\
&\leq \underbrace{\left|\frac{\sum_{k<k_0} (N_S(k) - \delta N(k))\, q^{-ks}}{\sum_k N(k) q^{-ks}}\right|}_{\to 0 \text{ fuer } s\to 1} + \underbrace{\left|\frac{\sum_{k\geq k_0} \frac{\varepsilon}{2} N(k) q^{-ks}}{\sum_k N(k) q^{-ks}}\right|}_{=\varepsilon/2}.
\end{aligned}$$

Es gibt also ein $s_0 > 1$ so dass fuer jedes $1 < s < s_0$ gilt $\left|\frac{Z_S(s)}{Z(s)} - \delta\right| < \varepsilon$. □

4.2 Der Dirichletsche Primzahlsatz

Satz 4.2.1 (Dirichlet-Primzahlsatz)**.** *Seien $a, m \in A$ nicht-konstante, teilerfremde Polynome. Sei S die Menge aller Primpolynome P mit $P \equiv a \mod (m)$. Dann hat S die Dirichlet-Dichte $1/\Phi(m)$.*

Man kann auch zeigen, dass S die Dichte $1/\Phi(m)$ hat, aber nur mit erheblich mehr Aufwand.

Der Beweis des Satzes fuellt den Rest dieses Abschnitts.

Sei $m \in A$ ein nichtkonstantes Polynom. Ein **Dirichlet-Charakter** modulo M ist ein Gruppenhomomorphismus

$$\chi : (A/mA)^\times \to \mathbb{C}^\times.$$

Da $(A/mA)^\times$ eine endliche Gruppe ist, liegt das Bild von χ in der Gruppe der Einheitswurzeln, also in der **Kreisgruppe** $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. Man setzt χ fort zu einer Abbildung $A/mA \to \mathbb{C}$ indem man $\chi(a) = 0$ setzt, falls a keine Einheit in A/mA ist. Durch Vorschalten der Projektion $A \to A/mA$ kann man χ auch als eine Abbildung auf A auffassen. Dann ist insbesondere

$$\chi(a) \neq 0 \quad \Leftrightarrow \quad \mathrm{ggT}(a, m) = 1$$

und es gilt $\chi(ab) = \chi(a)\chi(b)$ fuer alle $a, b \in A$.

Sei G eine endliche abelsche Gruppe und sei $\widehat{G}$ die Menge aller Gruppenhomomorphismen $\chi : G \to \mathbb{C}^\times$. Durch das punktweise Produkt

$$\chi\eta(x) = \chi(x)\eta(x)$$

wird $\widehat{G}$ zu einer Gruppe. Wir nennen sie die **duale Gruppe** zu G.

Proposition 4.2.2 (Pontryagin-Dualitaet)**.** *Sei G eine endliche Gruppe. Die duale Gruppe $\widehat{G}$ hat ebensoviele Elemente wie G. Die Abbildung $D : x \mapsto D_x$, wobei*

$$\begin{aligned} D_x : \widehat{G} &\to \mathbb{C}^\times, \\ \chi &\mapsto \chi(x), \end{aligned}$$

Ist ein Gruppenisomorphismus $G \to \widehat{\widehat{G}}$.

Proof. Sind G, H abelsche Gruppen, so ist die Abbildung

$$\begin{aligned} \widehat{G} \times \widehat{H} &\to \widehat{G \times H}, \\ (\chi, \eta) &\mapsto \Big[(x, y) \mapsto \chi(x)\eta(y)\Big], \end{aligned}$$

ein Isomorphismus. Man sieht nun leicht, dass der Satz, wenn er fuer G und H gilt, auch fuer $G \times H$ richtig ist. Nach dem Hauptsatz ueber endliche abelsche Gruppen ist G ein Produkt von zyklischen Gruppen. Es reicht also, den Satz fuer eine endliche zyklische Gruppe zu zeigen. Sei also G zyklisch von der Ordnung k. Wir waehlen einen Erzeuger τ. Fuer jedes $m = 0, \ldots, k-1$ sei $\chi_m : G \to \mathbb{C}^\times$ gegeben durch

$$\chi_m(\tau^j) = e^{2\pi i \frac{jm}{k}}.$$

Dann ist χ_m ein Gruppenhomomorphismus und die Abbildung $m \mapsto \chi_m$ ist eine Bijektion $\{0, \ldots, k-1\} \to \widehat{G}$, also haben G und $\widehat{G}$ gleichviele Elemente.

Die Abbildung D ist ein Gruppenhomomorphismus, denn

$$D(xy)(\chi) = \chi(xy) = \chi(x)\chi(y) = D(x)(\chi)D(y)(\chi) = D(x)D(y)(\chi).$$

Sei $x \in G$ im Kern von D. Dann folgt $\chi(x) = 1$ fuer jedes $\chi \in \widehat{G}$, also insbesondere fuer jedes χ_m. Nun ist etwa χ_1 aber injektiv, also ist $x = 1$, somit ist D injektiv ,da aber $|G| = |\widehat{G}| = |\widehat{\widehat{G}}|$, ist D eine Bijektion, also ein Isomorphismus. □

Fuer x, y aus irgendeiner Menge sei

$$\delta_{x,y} = \begin{cases} 1 & x = y, \\ 0 & x \neq y \end{cases}$$

das **Kronecker-Delta**. Auf dem endlich-dimensionalen Vektorraum aller Abbildungen von G nach $\mathbb{C}$ definieren wir ein Skalarprodukt

$$\langle f, g \rangle = \sum_{x \in G} f(x)\overline{g(x)}.$$

Proposition 4.2.3. *Sei G eine endliche abelsche Gruppe. Fuer zwei Charaktere $\chi, \eta \in \widehat{G}$ gilt*

$$\langle \chi, \eta \rangle = |G|\, \delta_{\chi,\eta}.$$

Ebenso gilt fuer zwei Elemente $x, y \in G$, dass

$$\sum_{\chi \in \widehat{G}} \chi(x)\overline{\chi(y)} = |G|\, \delta_{x,y}.$$

Beweis. Ist $\chi = \eta$, so gilt im ersten Fall

$$\langle \chi, \eta \rangle = \sum_{x \in G} \chi(x)\overline{\eta(x)} = \sum_{x \in G} \underbrace{|\chi(x)|^2}_{=1} = |G|.$$

Ist hingegen $\chi \neq \eta$, so gibt es ein $x_0 \in G$ mit $\chi(x_0) \neq \eta(x_0)$. Dann ist

$$\begin{aligned} \chi(x_0)\langle \chi, \eta \rangle &= \sum_{x \in G} \chi(x_0 x)\overline{\eta(x)} \\ &= \sum_{x \in G} \chi(x)\overline{\eta(x_0^{-1}x)} \\ &= \overline{\eta(x_0^{-1})} \sum_{x \in G} \chi(x)\overline{\eta(x)} \\ &= \eta(x_0)\langle \chi, \eta \rangle . \end{aligned}$$

Es folgt $\langle \chi, \eta \rangle = 0$. Mit der Pontryagin-Dualitaet tauschen G und $\widehat{G}$ die Rollen und der zweite Teil folgt auch. □

Im Spezialfall der Gruppe $G = (A/mA)^\times$ fuehrt diese Aussage zu

$$\sum_{a \mod (m)} \chi(a)\overline{\eta(a)} = \Phi(m)\delta_{\chi,\eta}.$$

Sei nun χ ein Dirichlet-Charakter modulo m. Die **L-Reihe** zu χ ist definiert als

$$L(s,\chi) = \sum_{f \text{ normiert}} \frac{\chi(f)}{|f|^s}.$$

Diese Reihe konvergiert wegen $|\chi(f)| \leq 1$ absolut fuer $\mathrm{Re}(s) > 1$ und da der Charakter multiplikativ ist, gilt in demselben Bereich die Euler-Produktentwicklung

$$L(s,\chi) = \prod_P \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1}.$$

Sei χ_0 der triviale Charakter modulo m. Dann folgt

$$L(s,\chi_0) = \prod_{P|m} \left(1 - \frac{1}{|P|^s}\right) \zeta_A(s).$$

Hieraus folgt, dass $L(\chi_0, s)$ zu einer meromorphen Funktion mit einfachem Pol bei $s = 1$ fortsetzt.

Proposition 4.2.4. *Sei χ ein nichttrivialer Dirichlet-Charakter modulo m. Dann ist $L(s,\chi)$ ein Polynom in q^{-s} vom Grad $\leq \deg(m) - 1$. Insbesondere ist $L(s,\chi)$ eine ganze Funktion.*

Beweis. Setze

$$A(n,\chi) = \sum_{\substack{\deg(f)=n \\ f \text{ normiert}}} \chi(f).$$

Dann ist

$$L(s,\chi) = \sum_{n=0}^{\infty} A(n,\chi) q^{-ns}.$$

Wir zeigen $A(n,\chi) = 0$ fuer alle $n \geq \deg(m)$. Damit folgt die Behauptung.

Wir koennen m als normiert annehmen. Sei also $n \geq \deg(m)$. Jedes f vom Grad n kann in der form $f = hm + r$ mit $\deg(r) < \deg(m)$ geschrieben werden. Dann ist h normiert vom Grad $n - \deg(m)$. Fuer h gibt es dann $q^{n-\deg(m)}$ viele Moeglichkeiten und r ist beliebig modulo (m). Daher ist

$$A(n,\chi) = q^{n-\deg(m)} \sum_{r \in A/mA} \chi(r) = 0.$$

und diese Summe ist Null nach Proposition 4.2.3 angewandt auf die Gruppe $G = (A/mA)^\times$, da die Summe bis auf ein Skalar das Skalarprodukt $\langle \chi, \chi_0 \rangle$ darstellt. □

Proposition 4.2.5. *Sei χ ein nichttrivialer Charakter modulo m. Dann gilt $L(1,\chi) \neq 0$.*

Der Beweis benoetigt ein Lemma.

Lemma 4.2.6. *Es gilt*

$$\prod_{\chi} L(s,\chi) = \prod_{P\nmid m} \left(1-|P|^{-f_P s}\right)^{-g_P},$$

wobei das Produkt links ueber alle Dirichlet Charaktere modulo m laeuft . Die Zahl f_P ist die Ordnung von P in der Gruppe $(A/mA)^\times$ und $g_P = \Phi(m)/f_P$.

Beweis. Fuer $f \in \mathbb{N}$ sei $\zeta = e^{2\pi i/f}$ der Standarderzeuger der Gruppe der f-ten Einheitswurzeln. Zunaechst beobachten wir, dass $\prod_{j=1}^{f} \zeta^j = (-1)^{f+1}$, denn in dem Produkt tritt neben $z = \zeta^j$ auch immer $\overline{z}$ auf, es sei denn $j = f$ oder $j = f/2$ falls f gerade ist. Des Weiteren hat das Polynom $z^f - 1$ genau die Potenzen von ζ als Nullstellen, also ist

$$\prod_{j=1}^{f}(1-\zeta^j z) = (-1)^{f+1}\prod_{j=1}^{f}(\zeta^j - z) = -\prod_{j=1}^{f}(z-\zeta^j) = -(z^f-1) = 1-z^f.$$

Sei $P \nmid m$ fest. Sei G die endliche abelsche Gruppe $(A/mA)^\times$. Das Bild des Gruppenhomomorphismus $D_P : \widehat{G} \to \mathbb{T}$ ist eine zyklische Gruppe der Ordnung f_P und der Kern hat die Maechtigkeit g_P. Es gilt daher

$$\prod_{\chi}(1-\chi(P)|P|^{-s}) = \prod_{i=0}^{f_P-1}\left(1-\zeta_{f_P}^i|P|^{-s}\right)^{g_P} = \left(1-|P|^{-f_P s}\right)^{g_P}. \qquad \square$$

Lemma 4.2.7. *Sei χ ein nichtquadratischer Dirichlet-Charakter modulo m, d.h., $\chi^2 \neq 1$, dann ist $L(1,\chi) \neq 0$.*

Beweis. Da χ nichtquadratisch ist, ist $\chi \neq \overline{\chi}$. **Angenommen**, $L(1,\chi) = 0$, dann ist auch $L(1,\overline{\chi}) = 0$. Der Faktor des trivialen Charakters χ_0 auf der linken Seite von Lemma 4.2.6 hat einen einfachen Pol bei $s = 1$, alle anderen Faktoren sich holomorph bei $s = 1$, wenn also zwei davon bei $s = 1$ verschwinden, hat die das Produkt in dem Lemma eine Nullstelle bei $s = 1$. Auf der anderen Seite ist

$$D(s) = \prod_{P\nmid m}\left(1-|P|^{-f_P s}\right)^{-g_P} = \prod_{P\nmid m}\left(\sum_{n=0}^{\infty}|P|^{-f_P n s}\right)^{g_P}$$

eine Dirichlet-Reihe mir positiven Koeffizienten und konstantem Term 1. Es folgt $D(s) \geq 1$ fuer $s > 1$, was der Annahme einer Nullstelle bei $s = 1$ **widerspricht!** $\square$

Beweis der Proposition. Um den Beweis von Proposition 4.2.5 abzuschliessen,

betrachten wir nun einen nichttrivialen quadratischen Charakter χ. Sei

$$G(s) = \frac{L(s,\chi_0)L(s,\chi)}{L(2s,\chi_0)}.$$

Dies ist ein Produkt ueber alle Primpolynome $P \nmid m$. Sei P ein Primpolynom $P \nmid m$. Der Faktor zu P in obigem Produkt ist

$$\frac{1-|P|^{-2s}}{(1-|P|^{-s})(1-\chi(P)|P|^{-s})}.$$

Ist $\chi(P) = -1$, ist dieser Faktor 1. Ist $\chi(P) = 1$, so ist er

$$\frac{1+|P|^{-s}}{1-|P|^{-s}} = (1+|P|^{-s})\sum_{k=0}^{\infty}|P|^{-ks} = 1 + 2\sum_{k=1}^{\infty}|P|^{-ks}.$$

Daher ist $G(s)$ eine Dirichlet-Reihe mit positiven Koeffizienten. Wir wissen

$$L(s,\chi_0) = \prod_{P|m}(1-|P|^{-s})\frac{1}{1-q^{1-s}}.$$

Daraus folgt

$$\frac{L(s,\chi_0)}{L(2s,\chi_0)} = \prod_{P|m}(1+|P|^{-s})^{-1}\frac{1-q^{1-2s}}{1-q^{1-s}}.$$

Daher ist auch

$$\frac{1-q^{1-2s}}{1-q^{1-s}}L(s,\chi) = \prod_{P|m}(1+|P|^{-s})G(s) = \sum_n \frac{a(n)}{|n|^s} \qquad \text{(Dies ist die Definition von } a(n).)$$

eine Dirichlet-Reihe mit positiven Koeffizienten. Setze $u = q^{-s}$. Dann folgt

$$\frac{1-qu^2}{1-qu}L^*(u,\chi) = \sum_{d=0}^{\infty}A(d)u^d,$$

wobei $L^*(u,\chi)$ ein Polynom in u ist und

$$A(d) = \sum_{n,\,\deg(n)=d} a(n) \geq 0$$

mit $A(0) = 1$. Die Dirichlet-Reihe konvergiert absolut fuer $\mathrm{Re}(s) > 1$, also konvergiert die Potenzreihe absolut fuer $|u| < q^{-1}$. Wir muessen zeigen, dass $L^*(q^{-1},\chi) \neq 0$ ist. **Angenommen,** $L^*(q^{-1},\chi) = 0$. Dann wird $L^*(u,\chi)$ von $(1-qu)$ geteilt, also ist die linke Seite obiger Gleichung ein Polynom. Dies ist dann also ein Polynom mit positiven Koeffizienten, kann also keine positive Nullstelle haben. Die linke Seite hat aber $\sqrt{q^{-1}}$

als Nullstelle, ein **Widerspruch!**. □

Mit Hilfe der Produktformel und der Technik aus dem Beweis von Proposition 4.1.1 sieht man

$$\log L(s,\chi) = \sum_P \frac{\chi(P)}{|P|^s} + R(s,\chi),$$

wobei $R(s,\chi)$ holomorph ist in $s = 1$. Wir multiplizieren mit $\overline{\chi(a)}$ und summieren ueber alle χ. Mit den Orthogonalitaetsrelationen erhalten wir

$$\sum_\chi \overline{\chi(a)} \log L(s,\chi) = \Phi(m) \sum_{P \equiv a \mod (m)} \frac{1}{|P|^s} + R(s),$$

wobei $R(s)$ beschraenkt ist fuer $s \downarrow 1$. Dividiere nun durch $\sum_P |P|^{-s}$ und lasse $s \to 1$ gehen. Die linke Seite geht dann gegen 1 und die rechte zeigt dann die Behauptung. Der Satz ist bewiesen. □

5 Allgemeine Funktionenkoerper

5.1 Primstellen

Sei $\mathbb{F}$ ein endlicher Körper. Eine Koerpererweiterung $K/\mathbb{F}$ heisst vom **Transzendenzgrad 1**, falls es ein $x \in K$ gibt, das nicht algebraisch ueber $\mathbb{F}$ ist so dass $K/\mathbb{F}(x)$ eine endliche Erweiterung ist. In diesem Fall nennt man K einen **Funktionenkoerper** ueber $\mathbb{F}$.

