Der Defekt von Torsionskörpern getwisteter Carlitz-Moduln

Masterarbeit

vorgelegt
der Naturwissenschaftlich-Technischen Fakultät I
der Universität des Saarlandes

von
Julius Klauck

Betreuer
Prof. Dr. Ernst-Ulrich Gekeler

September 2015

Hiermit versichere ich, die Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen geschrieben zu haben.

Vorwort

Die vorliegende Arbeit mit dem Titel "Der Defekt von Torsionskörpern getwisteter Carlitz-Moduln" ist in der Zeit vom 1.April 2015 bis zum 16.September 2015, unter der Betreuung von Herrn Prof. Dr. Ernst-Ulrich Gekeler an der Universität des Saarlandes entstanden.

Der Ring der ganzen Zahlen $\mathbb{Z}$ hat viele Analogien zu dem Polynomring $\mathbb{F}_q[T]$ über einem endlichen Körper $\mathbb{F}_q$, wobei q eine Primzahlpotenz ist (z.B. sind beide Ringe Hauptidealringe, die Einheitengruppen beider Ringe sind endlich und die Restklassenringe für von 0 verschiedene Ideale sind in beiden Fällen endlich). Eine tieferliegende Analogie wurde von David Hayes bewiesen [$Hay74$]:

Betrachten wir den Quotientenkörper $\mathbb{Q}$ von $\mathbb{Z}$ und die endliche Galois-Erweiterung $\mathbb{Q}(\xi_n)$ über $\mathbb{Q}$, wobei ξ_n eine primitive n-te Einheitswurzel ist, dann wissen wir :

$$Gal\left(\mathbb{Q}(\xi_n) \mid \mathbb{Q}\right) \xrightarrow{\cong} (\mathbb{Z}/(n))^*.$$

Hayes hat nun gezeigt, dass es zu der Gruppe $(\mathbb{F}_q[T]/(N))^*$, für ein $N \in \mathbb{F}_q[T]$, eine Körpererweiterung $\mathbb{F}_q(T)({}_NC)$ von $\mathbb{F}_q(T)$ gibt, so dass gilt:

$$Gal\left(\mathbb{F}_q(T)({}_NC) \mid \mathbb{F}_q(T)\right) \xrightarrow{\cong} (\mathbb{F}_q[T]/(N))^*.$$

Hierbei bezeichnet ${}_NC$ die Menge der Nullstellen eines durch N eindeutig bestimmten Polynoms mit Koeffizienten in $\mathbb{F}_q(T)$, dem sogenannten Carlitz-Polynom zu N. Deformieren wir dieses Polynom um einen Störterm $\Delta \in \mathbb{F}_q(T)^*$, so haben wir obige Isomorphie im Allgemeinen nicht mehr. Allerdings können wir die Galoisgruppe $Gal\left(\mathbb{F}_q(T)({}_N\Phi^{(\Delta)}) \mid \mathbb{F}_q(T)\right)$ immer in $(\mathbb{F}_q[T]/(N))^*$ einbetten (siehe Lemma 1.9), wobei ${}_N\Phi^{(\Delta)}$ die Menge der Nullstellen des um Δ deformierten Carlitz-Polynoms bezeichnet.
Das Ziel der Arbeit ist es nun zu untersuchen, wie stark die Einbettung

$$Gal\left(\mathbb{F}_q(T)({}_N\Phi^{(\Delta)}) \mid \mathbb{F}_q(T)\right) \hookrightarrow (\mathbb{F}_q[T]/(N))^*,$$

in Abhänigkeit von $N \in \mathbb{F}_q[T] \setminus \{0\}$ und $\Delta \in \mathbb{F}_q(T)^*$, davon abweicht bijektiv zu sein. Diese Abweichung beschreiben wir durch die natürliche Zahl

$$\frac{\#\left(\mathbb{F}_q[T]/(N)\right)^*}{[\mathbb{F}_q(T)({}_N\Phi^{(\Delta)}) : \mathbb{F}_q(T)]} =: \text{Defekt von } \mathbb{F}_q(T)({}_N\Phi^{(\Delta)}) \ .$$

Im ersten Kapitel werden die für die Arbeit grundlegenden Begriffe und Aussagen bereitgestellt. Außerdem reduzieren wir die Problemstellung der Arbeit auf die Fälle: $\Delta \in \mathbb{F}_q[T] \setminus \{0\}$, Δ frei von $(q-1)-$ten Potenzen und $N \in \mathbb{F}_q[T]$ normiert und nicht-konstant.
Wenn wir nun ein $N \in \mathbb{F}_q[T]$ und $\Delta \in \mathbb{F}_q[T] \setminus \{0\}$ gegeben haben, können wir grundsätzlich zwei Fälle unterscheiden:
1.Fall : N und Δ sind teilerfremd.

2.Fall : N und Δ sind nicht teilerfremd.
Der 1.Fall wird in Kapitel 2 abgehandelt: Hier zeigen wir, dass der Defekt von $\mathbb{F}_q(T)({}_N\Phi^{(\Delta)})$ Eins ist, d.h.

$$Gal\left(\mathbb{F}_q(T)({}_N\Phi^{(\Delta)}) \mid \mathbb{F}_q(T)\right) \xrightarrow{\cong} (\mathbb{F}_q[T]/(N))^*.$$

Dagegen treten im 2.Fall auch Situationen auf, wo der Defekt echt größer als Eins ist (siehe Beispiel 1.15). Um in dieser Situation den Defekt berechnen zu können, untersuchen wir in Kapitel 3 zunächst Zwischenerweiterungen von $\mathbb{F}_q(T)({}_NC) \mid \mathbb{F}_q(T)$. Genauer: Wir betrachten Erweiterungen der Form $\mathbb{F}_q(T)\left(\sqrt[q-1]{f}\right) \subset \mathbb{F}_q(T)({}_NC)$ für ein $f \in \mathbb{F}_q(T)$ und untersuchen wie ein $\sigma \in Gal\left(\mathbb{F}_q(T)({}_NC) \mid \mathbb{F}_q(T)\right)$ auf $\sqrt[q-1]{f}$ operiert.
Mit diesem Wissen leiten wir in Kapitel 4 das Hauptresultat der Arbeit her: Für nicht teilerfremde N und Δ können wir den Defekt von $\mathbb{F}_q(T)({}_N\Phi^{(\Delta)})$ in expliziter Weise als ggT bestimmter, durch N und Δ festgelegter, natürlicher Zahlen berechnen (siehe Satz 4.13).

Danksagung
Zunächst möchte ich mich an dieser Stelle bei allen bedanken, die mich bei der Anfertigung dieser Masterarbeit unterstützt haben. Mein besonderer Dank gilt dabei Prof. Dr. Ernst-Ulrich Gekeler für die intensive Betreuung, während der Anfertigung dieser Arbeit.

Notation
In der gesamten Arbeit gilt folgende Notation:

- $\mathbb{N} = \{1, 2, 3, \ldots\}$,
- $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$
- $\mathbb{P}$ =Menge der Primzahlen
- $\mathbb{F}_q$ =Körper mit q Elementen, wobei $q = p^n$ mit $p \in \mathbb{P}$ und $n \in \mathbb{N}$
- $A = \mathbb{F}_q[T]$
- $K = \mathbb{F}_q(T)$

Inhaltsverzeichnis

1 Grundlagen und Formulierung der Problemstellung

Zu Beginn von Kapitel 1 führen wir den Begriff des Drinfeld-Moduls vom Rang $r \in \mathbb{N}$ über $K = \mathbb{F}_q(T)$ ein. Hierbei ist zu beachten, dass die in der vorliegenden Arbeit verwendete Definition nur ein Spezialfall eines viel allgemeineren Sachverhaltes ist, siehe z.B. [Ros02], [Tha04] oder[Gos96] für eine umfassendere Einführung in die Theorie der Drinfeld-Moduln.

1.1 Definition.

Die Abbildung $x \mapsto x^q$ bezeichnen wir mit τ. Dann heißt $K\{\tau\} := \left\{\sum_{i=0}^{n} a_i\tau^i \mid n \in \mathbb{N}_0,\, a_i \in K\right\}$ der getwistete Polynomring.

1.2 Bemerkung.

Mit den Verknüpfungen

$$\text{“}+\text{”} : \sum_{i=0}^{n} a_i\tau^i + \sum_{j=0}^{n} b_j\tau^j = \sum_{i=0}^{n}(a_i + b_i)\tau^i$$

$$\text{“}\circ\text{”} : \sum_{i=0}^{n} a_i\tau^i \circ \sum_{j=0}^{m} b_j\tau^j = \sum_{k=0}^{n+m}(\sum_{i+j=k} a_i \cdot b_j^{q^i})\tau^k$$

ist $(K\{\tau\}, +, \circ)$ ein nicht-kommutativer Ring mit der Relation $\tau a = a^q\tau$ für alle $a \in K$ (vgl. Geb[03]).

1.3 Bemerkung.

Bezeichnen wir mit $M := \left\{\sum_{i=0}^{n} c_i x^{q^i} \mid n \in \mathbb{N}_0,\, c_i \in K\right\}$ die $\mathbb{F}_q$-linearen Polynome in $K[x]$, so können wir den getwisteten Polynomring $K\{\tau\}$ und M mittels folgendem $\mathbb{F}_q$-Ring-Isomorphismus identifizieren:

$$K\{\tau\} \longrightarrow M$$

$$\sum_{i=0}^{n} a_i\tau^i \mapsto \sum_{i=0}^{n} a_i x^{q^i} \quad .$$

1.4 Definition.

(i) Ein A-Drinfeld-Modul vom Rang 1 über K ist ein $\mathbb{F}_q$-Ringhomomorphismus

$$\begin{aligned}\Phi^{(\Delta)} : A &\longrightarrow K\{\tau\} \\ N &\mapsto \Phi_N^{(\Delta)} ,\end{aligned}$$

gegeben durch $\Phi_T^{(\Delta)} = T + \Delta\tau$ mit $\Delta \in K^*$.

(ii) In dem Spezialfall $\Delta = 1$ sprechen wir von dem Carlitz-Modul

$$C := \Phi^{(1)} : A \longrightarrow K\{\tau\}$$
$$N \mapsto \Phi_N^{(1)} = C_N \ ,$$

gegeben durch $C_T = T + \tau$.

1.5 Bemerkung.

(i) Die Rang-1-Drinfeld-Moduln $\Phi^{(\Delta)}$ mit $\Delta \neq 1$ bezeichnen wir auch als getwistete Carlitz-Moduln.

(ii) Analog zu Definition 1.4 kann man Drinfeld-Moduln Φ vom Rang $r \geq 2$ definieren durch $\Phi_T(x) = Tx + c_1 x^q + c_2 x^{q^2} + \cdots + c_r x^{q^r}$ mit $c_i \in K$ $(1 \leq i \leq r-1)$ und $c_r \in K^*$.

