Zur Struktur der Einheitengruppen von Quaternionenalgebren über Laurentreihenkörpern

Diplomarbeit*

Jochen Frieden

Saarbrücken, Mai 1998
Fachbereich 9, Mathematik

*Original mit korrigierten Druckfehlern

Ich erkläre hiermit an Eides statt, diese Arbeit selbständig geschrieben und keine Hilfsmittel außer den angegebenen verwendet zu haben.

Inhaltsverzeichnis

Kapitel 0

Einleitung

Für den Laurentreihenkörper $L = \{\sum_{i=m}^{\infty} a_i T^i \mid m \in \mathbb{Z}, a_m, a_{m+1}, \ldots \in \mathbb{F}_q\}$ über dem endlichen Körper $\mathbb{F}_q$ mit $q = p^h$ Elementen gibt es bekanntlich bis auf Isomorphie eine eindeutig bestimmte Quaternionendivisionsalgebra Q über L, wobei sich Q realisieren läßt durch

$$Q := \{\sum_{i=m}^{\infty} a_i \tau^i \mid m \in \mathbb{Z}, a_m, a_{m+1}, \ldots \in \mathbb{F}_{q^2}\}.$$

Dabei ist die Multiplikation auf Q durch die Vorschrift $\tau a = a^q \tau$ für alle $a \in \mathbb{F}_{q^2}$ eindeutig festgelegt. Die Einbettung von L in Q erfolgt durch die Identifikation von T mit τ^2. Für die reduzierte Norm $N = N_Q^L$ gilt dann $N(x) = x\bar{x}$, wobei $\bar{x} = \sum_{i=m}^{\infty} (-1)^i a_i^{q^{i+1}} \tau^i$ für alle $x = \sum_{i=m}^{\infty} a_i \tau^i \in Q$ ist. Ferner ist Q ein lokaler Schiefkörper mit der Uniformisierenden τ. Als Bewertungsring erhält man $B := \{\sum_{i=0}^{\infty} a_i \tau^i \mid a_0, a_1, \ldots \in \mathbb{F}_{q^2}\}$ mit der Einheitengruppe $U := \{\sum_{i=0}^{\infty} a_i \tau^i \mid a_0, a_1, \ldots \in \mathbb{F}_{q^2} \ \ mit \ \ a_0 \neq 0\}$ und dem maximalen Ideal $\mathfrak{m} := \{\sum_{i=1}^{\infty} a_i \tau^i \mid a_1, a_2, \ldots \in \mathbb{F}_{q^2}\}$. Die n-te Einseinheitengruppe ist $U_n := \{1 + \sum_{i=n}^{\infty} a_i \tau^i \mid a_n, a_{n+1}, \ldots \in \mathbb{F}_{q^2}\}$.

Es stellt sich nun die Frage, wie die Struktur der multiplikativen Gruppe Q^* aussieht. Da sich Q^* als semidirektes Produkt der Einheitengruppe U und $(\mathbb{Z}, +)$ auffassen läßt, besteht ein besonderes Interesse an der Struktur von U. Allgemein ist bekannt, daß man alle $x \in U$ als unendliches Produkt der Form

$$x = a_0(1 + a_1\tau^1)(1 + a_2\tau^2)(1 + a_3\tau^3) \cdot \ldots$$

mit $a_0 \in \mathbb{F}_{q^2}^*$ und $a_1, a_2, \ldots \in \mathbb{F}_{q^2}$ auffassen kann. Außerdem ist bekannt, daß für alle $i, j \in \mathbb{N}$ die Kommutatorrelationen $[U_i, U_j] \subset U_{i+j}$ gelten (siehe dazu [14]). Danaben gibt es Arbeiten, die sich mit den irreduziblen Darstellungen der multiplikativen Gruppe einer beliebigen zentralen Divisionsalgebra A mit endlichem Index über einem lokalen Körper K befassen. Dabei sind vor allem solche Darstellungen von Interesse, die auf kleinen Einseinheiten von A ebenso wie auf der Uniformisierenden von K trivial werden. Übertragen auf die Situation der Quaternionenalgebra Q über dem Laurentreihenkörper L bedeutet dies, daß man irreduzible unitäre Darstellungen von Q^* betrachtet, die auf Untergruppen der Form $< \tau^2 > U_n$ trivial werden. Diese entsprechen den Darstellungen auf den endlichen Faktorgruppen $Q^*/(< \tau^2 > U_n)$. Die Klassenzahl dieser Faktorgruppen ist bekannt und lautet

$$(q-1)\left(\frac{1}{2}(q+1)q^{2\left[\frac{n-1}{2}\right]} + 2q^{n-1} - \frac{1}{2}q^{\left[\frac{n-1}{2}\right]}\right)$$

(siehe dazu [8]).

In dieser Arbeit werden nun die Faktorgruppen $G_n := U/U_n$ untersucht, die sich als Untergruppen von den $Q^*/(< \tau^2 > U_n)$ auffassen lassen. Für alle $n \in \mathbb{N}$ werden dazu die Konjugationsklassen von G_n und deren Länge bestimmt. Außerdem wird gezeigt, daß alle G_n auflösbar sind, und deren auflösbare Länge bestimmt.

In Kapitel 1 wird zunächst das Lösungsverhalten einiger polynomialer Gleichungen auf dem Restkörper $\mathbb{F}_{q^2}$ bestimmt. Weiter werden einige grundlegende Dinge über Quaternionenalgebren und Bewertungen sowie deren Bedeutung für L und Q besprochen. Allgemein ist für einen beliebigen diskret bewerteten Divisionsring D die Folge der Einseinheitengruppen $\{U_D^n\}$ eine absteigende Folge von Normalteilern. Die Faktorgruppen bilden in natürlicher Weise ein projektives System. Für den Fall, daß D vollständig ist, wird gezeigt, daß der projektive Limes dieses Systems isomorph zur Einheitengruppe U_D ist. Das bedeutet, daß sich die Struktur U_D vollständig über die Struktur der Faktorgruppen G_D^n beschreiben läßt und man sich auf deren Untersuchung beschränken kann.

In Kapitel 2 wird auf diese Weise die Einheitengruppe U_L des Laurentreihenkörpers L bestimmt. Da die Faktorgruppen G_L^n alle endlich und kommutativ sind, lassen sie sich vollständig in zyklische Anteile zerlegen. Das Ergebnis lautet

$$G_L^n \cong \mathbb{Z}/(q-1)\mathbb{Z} \times \prod_{k=1}^{h} \left(\prod_{\substack{j=1 \\ p \nmid j}}^{n-1} \left(\mathbb{Z}/p^{M(j,n)}\mathbb{Z}\right)_j \right)_k$$

mit $M(j,n) := \max\{l \in \mathbb{N}_0 \mid jp^{l-1} \leq n-1\}$. Für die Einheitengruppe erhält man

$$U_L \cong \mathbb{Z}/(q-1)\mathbb{Z} \times \prod_{k=1}^{h} \left(\prod_{\substack{j=1 \\ p \nmid j}}^{\infty} (\mathbb{Z}_p)_j \right)_k ,$$

wobei $\mathbb{Z}_p$ die p-adische Vervollständigung von $\mathbb{Z}$ bezeichnet. Damit ist die Struktur der Einheitengruppe U_L vollständig bestimmt. Darüberhinaus läßt sich die Einseinheitengruppe U_L^1 als $\mathbb{Z}_p$-Modul auffassen, wobei hier die Isomorphie

$$U_L^1 \cong \prod_{k=1}^{h} \left(\prod_{\substack{j=1 \\ p \nmid j}}^{\infty} (\mathbb{Z}_p)_j \right)_k$$

gilt.

In Kapitel 3 wird nun die Konjugationsklasseneinteilung der Faktorgruppen G_n bestimmt. Zunächst ist zu bemerken, daß

$$V_n := \{\sum_{i=0}^{n-1} a_i \tau^i \mid a_0, a_1, \ldots \in \mathbb{F}_{q^2} \;\; mit \;\; a_0 \neq 0\} \subset U$$

ein Repräsentantensytem für die Restklassen von G_n ist. Es geht nun darum, eine Teilmenge $V_n^* \subset V_n$ anzugeben, so daß $G_n = \biguplus_{x \in V_n^*} [x]_n$ gilt. Dabei bezeichnet $[x]_n$ die Konjugationsklasse von xU_n in G_n. Um das Ergebnis von Kapitel 3 formulieren zu können, benötigt man zunächst

- ein Repräsentantensystem $\{\alpha_1, \ldots, \alpha_{q-1}\}$ der multiplikativen Faktorgruppe $\mathbb{F}_{q^2}^*/\mathbb{S}_{q^2}$, wobei $\mathbb{S}_{q^2} :=< \alpha^{q-1} >\subset \mathbb{F}_{q^2}^*$ und α ein zyklischer Erzeuger der multiplikativen Gruppe $\mathbb{F}_{q^2}^*$ ist,
- ein Repräsentantensystem $\{\beta_1, \ldots, \beta_q\}$ der additiven Faktorgruppe $\mathbb{F}_{q^2}/(\alpha - \alpha^q)\mathbb{F}_q$ sowie
- ein Repräsentantensystem $\{\gamma_1^{(k)}, \ldots, \gamma_q^{(k)}\}$ der additiven Faktorgruppe $\mathbb{F}_{q^2}/\alpha^k(\alpha - \alpha^q)\mathbb{F}_q$ für alle $k = 1, \ldots, q-1$.

Weiter sei im folgenden $g(n)$ bzw. $u(n)$ die größte gerade bzw. ungerade ganze Zahl, die echt kleiner als n ist. Außerdem setze man

$$V_n' := \{\alpha_k + \sum_{i=2}^{g(n)}{}'' \beta_{l_i} \tau^{i-1} + \sum_{i=3}^{u(n)}{}' \gamma_{l_i}^{(k)} \tau^{i-1} \mid k \in \{1, \ldots, q-1\}, l_i \in \{1, \ldots, q\} \;\; für \;\; i = 2, \ldots, n-1\}.$$

Dabei gibt $\sum''$ bzw. $\sum'$ die Summation über jeweils nur gerade bzw. nur ungerade Indizes an. Man setze nun

$$V_n^{(0)} := \{\sum_{i=0}^{g(n)}{}'' a_i\tau^i \mid a_0, a_2, \ldots, a_{g(n)} \in \mathbb{F}_{q^2} \;\; mit \;\; a_0 \notin \mathbb{F}_q\}.$$

Weiter definiere man für alle $m \in \{1, \ldots, n\}$ und $a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q$ mit $a_0 \neq 0$ die Mengen

$$V_n^{(m)}(a_0, a_2, \ldots, a_{g(m)}) := \sum_{i=0}^{g(m)}{}'' a_i\tau^i + \begin{cases} V_{n-m}^{(0)}\tau^m & \text{falls } m \text{ gerade und } m \neq n \\ V'_{n-m+1}\tau^m & \text{falls } m \text{ ungerade und } m \neq n \\ \{0\} & \text{falls } m = n. \end{cases}$$

Damit erhält man das folgende Repräsentantensystem für die Einteilung von G_n in Konjugationsklassen

$$V_n^* := V_n^{(0)} \uplus \biguplus_{m=1}^{n} \left(\biguplus_{\substack{a_0, a_2, \ldots, a_{g(n)} \in \mathbb{F}_q \\ mit \;\; a_0 \neq 0}} V_n^{(m)}(a_0, a_2, \ldots, a_{g(m)}) \right).$$

Bezüglich der Länge der einzelnen Konjugationsklassen wird folgendes Ergebnis gezeigt. Seien $m \in \{0, \ldots, n\}$ und $a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q$ mit $a_0 \neq 0$. Dann haben alle Konjugationsklassen $[x]_n$ mit $x \in V_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$ die gleiche Länge, und zwar

$$\#[x]_n = \begin{cases} q^{2(n-m)-g(n-m)-2} & \text{falls } m \text{ gerade und } m \neq n \\ (q+1)q^{n-m-1} & \text{falls } m \text{ ungerade und } m \neq n \\ 1 & \text{falls } m = n. \end{cases}$$

Durch eine einfache Kardinalitätsbetrachtung von V_n^* läßt sich nun die Klassenzahl s_n von G_n bestimmen. Es gilt

$$s_n = (q-1) \begin{cases} 2q^{n-1} + q^{n-2} - q^{\frac{1}{2}n-1} & \text{falls } n \text{ gerade} \\ q^n + 2q^{n-1} - q^{\frac{1}{2}n-\frac{1}{2}} & \text{falls } n \text{ ungerade.} \end{cases}$$

In Kapitel 4 werden für den Kommutator von U die Identitäten $[U, U] = \{xyx^{-1}y^{-1} \mid x, y \in U\}$ und $[U, U] = \{x \in U_1 \mid N(x) = 1\}$ gezeigt. Während die erste Identität nur von theoretischem Interesse ist, stellt die zweite Identität eine vollständige Charakterisierung von $[U, U]$ dar. Für ein beliebiges $x \in U$ liefert die Bedingung $\mathrm{N}(x) = 1$ ein leicht lösbares Gleichungssystem für die Koeffizienten von x. Somit erhält man ein Kriterium, mit dem man leicht entscheiden kann, ob ein $x \in U$ in $[U, U]$ liegt. Außerdem wird für alle $i, j \in \mathbb{N}_0$ die Kommutatorrelation $[U_i, U_j] = [U, U] \bigcap U_{m_0}$ für alle $i, j \in \mathbb{N}_0$ hergeleitet, wobei

$$m_0 := \left\{ \begin{array}{ll} i+j & \text{falls } i \text{ oder } j \text{ ungerade} \\ i+j+1 & \text{falls } i \text{ und } j \text{ gerade} \end{array} \right\}$$

ist. Damit erhält man insgesamt eine vollständige Charakterisierung aller Kommutatorgruppen der Form $[U_i, U_j]$.

In Kapitel 5 wird für den Fall, daß q ungerade ist, die Relation

$$\left[[U,U]\bigcap U_i,[U,U]\bigcap U_j\right]=[U_i,U_j]$$

hergeleitet. Damit läßt sich nun für alle $n\in\mathbb{N}_0$ sowohl die abgeleitete Reihe als auch die absteigende Zentralreihe von U_n explizit angeben. Das wichtigste Ergebnis ist dabei die abgeleitete Reihe von U. Man erhält $D^k(U)=[U,U]\bigcap U_{f_q(k)}$, wobei $f_q(k):=\frac{2^{k+1}}{3}-\frac{1}{2}-\frac{(-1)^k}{6}$ ist. Daraus läßt sich die auflösbare Länge l von G_n durch die Bedingung $f_q(l-1)<n\leq f_q(l)$ eindeutig bestimmen. Für große $n\in\mathbb{N}$ gilt näherungsweise $l(n)=\left\lceil\frac{\ln(3n)}{\ln(2)}\right\rceil$.

Das Kapitel 6 befaßt sich ausschließlich mit dem Fall q gerade. Die Charakterisierung der abgeleiteten Reihe sowie der absteigenden Zentralreihe der Einseinheitengruppen U_n bereitet erheblich mehr Schwierigkeiten als im Fall q ungerade. Hierzu wird der Begriff der „gutartigen" Untergruppe von $[U,U]$ eingeführt. Dabei handelt es sich um Untergruppen $\mathfrak{U}$ von $[U,U]$, die sich durch die Angabe einer ungeraden Zahl $R(\mathfrak{U})$ und einer geraden Zahl $S(\mathfrak{U})$ (sog. Charakterisierungsindizes) so gut beschreiben lassen, daß die Faktorgruppen $\mathfrak{U}\cdot U_n/U_n$ eindeutig bestimmt sind. Das heißt, wenn $\mathfrak{U},\mathfrak{V}\leq[U,U]$ gutartig sind mit $R(\mathfrak{U})=R(\mathfrak{V})$ und $S(\mathfrak{U})=S(\mathfrak{V})$, dann folgt schon $\mathfrak{U}\cdot U_n/U_n=\mathfrak{V}\cdot U_n/U_n$ für alle $n\in\mathbb{N}$. Das Minimum $\min\{R(\mathfrak{U}),S(\mathfrak{U})\}$ gibt die größte natürliche Zahl an, für die $U_n\subset\mathfrak{U}$ gilt. Es wird gezeigt, daß alle Untergruppen der Form $[U,U]\bigcap U_n$ gutartig sind, und deren Charakterisierungsindizes bestimmt. Weiter wird gezeigt, daß für alle gutartigen $\mathfrak{U},\mathfrak{V}\leq[U,U]$ der Kommutator $[\mathfrak{U},\mathfrak{V}]$ wieder gutartig ist, und angegeben, wie die Charakterisierungsindizes von $[\mathfrak{U},\mathfrak{V}]$ aus denen von $\mathfrak{U}$ und $\mathfrak{V}$ berechnet werden können. Damit läßt sich nun zeigen, daß alle höheren Glieder der absteigenden Zentralreihe sowie der abgeleiteten Reihe von U_n gutartig und man kann die entsprechenden Charakterisierungsindizes berechnen. Daraus ergibt sich die auflösbare Länge von G_n. Um das Ergebnis anzugeben, ist es notwendig, die Fälle $q\neq 2$ und $q=2$ zu unterscheiden. Im Fall $q\neq 2$ ist die auflösbare Länge l von G_n eindeutig bestimmt durch die Bedingung $f_q(l-1)<n\leq f_q(l)$, wobei $f_q(k)$ für alle $k\in\mathbb{N}_0$ definiert ist durch $f_q(0):=0$, $f_q(1):=1$, $f_q(2):=2$ und

$$f_q(k):=\frac{8}{\sqrt{17}}\left(\left(\frac{1+\sqrt{17}}{2}\right)^{k-3}-\left(\frac{1-\sqrt{17}}{2}\right)^{k-3}\right)+\frac{6}{\sqrt{17}}\left(\left(\frac{1+\sqrt{17}}{2}\right)^{k-2}-\left(\frac{1-\sqrt{17}}{2}\right)^{k-2}\right)$$

falls $k\geq 3$. Für großes n gilt näherungsweise

$$l=\left\lceil\frac{\ln(3+\frac{11}{\sqrt{17}})-\ln(n)}{\ln(\frac{2}{1+\sqrt{17}})}+4\right\rceil.$$

Im Fall $q=2$ ist die auflösbare Länge l von G_n eindeutig bestimmt durch die Bedingung $f_q(l-1)<n\leq f_q(l)$, wobei $f_q(k)$ für alle $k\in\mathbb{N}_0$ definiert ist durch $f_q(0):=0$, $f_q(1):=1$, $f_q(2):=2$, $f_q(3):=9$,$f_q(4):=18$ und

$$f_q(k):=\frac{72}{\sqrt{17}}\left(\left(\frac{1+\sqrt{17}}{2}\right)^{k-5}-\left(\frac{1-\sqrt{17}}{2}\right)^{k-5}\right)+\frac{58}{\sqrt{17}}\left(\left(\frac{1+\sqrt{17}}{2}\right)^{k-4}-\left(\frac{1-\sqrt{17}}{2}\right)^{k-4}\right)$$

falls $k\geq 5$. Für großes n gilt näherungsweise

$$l=\left\lceil\frac{\ln(29+\frac{101}{\sqrt{17}})-\ln(n)}{\ln(\frac{2}{1+\sqrt{17}})}+6\right\rceil.$$

Es ist also gelungen, sowohl die Konjugationsklasseneinteilung als auch die auflösbare Länge von G_n explizit anzugeben. Damit stellt sich nun die Frage, inwiefern sich diese Ergebnisse verallgemeinern lassen und ob man mit den in dieser Arbeit entwickelten Methoden auch andere Fälle von getwisteten Laurentreihenkörpern untersuchen kann. Eventuell könnte diese Arbeit ein erster Schritt für die Beschreibung der Einheitengruppe eines beliebigen getwisteten Laurentreihenkörpers über einem endlichen Körper sein.