Lemma 5.1.1. *Sei K ein Funktionenkoerper ueber $\mathbb{F}$.*

(a) *Der algebraische Abschluss von $\mathbb{F}$ in K ist endlich ueber $\mathbb{F}$.*

Man kann daher $\mathbb{F}$ durch diesen Abschluss ersetzen und folglich annehmen, dass $\mathbb{F}$ in K algebraisch abgeschlossen ist. In diesem Fall sagt man, dass $\mathbb{F}$ der **Konstantenkoerper** *von K ist.*

(b) *Ist $\mathbb{F}$ der Konstantenkoerper von K, dann ist jedes Element $y \in K \setminus \mathbb{F}$ transzendent ueber $\mathbb{F}$ und der Koerper K ist endlich ueber $\mathbb{F}(y)$.*

Beweis. (a) Ist $K/\mathbb{E}/\mathbb{F}$ ein Zwischenkoerper, der algebraisch ueber $\mathbb{F}$ ist, dann gilt

$$[\mathbb{E} : \mathbb{F}] = [\mathbb{E}(x) : \mathbb{F}(x)] \leq [K : \mathbb{F}(x)].$$

(b) Sei $y \in K \setminus \mathbb{F}$. Da $\mathbb{F}$ in K algebraisch abgeschlossen ist, ist y transzendent ueber $\mathbb{F}$. Da y algebraisch ueber $\mathbb{F}(x)$ ist, gibt es ein Polynom $0 \neq g(X, Y) \in \mathbb{F}[X, Y]$ so dass $g(x, y) = 0$. Da y transzendent ueber $\mathbb{F}$, ist $g(X, Y) \notin \mathbb{F}[Y]$. Daher ist x algebraisch ueber $\mathbb{F}(y)$ und also ist $\mathbb{F}(x, y)$ endlich ueber $\mathbb{F}(y)$. Da K endlich ueber $\mathbb{F}(x)$, ist K auch endlich ueber $\mathbb{F}(x, y)$ und damit ist $K/\mathbb{F}(y) = K/\mathbb{F}(x, y)/\mathbb{F}(y)$ endlich. □

Ist v eine diskrete Bewertung, dann ist $\mathcal{O} = \{x \in K : v(x) \geq 0\}$ ein Unterring K von und $P = \{x : v(x) > 0\}$ ein Ideal in dem Ring $\mathcal{O}$. Man nennt $\mathcal{O}$ den **Bewertungsring** zu v und P das **Bewertungsideal**. Ein Element $\pi \in K$ mit $v(\pi) = 1$ wird **uniformisierendes Element** genannt. Es folgt sofort, dass $\mathcal{O}^\times = \{x : v(x) = 0\} = \mathcal{O} \setminus P$ und dass $P = \pi\mathcal{O}$. Ferner ist $\{x : v(x) \geq k\} = P^k$ fuer $k \in \mathbb{N}$ und

$$P = \bigcup_{k \geq 1} \mathcal{O}^\times \pi^k.$$

Insbesondere folgt, dass in der Ungleichung $v(a + b) \geq \min(v(a), v(b))$ Gleichheit herrscht, falls $v(a) \neq v(b)$.

Beispiele 5.1.2. • Betrachte $K = \mathbb{F}(x)$ den rationalen Funktionenkoerper in einer Variablen. Die Elemente sind rationale Funktionen der Form $\frac{p(x)}{q(x)}$ mit $q \neq 0$. Die **Gradbewertung** $v = v_\infty$ ist

$$v\left(\frac{p}{q}\right) = \deg(q) - \deg(p).$$

Um einzusehen, dass dies in der Tat eine Bewertung ist, beachte, dass fuer Polynome p, q stets $\deg(p+q) \leq \max(\deg(p), \deg(q))$ gilt. Rechne dann

$$\begin{aligned} v\left(\frac{p}{q} + \frac{v}{w}\right) &= v\left(\frac{pw + qv}{qw}\right) \\ &= \deg(qw) - \deg(pw + qv) \\ &\geq \deg(q) + \deg(w) - \max(\deg(pw), \deg(qv)) \\ &= \min\left(\deg(q) - \deg(p), \deg(w) - \deg(v)\right) \\ &= \min\left(v\left(\frac{p}{q}\right), v\left(\frac{v}{w}\right)\right). \end{aligned}$$

- Sei R ein faktorieller Ring (etwa $\mathbb{Z}$) und sei $P \in R$ irreduzibel. Fuer $f \in R$ sei $v_P(f)$ die Ordnung von P in der Primfaktorzerlegung von f, es gilt also

$$P^{v_P(f)} \mid f, \quad \text{aber} \quad P^{v_P(f)+1} \nmid f.$$

Dann ist v_P eine diskrete Bewertung.

- Sei $R = \mathbb{F}[x]$ der Polynomring und $K = \mathbb{F}(x)$ der Funktionenkoerper. Auf K gibt es die Gradbewertung und fuer jedes irreduzible Polynom $f \in R$ die Bewertung v_f. Wir behaupten, dass dies genau alle Bewertungen von K sind.

  Zunaechst ist klar, dass $v_f \neq v_\infty$ fuer jedes irreduzible f. Seien nun f, g irreduzibel und normiert und es gelte $v_f = v_g$. Dann ist aber $1 = v_g(g) = v_g(f)$ und damit sind $f = g$ nach der Definition von v_g.

  Es bleibt zu zeigen, dass jede Bewertung eine der gegebenen ist. Sei also v eine Bewertung von K mit Bewertungsideal P und Bewertungsring B. Dann ist $P \cap \mathbb{F}[x] = P \cap R$ ein Ideal von R.

  1. Fall. $P \cap R = 0$.
  Dann muss die Bewertung von x streng negativ sein, denn sonst waere die Bewertung auf ganz R gleich Null, was nicht sein kann, da K der Quotientenkoerper von R ist. Wir behaupten, dass $v(x) = -1$. Fuer ein beliebiges Polynom $f(x) = a_0 + \cdots + a_n x^n$ mit $a_n \neq 0$ ist $v(a_j x^j) = jv(x)$, also sind die

Bewertungen der $a_j x^j$ mit $a_j \neq 0$ alle verschieden, also folgt $v(f) = nv(x)$. Da es aber ein f geben muss mit $v(f) = -1$, folgt $v(x) = -1$. Nun ist leicht zu erkennen, dass v die Gradbewertung ist.

2.Fall. $I = P \cap R \neq 0$.
Da R ein Hauptidealring ist, wird dieses Ideal I von einem Element π erzeugt. Wir zeigen, dass $v(\pi) = 1$ ist. Wie im ersten Fall sieht man, dass aus $v(x) < 0$ schon $P \cap R = 0$ folgt, also haben wir $v(x) \geq 0$ und daher $v(f) \geq 0$ fuer jedes Polynom $f \in R$. Da K der Quotientenkoerper von R ist und das Bild von v von $v(R \cap P)$ erzeugt wird, muss $v(\pi) = 1$ sein, woraus sofort $v = v_\pi$ folgt.

Sei wieder K ein beliebiger Funktionenkoerper mit Konstantenkoerper $\mathbb{F}$. Eine **Primstelle** oder **Stelle** von K ist eine diskrete Bewertung v mit $v(\mathbb{F}) = 0$. Dann ist

$$\mathcal{O} = \{a \in K : v(a) \geq 0\}$$

ein Unterring von K der K als Qutotientenkoerper hat und

$$P = \{a \in K : v(a) > 0\}$$

ist das einzige maximale Ideal von $\mathcal{O}$.

Lemma 5.1.3. (a) *Der $\mathbb{F}$-Vektorraum $\mathcal{O}/P$ ist endlich-dimensional. Seine Dimension wird der* **Grad** *von P genannt, also*

$$\deg(P) = \dim_{\mathbb{F}} (\mathcal{O}/P)\,.$$

(b) *Der Ring $\mathcal{O}$ und die Bewertung v ist durch das maximale Ideal P eindeutig festgelegt. Wir werden daher in Zukunft auch fuer die Stelle nur P schreiben und v_P fuer die zugehoerige Bewertung.*

Beweis. (a) Sei $y \in P \subset K \setminus \mathbb{F}$. Dann ist $K/\mathbb{F}(y)$ endlich. Wir behaupten $[\mathcal{O}/P : \mathbb{F}] \leq [K : \mathbb{F}(y)]$. Seien hierzu $u_1, \ldots, u_m \in \mathcal{O}$ so dass die Restklassen $\bar{u}_1, \ldots, \bar{u}_m$ modulo P linear unabhaengig ueber $\mathbb{F}$ sind. Wir behaupten, dass $u_1, \ldots, u_m$ linear unabhaengig ueber $\mathbb{F}(y)$ sind. Seien also $f_1(y), \ldots, f_m(y)$ Polynome, so dass

$$f_1(y)u_1 + \cdots + f_m(y)u_m = 0.$$

Nach Reduktion modulo P liefert die lineare Unabhaengigkeit von $\bar{u}_1, \ldots, \bar{u}_m$, dass $f_1(y), \ldots, f_m(y) \in P$ gilt, was gleichbedeutend damit ist, dass die Polynome $f_1(y), \ldots, f_m(y)$ konstanten Term Null haben, also durch y divisibel sind. Da man dann

aber durch y teilen und das Argument iterieren kann, folgt, dass alle f_j gleich Null sind.

(b) Es sei P gegeben. Wir wollen die Bewertung $v = v_P$ rekonstruieren. Fuer $p \in P$ setze

$$w(p) = \max\{k \in \mathbb{N} : p \in P^k\}.$$

Ist $x \in K^\times \setminus P$ mit $x^{-1} \in P$, so setze $w(x) = -w(x^{-1}$, andernfalls setze $w(x) = 0$. Man macht sich leicht klar, dass $w = v$ gilt. Damit folgt die Behauptung. □

5.2 Erweiterungen von Funktionenkoerpern

Satz 5.2.1. *Sei R ein Dedekind-Ring mit Quotientenkoerper K, sei L/K eine endliche Koerpererweiterung und sei R_L der ganze Abschluss von R in L.*

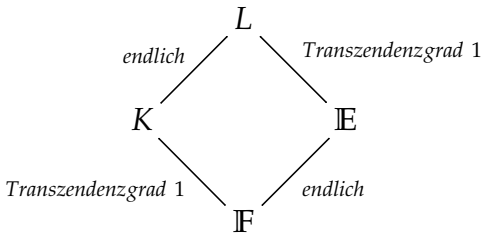
(a) *Dann ist auch R_L ein Dedekind-Ring und L ist der Quotientenkoerper von R_L.*

(b) *Ist L/K* **separabel**, *P ein Primideal in R und ist $\mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$ die Zerlegung des Ideals $R_L P$ in R_L, sei ferner $f_j = [R_L/\mathcal{P}_j : R/P]$ der Restklassengrad, dann gilt die fundamentale Gleichung*

$$\sum_{j=1}^{r} e_j f_j = n = [K : L].$$

Proof. Neukirch Kap. I, Saetze 8.1 und 8.2. □

Seien $K/\mathbb{F}$ und $L/\mathbb{E}$ Funktionenkoerper in einer Variablen. Dann heisst $L/\mathbb{E}$ eine **endliche Erweiterung** von $K/\mathbb{F}$, falls L/K und $\mathbb{E}/\mathbb{F}$ endliche Koerpererweiterungen sind und $\mathbb{E} \cap K = \mathbb{F}$ gilt.



Wir sagen, dass $L/\mathbb{E}$ eine **Konstantenerweiterung** von $K/\mathbb{F}$ ist, falls zusaetzlich $L = \mathbb{E}K$ gilt. In diesem Fall ist $[\mathbb{E} : \mathbb{F}] = [L : K]$.

Ist $v : L \to \mathbb{Z}$ eine Primstelle, dann ist die Restriktion $v|_K : K \to \mathbb{Z}$ eine Bewertung mit

$v(\mathbb{F}) = 0$, wir zeigen, dass sie nicht Null ist. Sei $\pi \in L$ ein Element mit $v(\pi) = 1$. Da L/K algebraisch ist, gibt es $n \in \mathbb{N}$ und $a_0, \ldots, a_{n-1} \in K$ so dass

$$\pi^n = a_1 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}.$$

Ist $v(a_j) = 0$ fuer jedes a_j, dann ist $v(a_j\pi^j) = j$ und damit

$$n = v(\pi^n) = v(a_0 + \cdots + a_{n-1}\pi^{n-1}) = \min(0, \ldots v(\pi^{n-1})) = 0,$$

was ein Widerspurch ist! Daher ist also $v|_K$ eine nichttriviale Bewertung. Sei $e\mathbb{Z}$ das Bild. Dann ist $w = \frac{1}{e}v$ eine diskrete Bewertung von K. In diesem Fall sagen wir, dass v *ueber* w liegt. Oder dass v die Stelle w teilt. Man schreibt dann $v|w$ oder $\mathcal{P}|P$, wenn P das Bewertungsideal zu w und $\mathcal{P}$ das von v ist. Die Zahl e heisst der **Verzweigungsindex** von v ueber w. Die Bewertung v heisst **unverzeigt** ueber K, falls $e = 1$. Ist P eine Primstelle von K, so gibt es nur endlich viele Primstellen $\mathcal{P}_1, \ldots, \mathcal{P}_r$ von L ueber P, wie wir gleich zeigen werden.

Definition 5.2.2. Sei $K/\mathbb{F}$ ein Funktionenkoerper. Sei $\mathrm{Div}(K/\mathbb{F})$ die freie abelsche Gruppe erzeugt von den Primstellen von $K/\mathbb{F}$, also

$$\mathrm{Div}(K/\mathbb{F}) = \left\{ \sum_P k_P P : k_P \in \mathbb{Z}, \text{ fast alle Null} \right\}.$$

Die Elemente heissen **Divisoren** und die Gruppe die **Divisorengruppe**. Ist $D = \sum_P k_P P$ ein Divisor, so definiert man den **Grad** des Divisors als

$$\deg(D) = \sum_P k_p \deg(P).$$

Proposition 5.2.3. (a) *Sei L/K separabel und sei $f_j = \left[\mathcal{O}_{\mathcal{P}_j}/\mathcal{P}_j : \mathcal{O}_P/P\right]$ der Grad der Restklassenkoerpererweiterung, dann gilt*

$$\sum_{j=1}^{r} e_j f_j = [L : K].$$

(b) *Sei L/K separabel. Ist D ein Divisor von $K/\mathbb{F}$, so koennen wir D als einen Divisor von $L/\mathbb{E}$ auffassen, indem wir jede Primstelle P durch $\sum_{j=1}^{r} e_j\mathcal{P}_j$ ersetzen. Dann gilt*

$$\deg_L(D) = \frac{[L : K]}{[\mathbb{E} : \mathbb{F}]} \deg_K(D).$$

Ist insbesondere $L/\mathbb{E}$ eine Konstantenerweiterung von $K/\mathbb{F}$, so ist $\deg_L(D) = \deg_K(D)$.