(iii) Falls man einen Drinfeld-Modul Φ über K vom Rang $r \geq 1$ gegeben hat, kann man auf $\overline{K}$ eine nicht-triviale A-Modulstruktur definieren durch:

$$a *_\Phi x := \Phi_a(x) \ , \text{ wobei } a \in A,\ x \in \overline{K} \ .$$

Für den zugehörigen A-Modul schreiben wir $(\overline{K},\Phi)$.

1.6 Definition.

(i) Sei Φ ein Drinfeld-Modul vom Rang $r \geq 1$ und $N \in A \setminus \{0\}$. Dann heißt ${}_N\Phi := \left\{x \in \overline{K} \mid \Phi_N(x) = 0\right\}$ die N-Torsion von Φ. Ein Element $x \in_N \Phi$ heißt Torsionspunkt.

(ii) Die Körpererweiterung $K({}_N\Phi)$ über K heißt Torsionskörper von Φ zum Führer N. Für die Torsionskörper $K({}_N\Phi^{(\Delta)})$ und $K({}_N C)$ schreiben wir in der gesamten Arbeit der Einfachheit halber $K^{(\Delta)}(N)$ bzw. $K(N)$.

1.7 Satz.

Sei Φ ein Drinfeld-Modul vom Rang $r \geq 1$ und $N \in A \setminus \{0\}$, dann gilt:
${}_N\Phi$ ist ein freier A/N-Modul vom Rang r.

Beweis: Proposition 12.4 in [Ros02].

1.8 Lemma.

Sei $N \in A \setminus \{0\}$. Die Körpererweiterung $K^{(\Delta)}(N) \mid K$ ist galoissch.

Beweis:

Die Normalität von $K^{(\Delta)}(N) \mid K$ ist klar, da ${}_N\Phi^{(\Delta)}$ die Menge der Nullstellen von $\Phi_N^{(\Delta)} \in K[x]$ ist.

Zur Separabilität von $K^{(\Delta)}(N) \mid K$: Es ist $(\Phi_N^{(\Delta)})' = N$. Daraus folgt, dass $(\Phi_N^{(\Delta)})'$ und $\Phi_N^{(\Delta)}$ keinen nicht-trivialen gemeinsamen Teiler haben, d.h. $\Phi_N^{(\Delta)}$ ist separabel.

□

1.9 Lemma.

Sei $N \in A \setminus \{0\}$. Die Galoisgruppe $Gal(K^{(\Delta)}(N) \mid K)$ ist isomorph zu einer Untergruppe von $(A/N)^*$.

Beweis:

Nach Satz 1.7 existiert ein Erzeuger λ von ${}_N\Phi^{(\Delta)}$, es gilt:

(i) Für $\sigma \in Gal(K^{(\Delta)}(N) \mid K)$ ist $\sigma(\lambda)$ ebenfalls ein Erzeuger von ${}_N\Phi^{(\Delta)}$.

(ii) Es existiert ein eindeutiges $R \in (A/N)^*$ mit $\Phi_R^{(\Delta)}(\lambda) = \sigma(\lambda)$.

Aus $(i) + (ii)$ folgt: $\sigma(\lambda_0) = \Phi_R^{(\Delta)}(\lambda_0)$ für alle Erzeuger λ_0 von ${}_N\Phi^{(\Delta)}$. Man findet also zu jedem $\sigma \in Gal(K^{(\Delta)}(N) \mid K)$ ein eindeutig bestimmtes Element $N_\sigma \in (A/N)^*$, so dass $\sigma(\lambda_0) = \Phi_{N_\sigma}^{(\Delta)}(\lambda_0)$ für alle Erzeuger λ_0 von ${}_N\Phi^{(\Delta)}$.

Definiere die Abbildung $\quad Gal(K^{(\Delta)}(N) \mid K) \longrightarrow (A/N)*$

$$\sigma \longmapsto N_\sigma \qquad .$$

Dies ist ein wohldefinierter, injektiver Homomorphismus.

□

1.10 Lemma.

Die Galois-Erweiterung $K^{(\Delta)}(N) \mid K$ ist abelsch.

Beweis: Folgt aus Lemma 1.9, da $(A/N)^*$ abelsch ist.

□

1.11 Satz.

Sei $N \in A \setminus \{0\}$. Es gilt:

Die Galoisgruppe $Gal(K(N) \mid K)$ ist isomorph zu $(A/N)^*$ und alle Primstellen P, welche $P \nmid N$ erfüllen, sind unverzweigt.

Beweis: [Hay74].

1.12 Bemerkung.

Im Folgenden schreiben wir ein Element von $Gal(K(N) \mid K)$ immer in der Form σ_a mit $a \in (A/N)^*$, wobei der Index a andeuten soll, dass σ_a auf einem Erzeuger λ von ${}_NC$ operiert durch $\sigma(\lambda) = C_a(\lambda)$.

1.13 Satz.

(i) Sei $J = \left\{\sigma_\alpha \in Gal(K(N) \mid K) \mid \alpha \in \mathbb{F}_q^*\right\}$ und $K(N)^+$der Fixkörper von J. Dann zerfällt die Stelle ∞ vollständig in $K(N)^+$ und jede Stelle über ∞ in $K(N)^+$ ist voll verzweigt und zahm verzweigt in $K(N)$.

(ii) Die Konstantenerweiterung von $K(N) \mid K$ ist trivial.

Beweis: Theorem 12.14 in [Ros02].

1.14 Bemerkung.

Die Sätze 1.11 und 1.13 gelten im Allgemeinen nicht mehr für Torsionskörper von getwisteten Carlitz-Moduln.

1.15 Beispiel.

(i) Sei $N = T$ und $\Delta = -T$ und somit $\Phi_T^{(\Delta)}(x) = Tx - Tx^q$. Dann gilt ${}_T\Phi^{(\Delta)} = \{0\} \cup \mathbb{F}_q^* = \mathbb{F}_q \subset K$, d.h. die Galoisgruppe $Gal(K^{(\Delta)}(T) \mid K)$ ist trivial, aber $(A/T)^* = \mathbb{F}_q^*$.

(ii) Sei $N = T$ und $\Delta = T$ und somit $\Phi_T^{(\Delta)}(x) = Tx + Tx^q = Tx(1 + x^{q-1})$.
Dann gilt ${}_T\Phi^{(\Delta)} = \left\{\lambda \in \overline{K} \mid \lambda^{q-1} = -1\right\} \cup \{0\}$ und somit
$K^{(\Delta)}(T) = K({}_T\Phi^{(\Delta)}) = K\mathbb{F}_{q^2}$, d.h. hier hat man eine nicht-triviale Konstantenerweiterung.
Außerdem gilt: $\#(A/N)^* = q - 1 > \#Gal(K^{(\Delta)}(T) \mid K) = 2$ für $q > 3$.

Wir sehen somit, dass für Torsionskörper $K^{(\Delta)}(N) = K({}_N\Phi^{(\Delta)})$ im Allgemeinen nicht gilt:

$$\#Gal(K^{(\Delta)}(N) \mid K) = \#(A/N)^* \ .$$

Dies motiviert folgende Definition:

1.16 Definition.

Die natürliche Zahl $\dfrac{\#(A/N)^*}{\#Gal(K^{(\Delta)}(N) \mid K)}$ heißt der Defekt von $K^{(\Delta)}(N) \mid K$.

1.17 Bemerkung.

(i) Der Defekt von $K^{(1)}(N) = K(N)$ ist 1 (Satz 1.11).

(ii) Das Ziel der Arbeit ist es, den Defekt von $K^{(\Delta)}(N)$, in Abhängigkeit von $\Delta \in K^*$ und $N \in A \setminus \{0\}$, zu berechnen.

Die folgenden Überlegungen erlauben es die Problemstellung auf die Fälle, $\Delta \in A \setminus \{0\}$ und Δ frei von $(q-1)$-ten Potenzen, zu reduzieren.

1.18 Satz.

Seien Δ, $\widetilde{\Delta} \in K^*$ und $\gamma := \sqrt[q-1]{\frac{\widetilde{\Delta}}{\Delta}} \in \overline{K}$, dann ist die Abbildung

$$\begin{aligned} \Gamma : \ (\overline{K}, \Phi^{(\widetilde{\Delta})}) &\longrightarrow (\overline{K}, \Phi^{(\Delta)}) \\ x &\longmapsto \gamma x \end{aligned}$$

ein Isomorphismus von A-Moduln.

Beweis:

Die Bijektivität von Γ ist klar.
Um zu sehen, dass es sich bei Γ um einen A-Modulhomomorphismus handelt, betrachten wir folgende Äquivalenzen:

$$\begin{aligned} & a *_{\Phi^{(\Delta)}} \Gamma(x) = \Gamma(a *_{\Phi^{(\widetilde{\Delta})}} x) \text{ für alle } a \in A \\ \Leftrightarrow & \Phi_a^{(\Delta)}(\gamma x) = \gamma \Phi_a^{(\widetilde{\Delta})}(x) \text{ für alle } a \in A \\ \Leftrightarrow & \Phi_T^{(\Delta)}(\gamma x) = \gamma \Phi_T^{(\widetilde{\Delta})}(x) \\ \Leftrightarrow & T\gamma x + \Delta(\gamma x)^q = \gamma T x + \gamma \widetilde{\Delta} x^q \\ \Leftrightarrow & \Delta \gamma^q x^q = \gamma \widetilde{\Delta} x^q \\ \Leftrightarrow & \Delta \gamma^q = \gamma \widetilde{\Delta} \\ \Leftrightarrow & \gamma^{q-1} = \frac{\widetilde{\Delta}}{\Delta} \ . \end{aligned}$$

□

1.19 Korollar.

Γ induziert einen Isomorphismus von A-Moduln:

$$\begin{aligned} {}_N\Phi^{(\widetilde{\Delta})} &\longrightarrow {}_N\Phi^{(\Delta)} \\ x &\longmapsto \gamma x \ . \end{aligned}$$

Beweis:

Sei $x \in {}_N\Phi^{(\widetilde{\Delta})}$, d.h. $\Phi_N^{(\widetilde{\Delta})}(x) = 0$, dann erhält man $\Phi_N^{(\Delta)}(\gamma x) = \gamma \cdot \Phi_N^{(\widetilde{\Delta})}(x) = 0$.

□

1.20 Korollar.

Falls $\widetilde{\Delta} = u^{q-1}\Delta$ mit $u \in K^*$, dann gilt $K^{(\Delta)}(N) = K^{(\widetilde{\Delta})}(N)$ für alle $N \in A \setminus \{0\}$.