An dieser Stelle möchte ich mich bei allen bedanken, die mich beim Anfertigen dieser Diplomarbeit unterstützt haben. Als erstes ist Herr Prof. Dr. E.-U. Gekeler zu nennen, von dem ich von der Auswahl des Themas bis hin zur Lösung von formalen Problemen optimal betreut wurde. Dank gilt auch Herrn Dipl. Math. M. Gebhardt und Herrn Dipl. Math. B. Wack, die mich vor allem bei technischen Fragen berieten, sowie Herrn Dipl. Inf. O. Scheja, der mir vor allem bei inhaltlichen Fragen weiterhalf. Ferner möchte ich mich auch noch bei meinen Eltern dafür bedanken, daß sie mein Studium mitfinanziert und damit auch die Anfertigung dieser Arbeit in dieser Form ermöglicht haben. Schließlich ist noch zu erwähnen, daß ein Teil des Studiums mit öffentlichen Mitteln finanziert wurde.

Kapitel 1

Theoretische Grundlagen

1.0 Vereinbarungen

Für die gesamte vorliegende Arbeit seien $\mathbb{N} := \{1, 2, \ldots\}$ und $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$. Weiter sei vereinbart, daß die Symbole $\sum''$ bzw. $\sum'$ immer für die Summation über jeweils nur gerade bzw. ungerade Indizes stehen.

Mit $\mathbb{F}_q$ und $\mathbb{F}_{q^2}$ werden die endlichen Körper mit q bzw. q^2 Elementen bezeichnet. Dabei ist $q = p^h$ mit $h \in \mathbb{N}$ und $p \in \mathbb{P}$ (Menge aller Primzahlen). Zur Vereinfachung wird $\mathbb{F}_q$ als Teilmenge von $\mathbb{F}_{q^2}$ aufgefaßt. Ferner sei $\alpha \in \mathbb{F}_{q^2}$ stets ein festgewählter zyklischer Erzeuger der multiplikativen Gruppe, d.h. $\langle \alpha \rangle = \mathbb{F}_{q^2}^*$. In der gesamten Arbeit steht für einen beliebigen Ring R das Symbol R^* zur Kennzeichnung seiner multiplikativen Gruppe.

Weiter sei $Q := \{\sum_{i=m}^{\infty} a_i \tau^i \mid m \in \mathbb{Z}, a_m, a_{m+1}, \ldots \in \mathbb{F}_{q^2}\}$. Die Addition auf Q sei komponentenweise und die Multiplikation erklärt durch

$$\left(\sum_{i=m}^{\infty} a_i \tau^i\right)\left(\sum_{i=n}^{\infty} b_i \tau^i\right) := \sum_{i=m+n}^{\infty} \left(\sum_{k=m}^{i-n} a_k b_{i-k}^{q^k}\right) \tau^i.$$

Man beachte, daß $a \longmapsto a^{q^k}$ für alle $k \in \mathbb{N}_0$ ein Isomorphismus auf $\mathbb{F}_{q^2}$ ist und $a^{q^k} = a$ bzw. $a^{q^k} = a^q$ gilt, falls k gerade bzw. ungerade ist. Für $k \in \mathbb{Z}$ mit $k < 0$ und $a \in \mathbb{F}_q$ sei a^{q^k} erklärt durch $a^{q^k} := a^{q^{-k}}$. Man kann nun elementar nachrechnen, daß Q mit der eben erklärten Addition und Multiplikation einen nullteilerfreien Ring bildet. Später wird noch gezeigt, daß jedes von 0 verschiedene Element invertierbar und somit Q ein Schiefkörper ist. Es handelt sich hierbei um einen sogenannten *getwisteten Laurentreihenschiefkörper über* $\mathbb{F}_{q^2}$. Weiter sei $T := \tau^2$ und $L := \{\sum_{i=m}^{\infty} a_i T^i \mid m \in \mathbb{Z}, a_m, a_{m+1}, \ldots \in \mathbb{F}_q\} \subset Q$ definiert. Die Addition auf Q bedingt eine komponentenweise Addition auf L, und die Multiplikation auf L bekommt die Form

$$\left(\sum_{i=m}^{\infty} a_i T^i\right)\left(\sum_{i=n}^{\infty} b_i T^i\right) = \sum_{i=m+n}^{\infty} \left(\sum_{k=m}^{i-n} a_k b_{i-k}\right) T^i.$$

Es läßt sich nun wieder elementar nachrechnen, daß L ein Körper ist. In der Literatur wird L als der *Laurentreihenkörper über* $\mathbb{F}_q$ bezeichnet. Wegen der komponentenweisen Addition haben Q und L die selbe Charakteristik wie $\mathbb{F}_q$, nämlich p.

1.1 Die Körpererweiterung $\mathbb{F}_{q^2} \supset \mathbb{F}_q$

In diesem Abschnitt geht es darum, eine geeignete Basis von $\mathbb{F}_{q^2}$ als $\mathbb{F}_q$-Vektorraum zu finden und mit Hilfe dieser Basis das Lösungsverhalten von Gleichungen zu bestimmen, die für die späteren Betrachtungen wichtig sind.

Lemma 1.1.1 *Für alle $a \in \mathbb{F}_{q^2}$ gilt $a^{q+1}, a^q + a, (a - a^q)^2 \in \mathbb{F}_q$.*

Beweis: Es gilt $(a^{q+1})^q = a^{q^2+q} = a^{q+1}$ und $(a + a^q)^q = a^q + a^{q^2} = a + a^q$. Daraus folgt $a^{q+1}, a + a^q \in \mathbb{F}_q$. Weiter gilt $(a - a^q)^2 = a^2 + (a^2)^q - 2a^{q+1}$. Wegen $a^{q+1}, a^2 + (a^2)^q \in \mathbb{F}_q$ erhält man auch $(a - a^q)^2 \in \mathbb{F}_q$. □

Lemma 1.1.2 *Die Menge $\{\alpha, \alpha^q\}$ ist eine $\mathbb{F}_q$-Basis von $\mathbb{F}_{q^2}$.*

Beweis: Da $\mathbb{F}_{q^2}$ den Grad 2 über $\mathbb{F}_q$ hat, ist lediglich zu zeigen, daß $\{\alpha, \alpha^q\}$ über $\mathbb{F}_q$ linear unabhängig ist. Angenommen, die Menge $\{\alpha, \alpha^q\}$ wäre $\mathbb{F}_q$-linear abhängig. Dann folgte $\alpha(\alpha^q)^{-1} = \alpha^{1-q} \in \mathbb{F}_q$ und damit $(\alpha^{(q-1)})^q = \alpha^{1-q}$. Daraus ergäbe sich $\alpha^{q-1} = \alpha^{1-q}$ und daraus wiederum $\alpha^{2(q-1)} = 1$. Dies steht aber wegen $q^2 - 1 = (q+1)(q-1) > 2(q-1)$ im Widerspruch zur Zyklizität der multiplikativen Gruppe $\mathbb{F}_{q^2}^*$. □

Sei $a = a_1\alpha + a_2\alpha^q \in \mathbb{F}_{q^2}$ mit $a_1, a_2 \in \mathbb{F}_q$ beliebig. Dann gilt $a^q = a_2\alpha + a_1\alpha^q$. Unter dem Automorphismus $a \longmapsto a^q$ werden also lediglich die Koordinaten a_1 und a_2 vertauscht.

Für den Fall, daß q ungerade und damit $\mathrm{char}(\mathbb{F}_{q^2}) \neq 2$ ist, liegt $\alpha - \alpha^q$ außerhalb von $\mathbb{F}_q$. Folglich ist $\{1, \alpha - \alpha^q\}$ eine $\mathbb{F}_q$- Basis von $\mathbb{F}_{q^2}$. Bei dieser Basis bleibt die 1 unter dem Automorphismus $a \longmapsto a^q$ invariant, während sich bei $\alpha - \alpha^q$ nur das Vorzeichen ändert. Dies hat gewisse Vorteile gegenüber dem Verhalten der Basis $\{\alpha, \alpha^q\}$. Der Grund, warum in dieser Arbeit dennoch mit der Basis $\{\alpha, \alpha^q\}$ gerechnet wird, besteht darin, daß sich hiermit auch der Fall $\mathrm{char}(\mathbb{F}_{q^2}) = 2$ beschreiben läßt und so eine unnötige Fallunterscheidung vermieden wird.

Die folgenden beiden Sätze sind grundlegend für die späteren Rechnungen.

Satz 1.1.3 *Sei $c \in \mathbb{F}_{q^2}$. Dann hat die Gleichung $x^q + x = c$ in $\mathbb{F}_{q^2}$ die Lösungsmenge*

$$\mathbb{L} = \begin{cases} \emptyset & \textit{falls } c \notin \mathbb{F}_q \\ c\frac{\alpha}{\alpha+\alpha^q} + (\alpha - \alpha^q)\mathbb{F}_q & \textit{falls } c \in \mathbb{F}_q. \end{cases}$$

Insbesondere gibt es genau q verschiedene Lösungen, falls $c \in \mathbb{F}_q$ ist.

Beweis: Für $c \notin \mathbb{F}_q$ ist $\mathbb{L} = \emptyset$ nach Lemma 1.1.1. Sei nun $c \in \mathbb{F}_q$ und $x = x_1\alpha + x_2\alpha^q \in \mathbb{F}_{q^2}$ beliebig mit $x_1, x_2 \in \mathbb{F}_q$. Wegen $x^q + x = (x_1 + x_2)(\alpha + \alpha^q)$ ist $x^q + x = c$ äquivalent zu $x_2 = \frac{c}{\alpha+\alpha^q} - x_1$ bzw. zu

$$x = x_1\alpha + \left(\frac{c}{\alpha + \alpha^q} - x_1\right)\alpha^q = c\frac{\alpha^q}{\alpha + \alpha^q} + x_1(\alpha - \alpha^q).$$

Somit ist $\mathbb{L} = c\frac{\alpha^q}{\alpha+\alpha^q} + (\alpha - \alpha^q)\mathbb{F}_q$. □

Satz 1.1.4 *Sei $c \in \mathbb{F}_{q^2}$. Dann hat die Gleichung $x^q - x = c$ in $\mathbb{F}_{q^2}$ die Lösungsmenge*

$$\mathbb{L} = \begin{cases} \emptyset & \textit{falls } c \notin (\alpha - \alpha^q)\mathbb{F}_q \\ c\frac{\alpha^q}{\alpha-\alpha^q} + \mathbb{F}_q & \textit{falls } c \in (\alpha - \alpha^q)\mathbb{F}_q. \end{cases}$$

Insbesondere gibt es genau q verschiedene Lösungen, falls $c \in (\alpha - \alpha^q)\mathbb{F}_q$ ist.

Beweis: Sei $x = x_1\alpha + x_2\alpha^q \in \mathbb{F}_{q^2}$ beliebig mit $x_1, x_2 \in \mathbb{F}_q$. Wegen $x^q - x = (x_2 - x_1)(\alpha - \alpha^q) \in (\alpha - \alpha^q)\mathbb{F}_q$ folgt $\mathbb{L} = \emptyset$ für den Fall $c \notin (\alpha - \alpha^q)\mathbb{F}_q$. Sei nun $c \in (\alpha - \alpha^q)\mathbb{F}_q$. Dann ist $x^q - x = c$ äquivalent zu $x_2 = x_1 + \frac{c}{\alpha - \alpha^q}$. bzw. zu

$$\begin{aligned} x &= x_1\alpha + \left(x_1 + \tfrac{c}{\alpha-\alpha^q}\right)\alpha^q \\ &= c\tfrac{\alpha^q}{\alpha-\alpha^q} + x_1(\alpha + \alpha^q). \end{aligned}$$

Wegen $0 \neq (\alpha + \alpha^q) \in \mathbb{F}_q$ folgt $\mathbb{L} = c\frac{\alpha^q}{\alpha-\alpha^q} + \mathbb{F}_q$. □

Korollar 1.1.5 *Sei $a \in \mathbb{F}_{q^2}^*$ und $c \in \mathbb{F}_{q^2}$. Dann hat die Gleichung $ax^q - a^q x = c$ in $\mathbb{F}_{q^2}$ die Lösungsmenge*

$$\mathbb{L} = \begin{cases} \emptyset & falls\ \ c \notin (\alpha - \alpha^q)\mathbb{F}_q \\ \frac{c}{a^q}\frac{\alpha^q}{\alpha-\alpha^q} + \frac{1}{a^q}\mathbb{F}_q & falls\ \ c \in (\alpha - \alpha^q)\mathbb{F}_q. \end{cases}$$

Insbesondere gibt es genau q verschiedene Lösungen, falls $c \in (\alpha - \alpha^q)\mathbb{F}_q$ ist.

Beweis: Man setze $y := a^q x$. Dann gilt $x = \frac{y}{a^q}$ sowie $y^q = ax^q$. Damit ist $ax^q - a^q x = c$ äquivalent zu $y^q - y = c$. Ist $c \notin (\alpha - \alpha^q)\mathbb{F}_q$, so gibt es nach Satz 1.1.4 keine Lösung y von $y^q - y = c$. Daraus folgt, daß es keine Lösung x von $ax^q - a^q x = c$ gibt. Also ist $\mathbb{L} = \emptyset$. Ist dagegen $c \in (\alpha - \alpha^q)\mathbb{F}_q$, gilt nach Satz 1.1.4 die Gleichung $y^q - y = c$ genau dann, wenn $y = a^q x$ in $c\frac{\alpha^q}{\alpha-\alpha^q} + \mathbb{F}_q$ liegt. Das ist äquivalent zu $x \in \frac{c}{a^q}\frac{\alpha^q}{\alpha-\alpha^q} + \frac{1}{a^q}\mathbb{F}_q$. Also ist $\mathbb{L} = \frac{c}{a^q}\frac{\alpha^q}{\alpha-\alpha^q} + \frac{1}{a^q}\mathbb{F}_q$. □

Die folgenden beiden Lemmata befassen sich mit dem Lösungsverhalten von Gleichungen, die im Fall $\mathrm{char}(\mathbb{F}_{q^2}) = 2$ von Interesse sind.

Lemma 1.1.6 *Sei q gerade. Man definiere die Menge*

$$F := \{ab^{q+1} \mid a, b \in \mathbb{F}_{q^2} \ \ mit\ \ ab^q + a^q b = 0\}.$$

Dann gilt $F = \mathbb{F}_{q^2}$.

Beweis: Sei $b := ax$ mit $x \in \mathbb{F}_q$ und $a \in \mathbb{F}_{q^2}$ beliebig. Dann gilt

$$ab^q + a^q b = a(ax)^q + a^q ax = a^{q+1}x + a^{q+1}x = 0$$

und $ab^{q+1} = a(ax)^{q+1} = a^{q+2}x^2$. Daraus folgt $F \supset \{a^{q+2}x^2 \mid a \in \mathbb{F}_{q^2}, x \in \mathbb{F}_q\}$.Weil nun die Abbildung $x \longmapsto x^2$ auf $\mathbb{F}_q$ ein Automorphismus ist, gilt sogar $F \supset \{a^{q+2}x \mid a \in \mathbb{F}_{q^2}, x \in \mathbb{F}_q\}$.

Da $q+1$ und $q+2$ teilerfremd sind, gibt es nun Zahlen $r, s \in \mathbb{Z}$, so daß $r(q+2) + s(q+1) = 1$ ist. Man wähle nun $a := \alpha^r$ und $x := \alpha^{s(q+1)}$. Dann ist $x \in \mathbb{F}_q$, und es gilt $a^{q+2}x = (\alpha^r)^{q+2}\alpha^{s(q+1)} = \alpha$. Damit folgt $\alpha \in \{a^{q+2}x \mid a \in \mathbb{F}_{q^2}, x \in \mathbb{F}_q\}$. Wegen der multiplikativen Abgeschlossenheit von $\{a^{q+2}x \mid a \in \mathbb{F}_{q^2}, x \in \mathbb{F}_q\}$ erhält man $F \supset \{a^{q+2}x \mid a \in \mathbb{F}_{q^2}, x \in \mathbb{F}_q\} \supset \mathbb{F}_{q^2}^*$. Weil zusätzlich $0 \in F$ gilt, folgt $F = \mathbb{F}_{q^2}$. □

Lemma 1.1.7 *Sei q gerade. Man definiere die Menge*

$$F := \{ab^{q+1} + a^{q+1}b \mid a, b \in \mathbb{F}_{q^2} \ \ mit\ \ ab^q + a^q b = 0\}.$$

Weiter sei G die von F erzeugte additive Untergruppe von $\mathbb{F}_{q^2}$. Dann gilt

$$G = \begin{cases} \mathbb{F}_{q^2} & falls\ q \neq 2 \\ \{0\} & falls\ q = 2. \end{cases}$$

Beweis: Zunächst betrachtet man den Fall $q = 2$. Seien $a, b \in \mathbb{F}_4$ mit $ab^2 + a^2b = ab(a + b) = 0$. Falls $a = 0$ oder $b = 0$ ist, folgt $ab^3 + a^3b = 0$. Falls nun $a \neq 0$ und $b \neq 0$ ist, folgt ebenfalls $ab^3 + a^3b = a + b = 0$. Also gilt $F = \{0\}$ und somit auch $G = \{0\}$.