(c) *Ist $L/\mathbb{E}$ eine Konstantenerweiterung von $K/\mathbb{F}$, also separabel, und ist $\mathcal{P}$ eine Stelle von L, die ueber der Stelle P von K liegt, dann gilt $R_{\mathcal{P}}/\mathcal{P} = \mathbb{E}R_P/P$, wobei R_P und $R_{\mathcal{P}}$ die jeweiligen Bewertungsringe sind. Die Stelle $\mathcal{P}$ ist unverzweigt ueber P.*

Beweis. (a) Sei $x \in K$ mit $v_P(x) = 1$. Der Ring $\mathbb{F}[x]$ ist ein Dedekind-Ring. Sei R der ganze Abschluss von $\mathbb{F}[x]$ in K. Dann ist R ein Dedekind-Ring nach Satz 5.2.1. Der Ganze Abschluss R_L von R in L ist ebenfalls ein Dedekind-Ring. Dann ist v eine nicht-triviale Bewertung auf R, das Ideal $P \cap R$ ist ein Primideal von R und

$$R_L(P \cap R) = (\mathcal{P}_1 \cap R_L)^{e_1} \cdots (\mathcal{P}_r \cap R_L)^{e_r}$$

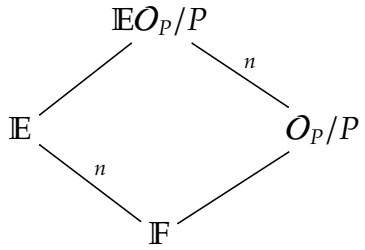
ist die Zerlegung in Primideale. Schliesslich gilt
$f_j = \left[\mathcal{O}_{\mathcal{P}_j}/\mathcal{P}_j : \mathcal{O}_P/P\right] = \left[R_L/(\mathcal{P}_j \cap R_L) : R/P\right]$, denn die Inklusion $R/P \to \mathcal{O}_P/P$ ist surjektiv, da K der Quotientenkoerper von R ist und ebenso fuer
$R_L/(\mathcal{P}_j \cap R_L) \to \mathcal{O}_{\mathcal{P}_j}/\mathcal{P}_j$. Damit folgt (a) aus Satz 5.2.1.

Fuer (b) rechnen wir

$$\begin{aligned}
\deg_L(D) &= \sum_P n_P \sum_j e_j \dim_{\mathbb{E}}(\mathcal{O}_{\mathcal{P}_j}/\mathcal{P}_j) \\
&= \frac{1}{[\mathbb{E}:\mathbb{F}]} \sum_P n_P \sum_j e_j \dim_{\mathbb{F}}(\mathcal{O}_{\mathcal{P}_j}/\mathcal{P}_j) \\
&= \frac{1}{[\mathbb{E}:\mathbb{F}]} \sum_P n_P \sum_j e_j f_j \dim_{\mathbb{F}}(\mathcal{O}_P/P) \\
&= \frac{[L:K]}{[\mathbb{E}:\mathbb{F}]} \sum_P n_P \dim_{\mathbb{F}}(\mathcal{O}_P/P) \\
&= \frac{[L:K]}{[\mathbb{E}:\mathbb{F}]} \deg_K(D)
\end{aligned}$$

(c) Eine Konstantenerweiterung ist immer separabel, denn ist E/F eine separable Koerpererweiterung und K/F irgendeine Koepererweiterung, dann ist EK/K separabel (Lang Algebra). Sei $n = [L:K] = [\mathbb{E}:\mathbb{F}]$ und $\mathcal{O}_{\mathcal{P}}$ der Bewertungsring und P die Stelle von K unter $\mathcal{P}$. Sei S die Menge aller Elemente von $L = \mathbb{E}K$ der Form $\sum_{j=1}^{n} a_j b_j$ mit $a_j \in \mathbb{E}$ und $b_j \in R_P$. Dann ist S ein Unterring von $\mathcal{O}_{\mathcal{P}}$ und der Quotientenkoerper von S ist L. Das Ideal $\mathfrak{M} = \mathcal{P} \cap S$ ist maximal mit $S/\mathfrak{M} = \mathbb{E}\mathcal{O}_P/P \subset \mathcal{O}_{\mathcal{P}}/\mathcal{P}$. Wir haben also das

Diagramm von Koepererweiterungen



Sei e der Verzweigungsindex, dann ist $n = e[\mathcal{O}_\mathcal{P}/\mathcal{P} : \mathcal{O}_P/P]$ und andererseits ist $n = [\mathbb{E}\mathcal{O}_P/P : \mathcal{O}_P/P]$ ein Teiler von $[\mathcal{O}_\mathcal{P}/\mathcal{P} : \mathcal{O}_P/P]$, woraus sich $e = 1$ und $\mathcal{O}_\mathcal{P}/\mathcal{P} = \mathbb{E}\mathcal{O}_P/P$ ergibt. □

Sei p die Charakteristik von von $\mathbb{F}$.

Sei L/K eine endliche separable Koerpererweiterung und $\mathcal{O}_P$ ein diskreter Bewertungsring (dBWR) in K mit K als Quotient. Sei P das maximale Ideal. Sei $\mathcal{O}_\mathcal{P}$ ein dBWR mit Quotientenkoerper L und maximalem Ideal $\mathcal{P}$. Wir sagen, dass $\mathcal{P}$ **ueber** P liegt, oder $\mathcal{P}$ **teilt** P, falls $\mathcal{O}_P = K \cap \mathcal{O}_\mathcal{P}$ und $P = K \cap \mathcal{P}$. Man schreibt dann

$$\mathcal{P}|P$$

und sagt auch, $\mathcal{P}$ teilt P. Sei $e = e(\mathcal{P}/P)$ der **Verzweigungsindex**, also die maximale natuerliche Zahl e mit $\mathcal{P}^e \subset P\mathcal{O}_\mathcal{P}$ (das heisst dann $\mathcal{P}^e = P\mathcal{O}_\mathcal{P}$). Sei ferner $f = f(\mathcal{P}/P)$ der **Restklassengrad**, also

$$f = \left[\mathcal{O}_\mathcal{P}/\mathcal{P} : \mathcal{O}_p/P\right].$$

Proposition 5.2.4. *Mit diesen Bezeichnungen gilt* $ef \leq n = [L : K]$.

Proof. Als $\mathcal{O}_\mathcal{P}$-ideal ist $\mathcal{P}$ von einem Element Π erzeugt. Seien $\omega_1, \ldots, \omega_m \in \mathcal{O}_\mathcal{P}$ so dass ihre Reduktionen modulo $\mathcal{P}$ ueber dem Koerper $\mathcal{O}_P/P$ linear unabhaengig sind. Wir zeigen, dass die em Elemente $\omega_i\Pi^j$ mit $1 \leq i \leq m$ und $0 \leq j < e$ linear unabhaengig ueber K sind, woraus die Behauptung folgt.

Seien also $a_{ij} \in K$ Koeffizienten, die nicht alle Null sind. Wir muessen zeigen, dass

$$\sum_{j=0}^{e-1} \sum_{i=1}^{m} a_{ij}\omega_i\Pi^j \neq 0.$$

Wir koennen annehmen, dass die a_{ij} alle in $\mathcal{O}_P$ liegen und mindestens einer nicht in P

liegt. Sei

$$A_j = \sum_{i=1}^{m} a_{ij}\omega_i \in \mathcal{O}_{\mathcal{P}}.$$

Ist ein $aij \notin P$, dann ist A_j eine Einheit in $\mathcal{O}_{\mathcal{P}}$, da die Reduktion modulo $\mathcal{P}$ nicht Null ist. Insbesondere ist dann $v(A_j) = 0$. Sind hingegen fuer gegebenes j alle a_{ij} in P, dann wird A_j vom Erzeuger π von P geteilt und daher ist dann $v_{\mathcal{P}}(A_j) \in e\mathbb{N}$. In jedem Fall ist aber $v_{\mathcal{P}}(A_j\Pi^j) \in e\mathbb{N}_0 + j$. Daher sind alle Bewertungen $v_{\mathcal{P}}(A_j\Pi^j)$ verschieden und also ist

$$v_{\mathcal{P}}\left(\sum_{j=0}^{e-1} A_j\Pi^j\right) = \min_j v_{\mathcal{P}}\left(A_j\Pi^j\right) < \infty = v_{\mathcal{P}}(0),$$

so dass $\sum_{j=0}^{e-1} A_j\Pi^j \neq 0$, also die Behauptung, folgt. □

Im separablen Fall wissen wir sogar mehr:

$$\sum_{j=1}^{r} e_j f_j = [L : K],$$

wobei $P\mathcal{O}_{\mathcal{P}} = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$ und $f_j = [\mathcal{O}_{\mathcal{P}_j}/\mathcal{P}_j : \mathcal{O}_P/P]$. Nun zum total inseparablen Fall:

Erinnerung:

- Eine Erweiterung L/K heisst **total inseparabel**, wenn fuer jedes $\alpha \in L \setminus K$ das Minimalpolynom inseparabel ist. In diesem Fall ist das Minimalpolynom immer schon von der Form $x^{p^n} - a$ fuer ein $n \in \mathbb{N}$ und ein $a \in K$, wobei $p > 0$ die Charakteristik von K ist.
- Ist L/K eine endliche normale Erweiterung und ist M der Fixkoerper von $\mathrm{Gal}(L/K)$, dann ist L/M separabel und M/K total inseparabel.

Ist L ein Koerper der Charakteristik p, dann ist

$$L^p = \{x^p : x \in L\}$$

ein Unterkoerper von L.

Proposition 5.2.5. *Sei L/K eine total inseparable Erweiterung vom Grad $p = \mathrm{char}(K)$. Nimm an, dass $K = L^p$ gilt. Sei $\mathcal{O}_P$ ein diskreter BWR mit Quotientenkoerper K. Dann gibt es genau einen dBWR $\mathcal{O}_{\mathcal{P}}$ in L ueber $\mathcal{O}_P$. Ferner gilt $e = p$, $f = 1$, also $ef = p = [L : K]$.*

Beweis. Sei $R = \{r \in L : r^p \in \mathcal{O}_P\}$ und $\mathcal{P} = \{r \in L : r^p \in P\}$. Dann ist R ein Ring, $\mathcal{P}$ ist ein Primideal in R und $\mathcal{P} \cap \mathcal{O}_P = P$. Wir zeigen, dass R ein dBWR ist.

Sei π ein Erzeuger von P. Da $L^p = K$, gibt es ein $\Pi \in L$ so dass $\Pi^p = \pi$. Nach Definition ist $\Pi \in \mathcal{P}$. Wir behaupten, dass jedes Element von L eine Potenz von Π ist mal einer Einheit von R. Sei also $t \in L$, dann ist $t^p = u\pi^s$ fuer eine Einheit u von $\mathcal{O}_P$ und $s \in \mathbb{Z}$. Dann ist $(t/\Pi^s)^p = u$ eine Einheit in $\mathcal{O}_P$ und daher ist t/Π^s eine Einheit in R und so ist R ein dBWR.

Sei nun $\mathcal{O}_{\mathcal{P}'}$ ein weiterer dBWR in L ueber $\mathcal{O}_P$ und sei $t \in \mathcal{O}_{\mathcal{P}'}$. Dann ist $t^p \in \mathcal{O}_{\mathcal{P}'} \cap K = \mathcal{O}_P$, also ist $t \in R$. Damit haben wir $\mathcal{O}_{\mathcal{P}'} \subset R$. Nun ist ein dBWR R stets ein maximaler Unterring seines Quotientenkoerpers L, was aus $L = \bigcup_{k\in\mathbb{Z}} \pi R^\times$ und $R = \bigcup_{k\geq 0} \pi^k R^\times$ folgt und was die Eindeutigkeit impliziert. □

Ein Koerper heisst **perfekt**, falls jede algebraische Erweiterung separabel ist.

Lemma 5.2.6. *Ein Koerper F der Charakteristik $p > 0$ ist genau dann perfekt, wenn $F = F^p$ gilt.*

Beweis. Es gelte $F^p \neq F$, dann gibt es ein $\alpha \in F$, so dass $f(X) = X^p - \alpha$ keine Nullstelle in F hat. Sei K/F der Zerfaellungskoerper von f und $\beta \in K$ eine Nullstelle, dann gilt $(X - \beta)^p = X^p - \beta^p = X^p - \alpha$, also hat f die mehrfache Nullstelle β und ist nicht separabel, also ist F nicht perfekt.

Die Umkehrung ist zB in Langs Algebra zu finden. □

Proposition 5.2.7. *Sei $\mathbb{F}$ ein perfekter Koerper der Charakteristik $p > 0$ und sei K ein Funktionenkoerper mit Konstantenkoerper $\mathbb{F}$. Dann ist $[K : K^p] = p$.*

Beweis. Sei $x \in K \setminus \mathbb{F}$. Dann ist $[K : \mathbb{F}(x)] < \infty$. Es gilt $\mathbb{F}(x)^p = \mathbb{F}(x^p)$ und $[\mathbb{F}(x) : \mathbb{F}(x^p)] = p$. Wegen

$$[K : K^p][K^p : \mathbb{F}(x)^p] = [K : \mathbb{F}(x^p)] = [K : \mathbb{F}(x)][\mathbb{F}(x) : \mathbb{F}(x^p)] = [K : \mathbb{F}(x)]p$$

reicht es zu zeigen, dass $[K : \mathbb{F}(x)] = [K^p : \mathbb{F}(x)^p]$ gilt. Dies ist aber klar, denn ist $v_1, \ldots, v_n$ eine $\mathbb{F}(x)$-Basis von K, dann ist $v_1^p, \ldots, v_n^p$ eine $\mathbb{F}(x)^p$-Basis von K^p. □

Korollar 5.2.8. *Sei K ein Funktionenkoerper der Charakteristik $p > 0$ mit perfektem Konstantenkoerper $\mathbb{F}$. Sei L eine rein inseparable Erweiterung vom Grad p. Dann ist $\mathbb{F}$ der Konstantenkoerper von L und es gilt $L^p = K$.*

Beweis. Sei $\alpha \in L$ eine Konstante, also algebraisch ueber $\mathbb{F}$. Dann ist α separabel ueber $\mathbb{F}$ also separabel ueber K. Da L/K rein inseparabel ist, ist $\alpha \in K$, also $\alpha \in \mathbb{F}$.

Sei nun $\alpha \in L \setminus K$. Da L/K rein inseparabel ist, ist das Minimalpolynom von α ueber K von der Form $x^{p^n} - a$ fuer ein $a \in K$ (Algebra). Da $[L : K] = p$, ist $\alpha^p - a = 0$, also $L^p \subset K$, da $[L : L^p] = p$, ist $L^p = K$. □

Proposition 5.2.9. *Sei K ein Funktionenkoerper mit perfektem Konstantenkoerper $\mathbb{F}$. Sei L eine endliche Erweiterung von K und sei M die maximale separable Erweiterung von K in L. Dann liegt ueber jedem Primideal P von M genau ein Primideal $\mathcal{P}$ von L. Es gilt dann $e(\mathcal{P}/P) = [L : M]$ und $f(\mathcal{P}/P) = 1$.*

Beweis. Der Konstantenkoerper $\mathbb{E}$ von M ist eine endliche Erweiterung des perfekten Koepers $\mathbb{F}$, also perfekt. Da L/M total inseparabel ist, gibt es eine Kette von Koerpererweiterungen

$$K \subset M = K_0 \subset K_1 \subset \cdots \subset K_n =,$$

wobei jede Erweiterung K_j/K_{j-1} total inseparabel vom Grad p ist.Damit ist $K_{j-1} = K_j^p$. Der Rest folgt durch iterierte Anwendung von Proposition 5.2.5. □

Satz 5.2.10. *Sei K ein Funktionenkoerper mit perfektem Konstantenkoerper $\mathbb{F}$. Sei L eine endliche Erweiterung von K vom Grad n. Sei P eine Primstelle von K und seien $\mathcal{P}_1, \ldots, \mathcal{P}_g$ die Primstellen ueber P. Dann gilt*

$$\sum_{j=1}^{g} e_j f_j = n.$$

wobei e_j der Verzweigungsindex und f_j der Restklassengrad von $\mathcal{P}_j$ ueber P ist.

Beweis. Sei M die maximale separable Erweiterung von K in L. Sei $\mathcal{P}'_j$ die Primstelle von M unter $\mathcal{P}_j$ und seien e'_j und f'_j der Verzweigungsindex und Restklassengrad von $\mathcal{P}'_j$ ueber P. Nach Proposition 5.2.3 gilt der Satz fuer M/K, also $\sum_{j=1}^{g} e'_j f'_j = [M : K]$. Nach Proposition 5.2.9 gilt $e'_j[L : M] = e_j$ und $f'_j = f_j$, woraus der Satz folgt. □

5.3 Der Satz von Riemann-Roch

Sei $\mathcal{D}_K$ die freie abelsche Gruppe erzeugt von den Primstellen von K. Man schreibt diese Gruppe additiv, die Elemente also $\sum_P n_P P$, und nennt die Elemente **Divisoren**. Der **Grad** eines Divisors $D = \sum_P n_P P$ ist

$$\deg(D) = \sum_P n_P \deg(P) \sum_P n_P \dim_{\mathbb{F}}(R_P/P).$$

Dann ist die Gradabbildung $\deg : \mathcal{D}_K \to \mathbb{Z}$ ein Gruppenhomomorphismus. Der Kern ist die Untergruppe $\mathcal{D}_K^0$ der Divisoren vom Grad Null.