Beweis:
Sei λ ein Erzeuger von ${}_N\Phi^{(\widetilde{\Delta})}$, dann ist nach Korollar 1.19

$$\sqrt[q-1]{\frac{\widetilde{\Delta}}{\Delta}} \cdot \lambda = \sqrt[q-1]{u^{q-1}} \cdot \lambda = \underbrace{(\alpha u)}_{\in K^*} \cdot \lambda$$

ein Erzeuger von ${}_N\Phi^{(\Delta)}$, wobei $\alpha \in \mathbb{F}_q^*$.
Also erhalten wir $K^{(\widetilde{\Delta})}(N) = K(\lambda) = K((\alpha u) \cdot \lambda) = K^{(\Delta)}(N)$.

□

1.21 Bemerkung.

(i) Es hängt also $K^{(\Delta)}(N)$ nur ab von der Klasse von Δ in $K^* \diagup (K^*)^{q-1}$. Daher können wir in den folgenden Betrachtungen oBdA annehmen, dass $\Delta \in A \setminus \{0\}$ gilt.

(ii) Außerdem können wir annehmen, dass Δ frei von $(q-1)$-ten Potenzen in K ist, denn sonst ist der zugehörige Rang-1-Drinfeld-Modul $\Phi^{(\Delta)}$ isomorph zum Carlitz-Modul.

(iii) Von dem Führer $N \in A \setminus \{0\}$ können wir voraussetzen, dass er normiert und nicht-konstant ist, denn:

- falls $N \in \mathbb{F}_q^*$, dann ist $K^{(\Delta)}(N)$ trivial.
- falls N normiert ist, gilt $K^{(\Delta)}(N) = K^{(\Delta)}(\alpha N)$ für alle $\alpha \in \mathbb{F}_q^*$.

2 Der Defekt von $K^{(\Delta)}(N)$ im Fall $(N, \Delta) = 1$

Im gesamten Kapitel soll der Führer N normiert, nicht-konstant und von der Form

$$N = \prod_{1 \leq i \leq r} Q_i^{n_i} \in A \quad (n_i \in \mathbb{N} \text{ für alle } 1 \leq i \leq r)$$

sein, mit paarweise verschiedenen Primpolynomen Q_i. Weiter sei

$$\Delta = c^{k_0} \prod_{1 \leq j \leq s} P_j^{k_j} \in A \setminus \{0\} \text{ mit } (N, \Delta) = 1, \ (k_j \in \mathbb{N} \text{ für alle } 0 \leq j \leq s)$$

wobei $c \in \mathbb{F}_q^*$ ein primitives Element ist.
Außerdem setzen wir für die gesamte Arbeit $\delta := \sqrt[q-1]{\Delta} \in \overline{K}$.
Nach Bemerkung 1.21 können wir annehmen:$\Delta \in A \setminus \{0\}$ und Δ frei von $(q-1)$-ten Potenzen.

2.1 Lemma.

Die Abbildung $\widehat{\Gamma}: \ (\overline{K}, C) \longrightarrow (\overline{K}, \Phi^{(\Delta)})$

$$x \longmapsto \delta^{-1} x$$

ist ein Isomorphismus von A-Moduln.

Beweis: Spezialfall von Satz 1.18 mit $\widetilde{\Delta} = 1$.

□

2.2 Lemma.

$\widehat{\Gamma}$ induziert einen Isomorphismus von A-Moduln

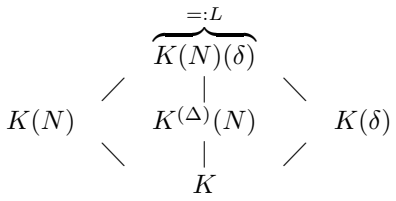
$$\begin{aligned} {}_N C &\longrightarrow {}_N \Phi^{(\Delta)} \\ x &\longmapsto \delta^{-1} x \ . \end{aligned}$$

Beweis: Spezialfall von Korollar 1.19 mit $\widetilde{\Delta} = 1$.

□

2.3 Bemerkung.

Wir betrachten nun folgende Situation:



Wir wissen, dass die Erweiterungen $K(N) \mid K$ und $K^{(\Delta)}(N) \mid K$ galoissch sind. Auch die Erweiterung $K(\delta) \mid K$ ist galoissch (genauer: Es handelt sich um eine zyklische Galois-Erweiterung, siehe z.B. [Bos09], Kapitel 4.8, Satz 3).Außerdem sieht man, dass L das Kompositum von jeweils zwei der drei Zwischenerweiterungen $K(N)$, $K^{(\Delta)}(N)$, $K(\delta)$ ist.

Nach Galois-Theorie([Bos09], Kapitel 4.1, Satz 12) gilt:

$$Gal(L \mid K) \hookrightarrow Gal(K(N) \mid K) \times Gal(K(\delta) \mid K),$$

wobei $Gal(K(N) \mid K) \xrightarrow{\cong} (A/N)^*$ und $Gal(K(\delta) \mid K) \hookrightarrow \mathbb{F}_q^*$
$\sigma_\omega \longmapsto \sigma_\omega(\delta)/\delta, \ (\omega \in \mathbb{F}_q^*)$.

Das nächste Lemma erlaubt es uns die Galoisgruppe $Gal(L \mid K^{(\Delta)}(N))$ zu beschreiben, unter der Voraussetzung, dass wir $Gal(L \mid K)$ kennen.

2.4 Lemma.

Ein Element $(\sigma_a, \sigma_\omega) \in Gal(L \mid K)$ gehört zu $Gal(L \mid K^{(\Delta)}(N))$ genau dann, wenn $a = w$ gilt.

Beweis:
$(\sigma_a, \sigma_\omega) \in Gal(L \mid K^{(\Delta)}(N))$
$\Leftrightarrow (\sigma_a, \sigma_\omega)$ operiert trivial auf $K^{(\Delta)}(N)$
$\Leftrightarrow$ für alle $y \in_N \Phi^{(\delta)}$ gilt: $(\sigma_a, \sigma_\omega)(y) = y$
$\Leftrightarrow$ für alle $x \in_N C$ gilt: $(\sigma_a, \sigma_\omega)(\frac{x}{\delta}) = \frac{x}{\delta}$
$\Leftrightarrow \frac{C_a(x)}{\omega\delta} = \frac{x}{\delta}$
$\Leftrightarrow C_a(x) = \omega x$
$\Leftrightarrow a = \omega$.

□

2.5 Proposition.

Für $N = \prod_{1\leq i\leq r} Q_i^{n_i} \in A$ normiert, nicht-konstant und $\Delta = c^{k_0} \prod_{1\leq j\leq s} P_j^{k_j} \in A\backslash\{0\}$ mit $(N, \Delta) = 1$ gilt:

$K(N)$ und $K(\delta)$ sind linear disjunkt über K (für Genaueres zum Begriff der linearen Disjunktheit siehe z.B. Kapitel 8.3 in [Lan02]).

Beweis:
1.Fall: $K(\delta) = K(\sqrt[q-1]{\Delta})$ sei an einem der P_j's voll verzweigt. Da wir wissen, dass $K(N)$ an P_j unverzweigt ist (wegen $P_j \nmid N$ und Satz 1.11), folgt aus Verzweigungsgründen $K(N) \cap K(\delta) = K$.

2.Fall: $K(\delta) = K(\sqrt[q-1]{\Delta})$ sei an keinem der P_j's voll verzweigt, d.h. es existiert ein $n \in \mathbb{N}$ mit

$\sqrt[q-1]{\prod_{1\leq j\leq s} P_j^{k_j n}} \in K$ und $\sqrt[q-1]{c^{k_0 n}} \notin K$. Es gilt nun

(i) Die Erweiterung $K(\delta) \mid K(\sqrt[q-1]{c^{k_0 n}})$ ist an einem der P_j's voll verzweigt.

(ii) Die Erweiterung $K(N)(\sqrt[q-1]{c^{k_0 n}}) \mid K(\sqrt[q-1]{c^{k_0 n}})$ ist unverzweigt an allen P_j's.

Aus $(i) + (ii)$ folgt $K(\delta) \cap K(N)(\sqrt[q-1]{c^{k_0 n}}) = K(\sqrt[q-1]{c^{k_0 n}})$.
Daraus folgt $K(N) \cap (K(\delta) \setminus K(\sqrt[q-1]{c^{k_0 n}})) = K$. Außerdem wissen wir:
$K(N) \cap K(\sqrt[q-1]{c^{k_0 n}}) = K$ (da $K(N) \mid K$ nur triviale Konstantenerweiterung hat).
Somit erhalten wir insgesamt $K(N) \cap K(\delta) = K$.

□

Nun können wir das Hauptresultat von Kapitel 2 formulieren:

2.6 Satz.

Für $N = \prod_{1\leq i\leq r} Q_i^{n_i} \in A$ normiert, nicht-konstant und $\Delta = c^{k_0} \prod_{1\leq j\leq s} P_j^{k_j} \in A\backslash\{0\}$ mit $(N, \Delta) = 1$ gilt:
Der Defekt des Torsionskörpers $K^{(\Delta)}(N)$ ist Eins, d.h.
$Gal(K^{(\Delta)}(N) \mid K) \xrightarrow{\cong} (A/N)^*$.

Beweis:
(i) Nach Proposition 2.5 wissen wir , dass $K(N)$ und $K(\delta)$ linear disjunkt sind über K.
(ii) Wegen (i) erhält man $[\underbrace{K(N)(\delta)}_{=L} : K(N)] = [K(\delta) : K] =: h.$
(iii)Wegen (i) erhält man außerdem: $Gal(L \mid K) = \underbrace{Gal(K(N) \mid K)}_{\cong (A/N)^*} \times \underbrace{Gal(K(\delta) \mid K)}_{\cong \mu_h}$,
wobei $\mu_h := \{h - te\ Einheitswurzeln\, in\ \mathbb{F}_q^*\}$.
(iv) Wegen Lemma 2.4 wissen wir

$Gal(L \mid K^{(\Delta)}(N)) = \{(\sigma_a, \sigma_\omega) \in (A/N)^* \times \mu_h \mid a = \omega\}$. Daraus folgt

$\#Gal(L \mid K^{(\Delta)}(N)) = [L : K^{(\Delta)}(N)] = \#\mu_h = h.$

(v) Somit gilt: $[K^{(\Delta)}(N) : K] = \dfrac{[L : K(N)][K(N) : K]}{[L : K^{(\Delta)}(N)]}$

$$= \frac{h \cdot \#(A/N)^*}{h}$$

$$= \#(A/N)^*.$$

□

3 Kummer-$(q-1)$-Teilerweiterungen von $K(N)$

3.1 Definition.

Eine Kummer-$(q-1)$-Erweiterung von K ist ein Körper der Form $K(\sqrt[q-1]{f})$ für ein $f \in K$.

3.2 Lemma.

Sei $P \in A$ ein normiertes Primpolynom vom Grad d. Für alle $m \in \mathbb{N}_0$ ist die Kummer$-(q-1)-$Erweiterung $K(\sqrt[q-1]{(-1)^{dm}P^m})$ von K enthalten in $K(P) = K({}_PC)$.