Für den Fall $q \neq 2$ sei $b := ax$ mit $x \in \mathbb{F}_q$ und $a \in \mathbb{F}_{q^2}$ beliebig. Dann gilt wieder $ab^q + a^qb = 0$. Außerdem erhält man

$$ab^{q+1} + a^{q+1}b = a^{q+2}(x^2 + x).$$

Daraus folgt $F \supset \{a^{q+2}(x^2 + x) \mid a \in \mathbb{F}_{q^2}, x \in \mathbb{F}_q\}$.

<u>1.Fall $q > 4$:</u> Man betrachte zunächst die Abbildung $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q,\ \ x \longmapsto x^2 + x$. Für alle $x, y \in \mathbb{F}_q$ gilt $(x+y)^2+x+y = x^2+x+y^2+y$. Also ist f ein additiver Gruppenhomomorphismus. Weil $0 = f(x) = x(x + 1)$ genau dann gilt, wenn $x = 0$ oder $x = 1$ ist, folgt $\#\mathrm{Kern(f)} = 2$ und damit $\#\mathrm{Bild(f)} = \frac{\#\mathbb{F}_q}{\#\mathrm{Kern(f)}} = \frac{q}{2}$ sowie $\#(\mathrm{Bild(f)} - \{0\}) = \frac{q}{2} - 1$.

Im folgenden bestimmt man nun die Werte, die der Ausdruck a^{q+2} annehmen kann. Man betrachte dazu den Gruppenhomomorphismus $g : \mathbb{F}^*_{q^2} \longrightarrow \mathbb{F}^*_{q^2},\ \ a \longmapsto a^{q+2}$. Wegen

$$\begin{aligned}\mathrm{ggT}(q+2, q^2-1) &= \mathrm{ggT}(q+2, (q-1)(q+1)) \\ &= \mathrm{ggT}(q+2, q-1) \\ &= \begin{cases} 1 \text{ falls } 3 \nmid (q+2) \\ 3 \text{ falls } 3 \mid (q+2) \end{cases}\end{aligned}$$

folgt für den Fall $3 \nmid (q+2)$, daß g bijektiv ist. Wegen $\#\mathrm{Bild(f)} > 0$ muß es ein $x \in \mathbb{F}_q$ geben mit $x^2 + x \neq 0$. Für ein solches x durchläuft dann der Ausdruck $a^{q+2}(x^2 + x)$ in Abhängigkeit von $a \in \mathbb{F}_{q^2}$ alle Elemente von $\mathbb{F}_{q^2}$. Also folgt $G = F = \mathbb{F}_{q^2}$. Sei nun $(q+2)$ ein Vielfaches von 3. Dann gilt $\mathrm{Bild}(g) = \{\alpha^s \mid s = 3, 6, \ldots, (q-1)(q+1)\}$. Damit erhält man $F \supset \{\alpha^s y \mid y \in \mathrm{Bild}(f), s = 3, 6, \ldots, (q-1)(q+1)\}$. Falls es nun gelingt zu zeigen, daß es Element $\alpha^{s_1}, \alpha^{s_2} \in \mathrm{Bild}(f) - \{0\}$ gibt mit $s_1 \not\equiv s_2 \mod 3$, folgt

$$\#F \geq \frac{2}{3}(q-1)(q+1) = \frac{1}{2}q^2 - \frac{q^2-4}{6} > \frac{1}{2}q^2.$$

Da $\#G$ ein Teiler von $\#\mathbb{F}_{q^2} = q^2$ sein muß, erhält man daraus $G = \mathbb{F}_{q^2}$.

Angenommen, es gäbe ein $r \in \{0, 1, 2\}$, so daß für alle $\alpha^s \in \mathrm{Bild}(f - \{0\})$ die Kongruenz $r \equiv s \mod 3$ gälte. Dann folgte $\#(\mathrm{Bild}(f) - \{0\}) \leq \frac{1}{3}\#\mathbb{F}^*_q$. Das hieße aber $\frac{q}{2} - 1 \leq \frac{1}{3}(q-1)$. Daraus ergäbe sich $3q - 6 \leq 2(q-1)$, was in Widerspruch zu $q > 4$ steht. Also muß es nun Elemente $\alpha^{s_1}, \alpha^{s_2} \in \mathrm{Bild}(f) - \{0\}$ geben mit $s_1 \not\equiv s_2 \mod 3$. Somit ist die Aussage gezeigt.

<u>2.Fall $q = 4$:</u> Der Körper $\mathbb{F}_4$ läßt sich realisieren durch $\mathbb{F}_4 = \{0, 1, \phi, \psi\}$ mit den Verknüpfungen

$+$	0	1	ϕ	ψ
0	0	1	ϕ	ψ
1	1	0	ψ	ϕ
ϕ	ϕ	ψ	0	1
ψ	ψ	ϕ	1	0

und

$\bullet$	0	1	ϕ	ψ
0	0	0	0	0
1	0	1	ϕ	ψ
ϕ	0	ϕ	ψ	1
ψ	0	ψ	1	ϕ

.

Man betrachte nun $f := X^2 + X + \psi \in \mathbb{F}_4[X]$. Wegen $x^2 + x \in \mathbb{F}_2$ für alle $x \in \mathbb{F}_2$ und $\psi \notin \mathbb{F}_2$ hat f keine Nullstellen. Weil f den Grad 2 hat, folgt die Irreduzibilität. Damit läßt sich $\mathbb{F}_{16}$ realisieren durch $\mathbb{F}_{16} = \mathbb{F}_4[X]/(f \cdot \mathbb{F}_4[X]) = \{\overline{a_1X + a_0} \mid a_0, a_1 \in \mathbb{F}_4\}$. Sei nun $\beta := \overline{X} \in \mathbb{F}_{16}$. Dann gilt
$\beta^2 = (\overline{X^2})^2 = \overline{X^2} + \overline{X^2 + X + \psi} = \overline{X + \psi}$,
$\beta^3 = (\overline{X + \psi})\overline{X} = \overline{X^2 + \psi X} + \overline{X^2 + X + \psi} = \overline{\phi X + \psi}$,

$\beta^6 = (\overline{\phi X + \psi})^2 = \overline{\psi X^2 + \phi} + \overline{\psi X^2 + \psi X + \phi} = \overline{\psi X}$,
$\beta^9 = (\overline{\phi X + \psi})\overline{\psi X} = \overline{X^2 + \phi X} + \overline{X^2 + X + \psi} = \overline{\psi X + \psi}$ und
$\beta^{12} = (\overline{\psi X})^2 = \overline{\phi X^2} + \overline{\phi X^2 + \phi X + 1} = \overline{\phi X + 1}$.
Außerdem gilt $(\beta^3)^6 = \beta^3, (\beta^6)^6 = \beta^6$, $(\beta^9)^6 = \beta^9, (\beta^{12})^6 = \beta^{12}$ und $1^6 = 1$ sowie $\psi^2 + \psi = 1$. Daraus folgt $F \supset \{1, \beta^3, \beta^6, \beta^9, \beta^{12}\} = \{\overline{1}, \overline{\phi X + \psi}, \overline{\psi X}, \overline{\psi X + \psi}, \overline{\phi X + 1}\}$. Wegen $\overline{1} + \overline{\phi X + \psi} = \overline{\phi X + \phi}$, $\overline{1} + \overline{\psi X} = \overline{\psi X + 1}$, $\overline{1} + \overline{\psi X + \psi} = \overline{\psi X + \phi}$ und $\overline{1} + \overline{\phi X + 1} = \overline{\phi X}$ folgt

$$G \supset \{\overline{1}, \overline{\phi X + \psi}, \overline{\psi X}, \overline{\psi X + \psi}, \overline{\phi X + 1}, \overline{\phi X + \phi}, \overline{\psi X + 1}, \overline{\psi X + \phi}, \overline{\phi X}\}.$$

Also gilt $\#G > 8$. Da $\#G$ ein Teiler von 16 sein muß, folgt $G = \mathbb{F}_{16}$. □

1.2 Q als Quaternionenalgebra über L

1.2.1 Definition von Quaternionenalgebren

Zunächst ist es notwendig den Begriff der 2-dimensionalen separablen K-Algebra einzuführen.

Definition 1.2.1.1 *Sei K ein Körper. Eine 2-dimensionale K-Algebra H heißt separabel, wenn für alle $x \in H$ das Minimalpolynom f von x über K separabel ist, d h nur einfache Nullstellen besitzt.*

Man kann nun 2-dimensionale separable K-Algebren auf folgende Weise charakterisieren.

Satz 1.2.1.2 *Sei K ein Körper und H eine 2-dimensionale K-Algebra. Dann gilt:*

(i) Die Algebra H ist, genau dann separabel, wenn H entweder eine separable Körpererweiterung von K ist oder die Isomorphie $H \cong K \times K$ gilt.

(ii) Falls H separabel ist, gibt es auf H genau einen nichttrivialen K-Algebra-Automorphismus.

Beweis: (i) Falls H ein Körper ist, gilt für H offensichtlich die Äquivalenz der Bedingungen „separabel als Körpererweiterung von K“ und „separabel als K-Algebra“. Man nehme nun an, daß H kein Körper ist. Sei weiter $x \in H - K$ beliebig und $f \in K[X]$ das Minimalpolynom von x über K. Dann gilt $H \cong K[X]/(f \cdot K[X])$, wobei f nicht irreduzibel über K sein kann. Falls H separabel ist, muß es zwei verschiedene Elemente $a, b \in K$ geben, so daß $f = (X-a)(X-b)$ gilt. Wegen $(X-a)K[X] + (X-b)K[X] = K[X]$ folgt aus dem chinesischen Restsatz die Isomorphie

$$H \cong K[X]/((X-a)K[X]) \times K[X]/((X-b)K[X]) \cong K \times K$$

(siehe dazu z.B. [11], corollary 2.2, p. 95). Sei nun $H \cong K \times K$. Angenommen, H wäre nicht separabel. Dann müßte es ein $c \in K$ geben mit $f(x) = (x-c)^2 = 0$. Das ist eine Widerspruch, da $K \times K$ keine von 0 verschiedenen nilpotenten Elemente enthält.

(ii) Sei H eine separable Körpererweiterung von K. Weil H dann den Grad 2 über K hat, ist H automatisch auch normal. Damit folgt, daß es genau einen nichttrivialen K-Algebra-Automorphismus auf H gibt. Damit bleibt zu zeigen, daß $K \times K$ genau einen nichttrivialen K-Algebra-Automorphismus besitzt. Man betrachte dazu die Abbildung $\phi : K \times K \longrightarrow K \times K, (a,b) \longmapsto (b,a)$. Offensichtlich ist ϕ eine additive und bijektive Abbildung, die die Menge $\{(a,a) \mid a \in K\} \cong K$ invariant läßt. Da ϕ lediglich die Koordinaten vertauscht, folgt auch die Multiplikativität von ϕ. Somit ist ϕ ein nichttrivialer K-Algebra-Automorphismus auf H. Sei nun ψ ebenfalls ein nichttrivialer K-Algebra-Automorphismus auf $K \times K$. Dann folgt $\psi((1,1)) = (1,1)$. Wegen $\psi((1,0))^2 = \psi((1,0)^2) = \psi((1,0))$ folgt $\psi((1,0)) = (1,0)$, $\psi((1,0)) = (0,1)$, $\psi((1,0)) = (1,1)$ oder $\psi((1,0)) = (0,0)$. Da aber die Fälle $\psi((1,0)) = (1,1)$ und $\psi((1,0)) = (0,0)$ im Widerspruch zur Bijektivität und der Fall $\psi((1,0)) = (1,0)$ im Widerspruch zur Nichttrivialität von ψ steht, folgt $\psi((1,0)) = (0,1)$ und damit $\psi = \phi$. Also gibt es genau einen nichttrivialen K-Algebra-Automorphismus auf $K \times K$. □

Damit kann man nun Quaternionenalgebren definieren.

Definition 1.2.1.3 *Sei K ein Körper. Eine K-Algebra H heißt zentral, wenn K das Zentrum von H ist.*

Definition 1.2.1.4 (Quaternionenalgebra) *Sei K ein Körper. Eine zentrale 4-dimensionale K-Algebra H heißt* Quaternionenalgebra über K, *wenn es eine 2-dimensionale separable K-Unteralgebra H_0 und ein $u \in H$ gibt mit $u^2 \in K^*$, so daß die folgenden beiden Bedingungen erfüllt sind:*

(i) Es gilt $H = H_0 \bigoplus H_0 u$ als K-Vektorräume.

(ii) Sei ϕ der nichttriviale K-Algebra-Automorphismus auf H_0. Dann gilt für alle $x \in H_0$ die Gleichung $ux = \phi(x)u$.

Quaternionenalgebren lassen sich durch Angabe von Basiselementen und den Relationen zwischen diesen Elementen charakterisieren. Dabei ist es notwendig, die Fälle $\mathrm{char}(K) = 2$ und $\mathrm{char}(K) \neq 2$ zu unterscheiden.

Satz 1.2.1.5 *Sei K ein Körper mit $\mathrm{char}(K) \neq 2$. Eine zentrale K-Algebra H ist genau dann eine Quaternionenalgebra, wenn es Elemente $u, v \in H$ gibt, so daß $\{1, u, v, uv\}$ eine K-Basis von H ist und die Relationen $u^2, v^2 \in K^*$ sowie $uv = -vu$ gelten.*

Beweis: Sei zunächst H eine Quaternionenalgebra über K. Dann gibt es ein $u \in H$ mit $u^2 \in K^*$ und eine 2-dimensionale Unteralgebra H_0, so daß $H = H_0 \bigoplus H_0 u$ ist. Für den nichttrivialen K-Algebra-Automorphismus gilt $ux = \phi(x)u$ für alle $x \in H_0$. Man wähle nun $a \in H_0 - K$ und setze $v := \phi(a) - a$. Dann gilt $\phi(v) = -v \neq 0$. Daraus folgt $uv = -vu$ sowie $v \notin K$. Folglich ist $\{1, u, v, uv\}$ eine K-Basis von H. Weiter gilt $\phi(v^2) = \phi(-\phi(v)v) = -v\phi(v) = v^2$ und damit $v^2 \in K$. Da das Minimalpolynom von v über K keine doppelten Nullstellen enthalten darf, muß $v^2 \neq 0$ gelten. Somit ist $v \in K^*$.

Sei nun H eine zentrale K-Algebra mit Elementen $u, v \in H$, so daß $\{1, u, v, uv\}$ eine K-Basis von H ist und die Relationen $u^2, v^2 \in K^*$ sowie $uv = -vu$ gelten. Man setze $H_0 := K + Kv$. Dann ist H_0 2-dimensional und es gilt $H = H_0 \bigoplus H_0 u$. Weiter setze man $a := v^2$. Dann ist $f := X^2 - a = (X - v)(X + v) \in K[X]$ das Minimalpolynom von v und es gilt $H_0 \cong K[X]/(f \cdot K[X])$. Es ist klar, daß f separabel ist. Falls f irreduzibel ist, ist H_0 der Zerfällungskörper eines separablen Polynoms und deshalb separabel. Falls f nicht irreduzibel ist, gilt $H_0 \cong K \times K$, womit wieder die Separabilität von H_0 folgt. In beiden Fällen sei nun ϕ der nichttriviale K-Algebra-Automorphismus auf H_0. Da u^2 in K^* liegt, folgt die Invertierbarkeit von u (mit $u^{-1} = \frac{u}{u^2}$). Es gilt nun $uvu^{-1} = -v \in H_0$. Daraus folgt, daß durch die Vorschrift $x \longmapsto uxu^{-1}$ für alle $x \in H_0$ ein innerer K-Algebra-Automorphismus auf H_0 definiert wird. Da dieser nichttrivial ist, folgt $uxu^{-1} = \phi(x)$ und damit $ux = \phi(x)u$ für alle $x \in H_0$. □

Satz 1.2.1.6 *Sei K ein Körper mit $\mathrm{char}(K) = 2$. Eine zentrale K-Algebra H ist genau dann eine Quaternionenalgebra, wenn es Elemente $u, v \in H$ gibt, so daß $\{1, u, v, uv\}$ eine K-Basis von H ist und die Relationen $u^2 \in K^*$ und $v^2 + v \in K$ sowie $uv = (v + 1)u$ gelten.*

Beweis: Sei zunächst H eine Quaternionenalgebra über K. Dann gibt es ein $u \in H$ mit $u^2 \in K^*$ und eine 2-dimensionale Unteralgebra H_0, so daß $H = H_0 \bigoplus H_0 u$ ist. Für den nichttrivialen K-Algebra-Automorphismus gilt $ux = \phi(x)u$ für alle $x \in H_0$. Man wähle nun $a \in H_0 - K$. Dann gilt $\phi(a) + a \neq 0$. Wegen $\phi(\phi(a) + a) = \phi(a) + a$ ist $\phi(a) + a \in K$ invertierbar. Man setze $v := \frac{a}{\phi(a)+a}$. Wegen $\phi(a) \neq a$ folgt $\phi(v) \neq v$ und damit $v \notin K$. Folglich ist $\{1, u, v, uv\}$ eine K-Basis von H. Weiter gilt $v + 1 = \frac{\phi(a)}{\phi(a)+a} = \phi(v)$. Somit folgt $uv = (v + 1)u$. Schließlich erhält man noch $\phi(v^2 + v) = (v + 1)^2 + v + 1 = v^2 + v$ und damit $v^2 + v \in K$.

Sei nun H eine zentrale K-Algebra mit Elementen $u, v \in H$, so daß $\{1, u, v, uv\}$ eine K-Basis von H ist und die Relationen $u^2 \in K^*$, $v^2 + v \in K$ sowie $uv = (v+1)u$ gelten. Man setze $H_0 := K + Kv$. Dann ist H_0 2-dimensional und es gilt $H = H_0 \bigoplus H_0 u$. Weiter setze man $a := v^2 + v$. Dann ist

$f := X^2 + X + a \in K[X]$ das Minimalpolynom von u, und es gilt $H_0 \cong K[X]/(f \cdot K[X])$. Angenommen, f wäre nicht separabel. Dann gäbe es ein $c \in H_0$ mit $f = (X+c)^2 = X^2 + c^2$. Weil dies ein Widerspruch ist, muß F separabel sein. Falls f irreduzibel ist, ist H_0 der Zerfällungskörper eines separablen Polynoms und deshalb separabel. Falls f nicht irreduzibel ist, gilt $H_0 \cong K \times K$, womit wieder die Separabilität von H_0 folgt. In beiden Fällen sei nun ϕ der nichttriviale K-Algebra-Automorphismus auf H_0. Da u^2 in K^* liegt, flogt die Invertierbarkeit von u (mit $u^{-1} = \frac{u}{u^2}$). Es gilt nun $uvu^{-1} = (v+1)u \in H_0$. Daraus folgt, daß durch die Vorschrift $x \longmapsto uxu^{-1}$ für alle $x \in H_0$ ein innerer K-Algebra-Automorphismus auf H_0 definiert wird. Da dieser nichttrivial ist, folgt $uxu^{-1} = \phi(x)$ und damit $ux = \phi(x)u$ für alle $x \in H_0$. $\square$

1.2.2 Der Zusammenhang zwischen Q und L

In diesem Unterabschnitt wird gezeigt, daß Q eine Quaternionenalgebra über L ist. Dazu bestimmt man zunächst das Zentrum von Q.