Wir werden gleich zeigen, dass jedes $a \in K^\times$ einen Divisor

$$(a) = \sum_P v_P(a)P$$

definiert. Man nennt einen solchen Divisor einen **Hauptdivisor**. Ist $v_P(a) > 0$, so sagen wir, dass P eine **Nullstelle** von a ist. Ist $v_P(a) < 0$, ist a eine **Polstelle** von a. Wir schreiben

$$(a)_0 = \sum_{P : v_P(a) > 0} v_P(a)P, \qquad (a)_\infty = -\sum_{P : v_P(a) < 0} v_P(a)P.$$

Es gilt dann $(a) = (a)_0 - (a)_\infty$. Der Divisor $(a)_0$ wird der **Nullstellendivisor** und $(a)_\infty$ der **Polstellendivisor** genannt.

Proposition 5.3.1. (a) *Sei $a \in K^\times$. Dann gibt es nur endlich viele Stellen P mit $v_P(a) \neq 0$. Das heisst, dass $(a) = \sum_P v_P(a)P$ ein Divisor in $\mathcal{D}_K$ ist.*

(b) *Fuer $a \in K^\times$ ist der Divisor (a) genau dann der Null-Divisor, wenn $a \in \mathbb{F}^\times$, also wenn a eine Konstante ist.*

(c) *Fuer $a \in K \setminus \mathbb{F}$ gilt $\deg(a)_0 = \deg(a)_\infty = [K : \mathbb{F}(a)]$. Insbesondere folgt, dass der Grad eines Hauptdivisors Null ist.*

Beweis. Ist $a \in \mathbb{F}^\times$, dann ist $(a) = 0$. Nimm also an $a \in K^\times \setminus \mathbb{F}^\times$. Dann ist K endlich ueber $\mathbb{F}(a)$. Sei R der ganze Abschluss von $\mathbb{F}[a]$ in K. Dann ist K der Quotientenkoerper von R und R ist ein Dedekind-Ring nach Satz 5.2.1. Sei also $Ra = P_1^{e_1} \cdots P_g^{e_g}$ die Primidealzerlegung von Ra. Die Lokalisierungen R_{P_j} sind Bewertungsringe, die zugehoerigen Bewertungen sind Primstellen von K mit $v_{P_j}(a) = e_j$. Die $P_1, \ldots, P_g$ sind genau die Nullstellen von a. Die Polstellen von a sind die Nullstellen von a^{-1}, dies sind also auch nur endlich viele. Damit folgt (a). Es folgt auch (b), denn ist der Divisor (a) trivial, dann folgt $Ra = R$, also ist a eine Einheit von R.

Wir kommen zum Beweis von (c). Es sei $f_i = \dim_F(R/P_i)$ und $n = [K : \mathbb{F}(a)]$. Nach Satz 5.2.10 gilt aber

$$\sum_{j=1}^{g} e_j f_j = n.$$

Daraus folgt (c). □

Zwei Divisoren D_1, D_2 heissen **linear aequivalent**, geschrieben

$$D_1 \sim D_2,$$

wenn $D_1 - D_2$ ein Hauptdivisor ist. Die **Divisorenklassengruppe** CL_K ist der Quotient der Divisorengruppe $\mathcal{D}_K$ modulo linearer Aequivalenz. Anders gesagt, sei $\mathcal{H}_K \subset \mathcal{D}_K$ die Untergruppe der Hauptdivisoren, dann ist die Divisorenklassengruppe gleich dem Quotienten

$$Cl_K = \mathcal{D}_K/\mathcal{H}_K.$$

Sei ferner CL_K^0 die Untergruppe der Klassen vom Grad Null. Sei $D = \sum_P n_P P$ ein Divisor wir sagen, D ist ein **effektiver Divisor**, wenn $n_P \geq 0$ fuer jedes P gilt. Wir schreiben dann $D \geq 0$.

Fuer einen Divisor D sei

$$L(D) = \left\{x \in K^\times : (x) + D \geq 0\right\} \cup \{0\}.$$

Lemma 5.3.2. (a) *Sind A und B linear aequivalente Divisoren, dann sind $L(A)$ und $L(B)$ isomorphe $\mathbb{F}$-Vektorraeume.*

(b) *Ist $\deg(A) \leq 0$, dann ist $L(A) = 0$ ausser wenn $A \sim 0$, in welchem Fall $L(A)$ eindimensional ist.*

(c) *Sei D ein Divisor. Dann ist $L(D)$ ein endlich-dimensionaler $\mathbb{F}$-Vektorraum. Wir schreiben $l(D) = \dim L(D)$. Genauer gilt*

$$l(D) \leq \deg(D) + 1, .$$

falls $\deg(D) \geq 0$.

Beweis. (a) Sei $A = B + (h)$. Dann ist die Abbildung $x \mapsto xh$ ein Isomorphismus von $L(A)$ nach $L(B)$.

(b) Sei $f \in L(A)$, $f \neq 0$, dann ist $(f) + A \geq 0$ und $\deg((f) + A) = \deg(A) \leq 0$, damit folgt $(f) + A = 0$ oder $A = -(f) = (1/f)$, also $A \sim 0$. Sei nun $g \in L(A) = L(-(f))$, dann ist $(g/f) = (g) - (f) = (g) + A \geq 0$, also hat das Element g/f von K keine Polstellen, liegt damit im Konstantenkoerper $\mathbb{F}$, d.h., $g = \lambda f$ fuer ein $\lambda \in \mathbb{F}$.

(c) Induktion nach dem Grad. Ist $\deg(D) = 0$, so folgt $l(D) \leq 1$ nach Teil (b). Sei also $\deg(D) > 0$ und sei $D = mP + \sum_{Q \neq P} n_Q Q$ mit $m > 0$. Wir koennen annehmen, dass die Behauptung fuer $D' = (m-1)P + \sum_{Q \neq P} n_Q Q$ bewiesen ist. Nun ist $L(D) \supset L(D')$, die Menge $L(D)$ liegt in $P^m \subset K$, und $P^{m-1} \cap L(D) = L(D')$, also bildet der $\mathbb{F}$-Vektorraum

$L(D)/L(D')$ injektiv ab in den Raum $P^m/P^{m-1} \cong R/P \cong \mathbb{F}$. □

Satz 5.3.3 (Riemann-Roch)**.** *Es gibt eine ganze Zahl $g \geq 0$ und eine Divisorenklasse $C \in CL_K$ so dass fuer jedes $C \in \mathcal{C}$ und $A \in \mathcal{D}_K$ gilt*

$$l(A) - l(C - A) = \deg(A) - g + 1.$$

Die Klasse $\mathcal{C}$ und die Zahl g haengen nur von K ab. Die Klasse $\mathcal{C}$ heisst die **kanonische Klasse** *und g wird das* **Geschlecht** *von K genannt.*

Dieser Satz wird im naechsten Abschnitt bewiesen.

Korollar 5.3.4. (a) *Fuer jeden Divisor A gilt*

$$\Big(\deg(A) + 1\Big) - g \leq l(A) \leq \max\Big(\deg(A) + 1, 0\Big).$$

(b) *Fuer $C \in \mathcal{C}$ gilt*

$$l(C) = g \quad \textit{und} \quad \deg(C) = 2g - 2.$$

(c) *Falls $\deg(A) \geq 2g - 2$, dann ist $l(A) = \deg(A) - g + 1$ außer im Fall $A \in \mathcal{C}$.*

(d) *Sind $\mathcal{C}'$ und g' mit denselben Eigenschaften wie im Satz gegeben, dann ist $\mathcal{C}' = \mathcal{C}$ und $g' = g$.*

Beweis. (a) ist klar nach dem Satz und Lemma 5.3.2.

(b) Setze $A = 0$ im Satz und erhalte $l(C) = g$. Setze dann $A = C$ im Satz und erhalte $\deg(C) = 2g - 2$.

(c) Ist $\deg(A) \geq 2g - 2$, dann ist $\deg(C - A) \leq 0$. Ist $A \notin \mathcal{C}$, so folgt aus Lemma 5.3.2, dass $l(C - A) = 0$.

(d) Sei A ein Divisor vom Grad groesser als $\max(2g - 2, 2g' - 2)$ und $A \notin \mathcal{C} \cup \mathcal{C}'$. Nach Teil (c) folgt

$$l(A) = \deg(A) - g + 1 = \deg(A) - g' + 1,$$

also $g = g'$. Als naechstes sei $A = C'$. Waere $\mathcal{C}' \neq \mathcal{C}$, so folgt aus Teil (c), dass $g = l(C') = \deg(C') - g + 1 = g - 1$, Widerspruch! □

Beispiel 5.3.5. Betrachte $K = \mathbb{F}(x)$ den rationalen Funktionenkoerper in einer

Variablen mit der Gradbewertung

$$v_\infty\left(\frac{p}{q}\right) = \deg(q) - \deg(p).$$

Sei P_∞ das Bewertungsideal. Fuer grosse natuerliche Zahlen n hat man $l(nP_\infty) = n - g + 1$. Andererseits bedeutet $f \in nP_\infty$, dass f keine Pole ausserhalb ∞ hat, also ein Polynom vom Grad n ist. Also folgt $l(nP_\infty) = n + 1$, so dass $g = 0$ folgt. Damit folgt $\deg(C) = -2$. Wir behaupten, dass $CL_K^0 = 0$ ist. Sei hierzu $D = \sum_P n_P P$ ein Divisor vom Grad Null. Betrachte zunaechst die Gradbewertung mit Ideal P_∞. Ist $n_\infty = n_{P_\infty} \neq 0$, dann ist D linear aequivalent zum Divisor $D + n_\infty(x)$, wobei (x) der Divisor des Polynoms x ist. Wir koennen also $n_\infty = 0$ annehmen. In Beispiel 5.1.2 haben wir gesehen, dass jedes P mit $n_P \neq 0$ ein uniformisierendes Element π_P in $R = \mathbb{F}[x]$ hat und dass $R \subset R_P$ gilt, wobei R_P der Bewertungsring zu P ist. Da R_P ein Teilring des Quotientenkoerpers von R ist, ist die Abbildung zwischen Koerpern, $R/P \cap R \to R_P/P$ surjektiv, insgesamt also bijektiv. Damit ist $\deg(P) = \dim_{\mathbb{F}}(R_P/P) = \dim_{\mathbb{F}}(R/R\pi_P) = \deg(\pi_P)$. Sei $f = \prod_P \pi_P^{n_P}$. Wir behaupten, dass $D = (f)$ gilt. Fuer $P \neq P_\infty$ ist $\mathrm{ord}_P(D) = \mathrm{ord}_P(f)$ klar. Fuer P_∞ gilt $\mathrm{ord}_\infty(f) = v_\infty(f) = -\sum_P n_P \deg(\pi_P) = -\sum_P n_P \deg(P) = -\deg(D) = 0 = \mathrm{ord}_\infty(D)$. Wir haben also $CL_K^0 = 0$ gezeigt. Damit gibt es genau eine Klasse vom Grad -2 und wir koennen jeden Divisor von Grad -2 als C waehlen. Eine uebliche Wahl ist $C = -2P_\infty$.

Proposition 5.3.6. *Eine Erweiterung $K/\mathbb{F}$ vom Transzendenzgrad 1 ist genau dann ein Funktionenkoerper, also $K \cong \mathbb{F}(x)$, wenn K das Geschlecht Null hat und es eine Primstelle P von K vom Grad 1 gibt.*

Beweis. Ist $K = \mathbb{F}(x)$, so ist das Geschlecht gleich Null und man kann $P = P_\infty$ waehlen.

Sei also umgekehrt $g = 0$ und es existiere ein P vom Grad 1. Da $g = 0$ ist, gilt fuer jeden Divisor D mit $\deg(D) \geq 2g - 2 = -2$, dass $l(D) = \deg(D) + 1$ Damit folgt $l(P) = 2$ und es gibt ein $x \in K \setminus \mathbb{F}$ so dass $(x) + P \geq 0$. Da $\deg(P + (x)) = 1$ ist, ist $P + (x) = Q$ eine Primstelle vom Grad 1. Also ist $(x) = Q - P$. Sei wieder R der ganze Abschluss von $\mathbb{F}(x)$ in K, dann ist die Primidealzerlegung von $Rx = Q$, also ist $[K : \mathbb{F}(x)] = n = 1$, also $K = \mathbb{F}(x)$. □

5.4 Der Beweis des Riemann-Roch-Satzes

Sei $K/\mathbb{F}$ ein Funktionenkoerper und sei $\mathcal{S}_K$ die Menge der Primdivisoren (Primstellen) von K. Fuer $P \in \mathcal{S}_K$ und $a \in K$ sei

$$|a|_P = \begin{cases} 2^{-v_P(a)} & a \neq 0 \\ 0 & a = 0. \end{cases}$$

Die Zahl 2 ist hier beliebig, jede Zahl > 1 wuerde gehen. Dann ist $\rho_P(a,b) = |a-b|_P$ eine Metrik auf K. Sei $\widehat{O}_P$ die Vervollstaendigung des Bewertungsrings O_P in dieser Metrik. Dann ist $\widehat{O}_P$ wieder ein diskreter Bewertungsring und sein Quotientenkoerper ist $\widehat{K}_P$, die Vervollstaendigung von K in der Metrik. Der **Adele-Ring** von K wird definiert als

$$\mathbb{A}_K = \left\{ (x_P)_P \in \prod_P \widehat{K}_P : x_P \in \widehat{O}_P \text{ fuer fast alle } P \right\}.$$

Hierbei laeuft das Produkt ueber alle Primdivisoren P von K. Der Koerper K wird diagonal in den Adele-Ring eingebettet, d.h., via $\gamma \mapsto (\gamma_P)_P$ mit $\gamma_P = \gamma$ fuer jedes P. Ist $D = \sum_P n(P)P$ ein Divisor von K, dann sei $\mathbb{A}_K(D)$ die Menge aller $(x_P) \in \mathbb{A}_K$ so dass $v_P(x_P) \geq -n(P)$ fuer alle P gilt. Dann ist $\mathbb{A}_K(D)$ ein $\mathbb{F}$-Vektorraum.

Fuer zwei Divisoren C, D seien die Divisoren Infimum (C,D) und Supremum $[C,D]$ definiert durch

$$v_P((C,D)) = \min(v_p(C), v_p(D)),$$
$$v_p([C,D]) = \max(v_p(C), v_p(D)).$$

Dann gilt

$$(C,D) \leq C, D \leq [C,D].$$

Lemma 5.4.1. *Es gilt*

(a) $D \leq C \quad \Rightarrow \quad \mathbb{A}_K(D) \subset \mathbb{A}_K(C)$,

(b) $\bigcup_D \mathbb{A}_K(D) = \mathbb{A}_K$,

(c) $\mathbb{A}_K(C) \cap \mathbb{A}_K(D) = \mathbb{A}_K((C,D))$,

(d) $\mathbb{A}_K(C) + \mathbb{A}_K(D) = \mathbb{A}_K([C,D])$,

(e) $\mathbb{A}_K(D) \cap K = L(D)$.

Beweis. Dies folgt alles direkt aus der Definition. □

Definition 5.4.2. Ein **Weil-Differential** ist eine $\mathbb{F}$-lineare Abbildung $\omega : \mathbb{A}_K \to \mathbb{F}$, so dass

- $\omega(K) = 0$ und
- es gibt einen Divisor D, so dass $\omega(\mathbb{A}_K(D)) = 0$.

Sei Ω_K die Menge aller Weil-Differentiale und $\Omega_K(D)$ die Menge aller $\omega \in \Omega_K$ mit $\omega(\mathbb{A}_K(D)) = 0$.