Beweis:
Setzen wir $g(x) := \frac{C_P(x)}{x}$, dann gilt:

$$g(x) = \prod_{b \in (A/P)^*} (x - C_b(\lambda)), \text{ wobei } 0 \neq \lambda \in_P C.$$

Also erhalten wir
$P = g(0) = \prod_{b \in (A/P)^*} C_b(\lambda)$

$$= \prod_{0 \leq j < \frac{q^d-1}{q-1}} \Big(\prod_{\alpha \in \mathbb{F}_q^*} \alpha \cdot C_{a^j}(\lambda) \Big) \qquad \text{(wobei } a \in (A/P)^* \text{ primitiv)}$$

$$= \prod_{0 \leq j < \frac{q^d-1}{q-1}} (-C_{a^j}(\lambda)^{q-1}) \qquad \Big(\text{da } \prod_{\alpha \in \mathbb{F}_q^*} \alpha = -1 \Big)$$

$$= \begin{cases} \prod\limits_{0 \leq j < \frac{q^d-1}{q-1}} C_{a^j}(\lambda)^{q-1}, & falls\ d\ gerade \\ -\prod\limits_{0 \leq j < \frac{q^d-1}{q-1}} C_{a^j}(\lambda)^{q-1} & falls\ d\ ungerade \end{cases}.$$

Somit haben wir die Darstellung:

$$\sqrt[q-1]{(-1)^d P} = \prod_{0 \leq j < \frac{q^d-1}{q-1}} C_{a^j}(\lambda).$$

Also gilt: $K(\sqrt[q-1]{(-1)^d P}) \subset K(P)$ und somit $K(\sqrt[q-1]{(-1)^{dm}P^m}) \subset K(P)$ für alle $m \in \mathbb{N}_0$.

□

3.3 Lemma.

Sei $N = \prod_{1 \le i \le r} Q_i^{n_i}$, wobei die Q_i paarweise verschiedene Primpolynome sind mit $d_i := deg(Q_i)$. Dann gilt:

Für alle $\underline{m} = (m_1, \ldots, m_r) \in \mathbb{N}_0^r$ ist die Kummer-$(q-1)$-Erweiterung $K\left(\sqrt[q-1]{(-1)^{\sum_{1 \le i \le r} d_i m i} \prod_{1 \le i \le r} Q_i^{m_i}} \right)$ von K enthalten in $K(N)$.

Beweis:
Es gilt $K(Q_i) \subset K(Q_i^{n_i}) \subset K(N)$ für alle $1 \le i \le r$, und somit wegen Lemma 3.2: $K(\sqrt[q-1]{(-1)^{d_i m_i} Q_i^{m_i}}) \subset K(N)$ für alle $m_i \in \mathbb{N}_0$ und für alle $1 \le i \le r$. Daraus folgt:

$$K\left(\sqrt[q-1]{(-1)^{\sum_{1 \le i \le r} d_i m i} \prod_{1 \le i \le r} Q_i^{m_i}} \right) \subset K(N) \text{ für alle } \underline{m} = (m_1, \ldots, m_r) \in \mathbb{N}_0^r.$$

□

3.4 Bemerkung.

Für gegebenes $N \in A$ wie in Lemma 3.3 und $\underline{m} = (m_1, \ldots, m_r) \in \mathbb{N}_0^r$ setzen wir für die gesamte Arbeit

$$G_{\underline{m}} := \sqrt[q-1]{(-1)^{\sum_{1 \le i \le r} d_i m i} \prod_{1 \le i \le r} Q_i^{m_i}} \in \overline{K}.$$

Das Hauptziel dieses Kapitels ist es die Untergruppe $H_{\underline{m}}$ von $(A/N)^*$ zu bestimmen, welche erfüllt: $K(N)^{H_{\underline{m}}} = K(G_{\underline{m}})$.

3.5 Lemma.

Wir betrachten die h-ten Einheitswurzeln $\mu_h := \{\omega \in \mathbb{F}_q^* \mid \omega^h = 1\}$ in $\mathbb{F}_q^*$, dann gilt:
$\#\{\omega \in \mu_h \mid \omega^i = 1\} = ggT(h, i)$ für ein $i \in \mathbb{N}$.

Beweis:
Sei b ein primitives Element in $\mathbb{F}_q^*$, dann ist $a := b^{\frac{q-1}{h}}$ ein Erzeuger von μ_h: $\mu_h = \{a^k \mid 1 \le k \le h\}$. Wir wollen nun untersuchen für wie viele k´s $(1 \le k \le h)$ gilt: $(a^k)^i = 1$:

$(a^k)^i = a^{ki} = b^{\frac{q-1}{h} \cdot ki} = 1$
$\quad \Leftrightarrow \frac{q-1}{h} \cdot ki \equiv 0\,(q-1)$

$\Leftrightarrow \frac{ki}{h} \in \mathbb{N} \Leftrightarrow ki \equiv 0\,(h)$.

Es gilt: $min\,\{k \in \mathbb{N} \mid ki \equiv 0\,(h)\} = \frac{h}{ggT(h,i)}$. Daraus folgt $(a^{\frac{h}{ggT(h,i)}})^i = 1$ und $\frac{h}{ggT(h,i)}$ minimal mit dieser Eigenschaft.
Somit erhalten wir $\#\left\{\omega \in \mu_h \mid \omega^i = 1\right\} = \{1 \leq k \leq h \mid ki \equiv 0\,(h)\} = ggT(h,i)$.

□

3.6 Lemma.

Sei $\mathbb{F}_{q^n} \mid \mathbb{F}_q$ eine Körpererweiterung von Grad $n \in \mathbb{N}$. Die Normabbildung

$$N_{\mathbb{F}_q}^{\mathbb{F}_{q^n}} : \mathbb{F}_{q^n}^* \longrightarrow \mathbb{F}_q^*$$

$$x \longmapsto x \cdot x^q \cdot \ldots \cdot x^{q^{n-1}} = x^{\frac{q^n-1}{q-1}}$$

ist surjektiv.

Beweis:
(0) Die Abbildung $N_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}$ ist ein Gruppenhomomorphismus.

(*i*) $\#(ker\, N_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}) \overset{Lemma\ 3.5}{=} ggT(q^n-1, \frac{q^n-1}{q-1}) = \frac{q^n-1}{q-1}$.

(*ii*) Es folgt $\#(Bild\, N_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}) = \frac{q^n-1}{\#(ker\, N_{\mathbb{F}_q}^{\mathbb{F}_{q^n}})} = q-1$.

Also ist die Normabbildung surjektiv.

□

3.7 Bemerkung.

Für ein Primpolynom P mit $d := deg(P)$ liefert die Normabbildung also einen surjektiven Gruppenhomomorphismus von $(A/P)^* \cong \mathbb{F}_{q^d}^*$ nach $\mathbb{F}_q^*$.

Das folgende Lemma benötigen wir zum Beweis von Satz 3.9.

3.8 Lemma.

Betrachten wir den Ring $\mathbb{Z}/(j+1)\mathbb{Z}$ für $j \in \mathbb{N}$ und die Menge
$B := \{l, l+1, \ldots, l+j\}$ für ein $l \in \mathbb{N}$, dann gilt:
(*i*) Zu jedem $y \in B$ gehört ein eindeutiges $\bar{y} \in \mathbb{Z}/(j+1)\mathbb{Z}$ mit $y \equiv \bar{y}\ (j+1)$.

(*ii*) $\sum\limits_{y \in B} \dfrac{y - \bar{y}}{j+1} = l$.

Beweis:
(i) klar.
(ii) Wir geben zu jedem $y \in B$ das eindeutig bestimmte Element $\bar{y} \in \mathbb{Z}/(j+1)\mathbb{Z}$ mit $y \equiv \bar{y}\ (j+1)$ an:

$0 \equiv (l - \bar{l}) + j + 1\ mod(j+1)$, wobei $\bar{l}$ die Restklasse von l modulo $(j+1)$ ist.
$1 \equiv (l - \bar{l}) + j + 2\ mod(j+1)$

$\vdots$

$x \equiv (l - \bar{l}) + j + x + 1\ mod(j+1)$, wobei $x = \bar{l} - 1$.
$x + 1 \equiv l\ mod(j+1)$
$x + 2 \equiv l + 1\ mod(j+1)$

$\vdots$

$j \equiv (l - \bar{l}) + j\ mod(j+1)$.

Also erhält man $\sum\limits_{y \in B} \frac{y-\bar{y}}{j+1} = (x+1)(\frac{l-\bar{l}}{j+1} + 1) + (j - x) \cdot \frac{l-\bar{l}}{j+1}$

$$= \tfrac{l-\bar{l}}{j+1} + x + 1 + j \cdot \tfrac{l-\bar{l}}{j+1}$$
$$= \tfrac{l-\bar{l}}{j+1} \cdot (j+1) + x + 1 = l - \bar{l} + x + 1 \overset{\bar{l}=x+1}{=} l.$$

□

3.9 Satz.

Sei $P \in A$ ein normiertes Primpolynom vom Grad d und $\nu :\ (A/P)^* \longrightarrow \mathbb{F}_q^*$ die Normabbildung (wie in Lemma 3.6).

(i) Für $\sigma_b \in Gal(K(P) \mid K) \cong (A/P)^*$gilt:

$$\sigma_b \left(\sqrt[q-1]{(-1)^d P} \right) = \nu(b) \cdot \left(\sqrt[q-1]{(-1)^d P} \right).$$

(ii) Insbesondere gilt also $K(P)^{ker(\nu)} = K\left(\sqrt[q-1]{(-1)^d P} \right)$.