Lemma 1.2.2.1 *Es gilt $L = Z(Q)$.*

Beweis: Sei $x = \sum\limits_{i=m}^{\infty} a_i\tau^i \in L$. Für alle $i \in \mathbb{Z}$ mit $i \geq m$ gilt dann $a_i =\in \mathbb{F}_q$. Falls i ungerade ist, gilt sogar $a_i = 0$. Sei nun $y = \sum\limits_{i=n}^{\infty} b_i\tau^i \in Q$ beliebig. Damit erhält man

$$\begin{aligned}
xy &= \sum_{i=m+n}^{\infty}\left(\sum_{k=m}^{i-n} a_k b_{i-k}^{q^k}\right)\tau^i \\
&= \sum_{i=m+n}^{\infty}\left(\sum_{k=m}^{i-n} a_k b_{i-k}\right)\tau^i && \text{(wegen } a_k = 0 \text{ falls } k \text{ gerade)} \\
&= \sum_{i=m+n}^{\infty}\left(\sum_{k=m}^{i-n} b_{i-k} a_k^{q^{i-k}}\right)\tau^i && \text{(wegen } a_k \in \mathbb{F}_q \text{ für alle } k \in \mathbb{Z} \text{ mit } k \geq m) \\
&= \sum_{i=m+n}^{\infty}\left(\sum_{k'=n}^{i-m} b_{k'} a_{i-k'}^{q^{k'}}\right)\tau^i && \text{(Substitutuion } k' := i-k) \\
&= yx.
\end{aligned}$$

Also gilt $x \in Z(Q)$. Somit ist $L \subset Z(Q)$ gezeigt.

Sei $x = \sum\limits_{i=m}^{\infty} a_i\tau^i \in Z(Q)$. Für ein beliebiges $c \in \mathbb{F}_{q^2} - \mathbb{F}_q$ gilt dann

$$0 = cx - xc = \sum_{i=m}^{\infty} a_i c\tau^i - \sum_{i=m}^{\infty} a_i c^{q^i}\tau^i = \sum_{i=m}^{\infty} a_i(c - c^{q^i})\tau^i.$$

Wegen $c \neq c^q$ erhält man $a_i = 0$ für alle ungeraden $i \geq m$. Damit ist x von der Form $\sum\limits_{i=m}^{\infty}{}'' a_i\tau^i$. Außerdem gilt

$$0 = \tau x - x\tau = \tau\sum_{i=m}^{\infty}{}'' a_i\tau^i - \sum_{i=m}^{\infty}{}'' a_i\tau^{i+1} = \sum_{i=m}^{\infty}{}''(a_i^q - a_i)\tau^{i+1}$$

und damit $a_i^q = a_i$ bzw. $a_i \in \mathbb{F}_q$ für alle geraden $i \geq m$. Also gilt $x \in L$. Somit ist $Z(Q) \subset L$ gezeigt. $\square$

Lemma 1.2.2.2 *Sei $\{\beta_1, \beta_2\}$ eine $\mathbb{F}_q$-Basis von $\mathbb{F}_{q^2}$. Dann ist $\{\beta_1, \beta_2, \beta_1\tau, \beta_2\tau\}$ eine L-Basis von Q.*

Beweis: Sei $x \in Q$. Dann gibt es ein $m \in \mathbb{Z}$ sowie $a_i = a_i^{(1)}\beta_1 + a_i^{(2)}\beta_2 \in \mathbb{F}_{q^2}$ mit $a_i^{(1)}, a_i^{(2)} \in \mathbb{F}_q$ für alle $i \in \mathbb{Z}$ mit $i \geq n$, so daß gilt

$$
\begin{aligned}
x &= \sum_{i=m}^{\infty} a_i \tau^i \\
&= \sum_{i=m}^{\infty}{}'' a_i \tau^i + \sum_{i=m}^{\infty}{}' a_i \tau^i \\
&= \sum_{i=m}^{\infty}{}'' (a_i^{(1)}\beta_1 + a_i^{(2)}\beta_2)\tau^i + \sum_{i=m}^{\infty}{}' (a_i^{(1)}\beta_1 + a_i^{(2)}\beta_2)\tau^i \\
&= \underbrace{\left(\sum_{i=m}^{\infty}{}'' a_i^{(1)}\tau^i\right)}_{\in L}\beta_1 + \underbrace{\left(\sum_{i=m}^{\infty}{}'' a_i^{(2)}\tau^i\right)}_{\in L}\beta_2 + \underbrace{\left(\sum_{i=m}^{\infty}{}' a_i^{(1)}\tau^{i-1}\right)}_{\in L}\beta_1\tau + \underbrace{\left(\sum_{i=m}^{\infty}{}' a_i^{(2)}\tau^{i-1}\right)}_{\in L}\beta_2\tau.
\end{aligned}
$$

Also ist $\{\beta_1, \beta_2, \beta_1\tau, \beta_2\tau\}$ ein L-Erzeugendensystem von Q.

Seien nun $x^{(1)}, x^{(2)}, y^{(1)}, y^{(2)} \in L$ mit $x^{(1)}\beta_1 + x^{(2)}\beta_2 + y^{(1)}\beta_1\tau + y^{(2)}\beta_2\tau = 0$. Dann gibt es eine gerade Zahl m sowie $a_i^{(1)}, a_i^{(2)}, b_i^{(1)}, b_i^{(2)} \in \mathbb{F}_q$ für alle geraden $i \geq m$, so daß $x^{(1)} = \sum_{i=m}^{\infty}{}'' a_i^{(1)}\tau^i$, $x^{(2)} = \sum_{i=m}^{\infty}{}'' a_i^{(2)}\tau^i$, $y^{(1)} = \sum_{i=m}^{\infty}{}'' b_i^{(1)}\tau^i$ und $y^{(2)} = \sum_{i=m}^{\infty}{}'' b_i^{(2)}\tau^i$ gilt. Damit erhält man

$$
\begin{aligned}
0 &= \left(\sum_{i=m}^{\infty}{}'' a_i^{(1)}\tau^i\right)\beta_1 + \left(\sum_{i=m}^{\infty}{}'' a_i^{(2)}\tau^i\right)\beta_2 + \left(\sum_{i=m}^{\infty}{}'' b_i^{(1)}\tau^i\right)\beta_1\tau + \left(\sum_{i=m}^{\infty}{}'' b_i^{(2)}\tau^i\right)\beta_2\tau \\
&= \sum_{i=m}^{\infty}{}'' (a_i^{(1)}\beta_1 + a_i^{(2)}\beta_2)\tau^i + \sum_{i=m}^{\infty}{}'' (a_i^{(1)}\beta_1 + a_i^{(2)}\beta_2)\tau^{i+1}.
\end{aligned}
$$

Daraus folgt $a_i^{(1)}\beta_1 + a_i^{(2)}\beta_2 = 0$ sowie $b_i^{(1)}\beta_1 + b_i^{(2)}\beta_2 = 0$ und damit $a_i^{(1)}, a_i^{(2)}, b_i^{(1)}, b_i^{(2)} = 0$ für alle geraden $i \geq m$. Hieraus ergibt sich $x^{(1)}, x^{(2)}, y^{(1)}, y^{(2)} = 0$. Also ist $\{\beta_1, \beta_2, \beta_1\tau, \beta_2\tau\}$ linear unabhängig über L. □

Satz 1.2.2.3 *Q ist eine Quaternionenalgebra über L.*

Beweis: Nach Lemma 1.2.2.1 ist Q eine zentrale L-Algebra. Falls q ungerade ist, setze man $v := \alpha - \alpha^q$. Dann gilt $v^q = -v$ und damit $v \notin \mathbb{F}_q$. Also ist $\{1, v\}$ eine $\mathbb{F}_q$-Basis von $\mathbb{F}_{q^2}$. Nach Lemma 1.2.2.2 folgt, daß $\{1, v, \tau, \tau v\}$ eine L-Basis von Q ist. Weiter gilt $v\tau = -\tau v$. Wegen $\tau^2 \in L^*$ und $v^2 \in \mathbb{F}_q^* \subset L^*$ nach Lemma 1.1.1 folgt nach Satz 1.2.1.5, daß Q eine Quaternionenalgebra über L ist.

Falls q gerade ist, setze man $v := \frac{\alpha}{\alpha + \alpha^q}$. Dann ist $v \notin \mathbb{F}_q$ und damit $\{1, v\}$ eine $\mathbb{F}_q$-Basis von $\mathbb{F}_{q^2}$. Nach Lemma 1.2.2.2 folgt, daß $\{1, v, \tau, \tau v\}$ eine L-Basis von Q ist. Außerdem ist

$$v\tau = \frac{\alpha}{\alpha + \alpha^q}\tau = \tau\frac{\alpha^q}{\alpha + \alpha^q} = \tau\left(1 + \frac{\alpha}{\alpha + \alpha^q}\right) = \tau(1 + v).$$

Wegen $\tau^2 \in L^*$ und

$$v^2 + v = \frac{\alpha^2}{(\alpha + \alpha^q)^2} + \frac{\alpha}{\alpha + \alpha^q} = \frac{\alpha^2 + \alpha(\alpha + \alpha^q)}{(\alpha + \alpha^q)^2} = \frac{\alpha^{q+1}}{(\alpha + \alpha^q)^2} \in \mathbb{F}_q \subset L$$

folgt, nach Satz 1.2.1.6, daß Q eine Quaternionenalgebra über L ist. □

1.2.3 Die Konjugation, Norm und Spur auf Q

Da $\{\alpha, \alpha^q\}$ nach Lemma 1.1.2 eine $\mathbb{F}_q$-Basis von $\mathbb{F}_{q^2}$ ist, folgt nach Lemma 1.2.2.2, daß die Menge $\{\alpha, \alpha^q, \alpha\tau, \alpha^q\tau\}$ eine L-Basis von Q ist. Mit dieser Basis läßt sich nun die Konjugation auf Q wie folgt erklären.

Definition 1.2.3.1 *Sei* $x = A\alpha + B\alpha^q + C\alpha\tau + D\alpha^q\tau \in Q$ *mit* $A, B, C, D \in L$. *Dann heißt* $\overline{x} := B\alpha + A\alpha^q - C\alpha\tau - D\alpha^q\tau$ das zu x konjugierte Element.

Lemma 1.2.3.2 *Sei* $x = \sum_{i=m}^{\infty} a_i\tau^i \in Q$. *Dann gilt* $\overline{x} = \sum_{i=m}^{\infty} (-1)^i a_i^{q^{i+1}} \tau^i$.

Beweis: Sei $x = \sum_{i=m}^{\infty} a_i\tau^i \in Q$. Dann gibt es für alle $i \in \mathbb{Z}$ mit $i \geq m$ Elemente $a_i^{(1)}, a_i^{(2)} \in \mathbb{F}_q$ mit $a_i = a_i^{(1)}\alpha + a_i^{(2)}\alpha^q$. Damit erhält man

$$\begin{aligned}
\overline{x} &= \overline{\left(\sum_{i=m}^{\infty}{}'' a_i^{(1)}\tau^i\right)\alpha + \left(\sum_{i=m}^{\infty}{}'' a_i^{(2)}\tau^i\right)\alpha^q + \left(\sum_{i=m}^{\infty}{}'' a_i^{(1)}\tau^{i-1}\right)\alpha\tau + \left(\sum_{i=m}^{\infty}{}'' a_i^{(2)}\tau^{i-1}\right)\alpha^q\tau} \\
&= \left(\sum_{i=m}^{\infty}{}'' a_i^{(2)}\tau^i\right)\alpha + \left(\sum_{i=m}^{\infty}{}'' a_i^{(1)}\tau^i\right)\alpha^q - \left(\sum_{i=m}^{\infty}{}'' a_i^{(1)}\tau^{i-1}\right)\alpha\tau - \left(\sum_{i=m}^{\infty}{}'' a_i^{(2)}\tau^{i-1}\right)\alpha^q\tau \\
&= \sum_{i=m}^{\infty}{}'' \left(a_i^{(2)}\alpha^q + a_i^{(1)}\alpha\right)\tau^i + \sum_{i=m}^{\infty}{}' \left(-a_i^{(1)}\alpha - a_i^{(2)}\alpha^q\right)\tau^i \\
&= \sum_{i=m}^{\infty}{}'' a_i^q\tau^i + \sum_{i=m}^{\infty}{}' (-a_i)\,\tau^i \\
&= \sum_{i=m}^{\infty} (-1)^i a_i^{q^{i+1}}\tau^i.
\end{aligned}$$

□

Lemma 1.2.3.3 *Seien* $x, y \in Q$ *und* $A \in L$. *Dann gelten die folgenden Rechenregeln:*

(i) $\overline{x+y} = \overline{x} + \overline{y}$,

(ii) $\overline{\overline{x}} = x$,

(iii) $\overline{Ax} = A\overline{x}$ *und*

(iv) $\overline{x} \cdot \overline{y} = \overline{yx}$.

Beweis: Die Rechenregeln (i),(ii) und (iii) folgen unmittelbar aus der Definition 1.2.3.1. Um (iv) zu zeigen, schreibt man x und y in der Form $x = \sum_{i=m}^{\infty} a_i\tau^i$ und $y = \sum_{i=n}^{\infty} b_i\tau^i$. Unter Anwendung von Lemma 1.2.3.2 erhält man

$$\begin{aligned}
\overline{x}\cdot\overline{y} &= \left(\sum_{i=m}^{\infty} (-1)^i a_i^{q^{i+1}}\tau^i\right)\left(\sum_{i=n}^{\infty} (-1)^i b_i^{q^{i+1}}\tau^i\right) \\
&= \sum_{i=m+n}^{\infty}\left(\sum_{k=m}^{i-n} (-1)^k a_k^{q^{k+1}}\left((-1)^{i-k} b_{i-k}^{q^{i-k+1}}\right)^{q^k}\right)\tau^i \\
&= \sum_{i=m+n}^{\infty}\left(\sum_{k=m}^{i-n} (-1)^i a_k^{q^{k+1}} b_{i-k}^{q^{i+1}}\right)\tau^i \\
&= \sum_{i=m+n}^{\infty} (-1)^i \left(\sum_{k=m}^{i-n} b_{i-k} a_k^{q^{i-k}}\right)^{q^{i+1}}\tau^i \\
&= \sum_{i=m+n}^{\infty} (-1)^i \left(\sum_{k'=n}^{i-m} b_{k'} a_{i-k'}^{q^{k'}}\right)^{q^{i+1}}\tau^i \qquad \text{(Substitution } k' := i-k\text{)} \\
&= \overline{yx}.
\end{aligned}$$

□

Definition 1.2.3.4 *Sei* $x \in Q$. *Dann heißt* $\mathrm{Tr}(x) := x + \overline{x}$ *die* reduzierte Spur von x *und* $\mathrm{N}(x) := x\overline{x}$ *die* reduzierte Norm von x.

Lemma 1.2.3.5 *Für alle* $x, y \in Q$ *gilt* *(i)* $\mathrm{Tr}(x) \in L$ *und*

(ii) $\mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$.

Das bedeutet, daß $\mathrm{Tr} : Q \longrightarrow L, x \longmapsto \mathrm{Tr}(x)$ *ein additiver Gruppenhomomorphismus ist.*

Beweis: (i) Sei $x = A\alpha + B\alpha^q + C\alpha\tau + D\alpha^q\tau \in Q$ beliebig mit $A, B, C, D \in L$. Dann gilt

$$\begin{aligned}\mathrm{Tr}(x) &= A\alpha + B\alpha^q + C\alpha\tau + D\alpha^q\tau + B\alpha + A\alpha^q - C\alpha\tau - D\alpha^q\tau \\ &= (A+B)\underbrace{(\alpha + \alpha^q)}_{\in \mathbb{F}_q} \in L.\end{aligned}$$

(ii) Für alle $x, y \in Q$ gilt nach Lemma 1.2.3.3, daß

$$\mathrm{Tr}(x+y) = x + y + \overline{x+y} = x + \overline{x} + y + \overline{y} = \mathrm{Tr}(x) + \mathrm{Tr}(y)$$

ist. □

Lemma 1.2.3.6 *Für alle* $x, y \in Q$ *gilt*

(i) $\mathrm{N}(x) \in L$,

(ii) $\mathrm{N}(x) \neq 0$, *falls* $x \neq 0$, *und*

(iii) $\mathrm{N}(xy) = \mathrm{N}(x)\mathrm{N}(y)$.

Das bedeutet, daß $\mathrm{N} : Q^* \longrightarrow L^*, x \longmapsto \mathrm{N}(x)$ *ein multiplikativer Gruppenhomomorphismus ist.*

Beweis: (i) Sei $x = A\alpha + B\alpha^q + C\alpha\tau + D\alpha^q\tau \in Q$ beliebig mit $A, B, C, D \in L$. Dann gilt

$$\begin{aligned}\mathrm{N}(x) &= (A\alpha + B\alpha^q + C\alpha\tau + D\alpha^q\tau)(B\alpha + A\alpha^q - C\alpha\tau - D\alpha^q\tau) \\ &= (A\alpha + B\alpha^q)(B\alpha + A\alpha^q) + (A\alpha + B\alpha^q)(-C\alpha\tau - D\alpha^q\tau) \\ &\quad + (C\alpha\tau + D\alpha^q\tau)(B\alpha + A\alpha^q) + (C\alpha\tau + D\alpha^q\tau)(-C\alpha\tau - D\alpha^q\tau) \\ &= (A\alpha + B\alpha^q)(B\alpha + A\alpha^q) - (A\alpha + B\alpha^q)(C\alpha + D\alpha^q)\tau \\ &\quad + (C\alpha^q + D\alpha)(A\alpha + B\alpha^q)\tau - (C\alpha + D\alpha^q)(C\alpha^q + D\alpha)\tau^2 \\ &= AB\underbrace{(\alpha^2 + \alpha^{2q})}_{\in \mathbb{F}_q} + (A^2 + B^2)\underbrace{\alpha^{q+1}}_{\in \mathbb{F}_q} - (CD\underbrace{(\alpha^2 + \alpha^{2q})}_{\in \mathbb{F}_q} + (C^2 + D^2)\underbrace{\alpha^{q+1}}_{\in \mathbb{F}_q})\tau^2 \in L.\end{aligned}$$

(ii) Sei $x \in Q$ mit $x \neq 0$. Dann gilt auch $\overline{x} \neq 0$. Wegen der Nullteilerfreiheit von Q folgt $\mathrm{N}(x) = x\overline{x} \neq 0$.