Lemma 5.4.3. *Sei $\omega \in \Omega_K(D)$ und sei $x \in K$. Die Abbildung $x\omega$ definiert durch*

$$(x\omega)(\xi) = \omega(x\xi)$$

liegt dann in $\Omega(D + (x))$. Also ist $x\omega$ wieder ein Weil-Differential. Durch diese Skalarmultiplikation wird Ω_K ein K-Vektorraum.

Beweis. Wegen $xK \subset K$ ist $x\omega(K) = 0$. Ferner sei $(\xi_P) \in \mathbb{A}_K(D + (x))$. Das bedeutet $v_P(\xi_P) \geq -n_P(D) - v_P(x)$ fuer jedes P, also ist
$v_P((x\xi)_P) = v_P(x\xi_P) = v_P(x) + v_P(\xi_P) \geq -n_P(D)$, woraus folgt

$$(x\omega)(\xi) = \omega(x\xi) = 0.$$ □

Statt Weil-Differential sagen wir ab jetzt einfach Differential.

Lemma 5.4.4. *Seien $D \leq C$ Divisoren von K. Dann gilt*

$$\dim_{\mathbb{F}} (\mathbb{A}_K(C)/\mathbb{A}_K(D)) = \deg(C) - \deg(D).$$

Beweis. Ist $C = D$ so ist die Behauptung klar. Andernfalls erhaelt man C aus D durch Addition endlich vieler Primstellen. Es reicht also zu zeigen, dass

$$\dim_{\mathbb{F}} (\mathbb{A}_K(D + P)/\mathbb{A}_K(D)) = \deg(P).$$

Sei $\hat{P} = P\widehat{\mathcal{O}}_P$ der Abschluss von P in $\widehat{\mathcal{O}}_P$ und sei $n = n_P(D)$. Fuer $\xi = (\xi_P) \in \mathbb{A}_K(D + P)$ gilt $v_P(\xi_P) \geq -n - 1$, was aequivalent ist zu $\xi_P \in \hat{P}^{-n-1}$. Die Abbildung

$$\begin{aligned} \mathbb{A}_K(D + P) &\to \hat{P}^{-n-1}/\hat{P}^{-n} \\ \xi &\mapsto \xi_P \mod (\hat{P}^{-n}) \end{aligned}$$

ist ein epimorphismus und der Kern ist $\mathbb{A}_K(D)$. Also ist

$$\mathbb{A}_K(D + P)/\mathbb{A}_K(D) \cong \hat{p}^{-n-1}/\hat{P}^{-n} \cong \mathcal{O}_P/P$$

und damit $\dim_{\mathbb{F}} (\mathbb{A}_K(D+P)/\mathbb{A}_K(D)) = \dim (\mathcal{O}_P/P) = \deg(P)$. □

Lemma 5.4.5. *Fuer Divisoren $D \leq C$ gilt*

$$\dim_{\mathbb{F}} \frac{\mathbb{A}_K(C)+K}{\mathbb{A}_K(D)+K} = (\deg(C) - l(C)) - (\deg(D) - l(D)).$$

Beweis. Wir benutzen $L(C) = \mathbb{A}_K(C) \cap K$ um mit den Isomorphiesaetzen zu sehen

$$\frac{\mathbb{A}_K(C)+K}{\mathbb{A}_K(D)+K} \cong \frac{\mathbb{A}_K(C)}{\mathbb{A}_K(D)+L(C)} \cong \frac{\mathbb{A}_K(C)/\mathbb{A}_K(D)}{(\mathbb{A}_K(D)+L(C))/\mathbb{A}_K(D)},$$

sowie

$$(\mathbb{A}_K(D)+L(C))/\mathbb{A}_K(D) \cong L(C)/L(D).$$

Es folgt

$$\dim_{\mathbb{F}} \frac{\mathbb{A}_K(C)+K}{\mathbb{A}_K(D)+K} = \dim_{\mathbb{F}} \mathbb{A}_K(C)/\mathbb{A}_K(D) - \dim_{\mathbb{F}} L(C)/L(D).$$

Mit Lemma 5.4.4 folgt die Behauptung. □

Korollar 5.4.6. *Fuer einen Divisor D sei $r(D) = \deg(D) - l(D)$, dann ist r monoton wachsend, d.h.,*

$$D \leq C \quad \Rightarrow \quad r(D) \leq r(C).$$

Proof. Folgt aus dem Lemma, da die Dimension eines Vektorraums ≥ 0 ist. □

Satz 5.4.7 (Riemann)**.** *Sei $K/\mathbb{F}$ ein Funktionenkoerper mit Konstantenkoerper $\mathbb{F}$. Es gibt dann eine eindeutig bestimmte ganze Zahl $g \geq 0$ so dass*

- *$l(D) \geq \deg(D) - g + 1$ fuer jeden Divisor, oder $r(D) \leq g - 1$ und*
- *es gibt eine Konstante c, so dass fuer jeden Divisor D mit $\deg(D) \geq c$ gilt $l(D) = \deg(D) - g + 1$ oder $r(D) = g - 1$.*

Beweis. Waehle ein Element $x \in K \setminus \mathbb{F}$ und sei n der Grad der endlichen Erweiterung $K/\mathbb{F}(x)$. Sei $B = (x)_\infty$ der Polstellendivisor von x. Nach Proposition 5.3.1 gilt $\deg(x)_\infty = n$.

Sei R der ganze Abschluss von $\mathbb{F}[x]$ in K. Ist $\rho \in R$, dann hat ρ nur Pole an den Polstellen von x, denn gilt $v_P(\rho) < 0$ und $a_0 + \cdots + a_{n-1}\rho^{n-1} + \rho^n = 0$ mit

$a_0, \ldots, a_{n-1} \in \mathbb{F}[x]$, so folgt

$$\begin{aligned} 0 > nv_P(\rho) = v_P(\rho^n) &= v_P(a_0 + \cdots + a_{n-1}\rho^{n-1}) \\ &\geq \min(v_P(a_0), v_P(a_1) + v_P(\rho), \ldots, v_P(a_{n-1}) + (n-1)v_P(\rho)), \end{aligned}$$

was nur sein kann, wenn $v_P(a_j) < 0$ fuer ein j. Das a_j ist aber ein Polynom in x mit Koeffizienten in $\mathbb{F}$, so dass $v_P(x) < 0$ folgt.

Daher ist $\rho \in L(m_0 B)$ fuer ein $m_0 \geq 0$. Da K der Quotientenkoerper von R ist, gibt es eine Basis $\rho_1, \ldots, \rho_n$ von $K/\mathbb{F}(x)$ mit $\rho_j \in R$ fuer jedes j. Waehle ein $m_0 \geq 0$ so dass $\rho_j \in L(m_0 B)$ fuer jedes j gilt. Fuer jedes $m \geq m_0$ liegen die Elemente $x^j \rho_i$ mit $0 \leq j \leq m - m_0$ und $1 \leq i \leq n$ alle in $L(mB)$ und sind linear unabhaengig ueber $\mathbb{F}$. Daher gilt

$$l(mB) \geq n(m - m_0 + 1)$$

und

$$r(mB) = \deg(mB) - l(mB) \leq mn - n(m - m_0 + 1) = nm_0 - n.$$

Daher ist die wachsende Folge $r(mB)$ ganzer Zahlen nach oben beschraenkt und muss daher ab einem Punkt konstant sein. Sei dieser Maximalwert $g - 1$. Wegen $(0) \leq mB$ und $-1 = r((0)) \leq r(mB) \leq g - 1$ folgt $g \geq 0$.

Sei nun D irgendein Divisor. Wir schreiben $-D = D_1 + D_2$, wobei der Traeger von D_1 disjunkt zu dem von B ist und der von D_2 eine Teilmenge von dem von B ist. Sei P im Traeger von D_1. Es folgt $\mathbb{F}[x] \subset \mathcal{O}_P$ und $P \cap \mathbb{F}[x] = (g(x))$ fuer ein normiertes irreduzibles Polynom g. Dann ist P eine Nullstelle von $g(x)$ und fuer ein $\mu \in \mathbb{N}$ hat der Divisor $(g(x)^\mu) + D_1$ keinen Pol in P. Wir machen dies fuer jedes P im Traeger von D_1 und multiplizieren die Polynome, so dass wir ein Polynom $f(x)$ erhalten, so dass $(f(x)) + D_1$ nur Pole hat, wo auch x welche hat. Dasselbe gilt fuer D_2 und daher gilt es auch fuer $(f(x)) - D$. Es gibt also ein $m \geq 0$ so dass

$$(f(x)) - D + mB \geq 0$$

oder $D \leq (f(x)) + mB$, so dass $r(D) \leq r((f(x)) + mB) = r(mB) \leq g - 1$, so dass Riemanns Ungleichung bewiesen ist.

Zur Existenz von c: Sei $m_1 \in \mathbb{N}$ so gross, dass $r(m_1 B) = g - 1$ und setze $c = m_1 n + g$. Ist nun D ein Divisor mit $\deg(D) \geq c$, dann folgt aus Riemanns Ungleichung, dass

$$l(D - m_1 B) \geq \deg(D - m_1 B) - g + 1 \geq 1.$$

Es gibt also ein $y \in K^\times$, so dass $(y) + D - m_1 B \geq 0$ oder $m_1 B \leq D + (y)$ und damit

$$g - 1 = r(m_1 B) \leq r(D + (y)) = r(D).$$

Zusammen folgt $r(D) = g - 1$ oder $l(D) = \deg(D) - g + 1$. □

Proposition 5.4.8. *Fuer jeden Divisor D ueber K ist der Raum $\Omega_K(D)$ endlich-dimensional ueber $\mathbb{F}$ und es gilt*

$$l(D) = \deg(D) - g + 1 + \dim_{\mathbb{F}} \Omega_K(D).$$

Beweis. Lemma 5.4.5 sagt, dass fuer Divisoren $D \leq C$ gilt

$$\dim_{\mathbb{F}} \frac{\mathbb{A}_K(C) + K}{\mathbb{A}_K(D) + K} = r(C) - r(D).$$

Wir halten D fest und lassen C ueber alle Divisoren $C \geq D$ laufen. Nach Riemanns Ungleichung ist $r(C) \leq g - 1$, so dass

$$\dim_{\mathbb{F}} \frac{\mathbb{A}_K(C) + K}{\mathbb{A}_K(D) + K} \leq g - 1 - r(D).$$

Ist $\deg(C) \geq c$, gilt Gleichheit. Sei also $C_0 \geq D$ mit $\deg(C_0) \geq c$. Dann herrsch Gleicheit fuer alle Divisoren $C \geq C_0$ und also $\mathbb{A}_K(C) + K = \mathbb{A}_K(C_0) + K$ fuer alle $C \geq C_0$. Aber fuer jedes Adele ξ gibt es ein $C \geq C_0$, so dass $\xi \in \mathbb{A}_K(C)$, so dass also folgt $\mathbb{A}_K(C_0) + K = \mathbb{A}_K$ und

$$l(D) = \deg(D) - g + 1 + \dim_{\mathbb{F}} \frac{\mathbb{A}_K}{\mathbb{A}_K(D) + K}.$$

Die Proposition ist bewiesen, da der Raum $\Omega_K(D)$ der $\mathbb{F}$-Dualraum von $\frac{\mathbb{A}_K}{\mathbb{A}_K(D)+K}$ ist. □

Korollar 5.4.9. (a) *Sei c die Konstante aus Riemanns Satz. Ist Dann D ein Divisor mit $\deg(D) \geq c$, so gilt $\mathbb{A}_K = \mathbb{A}_K(D) + K$.*

(b) *Es gilt $g = \dim_{\mathbb{F}} \Omega_K(0)$.*

Beweis. Die Aussage (a) wurde im Beweis der Proposition benutzt und (b) folgt, indem man die Proposition auf der Nulldivisor anwendet. □

Lemma 5.4.10. *Sei $\omega \in \Omega_K$ ein nichtverschwindendes Differential. Dann existiert genau ein Divisor D so dass fuer jeden Divisor D' gilt*

$$\omega(\mathbb{A}_K(D')) = 0 \quad \Leftrightarrow \quad D' \leq D.$$

Beweis. Sei $\mathcal{T} = \{D' : \omega(\mathbb{A}_K(D')) = 0\} \neq \emptyset$. Da $\omega \neq 0$, folgt nach Korollar 5.4.9 (a), dass $\deg(D') < c$ fuer jeden Divisor $D' \in \mathcal{T}$. Sei D ein Divisor maximalen Grads in $\mathcal{T}$. Wir

behaupten, dass D der verlangte Divisor ist. Es gilt $\omega(\mathbb{A}_K(D)) = 0$. Sei nun $D' \in \mathcal{T}$, dann verschwindet ω auf $\mathbb{A}_K(D) + \mathbb{A}_K(D') = \mathbb{A}_K([D, D'])$, d.h. das Maximum $[D, D']$ liegt in $\mathcal{T}$. Da nun $\deg[D, D'] \geq \deg D$, der Divisor D aber maximalen Grad in $\mathcal{T}$ hat, muessen die Grade gleich sein und das bedeutet $[D, D'] = D$, also $D' \leq D$. Die Eindeutigkeit ist klar. □

Der **Divisor des Differentials** ω ist nach Definition der Divisor D aus dem Lemma. Wir schreiben ihn als $D = (\omega)$.

Lemma 5.4.11. *Sei $\omega \in \Omega_K$ und $x \in K^\times$. Dann gilt*

$$(x\omega) = (x) + (\omega).$$

Beweis. Das Differential ω verschwindet genau dann auf $\mathbb{A}_K(D)$, wenn $x\omega$ auf $\mathbb{A}_K(D + (x))$ verschwindet. Daraus folgt die Behauptung. □

Proposition 5.4.12. $\dim_K(\Omega_K) = 1$.

Beweis. Sei D ein Divisor, $\omega \neq 0$ ein Differential und sei $x \in L((\omega) - D)$. Wir behaupten, dass $x\omega \in \Omega_K(D)$. Wir wissen, dass $x\omega$ auf $\mathbb{A}_K((x) + (\omega))$ verschwindet. Da $x \in L((\omega) - D)$, folgt $(x) + (\omega) - D \geq 0$, also $(x) + (\omega) \geq D$. Daher verschwindet $x\omega$ auf $\mathbb{A}_K(D)$.

Seien nun $\omega, \omega' \in \Omega_K$ nichtverschwindende Differentiale. Wir haben gerade gesehen, dass

$$L((\omega) - D)\omega,\ L((\omega') - D)\omega' \ \subset\ \Omega_K(D).$$

Wir zeigen, dass fuer geeignetes D diese beiden $\mathbb{F}$-Vektorraeume einen nichtverschwindenden Schnitt haben, was die Behauptung liefert.

Fuer eine Primstelle P setze $D = -nP$ fuer $n \in \mathbb{N}$. Nach Proposition 5.4.8 gilt

$$\dim_{\mathbb{F}} \Omega_K(-nP) = l(-nP) + n\deg(P) + g - 1 = n\deg(P) + g - 1,$$

wobei wir benutzt haben, dass $L(-nP) = 0$ ist, denn jedes Element dieses Raums haette keinen Pol und eine Nullstelle bei P. Nach der Riemann-Ungleichung ist

$$\dim_{\mathbb{F}} L((\omega) + nP) \geq \deg(\omega) + n\deg P - g + 1,$$

und ebenso fuer ω'. Daher

$$\begin{aligned}&\dim_{\mathbb{F}} L((\omega) + nP)\omega + \dim_{\mathbb{F}} L((\omega') + nP)\omega' \\ &\geq 2n \deg P + \deg(\omega) + \deg(\omega') - 2g + 2 \\ &= n \deg(P) + g - 1 + \deg(\omega) + \deg(\omega') + \dim_{\mathbb{F}} \Omega(-nP)\end{aligned}$$

Fuer hinreichend grosses n wird daher die Summe der Dimensionen links groesser als die Dimension des umgebenden Raumes $\Omega(-nP)$, also muss es einen nichtverschwindenden Schnitt geben. □

Korollar 5.4.13. *Sei $0 \neq \omega \in \Omega_K$ und sei D ein Divisor. Dann ist die Abbildung $x \mapsto x\omega$ ein $\mathbb{F}$-linearer Isomorphismus zwischen $L((\omega) - D)$ und $\Omega_K(D)$.*

Beweis. Da Ω_K ein K-Vektorraum ist, ist $x \mapsto x\omega$ injektiv. Im Beweis der Proposition wurde $L((\omega) - D)\omega \subset \Omega_K(D)$ gezeigt. Wir zeigen Gleichheit. Sei also $\omega' \in \Omega_K(D)$. Nach der Proposition gibt es ein $x \in K$ mit $\omega' = x\omega$. Da ω' auf $\mathbb{A}_K(D)$ verschwindet, folgt $D \leq (\omega') = (x) + (\omega)$. Damit also $(x) \geq D - (\omega) = -((\omega) - D)$, d.h. $x \in L((\omega) - D)$. □

Korollar 5.4.14. *Die Divisoren der Differentiale bilden eine Divisorenklasse, diese wird die kanonische Klasse von K genannt.*

Beweis. Klar. □

Beweis des Riemann-Roch-Satzes. Nach Proposition 5.4.8 und Korollar 5.4.13 gilt

$$l(D) = \deg(D) - g + l((\omega) - D).$$

Als Divisor C koennen wir irgendeinen Divisor in der kanonischen Klasse nehmen und haben den RR-Satz bewiesen. □

6 Zetafunktionen allgemeiner Funktionenkoerper

6.1 Globale Funktionenkoerper

Sei nun $\mathbb{F}$ ein endlicher Koerper und $K/\mathbb{F}$ von Transzendenzgrad 1. Dann heisst K ein **globaler Funktionenkoerper**.