Die Situation kann man mit folgendem Diagramm veranschaulichen:

$$(A/P)^* \begin{cases} ker(\nu) \begin{cases} \\ \\ \end{cases} & \begin{array}{c} K(P) \\ | \\ | \\ K(P)^{ker(\nu)} = K\left(\sqrt[q-1]{(-1)^d P} \right) \\ | \\ | \\ K \end{array} \\ Bild(\nu) \begin{cases} \\ \\ \end{cases} & \end{cases}$$

Beweis:
(ii) ist eine direkte Folge von (i), also müssen wir nur (i) zeigen.
Sei $a \in (A/P)^*$ primitiv und $a^z = b$ $(z \in \mathbb{N})$.
Nach dem Beweis von Lemma 3.2 gilt:

$$\sqrt[q-1]{(-1)^d P} = \prod_{0 \le m < \frac{q^d-1}{q-1}} C_{a^m}(\lambda) \quad (0 \neq \lambda \in_P C).$$

Berechnung von $\sigma_b\left(\sqrt[q-1]{(-1)^d P}\right)$:

$$\sigma_b\left(\sqrt[q-1]{(-1)^d P}\right) = \prod_{0 \le m < \frac{q^d-1}{q-1}} \sigma_b\left(C_{a^m}(\lambda)\right)$$
$$= \prod_{0 \le m < \frac{q^d-1}{q-1}} C_{a^{z+m}}(\lambda).$$

Sei $\overline{z+m}$ die Restklasse von $z+m$ modulo $\left(\frac{q^d-1}{q-1}\right)$, dann gilt:

$$C_{a^{z+m}}(\lambda) = C_{a^{\overline{z+m}+z+m-\overline{z+m}}}(\lambda)$$
$$= C_{a^{\overline{z+m}} \cdot a^{z+m-\overline{z+m}}}(\lambda)$$
$$= a^{z+m-\overline{z+m}} \cdot C_{a^{\overline{z+m}}}(\lambda) \quad (da\ a^{z+m-\overline{z+m}} \in \mathbb{F}_q^*)$$
$$= \nu(a)^{\frac{z+m-\overline{z+m}}{(q^d-1)/q-1}} \cdot C_{a^{\overline{z+m}}}(\lambda).$$

Somit erhalten wir also:

$$\sigma_b\left(\sqrt[q-1]{(-1)^d P}\right) = \prod_{0 \le m < \frac{q^d-1}{q-1}} C_{a^{z+m}}(\lambda)$$
$$= \nu(a)^{\sum_{m=0}^{\frac{q^d-1}{q-1}-1} \frac{z+m-\overline{z+m}}{(q^d-1)/q-1}} \cdot \prod_{0 \le m < \frac{q^d-1}{q-1}} C_{a^{\overline{z+m}}}(\lambda)$$
$$\overset{Lemma\ 3.8(ii)}{=} \nu(a)^z \cdot \prod_{0 \le m < \frac{q^d-1}{q-1}} C_{a^{\overline{z+m}}}(\lambda)$$
$$= \nu(a)^z \cdot \prod_{0 \le j < \frac{q^d-1}{q-1}} C_{a^j}(\lambda)$$
$$= \nu(a^z) \cdot \prod_{0 \le j < \frac{q^d-1}{q-1}} C_{a^j}(\lambda)$$
$$= \nu(b) \cdot \left(\sqrt[q-1]{(-1)^d P}\right). \qquad \square$$

Zum Abschluss des Kapitels wollen wir das Resultat aus Satz 3.9 verallgemeinern für $N = \prod_{1 \leq i \leq r} Q_i^{n_i}$.
Dazu betrachten wir zunächst folgendes Lemma:

3.10 Lemma.

Sei $N = \prod_{1 \leq i \leq r} Q_i^{n_i}$ wie in Lemma 3.3 und λ ein Erzeuger von ${}_NC$. Weiter sei ein j zwischen 1 und r gegeben. Setze

$N_j := \frac{N}{Q_j} = \left(\prod_{1 \leq i \leq r,\, i \neq j} Q_i^{n_i} \right) \cdot Q_j^{n_j - 1}$, dann gilt:

(i) $\lambda_j := C_{N_j}(\lambda)$ ist ein Erzeuger von ${}_{Q_j}C$.

(ii) Für $\sigma_b \in Gal(K(N) \mid K) \cong (A/N)^*$ gilt: $\sigma_b(\lambda_j) = C_{\bar{b_j}}(\lambda_j)$, wobei $\overline{b_j}$ gegeben ist durch die kanonische Projektion

$$\begin{aligned} (A/N)^* &\xrightarrow{\cong} \prod_{1 \leq i \leq r} (A/Q_i^{n_i})^* \longrightarrow (A/Q_j)^* \\ b &\longmapsto (b_1, \ldots, b_r) \longmapsto \overline{b_j} \end{aligned} .$$

Beweis:
(i) $C_{Q_j}(\lambda_j) = C_{Q_j}(C_{N_j}(\lambda)) = C_N(\lambda) = 0$ und $\lambda_j \neq 0$, da λ ein Erzeuger von ${}_NC$ ist.
(ii) $\sigma_b(\lambda_j) = \sigma_b(C_{N_j}(\lambda)) = C_{N_j}(\sigma_b(\lambda)) = C_{N_j}(C_b(\lambda)) = C_b(C_{N_j}(\lambda)) = C_b(\lambda_j) = C_{\bar{b_j}}(\lambda_j)$, wobei die letzte Gleichheit gilt, da $\lambda_j \in_{Q_j} C$ und wegen der Tatsache, dass ${}_{Q_j}C$ ein A/Q_j-Modul ist (Satz 1.7).

□

3.11 Definition.

Sei $N = \prod_{1 \leq i \leq r} Q_i^{n_i}$ wie in Lemma 3.3 und $\nu_i : (A/Q_i)^* \longrightarrow \mathbb{F}_q^*$ die Normabbildung für alle $1 \leq i \leq r$. Definiere $\chi_{\underline{m}} \in Hom((A/N)^*, \mathbb{F}_q^*)$ für $\underline{m} = (m_1, \ldots, m_r) \in \mathbb{N}_0^r$ durch

$$\begin{aligned} \chi_{\underline{m}} : \ (A/N)^* &\longrightarrow \mathbb{F}_q^* \\ b &\longmapsto \chi_{\underline{m}}(b) := \prod_{1 \leq i \leq r} \nu_i(\bar{b_i})^{m_i}, \end{aligned}$$

wobei $\bar{b_i} \in (A/Q_i)^*$ gegeben ist durch die kanonische Projektion wie in Lemma 3.10.

3.12 Satz.

Sei $N = \prod\limits_{1\le i\le r} Q_i^{n_i}$ wie in Lemma 3.3 und $\underline{m} = (m_1, \ldots, m_r) \in \mathbb{N}_0^r$ gegeben.

(i) Für $\sigma_b \in Gal(K(N) \mid K) \cong (A/N)^*$ gilt:

$$\sigma_b\left(G_{\underline{m}}\right) = \sigma_b\left(\sqrt[q-1]{(-1)^{\sum\limits_{1\le i\le r} d_i m i} \prod_{1\le i\le r} Q_i^{m_i}}\right) = \chi_{\underline{m}}(b)\cdot G_{\underline{m}}.$$

(ii) Insbesondere gilt $K(N)^{ker\left(\chi_{\underline{m}}\right)} = K\left(G_{\underline{m}}\right)$.

Die Situation kann man mit folgendem Diagramm veranschaulichen:

$$(A/N)^* \begin{cases} ker\left(\chi_{\underline{m}}\right) \begin{cases} \\ \\ \end{cases} & \begin{array}{c} K(N) \\ | \\ | \\ K(N)^{ker(\chi_{\underline{m}})} = K(G_{\underline{m}}) \\ | \\ | \\ K \end{array} \\ Bild\left(\chi_{\underline{m}}\right) \begin{cases} \\ \\ \end{cases} & \end{cases}$$

Beweis:
(ii) ist eine direkte Folgerung aus (i), wir müssen also nur (i) zeigen.
Für $G_{\underline{m}}$ hat man folgende Darstellung:

$$\begin{aligned} G_{\underline{m}} &= \sqrt[q-1]{(-1)^{\sum\limits_{1\le i\le r} d_i m i} \prod_{1\le i\le r} Q_i^{m_i}} \\ &= \prod_{1\le i\le r} \sqrt[q-1]{(-1)^{d_i m_i} Q_i^{m_i}} \\ &= \prod_{1\le i\le r} \left(\sqrt[q-1]{(-1)^{d_i} Q_i}\right)^{m_i} \\ &\overset{\substack{Beweis \\ Lemma\ 3.2}}{=} \prod_{1\le i\le r} \left(\prod_{0\le j^{(i)} < \frac{q^{d_i}-1}{q-1}} C_{a_i^{j^{(i)}}}(\lambda_i)\right)^{m_i}, \end{aligned}$$

wobei λ_i ein Erzeuger von ${}_{Q_i}C$ ist und $a_i \in (A/Q_i)^*$ ein primitives Element ist.

$$\sigma_b\left(G_{\underline{m}}\right) = \prod_{1\le i\le r} \left(\prod_{0\le j^{(i)} < \frac{q^{d_i}-1}{q-1}} C_{a_i^{j^{(i)}}}\left(\sigma_b(\lambda_i)\right)\right)^{m_i}$$

$$\overset{Lemma}{\underset{3.10(ii)}{=}} \prod_{1\le i\le r}\left(\prod_{0\le j^{(i)}<\frac{q^{d_i}-1}{q-1}} C_{a_i^{j^{(i)}}}\left(\sigma_{\bar{b_i}}(\lambda_i)\right)\right)^{m_i}$$

$$\overset{Satz}{\underset{3.9}{=}} \prod_{1\le i\le r}\left(\nu_i(\bar{b_i})\cdot \sqrt[q-1]{(-1)^{d_i}Q_i}\right)^{m_i}$$

$$= \prod_{1\le i\le r}\left(\left(\nu_i(\bar{b_i})\right)^{m_i}\cdot \sqrt[q-1]{(-1)^{d_i m_i}Q_i^{m_i}}\right)$$

$$= \prod_{1\le i\le r}\left(\left(\nu_i(\bar{b_i})\right)^{m_i}\right)\cdot G_{\underline{m}} = \chi_{\underline{m}}(b)\cdot G_{\underline{m}}.$$

□

4 Der Defekt von $K^{(\Delta)}(N)$ im Fall $(N, \Delta) \neq 1$

Falls N und Δ nicht teilerfremd sind, müssen $K(N)$ und $K(\delta)$ mit $\delta := \sqrt[q-1]{\Delta} \in \overline{K}$ im Allgemeinen nicht mehr $K - linear$ disjunkt sein. Um in dieser Situation den Defekt der Erweiterung $K^{(\Delta)}(N) \mid K$ bestimmen zu können, müssen wir daher zunächst $K(N) \cap K(\delta)$ berechnen. Im ganzen Kapitel sei folgende Situation gegeben:

- $N = \prod_{1 \leq i \leq r} Q_i^{n_i} \in A$ normiert, wobei $n_i \in \mathbb{N}$ für alle $1 \leq i \leq r$ und Q_i paarweise verschiedene Primpolynome.
- $\Delta = c^{k_0} \prod_{1 \leq j \leq s'} P_j^{k_j} \prod_{s' < j \leq s} P_j^{k_j} \in A \setminus \{0\}$,
  wobei $k_j \in \mathbb{N}$ für alle $0 \leq j \leq s$, $d_j := deg(P_j)$ und $c \in \mathbb{F}_q^*$ primitiv.

Außerdem gelte $P_j \mid N$ für alle $1 \leq j \leq s$' und $P_j \nmid N$ für alle $s' < j \leq s$.

- $\delta := \sqrt[q-1]{\Delta} \in \overline{K}$.

4.1 Lemma.

Seien $a_1, \ldots, a_l \in \mathbb{Z}$, $m \in \mathbb{N}$, dann gilt:
$min\{n \in \mathbb{N} \mid a_i \cdot n \equiv 0 \ (mod\ m)\ für\ alle\ 1 \leq i \leq l\} = \frac{m}{ggT(m, a_1, \ldots, a_l)}$.