(iii) Für alle $x, y \in Q$ gilt

$$\mathrm{N}(xy) = xy\overline{xy} \overset{1.2.3.3}{=} x\underbrace{y\overline{y}}_{\in L}\overline{x} = x\overline{x}y\overline{y} = \mathrm{N}(x)\mathrm{N}(y).$$

□

Lemma 1.2.3.7 (Invertieren von Elementen) *Sei* $x \in Q$ *mit* $x \neq 0$. *Dann ist* x *invertierbar mit* $x^{-1} = \overline{x}\frac{1}{\mathrm{N}(x)}$.

Beweis: Es gilt $x(\overline{x}\frac{1}{\mathrm{N}(x)}) = 1$. □

1.2.4 Die Graduierung auf Q

Für die folgenden Betrachtungen und den gesamten Rest dieser Arbeit sei $Q_0 := \{\sum_{i=m}^{\infty}{}'' a_i\tau^i \in Q\}$ und $Q_1 := \{\sum_{i=m}^{\infty}{}' a_i\tau^i \in Q\}$.

Lemma 1.2.4.1 *(i) Für alle $x \in Q_0$ gilt $x\tau = \tau\overline{x}$.*

(ii) Es gilt $Q = Q_0 \oplus Q_1$ als L-Vektorräume.

(iii) Es gilt $Q_1 = Q_0\tau$

Beweis: (i) Für alle $x = \sum_{i=m}^{\infty}{}'' a_i\tau^i \in Q_0$ gilt die Identität

$$x\tau = \left(\sum_{i=m}^{\infty}{}'' a_i\tau^i\right)\tau = \tau\left(\sum_{i=m}^{\infty}{}'' a_i^q\tau^i\right) = \tau\overline{x}.$$

(ii) Für alle $A, B \in L$ liegt $A\alpha + B\alpha^q$ in Q_0 und $A\alpha\tau + B\alpha^q\tau$ in Q_1. Außerdem gilt $Q_0 \cap Q_1 = \{0\}$. Da $\{\alpha, \alpha^q, \alpha\tau, \alpha^q\tau\}$ eine L-Basis von Q ist, folgt, daß Q_0 und Q_1 zweidimensionale Unterräume von Q sind und die Isomorphie $Q_0 \bigoplus Q_1$ gilt. (iii) Offensichtlich gilt $Q_0\tau \subset Q_1$. Da Q_0 und Q_1 die gleiche L-Dimension haben und τ invertierbar ist, folgt $Q_1 = Q_0\tau$. □

Satz 1.2.4.2 *Seien $x_0, y_0 \in Q_0$ und $x_1, y_1 \in Q_1$. Dann gilt*

(i) $\overline{x}_0 \in Q_0$ und $\overline{x}_1 = -x_1 \in Q_1$,

(ii) $x_0y_0 = y_0x_0 \in Q_0$,

(iii) $x_0y_1 = y_1\overline{x}_0 \in Q_1$ und

(iv) $x_1y_1 = \overline{y}_1 \cdot \overline{x}_1 \in Q_0$.

Beweis: (i) Es gibt Elemente $A, B \in L$ mit $x_0 = A\alpha + B\alpha^q$. Daraus folgt $\overline{x}_0 = B\alpha + A\alpha^q \in Q_0$. Sei $x_1 \in Q_1$. Dann gibt es $C, D \in L$ mit $x_1 = C\alpha\tau + D\alpha^q\tau$. Daraus folgt $\overline{x}_1 = -C\alpha\tau - D\alpha^q\tau \in Q_1$.

(ii) Da $\{\alpha, \alpha^q\}$ eine L-Basis von Q_0 ist und die Relationen $\alpha^2, \alpha^{2q} \in Q_0$ und $\alpha\alpha^q = \alpha^q\alpha \in Q_0$ gelten, muß Q_0 kommutativ und multiplikativ abgeschlossen sein.

(iii) Es gibt ein $\tilde{y}_1 \in Q_1$ mit $y_1 = \tilde{y}_1\tau$. Daraus folgt $x_0y_1 = x_0\tilde{y}_1\tau \overset{(ii)}{=} \tilde{y}_1x_0\tau \overset{1.2.4.1}{=} \tilde{y}_1\tau\overline{x}_0 = y_1\overline{x}_0$. Wegen $x_0\tilde{y}_1 \in Q_0$ gilt $x_0y_1 = x_0\tilde{y}_1\tau \in Q_1$.

(iv) Nach Lemma 1.2.3.3 gilt die Gleichung

$$x_1y_1 = \overline{\overline{x_1y_1}} = \overline{\overline{y}_1 \cdot \overline{x}_1} \overset{(i)}{=} \overline{(-y_1)(-x_1)} = \overline{y_1x_1}.$$

Seien nun $\tilde{y}_1, \tilde{x_1} \in Q_0$ mit $y_1 = \tilde{y}_1\tau$ und $x_1 = \tilde{x}_1\tau$. Dann folgt $x_1y_1 = \tilde{x}_1\tau\tilde{y}_1\tau = \tilde{x}_1\overline{\tilde{y}}_1\tau^2 \in Q_0$. □

Mit diesem Satz läßt sich Q als $\mathbb{Z}/2\mathbb{Z}$-graduierte L-Algebra auffassen. Das folgende Korollar vereinfacht nun die Berechnung der reduzierten Norm.

Korollar 1.2.4.3 *Sei $x = x_0 + x_1 \in Q$ beliebig mit $x_0 \in Q_0$ und $x_1 \in Q_1$. Dann gilt*

$$\mathrm{N}(x) = x_0\overline{x}_0 - x_1x_1.$$

Beweis: Nach Satz 1.2.4.2 gilt $\mathrm{N}(x) = x\overline{x} = (x_0 + x_1)(\overline{x}_0 - x_1) = x_0\overline{x}_0 + x_1\overline{x}_0 - x_0x_1 - x_1x_1$. Wegen $x_1\overline{x}_0 = x_0x_1$ folgt die Aussage des Korollares. □

1.3 Die Bewertungen auf Q und L

1.3.1 Allgemeines über Bewertungen

Definition 1.3.1.1 *Sei D ein beliebiger (nicht notwendigerweise kommutativer) Divisionsring. Eine surjektive Abbildung $\nu : D \longrightarrow \mathbb{Z} \cup \{\infty\}$ heißt* Bewertung *auf D, falls die folgenden 3 Bedingungen gelten:*

(Bew 1) *Für alle $x \in D$ ist $\nu(x) = \infty$ äquivalent zu $x = 0$.*

(Bew 2) *Für alle $x, y \in D^*$ gilt $\nu(xy) = \nu(x) + \nu(y)$.*

(Bew 3) *Für alle $x, y \in D^*$ gilt die Ungleichung $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$.*

Für die nachfolgenden Betrachtungen sei nun D ein festgewählter Divisionsring und ν eine festgewählte Bewertung auf D.

Die Bedingung **(Bew 2)** besagt, daß die Einschränkung von ν auf D^* ein Gruppenhomomorphismus von D^* nach $\mathbb{Z}$ ist. Daraus ergibt sich $\nu(x^{-1}) = -\nu(x)$ sowie $0 = \nu(1) = \nu((-1)^2) = 2\nu(-1)$. Also gilt $\nu(-1) = 0$ und damit $\nu(-x) = \nu(x)$ für alle $x \in D^*$.

Aus **(Bew 3)** läßt sich die folgende elementare Aussage ableiten.

Lemma 1.3.1.2 *Für alle $x_1, \ldots, x_n \in D^*$ mit $\nu(x_1) < \nu(x_2) < \ldots < \nu(x_n)$ gilt*

$$\nu\left(\sum_{i=1}^{n} x_i\right) = \nu(x_1).$$

Beweis: Die Aussage wird durch Induktion über alle $n \in \mathbb{N}$ gezeigt. Für $n = 1$ ist die Aussage trivial. Für $n \in \mathbb{N}$ beliebig setze man $y_n := \sum_{i=1}^{n} x_i$ und $y_{n+1} := \sum_{i=1}^{n+1} x_i$. Dann ist nach Induktionsannahme $\nu(y_n) = \nu(x_1)$. Damit erhält man

$$\nu(y_{n+1}) = \nu(y_n + x_{n+1}) \geq \min\{\nu(y_n), \nu(x_{n+1})\} = \nu(x_1).$$

Außerdem gilt $\nu(x_1) = \nu(y_n) = \nu(y_{n+1} - x_{n+1}) \geq \min\{\nu(y_{n+1}), \nu(x_{n+1})\}$. Wegen $\nu(x_1) < \nu(x_{n+1})$ folgt $\nu(x_1) \geq \nu(y_{n+1})$ und damit $\nu(x_1) = \nu(y_{n+1})$. □

Man setze nun $B_D := \{x \in D \mid \nu(x) \geq 0\}$. Weil für alle $x, y \in B_D$ die Ungleichungen $\nu(xy) = \nu(x) + \nu(y) \geq 0$ und $\nu(x - y) \geq \min\{\nu(x), \nu(y)\} \geq 0$ gelten, folgt $x - y, xy \in B_D$. Also ist B_D ein Unterring von D. Dieser Ring B_D heißt *Bewertungsring von D* und hat die Eigenschaft, daß für alle $x \in D$ die Bedingung $x \in B_D$ oder $x^{-1} \in B_D$ erfüllt ist. Die hinreichende und notwendige Bedingung dafür, daß ein $x \in B_D$ invertierbar ist lautet $\nu(x) = 0$. Daraus folgt, daß $U_D := \{x \in B_D \mid \nu(x) = 0\}$ die multiplikative Gruppe von B_D ist. Diese Gruppe heißt *Einheitengruppe von D*.

Die Ideale des Bewertungsringes B_D lassen sich nun folgendermaßen charakterisieren. Man setze $\mathfrak{m}_D^n := \{x \in B_D \mid \nu(x) \geq n\}$ für alle $n \in \mathbb{N}$. Offensichtlich ist $0 \in \mathfrak{m}_D^n \neq \emptyset$. Außerdem gelten für alle $x, y \in \mathfrak{m}_D^n$ und $z \in B_D$ die Ungleichungen $\nu(x - y) \geq \min\{\nu(x), \nu(y)\} \geq n$ und $\nu(zx) = \nu(zx) = \nu(z) + \nu(x) \geq n$, woraus $x - y, xz, zx \in \mathfrak{m}_D^n$ folgt. Das bedeutet, daß $\mathfrak{m}_D^n$ für alle $n \in \mathbb{N}$ ein zweiseitiges Ideal ist. Dabei ist $\mathfrak{m}_D := \mathfrak{m}_D^1$ die Menge aller Nichteinheiten und deshalb ein maximales Ideal von B_D. Weiter läßt sich zeigen, daß alle Ideale von B_D die Form $\mathfrak{m}^n$ haben. Sei dazu $\tilde{\mathfrak{m}}$ ein Ideal von B_D. Man setze $n := \min\{\nu(x) \mid x \in \tilde{\mathfrak{m}}\}$ und wähle $\tilde{x} \in \tilde{\mathfrak{m}}$, so daß $\nu(\tilde{x}) = n$ ist. Offensichtlich gilt nun $\tilde{\mathfrak{m}} \subset \mathfrak{m}_D^n$. Sei nun $y \in \mathfrak{m}_D^n$ beliebig. Dann folgt $\nu(y\tilde{x}^{-1}) = \nu(\tilde{x}^{-1}y) \geq 0$ und damit $y\tilde{x}^{-1}, \tilde{x}^{-1}y \in B_D$. Also ist $y \in \tilde{\mathfrak{m}}$. Daraus folgt $\tilde{\mathfrak{m}} = \mathfrak{m}_D^n$. Falls nun $t \in B_D$ so gewählt ist, daß $\nu(t) = 1$ ist, gilt $\mathfrak{m}_D^n = (t^n)$ (von t^n erzeugtes Ideal) für alle $n \in \mathbb{N}$. Man nennt t dann eine *Uniformisierende von D*.

Für die weiteren Betrachtungen verwendet man die Bezeichnungen $U_D^n := 1 + \mathfrak{m}_D^n = \{x \in B_D \mid \nu(x - 1) \geq n\}$ für alle $n \in \mathbb{N}$ sowie $U_D^0 := U_D$.

Lemma 1.3.1.3 *Durch $\{U_D^n\}_{n\in\mathbb{N}_0}$ ist eine absteigende Folge von Normalteilern gegeben*

$$U_D = U_D^0 \trianglerighteq U_D^1 \trianglerighteq U_D^2 \trianglerighteq U_D^3 \ldots\ .$$

Beweis: Aus Lemma 1.3.1.2 und der Tatsache, daß $\nu(-1) = 0$ ist, folgt $U_D^n \subset U_D$ für alle $n \in \mathbb{N}$. Für alle $x, y \in U_D$ gilt $x, y \equiv 1 \mod \mathfrak{m}_D^n$ und damit $xy^{-1} \equiv 1 \mod \mathfrak{m}_D^n$, woraus $xy^{-1} \in U_D^n$ folgt. Wegen $1 \in U_D \neq \emptyset$ erhält man, daß U_D^n für alle $n \in \mathbb{N}$ eine Untergruppe von U_D ist. Seien nun $x \in U_D^n$ und $y \in U_D$. Dann ergibt sich $\nu(yxy^{-1} - 1) = \nu(y) + \nu(x-1) + \nu(y^{-1}) = \nu(x-1) \geq n$ und damit $yxy^{-1} \in U_D^n$. Das bedeutet, daß U_D^n ein Normalteiler von U_D ist. □

In der Literatur wird U_D^n für alle $n \geq 1$ als die n-te Einseinheitengruppe bezeichnet. Es lassen sich nun für alle $n \in \mathbb{N}_0$ die Faktorgruppen $G_D^n := U_D/U_D^n$ definieren.

Lemma 1.3.1.4 *(i) Seien $x, y \in U_D$. Dann sind die Kongruenzbedingungen $x \equiv y \mod U_D^n$ und $x \equiv y \mod \mathfrak{m}_D^n$ für alle $n \in \mathbb{N}$ äquivalent.*

(ii) Es gilt $\{1\} = \bigcap_{n\in\mathbb{N}} U_D^n$.

(iii) Seien $x, y \in U_D$ mit $x \equiv y \mod \mathfrak{m}_D^n$ für alle $n \in \mathbb{N}$. Dann gilt $x = y$.

Beweis: (i) Offensichtlich gilt $x \equiv y \mod U_D^n$ genau dann, wenn $xy^{-1} \equiv 1 \mod U_D^n$ ist. Das ist gleichbedeutend mit $n \leq \nu(xy^{-1} - 1) = \nu(x - y)$ und folglich mit $x - y \in \mathfrak{m}_D^n$. Das wiederum gilt genau dann, wenn $x \equiv y \mod \mathfrak{m}_D^n$ ist.

(ii) Wegen $1 \in U_D^n$ für alle $n \in \mathbb{N}$ gilt $\{1\} \subset \bigcap_{n\in\mathbb{N}} U_D^n$. Sei $x \in \bigcap_{n\in\mathbb{N}} U_D^n$. Dann ist $\nu(x-1) \geq n$ für alle $n \in \mathbb{N}$ und damit $\nu(x-1) = \infty$. Daraus folgt $x = 1$. Somit gilt auch $\{1\} \supset \bigcap_{n\in\mathbb{N}} U_D^n$.

(iii) Aus $x \equiv y \mod \mathfrak{m}_D^n$ fogt $x \equiv y \mod U_D^n$ und damit $yx^{-1} \in U_D^n$ für alle $n \in \mathbb{N}$. Also ist $yx^{-1} \in \bigcap_{n\in\mathbb{N}} U_D^n$, woraus nach Teil (ii) die Gleichung $yx^{-1} = 1$ bzw. $x = y$ folgt. □

Satz 1.3.1.5 *Sei $t \in B_D$ eine Uniformisierende und $V_D \subset B_D$ ein Repräsentantensystem des Restklassenringes $B_D/\mathfrak{m}_D$. Dann ist*

$$V_D^n := \{\sum_{i=0}^{n-1} a_i t^i \mid a_0, \ldots, a_{n-1} \in V_D \ \ mit \ \ a_0 \notin \mathfrak{m}_D\}$$

ein Repräsentantensystem der Faktorgruppe G_D^n.

Beweis: Die Aussage wird durch Induktion über alle $n \in \mathbb{N}$ gezeigt.

Induktionsanfang $n = 1$: Weil $\mathfrak{m}_D$ und U_D disjunkt sind, folgt $V_D^1 \subset U_D$. Sei nun $xU_D^1 \in G_D^1$ beliebig. Dann gibt es ein $a_0 \in V_D$ mit $a_0 \equiv x \mod \mathfrak{m}_D^1$. Wegen $x \in U_D$ folgt $a_0 \notin \mathfrak{m}_D$, und somit ist $a_0 \in V_D^1$. Nach Lemma 1.3.1.4 folgt $a_0 \equiv x \mod U_D^1$. Seien schließlich $a_0, b_0 \in V_D^1$ mit $a_0 \equiv b_0 \mod U_D^1$. Dann folgt wegen $V_D^1 \subset V_D$ sofort $a_0 = b_0$.