Lemma 6.1.1. *Fuer jedes $n \geq 0$ ist die Anzahl der effektiven Divisoren vom Grad n endlich.*

Beweis. Sei $x \in K \setminus \mathbb{F}$. Dann ist $K/\mathbb{F}(x)$ endlich. Die Stellen von $\mathbb{F}(x)$ sind gegeben durch die Stelle ∞ und alle irreduziblen Polynome. Also gibt es nur endlich viele Stellen von $\mathbb{F}(x)$ von gegebenem Grad. Nun zu K. Sei nun (P, v_P) eine Stelle von K. **Angenommen,** $v_P|_{\mathbb{F}(x)}$ ist trivial. Sei dann $\alpha \in K$ mit $v(\alpha) = 1$. Dann gibt es $a_1, \ldots, a_{n-1} \in \mathbb{F}(x)$ mit $a_0 + a_1\alpha + \cdots = \alpha^n$, wobei $a_0 \neq 0$. Da $v_P(a_j) = 0$ ist

$$\begin{aligned} n = v(\alpha^n) &= v(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) \\ &= \min(0 = v(a_0), v(a_1\alpha), \ldots, v(a_{n-1}\alpha^{n-1})) \\ &= 0. \end{aligned}$$

In dem Minimum treten nur die $a_j \neq 0$ auf. **Widerspruch!** Also ist v nichttrivial auf $\mathbb{F}(x)^\times$. Das Bild ist $d\mathbb{Z}$ fuer ein $d \in \mathbb{N}$, damit ist $w = \frac{1}{d}v$ eine Bewertung, also eine Primstelle von $\mathbb{F}(x)$. Dann ist $\deg(P) = \dim_{\mathbb{F}}(\mathcal{O}_P/P) \geq \dim_{\mathbb{F}}(\bar{\mathcal{O}}_P/P \cap \bar{\mathcal{O}}_P)$, wobei $\bar{\mathcal{O}}_P$ der Bewertungsring von w ist. Damit folgt die Behauptung, wenn wir zeigen koennen, dass es hoechstens $n = [K : \mathbb{F}(x)]$ viele verschiedene Bewertungen v von K gibt, die auf eine gegebene Bewertung w von $\mathbb{F}(x)$ einschraenken. Dies folgt aber aus dem bereits erwaehnten Satz (Neukirch) ueber Dedekind-Ringe, jetzt auf die Bewertungsrunge angewendet. □

Wir schreiben B_n fuer die Anzahl der effektiven Divisoren vom Grad n.

Lemma 6.1.2. *Die Gruppe CL_K^0 ist endlich. Ihre Kardinalitaet wird die* **Klassenzahl** *von K genannt und h_K geschrieben.*

Beweis. Sei D ein Divisor vom Grad $d > 0$. Ist A ein Divisor vom Grad Null, dann ist $\deg(gD + A) = dg$ und nach der Ungleichung in Korollar 5.3.4 (a) folgt $l(gD + A) \geq dg - g + 1 \geq 1$. Sei $f \in L(gD + A)$. Dann ist $B = (f) + gD + A \geq 0$, also ist $A \sim B - gD$, wobei B ein effektiver Divisor vom Grad gd ist. Es folgt $h_K \leq B_{dg} < \infty$. □

Fuer einen Divisor A sei $\bar{A}$ seine Klasse in CL_K.

Lemma 6.1.3. *Ist A ein Divisor, dann ist die Anzahl der effektiven Divisoren in $\bar{A}$ gleich $\frac{q^{l(A)}-1}{q-1}$. Ist also $n = \deg(A) > 2g-2$, so folgt nach Korollar 5.3.4, dass $B_n = h_K \frac{q^{n-g+1}-1}{q-1}$.*

Beweis. Wir zeigen zunaechst, dass $\bar{A}$ genau dann effektive Divisoren enthaelt, wenn $l(A) > 0$. Sei also $B \in \bar{A}$ ein effektiver Divisor. Es gibt dann $f \in K^\times$ so dass $(f) + A = B \geq 0$. Also ist $f \in L(A)$. Die Umkehrung folgt durch Rueckwaertslesen des Beweises.

Sei nun $l(A) > 0$. Die Abbildung von $L(A) \setminus \{0\}$ zur Menge aller effektiven Divisoren in $\bar{A}$, gegeben durch $f \mapsto (f) + A$ ist surjektiv und zwei Funktionen f, f' haben genau dann dasselbe Bild, wenn $(f) + A = (f') + A$, d.h., wenn $(f) = (f')$ oder $(f'f^{-1}) = 0$, also wenn $f' = cf$ fuer ein $c \in \mathbb{F}^\times$. Daher haben die Fasern dieser Abbildung jeweils $q-1$ Elemente und die Behauptung folgt. □

6.2 Konvergenz und Fortsetzung

Sei D ein Divisor. Wir definieren die **Norm** von D durch

$$N(D) = q^{\deg(D)}.$$

Dann ist $N(D) \in \mathbb{Q}_{>0}$ und es gilt $N(D+E) = N(D)N(E)$.

Wir definieren die **Zetafunktion** des Koerpers K als

$$\zeta_K(s) = \sum_{D \geq 0} N(D)^{-s}.$$

Die Summe wird ueber alle effektiven Divisoren erstreckt. Wir schreiben wieder B_n fuer die Anzahl der effektiven Divisoren vom Grad n, dann ist

$$\zeta_K(s) = \sum_{n=0}^{\infty} \frac{B_n}{q^{ns}}.$$

Um die Rechnungen zu vereinfachen fuehren wir die Potenzreihe $Z_K(u)$ ein:

$$Z_K(u) = \sum_{n=0}^{\infty} B_n u^n.$$

Dann gilt $\zeta_K(s) = Z_K(q^{-s})$.

Lemma 6.2.1. (a) *Die Reihe $\zeta_K(s)$ konvergiert fuer* $\mathrm{Re}(s) > 1$ *und dort gilt*

$$\zeta_K(s) = \prod_P \left(1 - \frac{1}{N(P)^s}\right)^{-1},$$

wobei das Produkt ueber alle Primstellen P von K erstreckt wird.

(b) *Im Fall $K = \mathbb{F}(x)$ gilt*

$$\zeta_K(s) = \zeta_A(s)(1 - q^{-s})^{-1},$$

wobei $A = \mathbb{F}[x]$ der Polynomring ist.

Beweis. (a) Wir schreiben wieder B_n fuer die Anzahl der effektiven Divisoren vom Grad n, dann ist

$$\zeta_K(s) = \sum_{n=0}^{\infty} \frac{B_n}{q^{ns}}.$$

Ist $n > 2g - 2$, dann folgt aus Korollar 5.3.4 und Lemma 6.1.3, dass $B_n = \frac{q^{n-g+1}-1}{q-1} = O(q^n)$, woraus die Konvergenz folgt. Das Euler-Produkt ist dann klar.

(b) Wir erinnern uns

$$\zeta_A(s) = \sum_{\substack{f \in A \\ \text{normiert}}} \frac{1}{|f|^s} = \prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1},$$

wopei dieses Euler-Produkt ueber alle Primpolynome laeuft. Nun sind die Primstellen von $\mathbb{F}(x)$ gegeben durch die Primpolynome und die Gradbewertung, woraus sich (b) ergibt. □

Sei $\delta\mathbb{Z}$ das Bild der Gradabbildung $\deg : \mathcal{D}_K \to \mathbb{Z}$. Dann ist δ der ggT aller Grade von Primstellen P von K. Wir werden spaeter zeigen, dass $\delta = 1$ ist.

Lemma 6.2.2. *Sei $h = h_K$. Fuer jede ganze Zahl $n \in \delta\mathbb{Z}$ gibt es h Divisorenklassen. Sei $n \geq 0$ und seien $\overline{A}_1, \ldots, \overline{A}_h$ die Divisorenklassen vom Grad n. Dann folgt*

$$B_n = \sum_{j=1}^{h} \frac{q^{l(A_j)} - 1}{q - 1}.$$

Beweis. h ist die Anzahl $|Cl_K^0|$ der Divisorenklassen vom Grad Null. Die Menge der Divisorenklassen vom Grad n ist dass $\overline{D} + CL_K^0$ fuer einen beliebigen Divisor D vom Grad n. Daher gibt es h Klassen vom Grad n, falls es einen Divisor vom Grad n gibt. □

Proposition 6.2.3. *Die Potenzreihe $Z_K(u)$ konvergiert fuer $|u| < q^{-1}$. Sie setzt zu einer rationalen Funktion auf $\mathbb{C}$ fort. Die einzigen Pole liegen bei den komplexen Zahlen u mit $u^\delta = 1$ oder $u^\delta = q^{-\delta}$. Diese Pole sind einfach.*

Die Zetafunktion ζ_K setzt fort zu einer meromorphen Funktion auf $\mathbb{C}$ mit einfachen Polen in allen Punkten von $\{s \in \mathbb{C} : q^{\delta s} = 1, q^\delta\}$.

Beweis. Mit Lemma 6.1.3 folgt fuer jedes $m \in \mathbb{N}$ mit $m > \frac{2g-2}{\delta}$,

$$\begin{aligned} Z_K(u) &= \sum_{n=0}^{\infty} B_{\delta n} u^{\delta n} \\ &= \sum_{n=0}^{m-1} B_{\delta n} u^{\delta n} + \sum_{n=m}^{\infty} h_K \frac{q^{\delta n - g + 1} - 1}{q-1} u^{\delta n} \\ &= \sum_{n=0}^{m-1} B_{\delta n} u^{\delta n} + \frac{h_K}{q-1} \sum_{n=m}^{\infty} (q^{\delta n - g + 1} - 1) u^{\delta n} \\ &= \sum_{n=0}^{m-1} B_{\delta n} u^{\delta n} + \frac{h_K}{q-1} \left(q^{\delta m - g + 1} u^{\delta m} \frac{1}{1 - (uq)^\delta} - u^{\delta m} \frac{1}{1 - u^\delta} \right), \end{aligned}$$

woraus sich die Behauptung ergibt. □

6.3 Zetafunktionen und Konstantenerweiterungen

Sei $r \in \mathbb{N}$. Der Koerper $\mathbb{E} = \mathbb{F}_{q^r}$ ist die eindeutig bestimmt Erweiterung von $\mathbb{F} = \mathbb{F}_q$ vom Rang r. Das Kompositum $K_r = K\mathbb{E}$ ist ein Funktionenkoerper ueber $\mathbb{E}$ und $K_r/\mathbb{E}$ ist eine Konstantenerweiterung von $K/\mathbb{F}$.

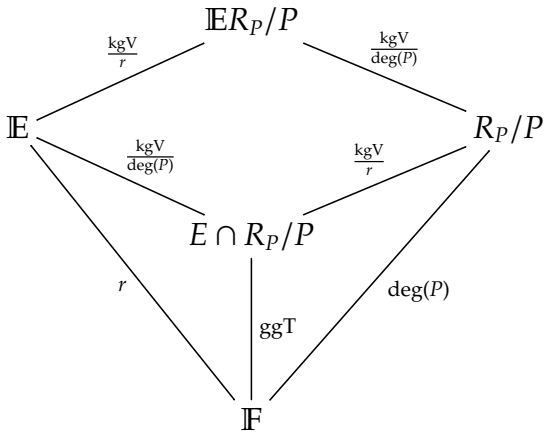
Lemma 6.3.1. *Sei P ein Primdivisor von $K/\mathbb{F}$. In K_r zerlegt sich P in paarweise verschiedene Primdivisoren $P = \mathcal{P}_1 + \cdots + \mathcal{P}_d$, die alle denselben Grad*

$$\deg(\mathcal{P}_j) = \frac{\mathrm{kgV}(r, \deg(P))}{r}$$

haben. Es folgt dann $d = \mathrm{ggT}(r, \deg(P))$.

Beweis. Nach Proposition 5.2.3 ist P in K_r unverzweigt, so dass die $\mathcal{P}_1, \ldots, \mathcal{P}_d$ verschieden sind. Ausserdem gilt $\mathcal{O}_{\mathcal{P}_j}/\mathcal{P}_j = \mathbb{E}\mathcal{O}_P/P$. Damit haben alle $\mathcal{P}_j$ denselben Grad $\deg(\mathcal{P}_j) = \dim_{\mathbb{E}}(\mathbb{E}\mathcal{O}_P/P) = \frac{\mathrm{kgV}(r,\deg(P))}{r}$. Die letzte Gleichheit wird klar aus dem

Diagramm der endlichen Koerpererweiterungen



□

Proposition 6.3.2. *Schreibe $Z = Z_K$ und $Z_r = Z_{K_r}$. Fuer jede komplexe Zahl u gilt*

$$Z_r(u^r) = \prod_{\xi^r=1} Z(\xi u).$$

Beweis. Es reicht, $|u| < q^{-1}$ anzunehmen. Dann gilt

$$\begin{aligned} Z_r(u^r)^{-1} &= \prod_P \prod_{\mathcal{P}|P} (1 - u^{r\deg(\mathcal{P})}) \\ &= \prod_P \prod_{\mathcal{P}|P} (1 - u^{\text{kgV}(r,\deg(P))}) \\ &= \prod_P (1 - u^{\text{kgV}(r,\deg(P))})^{\text{ggT}(r,\deg(P))} \end{aligned}$$

und

$$\prod_{\xi^r=1} Z(\xi u)^{-1} = \prod_P \prod_{\xi^r=1} (1 - (\xi u)^{\deg(P)}).$$

Es ist also zu zeigen, dass

$$\prod_{\xi^r=1} (1 - (\xi u)^d) = (1 - u^{\text{kgV}(r,d)})^{\text{ggT}(r,d)}$$

fuer jedes $d \in \mathbb{N}$ gilt. Damit diese beiden Polynome mit konstantem Term 1 gleich sind, reicht es, dass sie dieselben Nullstellen mit denselben Vielfachheiten haben. Wir

schreiben die linke Seite als

$$\prod_{\xi^r=1} \xi^d(\bar{\xi}^d - u^d).$$

Laeuft ξ durch die r-ten Einheitswurzeln, dann laeuft ξ^d durch die $\frac{r}{\mathrm{ggT}(d,r)}$-ten Einheitswurzeln, wobei jede genau $\mathrm{ggT}(d,r)$-mal auftritt. Also ist dieses Polynom

$$\left[\prod_{\varepsilon^{\frac{r}{\mathrm{ggT}(d,r)}}=1} \bar{\varepsilon}(\varepsilon - u^d)\right]^{\mathrm{ggT}(d,r)}.$$

Hiervon ist u genau dann eine Nullstelle, wenn $u^{d\frac{r}{\mathrm{ggT}(d,r)}} = 1$ und dies ist genau dann der Fall, wenn $u^{\mathrm{kgV}(d,r)} = 1$. □

Korollar 6.3.3. $\delta = 1$.