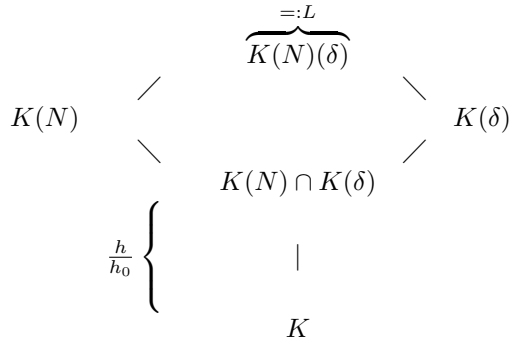
Beweis:
Induktion nach l :
$\underline{l = 1}$: Es gilt $min\{n \in \mathbb{N} \mid a_1 \cdot n \equiv 0 \ (mod\ m)\} = \frac{m}{ggT(m, a_1)}$.

Sei die Aussage des Lemmas richtig für $l - 1 \in \mathbb{N}$, dann gilt:

$$min\{n \in \mathbb{N} \mid a_i \cdot n \equiv 0 \ (mod\ m)\ für\ alle\ 1 \leq i \leq l-1\ und\ a_l \cdot n \equiv 0 \ (mod\ m)\}$$
$$= kgV\left(\frac{m}{ggT(m, a_1, \ldots, a_{l-1})}, \frac{m}{ggT(m, a_l)}\right) = \frac{m}{ggT(m, a_1, \ldots, a_l)}.$$

□

Wir wollen als nächstes die Größen $h := [K(\delta) : K]$ und
$h_0 := [K(\delta) : K(N) \cap K(\delta)]$ ausrechnen, welche man sich in folgendem Diagramm veranschaulichen kann:



4.2 Lemma.

Es gilt $h := [K(\delta) : K] = \dfrac{q-1}{ggT(k_0, k_1, \ldots, k_s, q-1)}$.

Beweis:
$[K(\delta) : K] = min\{n \in \mathbb{N} \mid \delta^n \in K\}$

$$= \frac{q-1}{ggT(k_0, k_1, \ldots, k_s, q-1)},$$

wobei die erste Gleichheit gilt nach Kummer-Theorie und die zweite Gleichheit nach Lemma 4.1.

□

4.3 Lemma.

Sei $N = \prod\limits_{1 \le i \le r} Q_i^{n_i} \in A$ wie am Anfang des Kapitels festgelegt, $P_1, \ldots, P_t$ seien Primpolynome mit $P_j \nmid N \ \ (1 \le j \le t)$. Weiter seien $k_0, k_1, \ldots, k_t \in \mathbb{N}$ und $c \in \mathbb{F}_q^*$ primitiv, dann gilt:

$$\sqrt[q-1]{c^{k_0} \prod_{1 \le j \le t} P_j^{k_j}} \in K(N) \Longleftrightarrow \begin{cases} (i)\ k_j \equiv 0\ (q-1)\ \textit{für alle}\ 1 \le j \le t \\ (ii)\ k_0 \equiv 0\ (q-1) \end{cases}.$$

Beweis:
" $\Longleftarrow$ " : Falls (i) und (ii) gelten, dann gilt $\sqrt[q-1]{c^{k_0} \prod\limits_{1 \le j \le t} P_j^{k_j}} \in K \subset K(N)$.

" $\Longrightarrow$ " : Sei $\sqrt[q-1]{c^{k_0}\prod_{1\le j\le t}P_j^{k_j}} \in K(N)$. Wir nehmen an: Es gibt ein j zwischen 1 und t mit $k_j \not\equiv 0 (q-1)$ oder $k_0 \not\equiv 0\ (q-1)$ und führen dies zum Widerspruch:

1.*Fall* : $k_0 \not\equiv 0\ (q-1)$, $k_j \equiv 0\ (q-1)$ *für alle* $1 \le j \le t$. Dann würde folgen :

$$\sqrt[q-1]{c^{k_0}} \in K(N) \quad \left(wegen \ \sqrt[q-1]{\prod_{1\le j\le t}P_j^{k_j}} \in K \subset K(N) \right).$$

Dies ist ein Widerspruch, da $K(N) \mid K$ nach Satz 1.13(ii) nur triviale Konstantenerweiterung hat.

2.*Fall* : $k_0 \equiv 0\ (q-1)$ und für eine Teilmenge U von $\{1,\dots,t\}$ gilt:
$k_l \not\equiv 0\ (q-1)$ für alle $l \in U$ und $k_i \equiv 0\ (q-1)$ für alle $i \in \{1,\dots,t\} \setminus U$. Dann ist die Erweiterung $K\left(\sqrt[q-1]{c^{k_0}\prod_{1\le j\le t}P_j^{k_j}}\right) \mid K$ an einem der P_j voll verzweigt. Andererseits ist $K(N)$ an diesem P_j unverzweigt (da $P_j \nmid N$). Also sind $K(N)$ und $K\left(\sqrt[q-1]{c^{k_0}\prod_{1\le j\le t}P_j^{k_j}}\right)$ aus Verzweigungsgründen linear disjunkt über K. Dies ist ein Widerspruch zur Annahme $\sqrt[q-1]{c^{k_0}\prod_{1\le j\le t}P_j^{k_j}} \in K(N)$.

3.*Fall* : $k_0 \not\equiv 0\ (q-1)$, $k_l \not\equiv 0\ (q-1)$ für alle $l \in U$ und $k_i \equiv 0\ (q-1)$ für alle $i \in \{1,\dots,t\} \setminus U$, wobei U wie oben.

- Falls $K\left(\sqrt[q-1]{c^{k_0}\prod_{1\le j\le t}P_j^{k_j}}\right) \mid K$ voll verzweigt ist an einem der P_j, dann können wir wie im 2.Fall argumentieren.
- Falls $K\left(\sqrt[q-1]{c^{k_0}\prod_{1\le j\le t}P_j^{k_j}}\right) \mid K$ an keinem der P_j voll verzweigt ist, dann gibt es ein $n \in \mathbb{N}$, so dass $nk_j \equiv 0\ (q-1)$ für alle $1 \le j \le t$ und $nk_0 \not\equiv 0\ (q-1)$. Daraus folgt $\sqrt[q-1]{c^{nk_0}} \in K(N)$.

Dies ist ein Widerspruch, da $K(N) \mid K$ nach Satz 1.13(ii) nur triviale Konstantenerweiterung hat.

□

4.4 Satz.

Für $\delta := \sqrt[q-1]{\Delta} \in \overline{K}$, mit $\Delta \in A \setminus \{0\}$ und $N \in A$ wie am Anfang des Kapitels festgelegt, gilt:

$$\delta^n \in K(N) \Longleftrightarrow \begin{cases} (i)\ k_j \cdot n \equiv 0\ (q-1)\ \textit{für alle}\ s' < j \leq s \\ (ii)\ k_0^* \cdot n \equiv 0\ (q-1) \end{cases}, \text{ wobei}$$

$$k_0^* := \begin{cases} k_0, & \textit{falls } q \textit{ gerade oder } \sum\limits_{1 \leq j \leq s'} d_j k_j \textit{ gerade} \\ k_0 + \frac{q-1}{2}, & \textit{sonst} \end{cases}.$$

Beweis:
1.*Fall* : sei q *gerade oder* $\sum\limits_{1 \leq j \leq s'} d_j k_j$ *gerade*:
" $\Longleftarrow$ ": Es gelte (i) und (ii), dann

$$\delta^n = \sqrt[q-1]{c^{nk_0} \prod_{1 \leq j \leq s'} P_j^{nk_j}} \cdot \sqrt[q-1]{\prod_{s' < j \leq s} P_j^{nk_j}}$$

$$\overset{(ii)}{=} \alpha \cdot \underbrace{\left(\sqrt[q-1]{\prod_{1 \leq j \leq s'} P_j^{k_j}} \right)^n}_{\in K(N)\ (\textit{wegen Lemma 3.3})} \cdot \underbrace{\sqrt[q-1]{\prod_{s' < j \leq s} P_j^{nk_j}}}_{\in K\ (\textit{wegen } (i))} \text{ mit } \alpha \in \mathbb{F}_q^*.$$

Also gilt $\delta^n \in K(N)$.

" $\Longrightarrow$ ": Es gelte $\delta^n \in K(N)$, dann können wir schreiben:

$$\delta^n = \underbrace{\sqrt[q-1]{\prod_{1 \leq j \leq s'} P_j^{nk_j}}}_{\in K(N)\ (\textit{nach Lemma 3.3})} \cdot \sqrt[q-1]{\prod_{s' < j \leq s} P_j^{nk_j} \cdot c^{nk_0}}.$$

Daraus folgt, dass auch $\sqrt[q-1]{\prod\limits_{s' < j \leq s} P_j^{nk_j} \cdot c^{nk_0}}$ in $K(N)$ liegen muss. Dies hat nach Lemma 4.3 aber zur Folge: $k_j \cdot n \equiv 0\ (q-1)\ \textit{für alle}\ s' < j \leq s$ und $k_0 \cdot n \equiv 0\ (q-1)$.

2.*Fall* : sei q *ungerade und* $\sum_{1\leq j\leq s'} d_j k_j$ *ungerade*:
" $\Longleftarrow$ " : Es gelte (i) und (ii), dann können wir schreiben:

$$\delta^n = \underbrace{\sqrt[q-1]{c^{nk_0}\prod_{1\leq j\leq s'} P_j^{nk_j}}}_{(*)} \cdot \underbrace{\sqrt[q-1]{\prod_{s'<j\leq s} P_j^{nk_j}}}_{\in K\ (wegen\ (i))}.$$

Zwischenüberlegung: $\left(k_0 + \frac{q-1}{2}\right)\cdot n \equiv 0\ (q-1)$

$\Leftrightarrow c^{\left(k_0+\frac{q-1}{2}\right)\cdot n} = 1$
$\Leftrightarrow c^{k_0 n}\cdot c^{\frac{q-1}{2}\cdot n} = 1$
$\Leftrightarrow c^{k_0 n} = c^{\frac{q-1}{2}\cdot n} = (-1)^n$.

Aus dieser Überlegung und wegen (ii) folgt:

$(*) = \sqrt[q-1]{(-1)^n\left(\prod_{1\leq j\leq s'} P_j^{k_j}\right)^n} \in K(N)$ nach Lemma 3.3 und somit
$\delta^n \in K(N)$.