Induktionsschritt $n \longmapsto n+1$: Nach Induktionsannahme ist $V_D^n \subset U_D$ ein Repräsentantensystem von G_D^n. Sei $y = \sum_{i=0}^{n} a_i t^i \in V_D^{n+1}$ beliebig. Dann gilt nach Lemma 1.3.1.2, daß $\nu(y) = 0$ und somit $y \in U_D$ ist. Daraus folgt $V_D^{n+1} \subset U_D$. Sei nun $x \in U_D$. Dann gibt es ein $y = \sum_{i=0}^{n-1} a_i t^i \in V_D^n$ mit $x \equiv y \mod U_D^n$. Daraus folgt $x \equiv y \mod \mathfrak{m}_D^n$ und damit $(x-y)t^{-n} \in B_D$. Da V_D ein Repräsentantensystem von $B_D/\mathfrak{m}_D^n$ ist, gibt es ein $a_n \in V_D$ mit $(x-y)t^{-n} \equiv a_n \mod \mathfrak{m}_D$. Daraus folgt $x \equiv y + a_n t^n \mod \mathfrak{m}_D^{n+1}$ und damit $x \equiv y + a_n t^n \mod U_D^{n+1}$, wobei $y + a_n t^n = \sum_{i=0}^{n} a_i t^i \in V_D^{n+1}$ ist. Seien schließlich $x = \sum_{i=0}^{n} a_i t^i, y = \sum_{i=0}^{n} b_i t^i \in V_D^{n+1}$ mit $x \equiv y \mod U_D^{n+1}$. Dann ergibt sich $x \equiv y \mod \mathfrak{m}_D^{n+1}$ und damit $\sum_{i=0}^{n-1} a_i t^i = \sum_{i=0}^{n-1} b_i t^i \mod \mathfrak{m}_D^n$ bzw. $\sum_{i=0}^{n-1} a_i t^i = \sum_{i=0}^{n-1} b_i t^i \mod U_D^n$. Nach Induktionsannahme folgt $a_i = b_i$ für $i = 0, \ldots, n-1$. Damit erhält man die Kongruenz $0 \equiv x - y \mod \mathfrak{m}_D^{n+1} \equiv (a_n - b_n)t^n \mod \mathfrak{m}_D^{n+1}$, woraus $a_n \equiv b_n \mod \mathfrak{m}_D^n$ folgt. Wegen $a_n, b_n \in V_D$ muß $a_n = b_n$ gelten. Somit ist $x = y$. □

Für die folgenden Betrachtungen sei $\rho \in (0, 1)$ festgewählt.

Definition 1.3.1.6 (Metrik auf D) *Die Abbildung $d : D \times D \longrightarrow \mathbb{R}$ sei definiert durch*

$$\mathrm{d}(x,y) := \begin{cases} \rho^{\nu(x-y)} & \textit{falls } x \neq y \\ 0 & \textit{falls } x = y. \end{cases}$$

Lemma 1.3.1.7 *Die Abbildung* d *ist eine Metrik auf D.*

Beweis: Die Axiome lassen sich elementar nachrechnen. Seien dazu $x, y, z \in D$. Wegen $\nu(x-y) = \nu(y-x)$ folgt $\mathrm{d}(x,y) = \mathrm{d}(y,x)$. Die Gleichheit $\mathrm{d}(x,y) = 0$ gilt offensichtlich genau dann, wenn $x = y$ ist. Falls x, y, z paarweise verschieden sind, erhält man

$$\begin{aligned} \mathrm{d}(x,z) &= \rho^{\nu(x-z)} \\ &= \rho^{\nu(x-y+y-z)} \\ &\leq \rho^{\min\{\nu(x-y),\nu(y-z)\}} \\ &= \max\{\rho^{\nu(x-y)}, \rho^{\nu(y-z)}\} \\ &\leq \rho^{\nu(x-y)} + \rho^{\nu(y-z)} \\ &= \mathrm{d}(x,y) + \mathrm{d}(y,z). \end{aligned}$$

Ansonsten gilt die Aussage $\mathrm{d}(x,z) \leq \mathrm{d}(x,y) + \mathrm{d}(y,z)$ trivialerweise. □

Bemerkung 1.3.1.8 Sei $\{x_n\}_{n\in\mathbb{N}}$ eine Folge in D und $x \in D$. Nach der Definition von d gilt $\lim_{n\to\infty} \mathrm{d}(x_n, x) = 0$, d. h. x ist Grenzwert der Folge $\{x_n\}_{n\in\mathbb{N}}$ genau dann, wenn $\lim_{n\to\infty} \nu(x - x_n) = \infty$ gilt.

Bekanntlich definiert jede Metrik eine Topologie. Im folgenden wird eine Menge $M \subset D$ als abgeschlossen bezeichnet, wenn sie abgeschlossen bezüglich der von d definierten Topologie ist. Das bedeutet, daß für alle konvergenten Folgen $\{x_n\}_{n\in\mathbb{N}} \subset M$ auch der Grenzwert $\lim_{x\to\infty} x_n$ in M liegt.

Lemma 1.3.1.9 *Für alle $n \in \mathbb{N}_0$ ist U_D^n abgeschlossen.*

Beweis: Sei $\{x_i\}_{i\in\mathbb{N}}$ eine konvergente Folge auf U_D^n mit Grenzwert x. Dann muß es wegen $\lim_{i\to\infty} \nu(x - x_i) = \infty$ ein $i \in \mathbb{N}$ geben mit $\nu(x - x_i) \geq n + 1$. Daraus folgt $x - x_i \in \mathfrak{m}_D^{n+1}$ und damit $x \equiv x_i \mod \mathfrak{m}_D^{n+1}$. Wegen $\nu(x_i) = 0 < n + 1$ folgt nach Lemma 1.3.1.2, daß $\nu(x) = 0$ ist. Also gilt $x \in U_D$. Mit Lemma 1.3.1.4 erhält man $x \equiv x_i \mod U_D^{n+1}$. Da $x_i \in U_D^n$ ist, folgt $x \in U_D^n$. □

Satz 1.3.1.10 *Seien $\{x_i\}_{i\in\mathbb{N}}$ und $\{y_i\}_{i\in\mathbb{N}}$ konvergente Folgen auf der Einheitengruppe U_D mit den Grenzwerten x und y. Dann sind $\{y_i x_i\}_{i\in\mathbb{N}}$ und $\{x_i^{-1}\}_{i\in\mathbb{N}}$ ebenfalls konvergent, und für die Grenzwerte gilt*

(i) $\lim_{i\to\infty} x_i y_i = xy$ *und*

(ii) $\lim_{i\to\infty} x_i^{-1} = x^{-1}$.

Beweis: (i) Sei $n \in \mathbb{N}$. Dann gibt es $r_1, r_2 \in \mathbb{N}$, so daß für alle $i \in \mathbb{N}$ mit $i \geq r_1$ die Bedingung $\nu(x_i - x) \geq n$ und für alle $i \in \mathbb{N}$ mit $i \geq r_2$ die Bedingung $\nu(y_i - y) \geq n$ erfüllt ist. Man setze nun $r := \max\{r_1, r_2\}$. Dann gilt für alle $i \in \mathbb{N}$ mit $i \geq r$, daß $\nu(x_i - x), \nu(y_i - y) \geq n$ ist. Daraus folgt $x_i - x, y_i - y \in \mathfrak{m}_D^n$ und damit $x_i \equiv x \mod \mathfrak{m}_D^n$ sowie $y_i \equiv y \mod \mathfrak{m}_D^n$. Also gilt $x_i y_i \equiv xy \mod \mathfrak{m}_D^n$. und somit auch $\nu(x_i y_i - xy) \geq n$. Damit ist gezeigt, daß $\lim_{i\to\infty} \nu(x_i y_i - yx) = \infty$ ist. Nach Bemerkung 1.3.1.8 folgt hieraus $\lim_{i\to\infty} x_i y_i = xy$.

(ii) Sei $n \in \mathbb{N}$. Dann gibt es ein $r \in \mathbb{N}$, so daß für alle $i \in \mathbb{N}$ mit $i \geq r$ die Bedingung $\nu(x_i - x) \geq n$ erfüllt ist. Daraus folgt $x_i \equiv x \mod \mathfrak{m}_D^n$ und damit $x_i^{-1} \equiv x^{-1} \mod \mathfrak{m}_D^n$, woraus sich schließlich $\nu(x_i^{-1} - x^{-1}) \geq n$ ergibt. Damit ist gezeigt, daß $\lim_{i\to\infty} \nu(x_i^{-1} - x^{-1}) = \infty$ ist. Nach Bemerkung 1.3.1.8 folgt hieraus $\lim_{i\to\infty} x_i^{-1} = x^{-1}$. □

Korollar 1.3.1.11 *Seien $i, j \in \mathbb{N}_0$. Dann ist die Menge $M := \{xyx^{-1}y^{-1} \mid x \in U_D^i \text{ und } y \in U_D^j\}$ abgeschlossen.*

Beweis: Man definiere $f : U_D^i \times U_D^j \longrightarrow U_D$ durch $(x,y) \longmapsto xyx^{-1}y^{-1}$. Dann gilt $f(U_D^i \times U_D^j) = M$. Sei nun $\{x_i\}_{i\in\mathbb{N}} \subset U_D^i$ eine konvergente Folge mit Grenzwert x und $\{y_i\}_{i\in\mathbb{N}} \subset U_D^j$ eine konvergente Folge mit Grenzwert y. Dann folgt nach Satz 1.3.1.10 die Konvergenz von $\{x_n y_n x_n^{-1} y_n^{-1}\}_{n\in\mathbb{N}}$ gegen $xyx^{-1}y^{-1}$ und damit die Stetigkeit von f. Da U_D^i und U_D^j nach Lemma 1.3.1.9 abgeschlossen sind, folgt die Abgeschlossenheit von M. □

Definition 1.3.1.12 *(i) Eine Folge $\{x_n\}_{n\in\mathbb{N}} \subset D$ heißt Cauchyfolge, wenn*

$$\lim_{n\to\infty} \nu(x_{n+1} - x_n) = \infty$$

gilt.

(ii) D heißt vollständig, wenn jede Cauchyfolge in D konvergiert.

Die Grenzwerte von Cauchyfolgen lassen sich nun folgendermaßen charakterisieren.

Lemma 1.3.1.13 *Sei D vollständig. Weiter sei $\{x_n\}_{n\in\mathbb{N}} \subset D$ eine Folge, so daß es eine streng monoton wachsende Folge $\{r_n\}_{n\in\mathbb{N}} \subset \mathbb{N}$ gibt, die der folgenden Bedingung genügt: Für alle $i, n \in \mathbb{N}$ mit $i \geq n$ gilt $\nu(x_{i+1} - x_i) \geq r_i$. Dann ist $\{x_n\}_{n\in\mathbb{N}}$ konvergent und für den Grenzwert x gilt $\nu(x - x_i) \geq r_n$ für alle $i \in \mathbb{N}$ mit $i \geq n$.*

Beweis: Die Folge $\{x_n\}_{n\in\mathbb{N}}$ ist konvergent, da sie eine Cauchyfolge ist. Seien nun $i, n \in \mathbb{N}$ mit $i \geq n$. Angenommen, es gälte $\nu(x - x_i) < r_n$. Wegen $x = \lim_{l\to\infty} x_l$ müßte es dann ein $l \in \mathbb{N}$ geben mit $l > i$ und $\nu(x - x_l) \geq r_n$. Daraus folgte $\nu(x_l - x_i) = \nu((x - x_i) - (x - x_l)) < r_n$ nach Lemma 1.3.1.2. Wegen $\nu(x_l - x_i) = \nu\left(\sum_{j=i}^{l-1} x_{j+1} - x_j\right) \geq \min\{\nu(x_{j+1} - x_j) \mid j = 1, \ldots, l-1\} \geq r_n$ ergäbe sich ein Widerspruch. Also muß $\nu(x - x_i) \geq r_n$ gelten. □

1.3.2 Der Zusammenhang zwischen U_D und den Faktorgruppen G_D^n

Es ist klar, daß die Struktur auf U_D die Struktur der Faktorgruppen G_D^n bedingt. Es stellt sich nun die Frage, was man bei Kenntnis der Faktorgruppen G_D^n über die Stuktur von U_D sagen kann. Um diese Frage zu klären, benötigt man zunächst einige Hilfsmittel.

Definition 1.3.2.1 *(i) Eine Folge von Gruppen $\{H_l\}_{l\in\mathbb{N}}$ zusammen mit den Homomorphismen $\phi_m^n : H_m \longrightarrow H_n$ für alle $m \geq n \in \mathbb{N}$ heißt* projektives System, *falls für alle $l \geq m \geq n \in \mathbb{N}$ die Relationen*

$$\phi_m^n \circ \phi_l^m = \phi_l^n \quad \textit{sowie} \quad \phi_l^l = \mathrm{id}_{\mathrm{H_l}}$$

gelten.

(ii) Eine Gruppe H zusammen mit den Homomorphismen $(\phi_l : H \longrightarrow H_l)_{l\in\mathbb{N}}$ heißt mit einem projektiven System $(\phi_m^n : H_m \longrightarrow H_n)_{m\geq n\in\mathbb{N}}$ verträglich, *falls das Diagramm*

$$\begin{tikzcd} & H \arrow[dl, "\phi_m"'] \arrow[dr, "\phi_n"] & \\ H_m \arrow[rr, "\phi_m^n"] & & H_n \end{tikzcd}$$

für alle $m \geq n \in \mathbb{N}$ kommutiert.

Für die folgenden Betrachtungen sei $\vartheta_l : U_D \longrightarrow G_D^l$ für alle $l \in \mathbb{N}$ der kanonische Homomorphismus. Weiter seien für alle $m \geq n \in \mathbb{N}$ die Homomorphismen $\vartheta_m^n : G_D^m \longrightarrow G_D^n$ durch die Vorschrift $xU_D^m \longmapsto xU_D^n$ erklärt (Wegen $U_D^m \subset U_D^n$ folgt die Wohldefiniertheit).

Lemma 1.3.2.2 *(i) Die Homomorphismen $(\vartheta_m^n : G_D^m \longrightarrow G_D^n)_{m \geq n \in \mathbb{N}}$ bilden ein projektives System.*

(ii) Das System der kanonischen Homomorphismen $\left(\vartheta_l : U_D \longrightarrow G_D^l\right)_{l \in \mathbb{N}}$ ist mit dem System $(\vartheta_m^n : G_D^m \longrightarrow G_D^n)_{m \geq n \in \mathbb{N}}$ verträglich.

Beweis: (i) Zunächst ist zu bemerken, daß die Homomorphismen ϑ_m^n wegen $U_D^m \subset U_D^n$ für alle $m \geq n \in \mathbb{N}$ wohldefiniert sind. Seien nun $l \geq m \geq n \in \mathbb{N}$ und $xU_D^l \in G_D^l$ beliebig. Dann gilt $\vartheta_m^n(\vartheta_l^m(xU_D^l)) = \vartheta_m^n(xU_D^m) = xU_D^n$, woraus $\vartheta_m^n \circ \vartheta_l^m = \vartheta_l^n$ folgt, sowie $\vartheta_l^l(xU_D^l) = xU_D^l$, woraus $\vartheta_l^l = \mathrm{id}_{G_D^l}$ folgt. Damit ist gezeigt, daß $(\vartheta_m^n : G_D^m \longrightarrow G_D^n)_{m \geq n \in \mathbb{N}}$ ein projektives System ist.

(ii) Für alle $m \geq n \in \mathbb{N}$ und $x \in U_D$ gilt $\vartheta_n^m(\vartheta_m(x)) = \vartheta_m^n(xU_m) = xU_D^n = \vartheta_n(x)$, woraus $\vartheta_n^m \circ \vartheta_m = \vartheta_n$ folgt. Damit ist gezeigt, daß $\left(\vartheta_l : U_D \longrightarrow G_D^l\right)_{l \in \mathbb{N}}$ mit $(\vartheta_m^n : G_D^m \longrightarrow G_D^n)_{m \geq n \in \mathbb{N}}$ verträglich ist. □

Definition 1.3.2.3 *Ein System von Homomorphismen der Form $(\phi_l : H \longrightarrow H_l)_{l \in \mathbb{N}}$, das mit dem projektiven System $(\phi_m^n : H_m \longrightarrow H_n)_{m \geq n \in \mathbb{N}}$ verträglich ist, nennt man einen* projektiven Limes von $(\phi_m^n : H_m \longrightarrow H_n)_{m \geq n \in \mathbb{N}}$, *wenn für alle Systeme von Homomorphismen $\left(\tilde{\phi}_l : \tilde{H} \longrightarrow H_l\right)_{l \in \mathbb{N}}$, die verträglich mit $(\phi_m^n : H_m \longrightarrow H_n)_{m \geq n \in \mathbb{N}}$ sind, die folgende universelle Eigenschaft erfüllt ist: Es gibt einen eindeutig bestimmten Homomorphismus $\Phi : \tilde{H} \longrightarrow H$, so daß $\phi_l \circ \Phi = \tilde{\phi}_l$ für alle $l \in \mathbb{N}$ gilt.*

Unter den Voraussetzungen dieser Definition kommutiert für alle $m \geq n \in \mathbb{N}$ das folgende Diagramm:

$$\begin{tikzcd}
 & H \arrow[ddl, "\phi_m"'] \arrow[ddr, "\phi_n"] & \\
 & \tilde{H} \arrow[u, "\Phi"'] \arrow[dl, "\tilde{\phi}_m"'] \arrow[dr, "\tilde{\phi}_n"] & \\
H_m \arrow[rr, "\phi_m^n"] & & H_n.
\end{tikzcd}$$

Satz 1.3.2.4 *Für jedes projektive System $(\phi_m^n : H_m \longrightarrow H_n)_{m \geq n \in \mathbb{N}}$ gibt es einen projektiven Limes $(\phi_l : H \longrightarrow H_l)_{l \in \mathbb{N}}$. Die Gruppe H ist dabei bis auf Isomorphie eindeutig bestimmt. Es läßt sich*

$$H := \{(x_l)_{l \in \mathbb{N}} \in \prod_{l \in \mathbb{N}} H_l \mid \phi_m^n(x_m) = x_n \;\; \textit{für alle} \;\; n \geq m \in \mathbb{N}\}$$

mit den kanonischen Projektionen

$$\phi_l : H \longrightarrow H_l, \;\; (x_m)_{m \in \mathbb{N}} \longmapsto x_l$$

für alle $l \in \mathbb{N}$ wählen.

Beweis: Um zu beweisen, daß das System $(\phi_l : H \longrightarrow H_l)_{l\in\mathbb{N}}$ ein projektiver Limes des Systems $(\phi_m^n : H_m \longrightarrow H_n)_{m\geq n\in\mathbb{N}}$ ist, zeigt man zunächst die Verträglichkeit. Seien dazu $m \geq n \in \mathbb{N}$. Dann gilt für alle $x = (x_l)_{l\in\mathbb{N}} \in H$, daß $\phi_m^n(\phi_m(x)) = \phi_m^n(x_m) = x_n$ ist, woraus $\phi_m^n \circ \phi_m = \phi_n$ und damit die Verträglichkeit folgt. Sei nun $\left(\tilde{\phi}_l : \tilde{H} \longrightarrow H_l\right)_{l\in\mathbb{N}}$ ein System von Homomorphismen, das mit $(\phi_m^n : H_m \longrightarrow H_n)_{m\geq n\in\mathbb{N}}$ verträglich ist. Man definiere $\Phi : \tilde{H} \longrightarrow H$ durch $\tilde{x} \longmapsto (\tilde{\phi}_l(\tilde{x}))_{l\in\mathbb{N}}$. Daß $(\tilde{\phi}(\tilde{x}))_{l\in\mathbb{N}}$ auch wirklich in H liegt, folgt aus der Tatsache, daß für alle $m \geq n \in \mathbb{N}$ die Gleichung $\phi_m^n(\tilde{\phi}_m(\tilde{x})) = \tilde{\phi}_n(\tilde{x})$ gilt. Die Abbildung Φ ist ein Homomorphismus, weil die einzelnen Komponenten $\tilde{\phi}_l : \tilde{H} \longrightarrow H_l$ Homomorphismen sind. Sei nun $l \in \mathbb{N}$. Dann gilt für alle $\tilde{x} \in \tilde{H}$, daß $\phi_l(\Phi(\tilde{x})) = \phi_l((\tilde{\phi}_m(\tilde{x}))_{m\in\mathbb{N}}) = \tilde{\phi}_l(\tilde{x})$ ist, woraus $\phi_l \circ \Phi = \tilde{\phi}_l$ folgt. Da für alle $\tilde{x} \in \tilde{H}$ durch die Verträglichkeitsbedingung $\phi_l(\Phi(\tilde{x})) = \tilde{\phi}_l(\tilde{x})$ jeweils die l-te Komponente von Φ eindeutig festgelegt ist, folgt die Eindeutigkeit von Φ.