Proof. Wir haben $Z(u) = \sum_{n=0}^{\infty} B_{\delta n} u^{\delta n}$. Gilt also $\xi^\delta = 1$, so ist $Z(u) = Z(\xi u)$. Nach der Proposition ist dann $Z_\delta(u^\delta) = Z(u)^\delta$. Nach Proposition 6.2.3, angewendet auf Z_δ, hat $Z_\delta(u^\delta)$ einen einfachen Pol bei $u = 1$, aber $Z(u)^\delta$ hat nur dann einen einfachen Pol, wenn $\delta = 1$. □

6.4 Die Funktionalgleichung

Satz 6.4.1. *Die Funktion $Z(u)$ erfuellt die Funktionalgleichung*

$$Z\left(\frac{1}{qu}\right) = (\sqrt{q}u)^{2-2g} Z(u).$$

Setzt man $\widehat{Z}(u) = (u\sqrt{q})^{1-g} Z(u)$, dann lautet die Funktionalgleichung

$$\widehat{Z}(u) = \widehat{Z}\left(\frac{1}{qu}\right).$$

Beweis. Erster Fall: $g = 0$. Dann folgt nach Korollar 5.3.4 fuer jeden Divisor A vom Grad ≥ 0, dass

$$l(A) = \deg(A) + 1$$

ist. Ist $\deg(A) = 0$, so folgt also $l(A) = 1$, was nach Lemma 5.3.2 bedeutet, dass $A \sim 0$ ist, es folgt also $h_K = 1$. Mit Lemma 6.1.3 folgt, dass $B_n = \frac{q^{n+1}-1}{q-1}$, was gleichbedeutend ist mit $Z(u) = \frac{1}{(1-u)(1-qu)}$, so dass man die Funktionalgleichung leicht nachrechnet.

Sei nun also $g > 0$. Mit Lemma 6.1.3 erhalten wir

$$Z(u) = \sum_{A \geq 0} u^{\deg(A)} = \sum_{n=0}^{2g-2} \sum_{\substack{[A] \\ \deg(A)=n}} \frac{q^{l(A)} - 1}{q-1} u^n + \sum_{n=2g-1}^{\infty} h \frac{q^{n-g+1} - 1}{q-1} u^n$$

$$= \underbrace{\left[\frac{1}{q-1} \sum_{n=0}^{2g-2} u^n \sum_{\substack{[A] \\ \deg(A)=n}} q^{l(A)} \right]}_{=P(u)} + \underbrace{\left[\frac{1}{q-1} \sum_{n=2g-1}^{\infty} h q^{n-g+1} u^n - \frac{h}{q-1} \sum_{n=0}^{\infty} u^n \right]}_{=Q(u)}.$$

Hierbei wurde der letzte Teil der ersten Summe in der ersten Zeile zur letzten Summe in der zweiten Zeile geschlagen, was moeglich ist, da es zu jedem Grad $0 \leq n \leq 2g-2$ genau h Divisorenklassen $[A]$ gibt. Nach Riemann-Roch gilt fuer jeden Divisor A

$$l(A) - l(C - A) = \deg(A) - g + 1$$

wobei C aus der kanonischen Klasse ist und $l(C) = g$ sowie $\deg(C) = 2g - 2$ erfuellt. Es folgt

$$\begin{aligned} l(A) - \frac{1}{2}\deg(A) &= \frac{1}{2}\deg(A) + 1 - g + l(C - A) \\ &= l(C - A) - \frac{1}{2}\deg(C - A). \end{aligned}$$

Wenn A durch alle Divisorenklassen vom Grad 0 bis $2g - 2$ laeuft, dann tut $C - A$

dasselbe. Also ist

$$
\begin{aligned}
(\sqrt{q}u)^{2-2g}P(u) &= \frac{(\sqrt{q}u)^{2-2g}}{q-1} \sum_{\substack{[A] \\ \deg(A)\le 2g-2}} q^{l(A)}u^{\deg(A)} \\
&= \frac{1}{q-1} \sum_{\substack{[A] \\ \deg(A)\le 2g-2}} q^{l(A)-\frac{1}{2}\deg(A)}(\sqrt{q}u)^{2-2g+\deg(A)} \qquad A \to C-A \\
&= \frac{1}{q-1} \sum_{\substack{[A] \\ \deg(A)\le 2g-2}} q^{l(C-A)-\frac{1}{2}\deg(C-A)}(\sqrt{q}u)^{2-2g+\deg(C-A)} \\
&= \frac{1}{q-1} \sum_{\substack{[A] \\ \deg(A)\le 2g-2}} q^{l(A)-\frac{1}{2}\deg(A)}(\sqrt{q}u)^{-\deg(A)} \\
&= \frac{1}{q-1} \sum_{\substack{[A] \\ \deg(A)\le 2g-2}} q^{l(A)-\frac{1}{2}\deg(A)}(\sqrt{q}u)^{-\deg(A)} \\
&= \frac{1}{q-1} \sum_{\substack{[A] \\ \deg(A)\le 2g-2}} q^{l(A)}(qu)^{-\deg(A)} = P\left(\frac{1}{qu}\right).
\end{aligned}
$$

Fuer $Q(u)$ gilt auf der anderen Seite

$$
\begin{aligned}
Q(u) &= \frac{hq^{1-g}}{q-1}\sum_{n=2g-1}^{\infty}(qu)^n - \frac{h}{q-1}\sum_{n=0}^{\infty}u^n \\
&= \frac{h}{q-1}\left[\frac{q^g u^{2g-1}}{1-qu} - \frac{h}{1-u}\right],
\end{aligned}
$$

woraus man

$$
(\sqrt{q}u)^{2-2g}Q(u) = Q\left(\frac{1}{qu}\right)
$$

direkt nachrechnet. □

7 Die Riemann-Hypothese

7.1 Formulierung der RH

Aus dem Beweis von Proposition 6.2.3 und aus Korollar 6.3.3 ($\delta = 1$) ergibt sich

$$Z(u) = \sum_{n=0}^{2g-2} B_n u^n + \frac{hu^{2g-1}}{q-1}\left(\frac{q^g}{1-uq} - \frac{1}{1-u}\right),$$

also gilt

$$Z(u) = \frac{L(u)}{(1-u)(1-qu)},$$

wobei $L(u) = a_0 + a_1 u + \cdots + a_{2g}u^{2g}$ ein Polynom mit rationalen Koeffizienten ist.

Ueber $\mathbb{C}$ laesst sich $L(u)$ zerlegen

$$L(u) = \prod_{j=1}^{2g}(1 - \omega_j u),$$

wobei die ω_j^{-1} die Nullstellen von $L(u)$ sind.

Lemma 7.1.1. (a) *Es gilt $a_0 = 1$ und $a_1 = N - (q+1)$, wobei N die Anzahl der Primdivisoren vom Grad 1 ist. Ferner ist $a_{2g} = q^g$ und $a_{2g-1} = q^{g-1}(N - (q+1))$.*

(b) *Es gilt die Funktionalgleichung $L(u) = q^g u^{2g} L\left(\frac{1}{qu}\right)$.*

(c) *Fuer jedes $r \in \mathbb{N}$ ist $L_r(u^r) = \prod_{\xi^r=1} L(\xi u)$, wobei L_r das entsprechende Polynom zur Konstantenerweiterung $K_r/\mathbb{F}_{q^r}$ ist.*

(d) *Es ist*

$$L_r(u) = \prod_{j=1}^{2g}(1 - \omega_j^r u).$$

Beweis. Ist $g = 0$, so ist $L(u) = 1$, also sei jetzt $g \geq 1$. Es gilt dann $a_0 = L(0) = B_0 = 1$, da der Nulldivisor der einzige effektive Divisor vom Grad Null ist. Fuer die Berechnung von a_1 sei $N = A_1$ die Anzahl der Primdivisoren vom Grad 1, dann ist

$$L(u) = (1-u)(1-qu)\sum_{n=0}^{\infty} B_n u^n \equiv 1 + (N - (q+1))t \mod t^2.$$

Daher ist $a_1 = N - (q+1)$.

Sei nun $x \in K$ transzendent ueber $\mathbb{F}$. Schreibe $K_0 = \mathbb{F}(x)$. Die Zetafunktion von $K_0/\mathbb{F}$ ist $Z_0(u) = \frac{1}{(1-u)(1-qu)}$. Nach der Funktionalgleichung der Zetafunktion gilt

$$L(u) = \frac{Z(u)}{Z_0(u)} = \frac{q^{g-1}u^{2g-2}Z(1/qu)}{q^{-1}u^{-2}Z_0(1/qu)} = q^g u^{2g} L\left(\frac{1}{qu}\right).$$

Anders geschrieben ist das

$$\sum_{j=0}^{2g} a_j u^j = \sum_{j=0}^{2g} a_{2g-j} q^{j-g} u^j,$$

oder $a_j = q^{j-g} a_{2g-j}$. Insbesondere fuer $j = 0, 1$ folgt

$$a_{2g} = q^g \quad \text{und} \quad a_{2g-1} = q^{g-1}(N - (q+1)).$$

Damit ist der Grad des Polynoms $L(u)$ gleich $2g$. Aus der Darstellung $L(u) = \frac{Z(u)}{Z_0(u)}$ folgt auch (c) und dies wiederum impliziert (d). □

Satz 7.1.2 (Riemann-Hypothese)**.** (a) *Die Nullstellen der Funktion $\zeta_K(s)$ liegen alle auf der Geraden* $\mathrm{Re}(s) = \frac{1}{2}$.

(b) *Die Nullstellen der Funktion $Z_K(u)$ liegen alle auf dem Kreis $|u| = q^{-\frac{1}{2}}$.*

(c) *Es gilt $|\omega_j| = \sqrt{q}$ fuer $j = 1, \ldots, 2g$.*

Die Drei Aussagen des Satzes sind aequivalent. Der Beweis des Satzes wird in den naechsten Abschnitten gefuehrt.

Satz 7.1.3. *Es gilt $|N - (q+1)| \leq 2g\sqrt{q}$.*

Proof. Dieser Satz folgt leicht aus der Riemann-Hypothese, denn

$$|N - (q+1)| = \left|\sum_{j=1}^{2g} \omega_j\right| \leq \sum_{j=1}^{2g} |\omega_j| = \sum_{j=1}^{2g} \sqrt{q} = 2g\sqrt{q}.$$ □

7.2 Reduktionsschritte

Satz 7.1.3 ist eine Konsequenz der Riemann-Hypothese. Wir zeigen nun, dass eine geeignete Version dieses Satzes umgekehrt die Riemann-Hypothese impliziert.

Sei wieder $r \in \mathbb{N}$ und $\mathbb{E} = \mathbb{F}_{q^r}$ die eindeutig bestimmt Erweiterung von $\mathbb{F} = \mathbb{F}_q$ vom Rang r. Das Kompositum $K_r = K\mathbb{E}$ ist ein Funktionenkoerper ueber $\mathbb{E}$ und $K_r/\mathbb{E}$ ist eine Konstantenerweiterung von $K/\mathbb{F}$.

Lemma 7.2.1. *Die Riemann-Hypothese gilt genau dann fuer $K/\mathbb{F}$, wenn sie fuer die Konstantenerweiterung $K_r/\mathbb{E}$ gilt.*

Proof. Dies folgt sofort aus Proposition 6.3.2, die besagt, dass fuer jede komplexe Zahl u gilt

$$Z_r(u^r) = \prod_{\xi^r=1} Z(\xi u)$$

ist, wobei beachtet werden muss, dass q in der Konstantenerweiterung durch q^r ersetzt wird. □

Wir schreiben N_r fuer die Anzahl der Primdivisoren von $K_r/\mathbb{E}$ vom Grad 1.

Lemma 7.2.2. *Sei K ein Funktionenkoerper mit $\mathbb{F} = \mathbb{F}_q$ als Konstantenkoerper. Existiert eine Konstante c so dass fuer jedes $r \in \mathbb{N}$ die Abschaetzung $|N_r - (q^r + 1)| \leq cq^{r/2}$ gilt, dann folgt die Riemann-Hypothese fuer $K/\mathbb{F}$.*

Beweis. Aus $L(u) = \prod_{j=1}^{2g}(1 - \omega_j u)$ folgt

$$\log L(u) = \sum_{j=1}^{2g} \log(1 - \omega_j u) = -\sum_{j=1}^{2g} \sum_{r=1}^{\infty} \frac{(\omega_j u)^r}{r}.$$

Ableiten beider Seiten gefolgt von einer Multiplikation mit $-u$ liefert

$$-u\frac{L'(u)}{L(u)} = \sum_{j=1}^{2g} \frac{\omega_j u}{1 - \omega_j u} = \sum_{j=1}^{2g} \sum_{r=1}^{\infty} (\omega_j u)^r = \sum_{r=1}^{\infty} \left(\sum_{j=1}^{2g} \omega_j^r \right) u^r.$$

Aus Lemma 7.1.1 folgt $-\sum_{j=1}^{2g} \omega_j^r = N_r - (q^r + 1)$. Aus unserer Annahme folgt $\left| \sum_{j=1}^{2g} \omega_j^r \right| \leq cq^{r/2}$. Daher ist der Konvergenzradius R der obigen Reihe $\geq q^{-1/2}$. Die Singulartitaeten von $-u\frac{L'(u)}{L(u)}$ sind aber die ω_j^{-1}, also ist $|\omega_j^{-1}| \geq R \geq q^{-1/2}$ oder $|\omega_j| \leq \sqrt{q}$. Wegen $q^g = \prod_{j=1}^{2g} \omega_j$ folgt daraus $|\omega_j| = \sqrt{q}$. □

7.3 Eine obere Schranke

Wir nehmen nun an, dass $K/\mathbb{F}$ die folgenden Bedingungen erfuellt:

- $q = a^2$ ist ein Quadrat,
- $q > (g+1)^4$,
- K besitzt einen Primdivisor P_0 vom Grad 1.

Diese Bedingungen lassen sich durch Konstantenerweiterung herstellen und nach Lemma 7.2.1 reicht es, die Riemann-Hypothese unter diesen Umstaenden zu zeigen.

Ein gegebenes Element $\sigma \in \mathrm{Gal}(K/\mathbb{F})$ permutiert die Primstellen von K. Ist P eine Primstelle, dann ist $P^\sigma = \sigma^{-1}(P)$ die Primstelle der Bewertung $v_{P^\sigma}(y) = v_P^\sigma(y) = v_P(\sigma(y))$. Hierzu erinnere, dass $P = \{x \in K : v_P(x) > 1\}$, so dass

$$\begin{aligned}\sigma^{-1}(P) &= \{\sigma^{-1}(x) : v_P(x) > 1\} \\ &= \{y : v_P(\sigma(y)) > 1\}.\end{aligned}$$

Fuer eine Stelle P von K sei $\phi_P : K \to \mathcal{O}_P/P \cup \{\infty\}$ definiert durch

$$\phi_P(x) = \begin{cases} [x] & x \in \mathcal{O}_P, \\ \infty & x \notin \mathcal{O}_P. \end{cases}$$

Wir setzen $\phi_P^\sigma(x) = \phi_P(\sigma(x))$, dann ist $\phi_P^\sigma : K \to \mathcal{O}_{P^\sigma}/P^\sigma$. Der Frobenius-Homomorphismus $\mathrm{Frob}_q : K \to K$, gegeben durch

$$\mathrm{Frob}_q(x) = x^q$$

ist ein Koerper-Homomorphismus $K \hookrightarrow K$. Wir definieren ϕ_P^q durch

$$\phi_P^q(x) = \phi_P(x^q) = \phi_P(x)^q.$$

Beachte, dass

$$\phi_P^q = \phi_P \quad \Leftrightarrow \quad \deg(P) = 1.$$

Sei

$$N^{(\sigma)} = \sum_{P : \phi_P^\sigma = \phi_P^q} \deg(P).$$

Proposition 7.3.1. *Es gilt*

$$N^{(\sigma)} - (q+1) < (2g+1)\sqrt{q}.$$

Der *Beweis* nimmt den Rest dieses Abschnitts ein. Seien

- $m = a - 1 = \sqrt{q} - 1$,
- $n = a + 2g$,
- $r = m + an = (2g + 1)\sqrt{q} + q$.

Sei P_0 ein Primdivisor vom Grad 1. Wir betrachten die aufsteigende Folge von $\mathbb{F}$-Vektorraeumen,

$$L(P_0) \subset L(2P_0) \subset \dots.$$

Wir behaupten, dass

$$\dim_{\mathbb{F}} (L(jP_0)/L((j-1)P_0)) \leq 1$$

gilt. Nehmen wir dazu an, dass diese Dimension ungleich Null ist. Dann gibt es ein $f \in L(jP_0) \setminus L((j-1)P_0)$. Das bedeutet, $f \in K$ und $v_{P_0}(f) = -j$. Die Abbildung $M : L(jP_0)/L((j-1)P_0) \to \mathcal{O}_{P_0}/P_0 \cong \mathbb{F}$ gegeben durch $g \mapsto [g/f]$ ist injektiv. Damit folgt die Behauptung.