" $\Longrightarrow$ " : Es gelte $\delta^n \in K(N)$, dann können wir schreiben:

$\delta^n = \sqrt[q-1]{\prod_{1\leq j\leq s'} P_j^{nk_j}} \cdot \sqrt[q-1]{\prod_{s'<j\leq s} P_j^{nk_j}\cdot c^{nk_0}}$, es folgt

$$c^n\delta^n = \sqrt[q-1]{c^{\frac{q-1}{2}\cdot n}\prod_{1\leq j\leq s'} P_j^{nk_j}} \cdot \sqrt[q-1]{c^{\frac{q-1}{2}\cdot n}\prod_{s'<j\leq s} P_j^{nk_j}\cdot c^{nk_0}}$$

$$= \underbrace{\sqrt[q-1]{(-1)^n\left(\prod_{1\leq j\leq s'} P_j^{k_j}\right)^n}}_{\in K(N)\ (nach\ Lemma\ 3.3)} \cdot \sqrt[q-1]{c^{(k_0+\frac{q-1}{2})\cdot n}\prod_{s'<j\leq s} P_j^{nk_j}} \in K(N).$$

Daraus folgt, dass auch $\sqrt[q-1]{c^{(k_0+\frac{q-1}{2})\cdot n}\prod_{s'<j\leq s} P_j^{nk_j}}$ in $K(N)$ liegen muss.
Somit erhält man nach Lemma 4.3:

$n\left(k_0+\frac{q-1}{2}\right) \equiv 0\ (q-1)$ und $n\cdot k_j \equiv 0\ (q-1)$ für alle $s' < j \leq s$.

□

4.5 Korollar.

Es gilt $h_0 := [K(\delta) : K(N) \cap K(\delta)] = \dfrac{q-1}{ggT\,(k_0^*, k_{s'+1}, \ldots, k_s, q-1)}$, wobei k_0^* wie in Satz 4.4.

Beweis: Die Aussage folgt aus Satz 4.4 und Lemma 4.1.

□

Als Nächstes wollen wir $Gal(K(N)(\delta) \mid K) = Gal(L \mid K)$ beschreiben. Wir wissen schon:

$$Gal(L \mid K) \hookrightarrow \underbrace{Gal(K(N) \mid K)}_{\cong (A/N)^*} \times \underbrace{Gal(K(\delta) \mid K)}_{\cong \mu_h}.$$

Um $Gal(L \mid K)$ genau charakterisieren zu können, überlegen wir uns:

- Wie operiert $\sigma_\omega \in Gal(K(\delta) \mid K)$ auf $K(N) \cap K(\delta) = K(\delta^{h_0})$?
- Wie operiert $\sigma_a \in Gal(K(N) \mid K)$ auf $K(N) \cap K(\delta) = K(\delta^{h_0})$?

4.6 Lemma.

Die Abbildung $\psi : \begin{array}{ccc} \mu_h & \longrightarrow & \mu_{h/h_0} \\ x & \longmapsto & x^{h_0} \end{array}$

beschreibt die Einschränkung von $Gal(K(\delta) \mid K)$ auf $Gal(\overbrace{K(N) \cap K(\delta)}^{=K(\delta^{h_0})} \mid K)$, d.h. für $\sigma_\omega \in Gal(K(\delta) \mid K)$ gilt $\sigma_w(\delta^{h_0}) = w^{h_0} \cdot \delta^{h_0}$.

Beweis: $\sigma_w(\delta^{h_0}) = (\sigma_\omega(\delta))^{h_0} = (\omega \cdot \delta)^{h_0} = \omega^{h_0} \cdot \delta^{h_0}$.

□

4.7 Lemma.

Setze $\underline{k} := (k_1, \ldots, k_{s'}) \in \mathbb{N}^{s'}$, wobei die k_j gegeben sind als die Exponenten in der Darstellung von $\Delta = c^{k_0} \prod\limits_{1 \le j \le s'} P_j^{k_j} \prod\limits_{s' < j \le s} P_j^{k_j}$.

Die Abbildung $\varphi : \begin{array}{ccc} (A/N)^* & \longrightarrow & \mu_{h/h_0} \end{array}$

$$a \longmapsto \big(\chi_{\underline{k}}(a)\big)^{h_0} = \left(\prod_{1 \le j \le s'} \nu_j(\bar{a_j})^{k_j} \right)^{h_0}$$

beschreibt die Einschränkung von $Gal(K(N) \mid K)$ auf $Gal(\overbrace{K(N) \cap K(\delta)}^{=K(\delta^{h_0})} \mid K)$, d.h. für $\sigma_a \in Gal(K(N) \mid K)$ gilt: $\sigma_a\left(\delta^{h_0}\right) = \left(\chi_{\underline{k}}(a)\right)^{h_0} \cdot \delta^{h_0}$, wobei $\chi_{\underline{k}}$ wie in Definition 3.11.

Beweis:
Betrachten wir

$$\begin{aligned} \chi_{\underline{k}} : \ (A/N)^* &\longrightarrow \mathbb{F}_q^* \\ a &\longmapsto \chi_{\underline{k}}(a) := \prod_{1 \le j \le s'} \nu_j(\bar{a_j})^{k_j}, \end{aligned}$$

dann wissen wir nach Satz 3.12:

$$\sigma_a \underbrace{\left((-1)^{\sum\limits_{1 \le j \le s'} d_j k_j} \cdot \sqrt[q-1]{\prod_{1 \le j \le s'} P_j^{k_j}} \right)}_{=:G_{\underline{k}}} = \chi_{\underline{k}}(a) \cdot G_{\underline{k}}.$$

Somit erhalten wir:

$$\begin{aligned} \sigma_a\left(\delta^{h_0}\right) &= \sigma_a\left(\left(\sqrt[q-1]{c^{k_0} \cdot \prod_{1 \le j \le s'} P_j^{k_j}} \right)^{h_0} \cdot \left(\sqrt[q-1]{\prod_{s' < j \le s} P_j^{k_j}} \right)^{h_0} \right) \\ &= \sigma_a\left(\sqrt[q-1]{c^{k_0 h_0} \cdot \prod_{1 \le j \le s'} P_j^{k_j h_0}} \right) \cdot \sigma_a\left(\sqrt[q-1]{\prod_{s' < j \le s} P_j^{k_j h_0}} \right) \\ &\underset{\substack{\\ \forall s' < j \le s}}{\overset{k_j h_0 \equiv 0 \ (q-1)}{=}} \sigma_a\left(\sqrt[q-1]{c^{k_0 h_0} \cdot \prod_{1 \le j \le s'} P_j^{k_j h_0}} \right) \cdot \left(\sqrt[q-1]{\prod_{s' < j \le s} P_j^{k_j h_0}} \right) \\ &= \sigma_a\left(G_{\underline{k}}^{h_0}\right) \cdot \left(\sqrt[q-1]{\prod_{s' < j \le s} P_j^{k_j h_0}} \right) = \sigma_a\left(G_{\underline{k}}\right)^{h_0} \cdot \left(\sqrt[q-1]{\prod_{s' < j \le s} P_j^{k_j h_0}} \right) \\ &= \left(\chi_{\underline{k}}(a)\right)^{h_0} \cdot \underbrace{G_{\underline{k}}^{h_0} \cdot \left(\sqrt[q-1]{\prod_{s' < j \le s} P_j^{k_j h_0}} \right)}_{=\delta^{h_0}} = \left(\chi_{\underline{k}}(a)\right)^{h_0} \cdot \delta^{h_0}. \end{aligned}$$

□

4.8 Satz.

$$\begin{aligned} Gal(L \mid K) &= \{(\sigma_a, \sigma_\omega) \in (A/N)^* \times \mu_h \mid \varphi(a) = \psi(\omega)\} \\ &= \left\{(\sigma_a, \sigma_\omega) \in (A/N)^* \times \mu_h \mid \left(\chi_{\underline{k}}(a)\right)^{h_0} = \omega^{h_0}\right\}, \end{aligned}$$

wobei $h_0 := [K(\delta) : K(N) \cap K(\delta)]$ gegeben ist durch Korollar 4.5 und die Abbildungen ψ und φ gegeben sind durch Lemma 4.6 bzw. Lemma 4.7.

Beweis:
Folge aus Lemma 4.6 und Lemma 4.7.

□

4.9 Korollar.

Seien N und Δ wie zu Beginn des Kapitels festgelegt, dann gilt:

$$t := \#Gal\left(L \mid K^{(\Delta)}(N)\right) = h_0 \cdot ggT\left(\frac{h}{h_0}, \sum_{1\leq j\leq s'} k_j d_j - 1\right),$$

wobei $d_j = deg(P_j)$.

Beweis:
Nach Lemma 2.4 gilt für $(\sigma_a, \sigma_\omega) \in Gal(L \mid K)$:

$(\sigma_a, \sigma_\omega) \in Gal\left((L \mid K^{(\Delta)}(N)\right) \Longleftrightarrow a = \omega$. Mit Satz 4.8 folgt:

$$Gal\left(L \mid K^{(\Delta)}(N)\right) = \left\{(\sigma_\omega, \sigma_\omega) \in (A/N)^* \times \mu_h \mid \left(\chi_{\underline{k}}(\omega)\right)^{h_0} = \omega^{h_0},\ \omega \in \mu_h\right\},$$

wobei $\underline{k} := (k_1, \ldots, k_{s'}) \in \mathbb{N}^{s'}$

Wir müssen also die Bedingung $\left(\chi_{\underline{k}}(\omega)\right)^{h_0} = \omega^{h_0}$ für $\omega \in \mu_h$ untersuchen:

$$\left(\chi_{\underline{k}}(\omega)\right)^{h_0} = \omega^{\left(\sum_{j=1}^{s'} k_j \frac{q^{d_j}-1}{q-1}\right)\cdot h_0} = \omega^{h_0}$$

$$\Leftrightarrow \omega^{\sum_{j=1}^{s'} k_j d_j h_0} = \omega^{h_0}$$

$$\Leftrightarrow \omega^{\sum_{j=1}^{s'} k_j d_j h_0 - h_0} = 1$$

Nach Lemma 3.5 gibt es genau $ggT\left(h, \sum_{1\leq j\leq s'} k_j d_j h_0 - h_0\right) = h_0 \cdot ggT\left(\frac{h}{h_0}, \sum_{1\leq j\leq s'} k_j d_j - 1\right)$ Elemente $\omega \in \mu_h$, welche diese Bedingung erfüllen.

□

4.10 Proposition.

Seien $N = \prod_{1\leq i\leq r} Q_i^{n_i} \in A$ und $\Delta = c^{k_0} \prod_{1\leq j\leq s'} P_j^{k_j} \prod_{s'<j\leq s} P_j^{k_j} \in A \setminus \{0\}$

mit $d_j := deg(P_j)$ wie zu Beginn des Kapitels festgelegt, dann gilt:
Der Defekt des Torsionskörpers $K^{(\Delta)}(N) \mid K$ ist $ggT\left(\frac{h}{h_0}, \sum_{1\leq j\leq s'} k_j d_j - 1\right)$,

wobei $h := [K(\delta) : K]$ gegeben ist durch Lemma 4.2 und
$h_0 := [K(\delta) : K(N) \cap K(\delta)]$ gegeben ist durch Korollar 4.5.