Um zu zeigen, daß H bis auf Isomorphie eindeutig bestimmt ist, seien $(\phi_l : H \longrightarrow H_l)_{l\in\mathbb{N}}$ und $({\phi'}_l : H' \longrightarrow H_l)_{l\in\mathbb{N}}$ jeweils projektive Limiten von $(\phi_m^n : H_m \longrightarrow H_n)_{m\geq n\in\mathbb{N}}$. Dann folgt aus der universellen Eigenschaft die Existenz von Homomorphismen $\Phi : H' \longrightarrow H$ und $\Phi' : H \longrightarrow H'$, so daß $\phi_l \circ \Phi = {\phi'}_l$ und $\phi'_l \circ \Phi' = \phi_l$ für alle $l \in \mathbb{N}$ efrüllt ist. Daraus folgt $\phi_l \circ \Phi \circ \Phi' = \phi_l$ sowie $\phi'_l \circ \Phi' \circ \Phi = {\phi'}_l$. Weil die identischen Abbildungen $\mathrm{id_H}$ und $\mathrm{id_{H'}}$ ebenfalls die Bedingungen $\phi_l \circ \mathrm{id_H} = \phi_l$ und ${\phi'}_l \circ \mathrm{id_{H'}} = {\phi'}_\mathrm{l}$ erfüllen, ergibt sich aus der Eindeutigkeitsforderung $\mathrm{id_H} = \Phi \circ \Phi'$ und $\mathrm{id_{H'}} = \Phi' \circ \Phi$. Daraus folgt schließlich die Bijektivität von Φ und Φ' und damit die Isomorphie $H \cong H'$. □

Satz 1.3.2.5 *Sei D vollständig. Dann läßt sich das System $\left(\vartheta_l : U_D \longrightarrow G_D^l\right)_{l\in\mathbb{N}}$ als ein projektiver Limes von $(\vartheta_m^n : G_D^m \longrightarrow G_D^n)_{m\geq n\in\mathbb{N}}$ auffassen.*

Beweis: Sei $G := \{(x_l U_D^l)_{l\in\mathbb{N}} \in \prod_{l\in\mathbb{N}} G_D^l \mid \vartheta_m^n(x_m U_D^l) = x_n U_D^n \textit{ für alle } m \geq n \in \mathbb{N}\}$ und $\tilde{\vartheta}_l : G \longrightarrow G_D^l,\ \ (x_m U_D^m)_{m\in\mathbb{N}} \longmapsto x_l U_D^l$ für alle $l \in \mathbb{N}$ die kanonische Projektion. Dann ist $\left(\tilde{\vartheta}_l : G \longrightarrow G_D^l\right)_{l\in\mathbb{N}}$ nach Satz 1.3.2.4 der projektive Limes von $(\vartheta_m^n : G_D^m \longrightarrow G_D^n)_{m\geq n\in\mathbb{N}}$. Daraus folgt, daß es einen Homomorphismus $\Theta : U_D \longrightarrow G$ gibt mit $\tilde{\vartheta}_l(\Theta(x)) = \vartheta_l(x) = xU_D^l$ für alle $x \in U_D$ und $l \in \mathbb{N}$. Daraus folgt $\Theta(x) = (xU_D^l)_{l\in\mathbb{N}}$ für alle $x \in U_D$. Sei nun $x \in \mathrm{Kern}\Theta$. Dann folgt $x \in U_D^l$ für alle $l \in \mathbb{N}$. Also ist $x \in \bigcap_{l\in\mathbb{N}} U_D^l$. Wegen Lemma 1.3.1.4 folgt $x = 1$ und damit $\mathrm{Kern}\Theta = \{1\}$. Das bedeutet, daß Θ injektiv ist. Sei nun $(x_l U_D^l)_{l\in\mathbb{N}} \in G$ beliebig. Dann gilt für alle $l \in \mathbb{N}$, daß $x_{l+1}U_D^l = \vartheta_l^{l+1}(x_{l+1}U_D^{l+1}) = x_l U_D^l$ und damit $x_{l+1} = x_l \mod \mathfrak{m}_D^l$ bzw. $\nu(x_{l+1} - x_l) \geq l$ ist. Die Anwendung von Lemma 1.3.1.13 (mit $r_n = n$) ergibt, daß $\{x_n\}_{n\in\mathbb{N}} \subset D$ konvergent ist, wobei für den Grenzwert x gilt $\nu(x - x_l) \geq l$ für alle $l \in \mathbb{N}$. Wegen $\nu(x_1) = 0$ folgt $\nu(x) = 0$ und damit $x \in U_D$. Damit ergibt sich nun $x \equiv x_l \mod \mathfrak{m}_D^l$ bzw. $x \equiv x_l \mod U_D^l$. Daraus folgt $\Theta(x) = (x_l U_D^l)_{l\in\mathbb{N}}$. Das bedeutet Θ ist surjektiv.

Damit läßt sich nun die universelle Eigenschaft von $\left(\vartheta_l : U_D \longrightarrow G_D^l\right)_{l\in\mathbb{N}}$ zeigen. Sei dazu $\left(\vartheta_l^* : H^* \longrightarrow G_D^l\right)$ ein System von Homomorphismen, das verträglich mit $(\vartheta_m^n : G_D^m \longrightarrow G_D^n)_{m\geq n\in\mathbb{N}}$ ist. Dann gibt es einen eindeutig bestimmten Homomorphismus $\Theta^* : H^* \longrightarrow G$, so daß $\tilde{\vartheta}_l \circ \Theta^* = \vartheta_l^*$ für alle $l \in \mathbb{N}$ gilt. Man definiere nun $\Phi : H^* \longrightarrow U_D$ durch $\Phi := \Theta^{-1} \circ \Theta^*$. Wegen $\tilde{\vartheta} \circ \Theta = \vartheta_l$ für alle $l \in \mathbb{N}$ folgt $\tilde{\vartheta} = \vartheta_l \circ$ und damit $\vartheta_l \circ \Phi = \vartheta_l \Theta^{-1} \circ \Theta^* = \vartheta_l^*$. Sei nun umgekehrt $\Phi' : H^* \longrightarrow U_D$ ein Homomorphismus, so daß $\vartheta_l \circ \Phi' = \vartheta_l^*$ für alle $l \in \mathbb{N}$ erfüllt ist. Dann folgt $\vartheta_l \circ \Phi' = \tilde{\vartheta}_l \circ \Theta^*$ und damit $\tilde{\vartheta}_l \circ \Theta^* \circ \Phi' = \vartheta_l$ für alle $l \in \mathbb{N}$. Daraus ergibt sich schließlich $\Theta = \Theta^* \circ (\Phi')^{-1}$ bzw. $\Phi' = \Theta^{-1} \circ \Theta^* = \Phi$. □

Falls D vollständig ist, besagt Satz 1.3.2.5, daß die Struktur von U_D *eindeutig* durch die Struktur der Faktorgruppen G_D^n bestimmt ist. Das heißt nun, daß jede Beschreibung der Gruppenstruktur auf G_D^n für alle $n \in \mathbb{N}$ sofort einen Beschreibung der Struktur auf U_D liefert. Es ist also gerechtfertigt, sich bei der Untersuchung von U_D auf die Untersuchung der Faktorgruppen G_D^n zu beschränken.

1.3.3 L als lokaler Körper und Q als vollständig bewerteter Divisionsring

Satz 1.3.3.1 *Die Abbildung $\nu_L : L \longrightarrow \mathbb{Z} \cup \{\infty\}$ mit der Vorschrift*

$$x = \sum_{i=m}^{\infty} a_i T^i \longmapsto \begin{cases} \min\{i \in \mathbb{Z} \mid a_i \neq 0\} & \textit{falls } x \neq 0 \\ \infty & \textit{falls } x = 0 \end{cases}$$

definiert eine Bewertung auf dem Laurentreihenkörper L. Außerdem ist L vollständig bezüglich ν_L.

Beweis: Wegen $\nu_L(T^n) = n$ für alle $n \in \mathbb{Z}$ folgt die Surjektivität von ν_L. Die übrigen Eigenschaften einer Bewertung rechnet man wie folgt nach.

(Bew 1): Sei $x \in L$. Dann folgt direkt aus der Definition von ν_L, daß $\nu_L(x) = \infty$ genau dann gilt, wenn $x = 0$ ist.

(Bew 2): Seien $x = \sum_{i=m}^{\infty} a_i \tau^i, y = \sum_{i=n}^{\infty} b_i \tau^i \in L^*$. Ohne Einschränkung kann man $\nu_L(x) = m$ und $\nu_L(y) = n$ annehmen. Daraus folgt

$$xy = \sum_{i=m+n}^{\infty} \left(\sum_{k=m}^{i-n} a_k b_{i-k} \right) T^i.$$

Wegen $a_n a_m \neq 0$ folgt $\nu(xy) = n + m = \nu(x) + \nu(y)$.

(Bew 3): Seien $x = \sum_{i=m}^{\infty} a_i T^i, y = \sum_{i=n}^{\infty} b_i T^i \in L^*$. Ohne Einschränkung sei $\nu_L(x) = m$ und $\nu_L(y) = n$ sowie $m \leq n$. Dann gilt $x + y = \sum_{i=m}^{\infty} (a_i + b_i) T^i$, wobei $b_i := 0$ sei für $i = m, \ldots, n-1$. Daraus folgt $\nu_L(x + y) \geq m = \min\{\nu_L(x), \nu_L(y)\}$.

Um die Vollständigkeit von L zu zeigen, sei $\{x_j = \sum_{i=m_j}^{\infty} a_i^{(j)} T^i\}_{j \in \mathbb{N}}$ eine Cauchyfolge bezüglich ν_L. Man definiere $r(n) := \max\{k \in \mathbb{N} \mid \nu_L(x_{k+1} - x_k) \leq n\} + 1$ für alle $n \in \mathbb{N}$. Dann gilt für alle $j \in \mathbb{N}$ mit $j \geq r(n)$, daß

$$\nu(x_j - x_{r(n)}) = \nu \left(\sum_{k=r(n)}^{j-1} x_{k+1} - x_k \right) \geq \min\{\nu(x_{k+1} - x_k) \mid k = r(n), \ldots, j-1\} > n$$

ist. Man setze nun $x = \sum_{i=m_{r(0)}}^{0} a_i^{(r(0))} T^i + \sum_{i=1}^{\infty} a_i^{(r(i))} T^i$. Dabei sei ohne Einschränkung angenommen, daß $m_{r(0)} \leq 0$ ist. Man zeigt nun durch Induktion, daß $\nu(x - x_{r(n)}) > n$ für alle $n \in \mathbb{N}_0$ gilt. Für $n = 0$ gilt $x - x_{r(0)} = \sum_{i=1}^{\infty} (a_i^{(r(i))} - a_i^{(r(0))}) T^i$ und somit $\nu(x - x_{r(0)}) > 0$. Sei nun $n \in \mathbb{N}_0$ beliebig. Dann gilt

$$\nu(x - x_{r(n+1)}) \geq \min\{\nu(x - x_{r(n)}), \nu(x_{r(n)} - x_{r(n+1)})\} > n$$

nach Induktionsannahme. Daraus folgt

$$x - x_{r(n+1)} = \sum_{i=n+1}^{\infty} (a_i^{(r(i))} - a_i^{(r(n+1))}) T^i = \sum_{i=n+2}^{\infty} (a_i^{(r(i))} - a_i^{(r(n+1))}) T^i$$

und damit $\nu(x - x_{r(n+1)}) > n + 1$.

Sei nun $n \in \mathbb{N}$ beliebig. Dann gilt für alle $j \in \mathbb{N}$ mit $j \geq r(n)$, daß $\nu(x - x_j) \geq \min\{\nu(x - x_{r(n)}), \nu(x_{r(n)} - x_j)\} > n$ ist. Damit ist die Konvergenz von $\{x_j\}_{j \in \mathbb{N}}$ gezeigt. □

Bemerkung 1.3.3.2 Als Uniformisierende von L kann man nun T wählen. Für den Bewertungsring ergibt sich $B_L = \{\sum_{i=0}^{\infty} a_i T^i \mid a_0, a_1, \ldots \in \mathbb{F}_{q^2}\}$ mit der Einheitengruppe $U_L = \{\sum_{i=0}^{\infty} a_i T^i \mid a_0, a_1, \ldots \in \mathbb{F}_{q^2}$ *mit* $a_0 \neq 0\}$ und dem maximalen Ideal $\mathfrak{m}_L = \{\sum_{i=1}^{\infty} a_i T^i \mid a_1, a_2, \ldots \in \mathbb{F}_{q^2}\}$. Für den Restklassenring gilt $B_L / \mathfrak{m}_L \cong \mathbb{F}_q$.

Definition 1.3.3.3 *Ein Körper K mit einer Bewertung ν heißt lokal, wenn dieser vollständig bezüglich ν ist und der Restklassenring $B_K/\mathfrak{m}_K$ ein endlicher Körper ist.*

Nach Satz 1.3.3.1 und Bemerkung 1.3.3.2 ist L mit der Bewertung ν_L ein lokaler Körper. Die Theorie liefert nun folgende Klassifizierung von Quaternionendivisionsalgebren über lokalen Körpern.

Satz 1.3.3.4 *Sei K ein lokaler Körper. Dann gibt es über K bis auf Isomorphie eine eindeutig bestimmte Quaternionenalgebra, die zugleich Divisionsalgebra ist.*

Beweis: Siehe [12], théorème 1.1, p. 31. □

Da Q nach Lemma 1.2.3.7 eine Divisionsalgebra ist, ist es von nun an gerechtfertigt, von Q als *der* Quaternionendivisionsalgebra über L zu sprechen.

Satz 1.3.3.5 *Die Abbildung $\nu_Q : Q \longrightarrow \mathbb{Z} \cup \{\infty\}$ mit der Vorschrift*

$$x = \sum_{i=m}^{\infty} a_i \tau^i \longmapsto \begin{cases} \min\{i \in \mathbb{Z} \mid a_i \neq 0\} & \textit{falls } x \neq 0 \\ \infty & \textit{falls } x = 0 \end{cases}$$

definiert eine Bewertung auf Q. Außerdem ist Q vollständig bezüglich ν_Q.

Beweis: Der Beweis verläuft analog zum Beweis von 1.3.3.1, wenn man L durch Q und T durch τ ersetzt. Lediglich beim Nachweis von (**Bew 2**) ist zu beachten, daß man hier $a_n b_m^{q^n}$ für den $n+m$-ten Koeffizienten von xy erhält. Dies ändert aber nichts an der Tatsache, daß auch hier $\nu(x) = n + m$ ist. □

Wegen der besseren Übersichtlichkeit läßt man den Index Q weg und wählt für den gesamten Rest dieser Arbeit die Bezeichnung B für den Bewertungsring von Q sowie $\mathfrak{m}$ für das maximale Ideal des Bewertungsringes und U für die Einheitengruppe von Q. Ebenso vewendet man das Symbol U_n anstelle von U_Q^n, und für die Faktorgruppen wählt man die Bezeichnung G_n statt G_Q^n.

Bemerkung 1.3.3.6 Als Uniformisierende von Q läßt sich nun τ wählen. Für den Bewertungsring erhält man $B = \{\sum_{i=0}^{\infty} a_i \tau^i \mid a_0, a_1, \ldots \in \mathbb{F}_{q^2}\}$ mit der Einheitengruppe $U = \{\sum_{i=0}^{\infty} a_i \tau^i \mid a_0, a_1, \ldots \in \mathbb{F}_{q^2} \textit{ mit } a_0 \neq 0\}$ und dem maximalen Ideal $\mathfrak{m} = (\tau) = \{\sum_{i=1}^{\infty} a_i \tau^i \mid a_1, a_2, \ldots \in \mathbb{F}_{q^2}\}$. Für den Restklassenring gilt $B/\mathfrak{m} \cong \mathbb{F}_{q^2}$.

Da sowohl L als auch Q vollständig bewertete Divisionsringe sind, gestattet es Satz 1.3.2.5, die Einheitengruppen U_L und U als projektive Limiten der Faktorgruppen G_L^n und G_n aufzufassen und sich damit auf deren Untersuchung zu beschränken.

Kapitel 2

Die Struktur der Einheitengruppe U_L des Laurentreihenkörpers L

2.1 Der Zusammenhang zwischen U_L und U_L^1

Zunächst läßt sich eine elementare Aussage über die Struktur von U_L ableiten.