Fuer gegebenes $k \in \mathbb{N}$ sei I_k die Menge der Zahlen $1 \leq j \leq k$, so dass $\dim_{\mathbb{F}} (L(jP_0)/L((j-1)P_0)) = 1$ gilt. Fuer jedes $j \in I_k$ waehle ein $u_j \in L(jP_0) \setminus L((j-1)P_0)$. Dann ist $(u_j)_\infty = jP_0$ und die Familie $(u_j)_{j \in I_k}$ ist eine $\mathbb{F}$-Basis fuer $L(jP_0)$. Dies gilt insbesondere fuer $k = m = \sqrt{q} - 1$. Da $a = \sqrt{q}$ eine Potenz der Charakteristik ist, ist die Menge

$$L(nP_0)^a = \{y^a : y \in L(nP_0)\}$$

ein $\mathbb{F}_a$-Vektorraum mit Basis $(u_j^a)_{j \in I_n}$. Daher ist

$$L = \left\{ \sum_{j \in I_m} u_j y_j^a : y_j \in L(nP_0) \right\}$$

ein $\mathbb{F}$-Vektorraum erzeugt von $U = \{u_i u_j^a : i \in I_m,\ j \in I_n\}$, denn L ist das Bild von $L(mP_0) \otimes_{\mathbb{F}_a} L(nP_0)^a$.

Lemma 7.3.2. *Die natuerliche Abbildung ist ein Isomorphismus* $L(mP_0) \otimes_{\mathbb{F}_a} L(nP_0)^a \xrightarrow{\cong} L$. *Insbesondere ist* $\dim_{\mathbb{F}} L = (\#I_m)(\#I_n) = \#U$ *und* U *ist linear unabhaengig ueber* $\mathbb{F}$.

Beweis. Es ist zu zeigen, dass die Abbildung vom Tensorprodukt injektiv ist. Hierzu beachte, dass fuer einen $\mathbb{F}$-Vektorraum V und einen $\mathbb{F}_a$-Vektorraum W, jedes Element des Tensorproduktes $V \otimes_{\mathbb{F}_a} W$ in eindeutiger Weise als $\sum_j v_i \otimes w_j$ geschrieben werden kann, wenn (w_j) eine $\mathbb{F}_a$-Basis von V ist.

Also angenommen, es gibt $y_j \in K$, fuer $j \in I_m$, nicht alle Null, so dass $\sum_{j\in I_m} u_j y_j^a = 0$. Dann existieren $i \neq j$ in I_m so dass $v_{P_0}(u_i y_i^a) = v_{P_0}(u_j y_j^a)$, $y_i y_j \neq 0$. Also ist $-i + a v_{P_0}(y_i) = -j + a v_{P_0}(y_j)$ und daher $i \equiv j \mod (a)$. Da aber $1 \leq i, j \leq m < a$, ist dies ein Widerspruch. □

Nach dem Riemann-Roch-Satz gilt dann

$$\begin{aligned}\dim(L) &= \dim(L(mP_0))\dim(L(nP_0)) \\ &\geq (m-g+1)(n-g+1) \\ &= (\sqrt{q}-g)(\sqrt{q}+g+1) = q + \sqrt{q} - g(g+1).\end{aligned}$$

Betrachte den $\mathbb{F}$-Vektorraum

$$L' = \left\{ \sum_{j\in I_m} (\sigma^{-1}u_j)^a y_j : y_j \in L(nP_0) \right\}.$$

Dann gilt $L' \subset L(amP_0^\sigma + nP_0)$ und $\deg(amP_0^\sigma + nP_o) = am + n = q + 2g > 2g - 2$, so dass, wieder mit Riemann-Roch,

$$\begin{aligned}\dim_{\mathbb{F}}(L') &\leq l(amP_0^\sigma + nP_0) \\ &= \deg(amP_0 + nP_0) + l(C - amP_0 - nP_0) - g + 1 \\ &= q + 2g + \underbrace{l(C - amP_0 - nP_0)}_{=0, \text{ da } \deg(\cdot)<0} - g + 1 \\ &= q + g + 1 \\ &< q + \sqrt{q} - g(g+1) \\ &\leq \dim_{\mathbb{F}}(L),\end{aligned}$$

wobei wir unsere Annahme $q > (g+1)^4$ benutzt haben, denn diese bewirkt $\sqrt{q} - g(g+1) = \sqrt{q} - (g+1)^2 + g + 1 > g + 1$.

Wir definieren nun eine $\mathbb{F}_a$-lineare Abbildung $\sigma^* : L \to L'$ durch

$$\sigma^*\left(\sum_{j\in I_m} u_j y_j^a\right) = \sum_{j\in I_m} (\sigma^{-1}u_j)^a y_j.$$

Beachte, dass diese Wohldefiniert ist, da $\mathbb{F}$ keine a-ten Einheitswurzeln enthaelt, denn fuer jedes $x \in \mathbb{F}$ gilt $x^{a^2} = x^q = x$. Nun muss er Kern von σ^* nichttrivial sein, es gibt also

$y_j \in L(nP_0)$, nicht alle Null, mit

$$\sum_{j \in I_m} (\sigma^{-1} u_j) y_j = 0.$$

Insbesondere ist $u = \sum_{j \in I_m} u_j y + j^a$ ein nichtverschwindendes Element von $L \subset L(rP_0)$. Ist $P \neq P_0$ ein Primdivisor, dann gilt $v_P(y_j) \geq 0$ und $v_P(u_j) \geq 0$, was soviel bedeutet wie $\phi_P(y_j) \neq \infty$ und $\phi_P(u_j) \neq \infty$. Gilt zusaetzlich $\phi_P^\sigma = \phi_P^q$, dann folgt

$$\begin{aligned} \phi_P(u) &= \sum_{j \in I_m} \phi_P(u_j) \phi_P(y_j)^a \\ &= \sum_{j \in I_m} \phi_P(\sigma^{-1} u_j)^q \phi_P(y_j)^a \\ &= \phi_P \left(\sum_{j \in I_m} (\sigma^{-1} u_j)^a y_j \right)^a = 0. \end{aligned}$$

Also liegt P im Nullstellendivisor von u, oder

$$\sum_{\substack{P \neq P_0 \\ \phi_P^\sigma = \phi_P^q}} P \leq (u)_0.$$

Damit also $N^{(\sigma)} - 1 \leq \deg((u_\infty)) \leq r$, was den Beweis von Proposition 7.3.1 abschliesst.

7.4 Eine untere Schranke

Wir werden nun zeigen, dass es ein $c' > 0$ gibt, das zwar von K abhaengt, sich aber bei Konstantenerweiterungen nicht aendert, so dass $N^{(\sigma)} - (q+1) > c' \sqrt{q}$ gilt.

Lemma 7.4.1. *Sei K ein Funktionenkoerper in einer Variablen mit Konstantenkoerper $\mathbb{F} = \mathbb{F}_q$. Sei K' eine endliche Galoiserweiterung von K mit Galoisgruppe G. Nimm an, dass $\mathbb{F}$ auch in K' algebraisch abgeschlossen ist und sei $\sigma \in \mathrm{Gal}(K'/\mathbb{F})$. Dann gilt*

$$N^{(\sigma)}(K) = \frac{1}{[K' : K]} \sum_{\tau \in G} N^{(\sigma\tau)}(K').$$

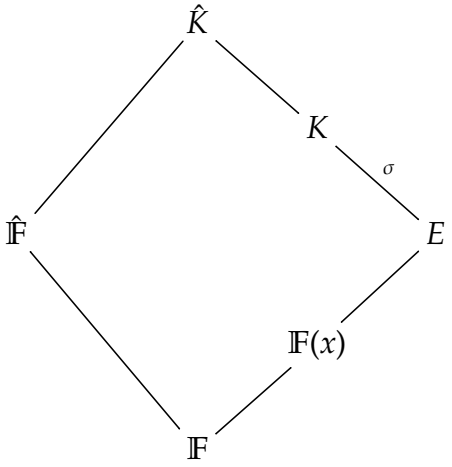
Beweis. Sei P' ein Primdivisor von K' und sei P seine Einschraenkung auf K. Dann ist $\phi_P^\sigma = \phi_P^q$ genau dann, wenn es ein $\tau \in G$ gibt, so dass $\phi_{P'}^{\sigma\tau} = \phi_{P'}^q$. Die Anzahl solcher τ ist der Verzweigungsindex $e_{P'/P}$ von P' ueber P. Sei $f_{P'/P}$ der Grad der

Restklassenerweiterung $\mathcal{O}_{P'}/P'$ ueber $\mathcal{O}_P/P$. Dann gilt

$$\begin{aligned}\sum_{\tau\in G} N^{(\sigma\tau)}(K') &= \sum_{\tau\in G}\sum_{\phi_{P'}^{\sigma\tau}=\phi_{P'}^{q}} \deg(P') \\ &= \sum_{\phi_P^{\sigma}=\phi_P^{q}}\sum_{P'|P} e_{P'/P}\deg(P') \\ &= \sum_{\phi_P^{\sigma}=\phi_P^{q}}\left(\sum_{P'|P} e_{P'/P}f_{P'/P}\right)\deg(P) \\ &= \sum_{\phi_P^{\sigma}=\phi_P^{q}} [K':K]\deg(P) \\ &= [K':K]N^{(\sigma)}(K)\end{aligned}$$

□

Sei K ein Funktionenkoerper in einer Variablen ueber $\mathbb{F} = \mathbb{F}_q$ und sei $\sigma \in \mathrm{Gal}(K/\mathbb{F})$ ein Element endlicher Ordnung. Sei E der Fixkoerper von σ. Dann ist K eine endliche Galoiserweiterung von E. Da der endliche Koerper $\mathbb{F}$ perfekt ist, gibt es ein $x \in E$ so dass E eine endliche separable Erweiterung von $\mathbb{F}(x)$ ist. Sei $\hat{K}$ die normale Huelle von $K/\mathbb{F}(x)$, dann ist $\hat{K}/\mathbb{F}(x)$ eine endliche Galois-Erweiterung. Sei $\hat{\mathbb{F}}$ der algebraische Abschluss von $\mathbb{F}$ in $\hat{K}$.



Dann dehnt σ zu einem Galoishomomorphismus von $\hat{K}$ ueber $\mathbb{F}(x)$ aus. Nach einer weiteren Konstantenerweiterung, wenn noetig, koennen wir annehmen, dass $\hat{K}/\hat{\mathbb{F}}$ die Bedingungen am Anfang von Abschnitt 7.3 erfuellt.

Lemma 7.4.2. *Es gilt*

$$N^{(\sigma)}(K) - (q+1) \geq -\frac{n-m}{m}(2\hat{g}+1)\sqrt{q},$$

wobei $m = [\hat{K}:K]$ *und* $n = [\hat{K}:\mathbb{F}(x)]$.

Proof. Sei $H = \mathrm{Gal}(\hat{K}/K)$ und $G = \mathrm{Gal}(\hat{K}/\mathbb{F}(x))$. Mit Lemma 7.4.1 folgt

$$N^{(\sigma)}(K) = \frac{1}{m}\sum_{\tau\in H} N^{(\sigma\tau)}(\hat{K}) \quad \text{und} \quad q+1 = N(\mathbb{F}(x)) = \frac{1}{n}\sum_{\theta\in G} N^{(\theta)}(\hat{K}).$$

Nach Proposition 7.3.1 gilt

$$\begin{aligned}\sum_{\theta\in G} N^{(\theta)}(\hat{K}) &= \sum_{\tau\in H} N^{(\sigma\tau)}(\hat{K}) + \sum_{\theta\in G\setminus\sigma H} N^{(\theta)}(\hat{K}) \\ &\leq \sum_{\tau\in H} N^{(\sigma\tau)}(\hat{K}) + \sum_{\theta\in G\setminus\sigma H} (q+1+(2\hat{g}+1)\sqrt{q}) \\ &= \sum_{\tau\in H} N^{(\sigma\tau)}(\hat{K}) + (n-m)(q+1+(2\hat{g}+1)\sqrt{q}).\end{aligned}$$

Nach der obigen Aussage gilt ausserdem

$$\begin{aligned}\sum_{\tau\in H} N^{(\sigma\tau)}(\hat{K}) &\geq n(q+1) - (n-m)(q+1+(2\hat{g}+1)\sqrt{q}) \\ &= m(q+1) - (n-m)(2\hat{g}+1)\sqrt{q},\end{aligned}$$

also

$$N^{(\sigma)}(K) \geq (q+1) - \frac{n-m}{m}(2\hat{g}+1)\sqrt{q}.$$ □

Aus diesem Lemma und den Ergebnissen von Abschnitt 7.3 folgt

Proposition 7.4.3. *Sei K ein Funktionenkoerper in einer Variablen ueber einem endlichen Koerper $\mathbb{F}$ und sei σ ein Automorphismus von K ueber $\mathbb{F}$ von endlicher Ordnung. Dann gibt es eine endliche Erweiterung $\mathbb{F}'$ von $\mathbb{F}$ mit q' Elementen und eine positive Konstante c so dass fuer jedes $r \in \mathbb{N}$ gilt*

$$|N^{(\sigma)}(K'_r) - ((q')^r - 1)| \leq c(q')^{r/2}.$$

wober $\mathbb{F}_r$ die Erweiterung von $\mathbb{F}'$ vom Grad r ist und $K'_r = \mathbb{F}'_r K'$. Ferner schreiben wir ebenfalls σ fuer die Ausdehnung von σ nach $K'_r/\mathbb{F}'_r$.

Die Riemann-Hypothese ist bewiesen.

Index

CL_K, 46
CL_K^0, 46
N_r, 67
$\mathcal{D}_K^0$, 45
d-te Potenz modulo f, 9

Adele-Ring , 49
assoziiert, 2

Bewertungsideal, 35
Bewertungsring, 35

Dedekind-Ring, 7
Dichte, 26
Dirchlet-Faltung, 17
Dirichlet-Charakter, 28
Dirichlet-Dichte, 26
Dirichlet-Reihe, 15
diskrete Bewertung, 6
diskreter Bewertungsring, 6
Divisor des Differentials ω, 55
Divisoren, 39, 45
Divisorengruppe, 39
Divisorenklassengruppe, 46
duale Gruppe, 28

effektiver Divisor, 46
endliche Erweiterung, 38
euklidisch, 3

faktoriell, 2
Frobenius-Homomorphismus, 1
Funktionenkoerper, 35

ganz, 6
ganz abgeschlossen, 6
ganz abgeschlossen in K, 6
ganzen Abschluss, 6
Geschlecht, 47
globaler Funktionenkoerper, 57
Grad, 1, 37, 39, 45
Gradbewertung, 36

Hauptdivisor, 45

Integritaetsring, 1
irreduzibel, 2

kanonische Klasse, 47
Klassenzahl, 57
Konstantenerweiterung, 39
Konstantenkoerper, 35
Kreisgruppe, 28
Kronecker-Delta, 29

L-Reihe, 30
Legendre-Symbol, 19
linear aequivalent, 46

moderates Wachstum, 15
Moebius-Funktion, 12
multiplikativ, 16

Norm, 58
normiert, 1
Nullstelle, 45
Nullstellendivisor, 45

perfekt, 43
Polstelle, 45
Polstellendivisor, 46
Primelement, 2
Primfaktorzerlegung, 4
Primstelle, 37
Primzahlsatz, 25
Primzahlsatz von Dirichlet, 25

quadratfreie Zahl, 12
quadratische Reziprozitaetsgesetz, 19

Restklassengrad, 42
Restsymbol, 20
Ring, 1

schwach multiplikativ, 12
Signum, 1
stark multiplikativ, 16
Stelle, 37

Teilerbetragsumme, 15
teilerfremd, 4
teilt, 42
total inseparabel, 43
Transzendenzgrad 1, 35

ueber, 41
uniformisierendes Element, 35
unverzeigt, 39

Verzweigungsindex, 39, 42

Weil-Differential, 50

Zetafunktion, 11, 58