Beweis:
$\#Gal\left(K^{(\Delta)}(N) \mid K\right) = [K^{(\Delta)}(N) : K]$

$$= \frac{[K(N)(\delta) : K(N)] \cdot [K(N) : K]}{[K(N)(\delta) : K^{(\Delta)}(N)]}$$

$$= \frac{[K(\delta) : K(N) \cap K(\delta)] \cdot [K(N) : K]}{[K(N)(\delta) : K^{(\Delta)}(N)]}$$

$$= \#(A/N)^* \cdot \frac{h_0}{t}$$

$$\overset{Korollar\ 4.9}{=} \#(A/N)^* \cdot \frac{h_0}{h_0 \cdot ggT\left(\frac{h}{h_0}, \sum\limits_{1 \le j \le s'} k_j d_j - 1\right)}$$

$$= \#(A/N)^* \cdot \frac{1}{ggT\left(\frac{h}{h_0}, \sum\limits_{1 \le j \le s'} k_j d_j - 1\right)} \quad .$$

□

Proposition 4.10 liefert uns zwar eine Formel zur Berechnung des Defekts von $K^{(\Delta)}(N)$. Allerdings ist die Formel etwas unangenehm auszuwerten, da man jeweils noch die Größen h und h_0 ausrechnen muss. Daher wollen wir nun eine Formel finden, die leichter auszuwerten ist.

4.11 Lemma.

Es gilt $h = \dfrac{q-1}{ggT(k_0^*, k_1, \ldots, k_s, q-1)}$.

Beweis:
Nach Lemma 4.2 wissen wir: $h = \dfrac{q-1}{ggT(k_0, k_1, \ldots, k_s, q-1)}$.

Nach Definition von k_0^* gilt: $k_0^* := \begin{cases} k_0, & falls\ q\ gerade\ oder \sum\limits_{1\le j\le s'} d_j k_j\ gerade \\ k_0 + \frac{q-1}{2}, & sonst \end{cases}$.

Falls $k_0^* = k_0$ ist, dann ist die Aussage des Lemmas trivial, also nehmen wir an: $q\ ungerade\ und \sum\limits_{1\le j\le s'} d_j k_j\ ungerade$ und somit $k_0^* = k_0 + \frac{q-1}{2}$. Außerdem können wir oBdA annehmen, dass $k_0, k_1, \ldots, k_s \le q-1$ gilt. Wegen der Annahme, dass $\sum\limits_{1\le j\le s'} d_i k_i\ ungerade$ ist, gibt es ein l zwischen 1 und s', so dass $k_l \equiv 1\ (mod\ 2)$. Daraus folgt: $ggT\,(q-1, k_1, \ldots, k_s)$ ist ein Teiler von $\dfrac{q-1}{2}$. Daher erhalten wir $ggT\left(q-1, k_1, \ldots, k_s, k_0 + \frac{q-1}{2}\right) = ggT\,(q-1, k_1, \ldots, k_s, k_0)$.

□

4.12 Lemma.

Die Situation sei wie immer in Kapitel 4, dann gilt:

$$ggT\left(\frac{h}{h_0}, \sum_{1\le j\le s'} k_j d_j - 1\right) = ggT\,(d-1, q-1, k_0^*, k_{s'+1}, \ldots, k_s),$$

wobei $d := deg(\Delta)$.

Beweis:
(i) Wir wollen zunächst zeigen: $ggT\left(\dfrac{h}{h_0}, \sum\limits_{1\le j\le s'} k_j d_j - 1\right) \ge ggT\,(d-1, q-1, k_0^*, k_{s'+1}, \ldots, k_s)$.

Sei dazu $ggT\,(d-1, q-1, k_0^*, k_{s'+1}, \ldots, k_s) = l$, dann gilt:

$$\sum_{1\le j\le s'} k_j d_j - 1 = \underbrace{d-1}_{Vielfaches\ von\ l} - \underbrace{\sum_{s'<j\le s} k_j d_j}_{Vielfaches\ von\ l}.$$

$\Longrightarrow \sum\limits_{1\le j\le s'} k_j d_j - 1$ ist ein Vielfaches von l.

Wenn wir nun zeigen können, dass auch h/h_0 ein Vielfaches von l ist, ist (i) bewiesen. h/h_0 können wir unter Beachtung von Lemma 4.11 folgendermaßen schreiben:

$$\frac{h}{h_0} = \frac{ggT\,(k_0^*, k_{s'+1}, \ldots, k_s, q-1)}{ggT(k_0^*, k_1, \ldots, k_s, q-1)} = \frac{\alpha \cdot l}{ggT(k_0^*, k_1, \ldots, k_s, q-1)}$$

für $\alpha \in \mathbb{N}$ geeignet gewählt.

Wir wissen: $\sum_{1\le j\le s'} k_j d_j \equiv 1\ (l).$ $\qquad (\#)$

Machen wir nun die Annahme: h/h_0 ist kein Vielfaches von l,
dann bedeutet dies:
$ggT(k_0^*, k_1, \ldots, k_s, q-1)$ enthält einen Primfaktor p von l, der nicht in α vorkommt.
$\Longrightarrow\ p \mid k_j$ für alle $1 \le j \le s'$, d.h. k_j =Vielfaches von p für alle $1 \le j \le s'$. Sei also $k_j = \beta_j p\ \ (\beta_j \in \mathbb{N})$, dann gilt aber:

$$\sum_{1\le j\le s'} k_j d_j = \sum_{1\le j\le s'} \beta_j p d_j = p \cdot \underbrace{\sum_{1\le j\le s'} \beta_j d_j}_{\in\mathbb{N}} \not\equiv 1\ (l)\ ,$$

da p ein Primteiler von l.

Dies liefert einen Widerspruch zu $(\#)$, also ist h/h_0 ein Vielfaches von l.

(ii) Nun zeigen wir: $ggT\left(\frac{h}{h_0}, \sum_{1\le j\le s'} k_j d_j - 1\right) \le ggT\,(d-1, q-1, k_0^*, k_{s'+1}, \ldots, k_s)$:

Sei $ggT\left(\frac{h}{h_0}, \sum_{1\le j\le s'} k_j d_j - 1\right) = l.$
$\Longrightarrow h/h_0$ ist ein Vielfaches von l.

$$\Longrightarrow ggT\,(k_0^*, k_{s'+1}, \ldots, k_s, q-1) = \underbrace{\frac{h}{h_0}}_{Vielf.\ von\ l} \cdot ggT(k_0^*, k_1, \ldots, k_s, q-1)$$

ist Vielfaches von l. Außerdem gilt:

$$d-1 = \underbrace{\sum_{1\le j\le s'} k_j d_j - 1}_{Vielf.\ von\ l} + \underbrace{\sum_{s'<j\le s} k_j d_j}_{Vielfaches\ von\ l}\ .$$

$\Longrightarrow d-1$ ist ein Vielfaches von l.

Also erhalten wir insgesamt $ggT\,(d-1, q-1, k_0^*, k_{s'+1}, \ldots, k_s) \ge l$.
Aus (i) und (ii) folgt die Behauptung des Lemmas.

□

Nun sind wir in der Lage das Hauptresultat der Arbeit zu formulieren:

4.13 Satz.

Die Situation sei wie immer in Kapitel 4, dann gilt:

Der Defekt des Torsionskörpers $K^{(\Delta)}(N) \mid K$ ist $ggT\,(d-1, q-1, k_0^*, k_{s'+1}, \ldots, k_s)$, wobei $d := deg(\Delta)$.

Beweis: Direkte Folge aus Proposition 4.10 und Lemma 4.12.

□

Der Formel in Satz 4.13 sieht man an, dass der Defekt in den meisten Fällen Eins ist. Zum Abschluss wollen wir daher noch ein Beispiel angeben, wo der Defekt größtmöglich ist.

4.14 Beispiel.

Sei $q = 19$, $N = Q_1^{n_1} \cdot \ldots \cdot Q_5^{n_5} \in A$ mit $n_i \in \mathbb{N}$ für alle $1 \leq i \leq 5$, und $deg(Q_1) = 3$, $deg(Q_5) = 2$, $deg(Q_j) = m_j \in \mathbb{N}$ $(2 \leq j \leq 4)$.

Weiter sei $\Delta = -Q_1^3 \cdot Q_5^5 \cdot R_1^{18} \cdot R_2^{18}$, wobei $R_1, R_2 \in A$ prim sind mit $R_1, R_2 \nmid N$ und $deg(R_l) = r_l \in \mathbb{N}$ $(l = 1, 2)$.

Es gilt also : $k_0^* = k_0 + \frac{q-1}{2} = \frac{q-1}{2} + \frac{q-1}{2} = q - 1 = 18$.
Nun können wir den Defekt von $K^{(\Delta)}(N) \mid K$ mit Satz 4.13 berechnen:
Defekt von $K^{(\Delta)}(N) = ggT\,(deg(\Delta) - 1, 18)$

$$= ggT\,(19 + 18(r_1 + r_2) - 1, 18)$$

$$= ggT\,(18(r_1 + r_2 + 1), 18) = 18.$$

Symbolverzeichnis

A	$\mathbb{F}_q[T]$, Polynomring über $\mathbb{F}_q$ in der Unbestimmten T
C	Carlitz-Modul, S.6-7
$\mathbb{F}_q$	endlicher Körper mit q Elementen
$G_{\underline{m}}$	S.17
h	$[K(\delta) : K]$, S.24
h_0	$[K(\delta) : K(N) \cap K(\delta)]$, S.24
K	$\mathbb{F}_q(T)$, Quotientenkörper von A
$\overline{K}$	algebraischer Abschluss von K
$K\{\tau\}$	getwisteter Polynomring, S.6
$K(N)$	Torsionskörper von Carlitz-Modul, S.7
$K^{(\Delta)}(N)$	Torsionskörper von getwistetem Carlitz-Modul, S.7
L	$K(N)(\delta)$, S.13
t	$[K(N)(\delta) : K^{(\Delta)}(N)]$, S.31
δ	$\sqrt[q-1]{\Delta}$, S.12
$\Phi^{(\Delta)}$	getwisteter Carlitz-Modul, S.6-7
${}_N\Phi^{(\Delta)}$	N-Torsion von $\Phi^{(\Delta)}$, S.7
${}_NC$	N-Torsion von C, S.7

Literaturverzeichnis

[Bos09]: S.Bosch, *Algebra,* Springer-Verlag*, 2009*

[Geb03]: M.Gebhardt, *Galoisdarstellungen auf den Torsionspunkten von Drinfeld-Moduln des Rangs zwei*, Dissertation, Saarbrücken, 2003

[Gos96]: D.Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag, 1996

[Hay74]: D.Hayes, *Explicit class field theory for rational function fields*, Trans.Amer.Math.Soc. 189(1974), 77-91

[Lan02]: S.Lang, *Algebra*, Revised Third Edition, Graduate Texts in Mathematics 211, Springer-Verlag, 2002

[Ros02]: M.Rosen, *Number Theory in Function Fields*, Springer-Verlag, 2002

[Tha04]: D.S.Thakur, *Function Field Arithmetic*, World Scientific, 2004