Lemma 2.1.1 *Es gilt die Isomorphie $U_L \cong \mathbb{F}_q^* \times U_L^1$.*

Beweis: Man zeigt, daß die Abbildung $\psi : \mathbb{F}_q^* \times U_L^1 \longrightarrow U_L, (a,x) \longmapsto ax$ ein Gruppenisomorphismus ist. Seien dazu $(a_1,x_1),(a_2,x_2) \in \mathbb{F}_q^* \times U_L^1$. Dann gilt

$$\begin{aligned}
\psi((a_1,x_1)\cdot(a_2,x_2)) &= \psi((a_1a_2,x_1x_2)) \\
&= a_1a_2x_1x_2 \\
&= a_1x_1a_2x_2 \\
&= \psi((a_1,x_1))\psi((a_1,x_2)).
\end{aligned}$$

Also ist ψ ein Gruppenhomomorphismus. Sei $(a,x) \in \mathbb{F}_q^* \times U_L^1$ mit $\psi((a,x)) = 1$. Dann gilt $ax = 1$. Daraus folgt $a \equiv 1 \mod \mathfrak{m}_L$. Wegen $a \in \mathbb{F}_q^*$ folgt $a = 1$. Damit ergibt sich $x = 1$. Also ist ψ injektiv. Sei nun $y \in U_L$ beliebig. Dann gibt es ein $a \in \mathbb{F}_q^*$ mit $a \equiv y \mod \mathfrak{m}_L$. Daraus folgt $(a,a^{-1}y) \in \mathbb{F}_q^* \times U_L^1$. Wegen $\psi((a,a^{-1}y)) = y$ erhält man die Surjektivität von ψ. □

Damit reduziert sich die Untersuchung von U_L auf die Untersuchung der sog. Einseinheitengruppe U_L^1. Wegen der Isomorphie $G_L^n = U_L/U_L^n \cong \mathbb{F}_q^* \times U_L^1/U_L^n$ für alle $n \in \mathbb{N}$ reicht es hierbei aus, sich auf die Untersuchung der Faktorgruppen $\hat{G}_L^n := U_L^1/U_L^n$ zu beschränken. Im folgenden Abschnitt werden nun deren zyklische Anteile bestimmt. Im darauffolgenden Abschnitt wird gezeigt, welche Konsequenzen sich daraus für die Struktur der Einheitengruppe U_L sowie der Einseinheitengruppe U_L^1 ergeben.

2.2 Die Struktur der Faktorgruppen $\hat{G}_L^n$

Nach Satz 1.3.1.5 ist $V_L^n := \{\sum_{i=0}^{n-1} a_iT^i \mid a_0,\ldots,a_{n-1} \in \mathbb{F}_q \ \ mit \ \ a_0 \neq 0\}$ ein Repräsentantensystem der Faktorgruppe G_L^n. Wegen $U_L^n \subset U_L^1 \subset U_L$ läßt sich $\hat{G}_L^n := U_L^1/U_L^n$ als Untergruppe von G_L^n auffassen. Ein $x = \sum_{i=0}^{n-1} a_iT^i \in V_L^n$ liegt genau dann in U_L^1, wenn $a_0 = 1$ ist. Daraus folgt, daß $\hat{V}_L^n := \{1 + \sum_{i=0}^{n-1} a_iT^i \mid a_1,\ldots,a_{n-1} \in \mathbb{F}_q\}$ ein Repräsentantensystem von $\hat{G}_L^n$ ist. Damit hat $\hat{G}_L^n$ die Kardinalität $\#\hat{G}_L^n = (\#\mathbb{F}_q)^{n-1} = q^{n-1}$. Wegen der Kommutativität von $\#\hat{G}_L^n$ bleibt nur die Zerlegung in zyklische Anteile zu bestimmen.

Nach dem Basissatz für endliche abelsche Gruppen gibt es nun eine eindeutig bestimmte natürliche Zahl m sowie eindeutig bestimmte Vielfachheiten $v_i \in \mathbb{N}_0$ für $i = 1, \ldots, m$, so daß $v_m \neq 0$ ist und die Isomorphie

$$\hat{G}_L^n \cong \prod_{i=1}^{m} \left(\prod_{j=1}^{v_i} \left(\mathbb{Z}/p^i\mathbb{Z}\right)_j \right)$$

gilt. Dabei entspricht p^m der höchsten vorkommenden Ordnung, die ein Element von $\hat{G}_L^n$ haben kann.

Für die weiteren Betrachtungen sowie den gesamten Rest dieser Arbeit sei $[\cdot]$ die Gaußklammer.

Lemma 2.2.1 *Es gilt* $m = \min\{k \in \mathbb{N} \mid \left[\frac{n-1}{p^k}\right] = 0\}$.

Beweis: Man zeigt die Aussage des Lemmas, indem man einfache Rechnungen mit dem Frobeniushomomorphismus ausführt. Sei $x = 1 + \sum_{i=1}^{n-1} a_i T^i \in \hat{V}_L^n$ beliebig. Für alle $k \in \mathbb{N}$ mit $\left[\frac{n-1}{p^k}\right] = 0$, was äquivalent ist zu $p^k > n-1$, folgt

$$x^{q^k} = 1 + \sum_{i=1}^{n-1} a_i^{p^k} T^{ip^k} \equiv 1 \mod U_L^n.$$

Andererseits gilt für alle $k \in \mathbb{N}$ mit $\left[\frac{n-1}{p^k}\right] \neq 0$ die Kongruenz

$$(1+T)^{p^k} = 1 + T^{p^k} \not\equiv 1 \mod U_L^n.$$

Damit folgt die Aussage des Lemmas. $\square$

Für die weiteren Betrachtungen definiert man für $k = 0, 1, \ldots m$ die Untergruppen

$$H^k := \{xU_L^n \in \hat{G}_L^n \mid (xU_L^n)^{p^k} = U_L^n\}.$$

(Um nachzuvollziehen, daß H^k tatsächlich eine Untergruppe von G_L^n ist, reicht es sich klarzumachen, daß H^k multiplikativ abgeschlossen ist.)

Lemma 2.2.2 *Für alle* $k \leq i \in \mathbb{N}$ *gilt* $\#\{\overline{z} \in \mathbb{Z}/p^i\mathbb{Z} \mid p^k\overline{z} = \overline{0}\} = p^k$.

Beweis: Man betrachte das Repräsentantensystem $V := \{1, 2, \ldots, p^i\}$ von $\mathbb{Z}/p^i\mathbb{Z}$. Für alle $z \in V$ ist die Bedingung $p^k\overline{z} = \overline{0}$ äquivalent dazu, daß $p^{i-k} \mid z$ gilt. Daraus folgt

$$\begin{aligned}\#\{\overline{z} \in \mathbb{Z}/p^i\mathbb{Z} \mid p^k\overline{z} = \overline{0}\} &= \#\{p^{i-k}, 2p^{i-k}, \ldots, p^i\} \\ &= \#\{1, 2, \ldots, p^k\} \\ &= p^k.\end{aligned}$$

$\square$

Satz 2.2.3 *Für alle* $k = 1, \ldots, m$ *gilt sowohl*

(i) $\#H^k = q^{\left(n-1-\left[\frac{n-1}{p^k}\right]\right)}$ *als auch*

(ii) $\#H^k = p^{\left(\sum_{i=1}^{k} iv_i + \sum_{i=k+1}^{m} kv_i\right)}$.

Beweis: (i) Es gilt $\#H^k = \#\{x \in \hat{V}_L^n \mid x^{p^k} \in U_L^n\}$. Sei nun $1+\sum_{i=1}^{n-1} a_i T^i \in \hat{V}_L^n$. Dann gilt $x^{p^k} = 1+\sum_{i=1}^{n-1} (a_i)^{p^k} T^{ip^k}$. Damit folgt, daß die Bedingung $x^{p^k} \in U_L^n$ äquivalent ist zu $(a_i)^{p^k} = 0$ für $i = 1,2,\ldots,\left[\frac{n-1}{p^k}\right]$ (man beachte dazu, daß $\left[\frac{n-1}{p^k}\right] = \max\{i \in \mathbb{N} \mid ip^k \leq n-1\}$ ist). Dies gilt genau dann, wenn die Koeffizienten $a_1, a_2, \ldots a_{\left[\frac{n-1}{p^k}\right]}$ verschwinden. Für $i = \left[\frac{n-1}{p^k}\right]+1,\ldots,n-1$ dagegen sind die Koeffizienten $a_i \in \mathbb{F}_{q^2}$ frei wählbar. Daraus folgt $\#H^k = q^{n-1-\left[\frac{n-1}{p^k}\right]}$.

(ii) Aus der Definition von H^k ergibt sich

$$\begin{aligned}
\#H^k &= \#\{(\overline{z}_{ij})_{\substack{j=1,\ldots,v_i\\ i=1,\ldots,m}} \in \prod_{i=1}^{m}\left(\prod_{j=1}^{v_i}\left(\mathbb{Z}/p^i\mathbb{Z}\right)_j\right) \mid p^k\overline{z}_{ij} = \overline{0}\} \\
&= \left(\prod_{i=1}^{k}\prod_{j=1}^{v_i} \#\left(\mathbb{Z}/p^i\mathbb{Z}\right)\right)\left(\prod_{i=k+1}^{m}\prod_{j=1}^{v_i} \#\{\overline{z}_{ij} \in \left(\mathbb{Z}/p^i\mathbb{Z}\right)_j \mid p^k\overline{z}_{ij} = \overline{0}\}\right) \\
&= \left(\prod_{i=1}^{k}\prod_{j=1}^{v_i} p^i\right)\left(\prod_{i=k+1}^{m}\prod_{j=1}^{v_i} p^k\right) \qquad \text{(nach Lemma 2.2.2)} \\
&= p^{\left(\sum_{i=1}^{k} iv_i + \sum_{i=k+1}^{m} kv_i\right)}.
\end{aligned}$$

□

Korollar 2.2.4 *Für alle $k = 1,\ldots,m$ gilt $h(n-1-\left[\frac{n-1}{p^k}\right]) = \sum_{i=1}^{k} iv_i + \sum_{i=k+1}^{m} kv_i$.*

Beweis: Die Aussage ergibt sich direkt aus 2.2.3, indem man $q = p^h$ einsetzt sowie (i) und (ii) gleichsetzt. □

Allein mit diesem Korollar kann man nun die Vielfachheiten v_i bestimmen.

Satz 2.2.5 *Für alle $k = 1,\ldots,m$ gilt $v_k = h(\left[\frac{n-1}{p^{k-1}}\right] - 2\left[\frac{n-1}{p^k}\right] + \left[\frac{n-1}{p^{k+1}}\right])$.*

Beweis: Die Anwendung von Korollar 2.2.4 liefert zunächst

$$\begin{aligned}
h(\left[\tfrac{n-1}{p^{k-1}}\right] - \left[\tfrac{n-1}{p^k}\right]) &= h(n-1-\left[\tfrac{n-1}{p^k}\right]) - h(n-1-\left[\tfrac{n-1}{p^{k-1}}\right]) \\
&= \sum_{i=1}^{k} iv_i + \sum_{i=k+1}^{m} kv_i - \left(\sum_{i=1}^{k-1} iv_i + \sum_{i=k}^{m}(k-1)v_i\right) \\
&= v_k + \sum_{i=k+1}^{m} v_i \\
&= \sum_{i=k}^{m} v_i.
\end{aligned}$$

Mit diesem Ergebnis erhält man

$$\begin{aligned}
v_k &= \sum_{i=k}^{m} v_i - \sum_{i=k+1}^{m} v_i \\
&= h(\left[\tfrac{n-1}{p^{k-1}}\right]) - \left[\tfrac{n-1}{p^k}\right]) - h(\left[\tfrac{n-1}{p^k}\right] - \left[\tfrac{n-1}{p^{k+1}}\right]) \\
&= h(\left[\tfrac{n-1}{p^{k-1}}\right] - 2\left[\tfrac{n-1}{p^k}\right] + \left[\tfrac{n-1}{p^{k+1}}\right]).
\end{aligned}$$

□

Damit ist die Isomorphieklasse von $\hat{G}_L^n$ bestimmt. Es stellt sich nun die Frage, welche Elemente die zyklischen Komponeten von $\hat{G}_L^n$ erzeugen. Für die weiteren Betrachtungen wählt man für alle $i \in \mathbb{N}$ mit $i \leq n-1$ die Bezeichnung

$$M(i,n) := \max\{l \in \mathbb{N} \mid ip^{l-1} \leq n-1\}.$$

Lemma 2.2.6 *Seien $k, i \in \mathbb{N}$ mit $\frac{n-1}{p^k} < i \leq \frac{n-1}{p^{k-1}}$. Dann gilt $M(i,n) = k$.*

Beweis: Aus $\frac{n-1}{p^k} < i \leq \frac{n-1}{p^{k-1}}$ ergibt sich $ip^{k-1} \leq n-1$ sowie $ip^k > n-1$. Aus der Definition von $M(i,n)$ folgt $M(i,n) = k$. □

Lemma 2.2.7 *Für alle $i \in \{1, \ldots, m\}$ gibt es genau $\frac{1}{h}v_i$ verschiedene natürliche Zahlen k mit $\frac{n-1}{p^i} < k \leq \frac{n-1}{p^{i-1}}$, die keine Vielfachen von p sind.*

Beweis: Es gilt

$$\begin{aligned}
\frac{1}{h}v_i &= \left[\tfrac{n-1}{p^{i-1}}\right] - 2\left[\tfrac{n-1}{p^i}\right] + \left[\tfrac{n-1}{p^{i+1}}\right] \\
&= \left[\tfrac{n-1}{p^{i-1}}\right] - \left[\tfrac{n-1}{p^i}\right] - \left(\left[\tfrac{n-1}{p^i}\right] - \left[\tfrac{n-1}{p^{i+1}}\right]\right) \\
&= \left[\tfrac{n-1}{p^{i-1}}\right] - \left[\tfrac{n-1}{p^i}\right] - \#\{l \in \mathbb{N} \mid \tfrac{n-1}{p^{i+1}} < l \leq \tfrac{n-1}{p^i}\} \\
&= \left[\tfrac{n-1}{p^{i-1}}\right] - \left[\tfrac{n-1}{p^i}\right] - \#\{l \in \mathbb{N} \mid \tfrac{n-1}{p^i} < lp \leq \tfrac{n-1}{p^{i-1}}\} \\
&= \left[\tfrac{n-1}{p^{i-1}}\right] - \left[\tfrac{n-1}{p^i}\right] - \#\{k \in \mathbb{N} \mid p \mid k \textit{ und } \tfrac{n-1}{p^i} < k \leq \tfrac{n-1}{p^{i-1}}\} \\
&= \#\{k \in \mathbb{N} \mid p \nmid k \textit{ und } \tfrac{n-1}{p^i} < k \leq \tfrac{n-1}{p^{i-1}}\}.
\end{aligned}$$

Damit folgt die Aussage des Lemmas. □

Mit den letzten beiden Lemmata läßt sich nun die foldende Isomorphie formulieren.

Satz 2.2.8 *Es gilt* $\hat{G}_L^n \cong \prod_{k=1}^{h} \left(\prod_{\substack{j=1 \\ p \nmid j}}^{n-1} \mathbb{Z}/p^{M(j,n)}\mathbb{Z} \right)_k$.

Beweis: Aus den Lemmata 2.2.1, 2.2.6 und 2.2.7 folgt

$$\begin{aligned}
\hat{G}_l^n &\cong \prod_{i=1}^{m} \left(\prod_{j=1}^{v_i} \left(\mathbb{Z}/p^i\mathbb{Z}\right)_j \right) \\
&\cong \prod_{k=1}^{h} \left(\prod_{i=1}^{m} \left(\prod_{j=1}^{\frac{1}{h}v_i} \left(\mathbb{Z}/p^i\mathbb{Z}\right)_j \right) \right)_k \\
&\overset{2.2.7}{\cong} \prod_{k=1}^{h} \left(\prod_{i=1}^{m} \left(\prod_{\substack{j=\left[\frac{n-1}{p^i}\right]+1 \\ p \nmid j}}^{\left[\frac{n-1}{p^{i-1}}\right]} \left(\mathbb{Z}/p^i\mathbb{Z}\right)_j \right) \right)_k \\
&\overset{2.2.6}{\cong} \prod_{k=1}^{h} \left(\prod_{i=1}^{m} \left(\prod_{\substack{j=\left[\frac{n-1}{p^i}\right]+1 \\ p \nmid j}}^{\left[\frac{n-1}{p^{i-1}}\right]} \left(\mathbb{Z}/p^{M(j,n)}\mathbb{Z}\right)_j \right) \right)_k \\
&\overset{2.2.1}{\cong} \prod_{k=1}^{h} \left(\prod_{\substack{j=1 \\ p \nmid j}}^{n-1} \mathbb{Z}/p^{M(j,n)}\mathbb{Z} \right)_k
\end{aligned}$$

$\square$

Damit lassen sich nun Erzeuger für die zyklischen Komponenten von $\hat{G}_L^n$ bestimmen.

Satz 2.2.9 *Sei* $\{\alpha_1, \ldots, \alpha_h\}$ *eine* $\mathbb{F}_p$*-Basis von* $\mathbb{F}_q$ *und* $x \in U_L^1$ *beliebig. Dann gibt es für alle* $k = 1, \ldots, h$ *und* $j = 1, \ldots, n-1$ *mit* $p \not| j$ *ganze Zahlen* $z_{jk} \in \mathbb{Z}$*, so daß die Kongruenz*

$$x \equiv \prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \not| j}}^{n-1} (1 + \alpha_k T^j)^{z_{jk}} \mod U_L^n$$

gilt.

Beweis: Man zeigt die Aussage des Satzes durch Induktion über alle $n \in \mathbb{N}$. Für $n = 1$ ist die Aussage wegen $x \equiv 1 \mod U_L^1$ trivial.

Sei nun $n \in \mathbb{N}$ beliebig. Dann gibt es nach Induktionsannahme für alle $k = 1, \ldots, h$ und $j = 1, \ldots, n-1$ mit $p \not| j$ ganze Zahlen $z_{jk} \in \mathbb{Z}$, so daß gilt

$$x \equiv \prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \not| j}}^{n-1} (1 + \alpha_k T^j)^{z_{jk}} \mod U_L^n.$$

Daraus folgt, daß es ein $a_n \in \mathbb{F}_q$ gibt mit

$$x \left(\prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \not| j}}^{n-1} (1 + \alpha_k T^j)^{z_{jk}} \right)^{-1} \equiv 1 + a_n T^n \mod U_L^{n+1}.$$

1. Fall $p \not| n$: Es muß nun $\lambda_1, \ldots, \lambda_h \in \{0, \ldots, p-1\}$ geben mit $a_n = \sum_{k=1}^{h} \lambda_k \alpha_k$. Für alle $k = 1, \ldots, h$ wähle man

$$\tilde{z}_{jk} := \begin{cases} z_{jk} & \text{für alle } j = 1, \ldots, n-1 \text{ mit } p \not| j \\ \lambda_{jk} & \text{für } j = n. \end{cases}$$

Damit erhält man

$$\begin{aligned} x \left(\prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \not| j}}^{n} (1 + \alpha_k T^j)^{\tilde{z}_{jk}} \right)^{-1} &= x \left(\prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \not| j}}^{n-1} (1 + \alpha_k T^j)^{z_{jk}} \right)^{-1} \left(\prod_{k=1}^{h} (1 + \alpha_k T^n)^{\lambda_k} \right)^{-1} \\ &\equiv (1 + a_n T^n) \left(1 + \left(\sum_{k=1}^{n} \lambda_k \alpha_k \right) T^n \right)^{-1} \mod U_L^{n+1} \\ &\equiv 1 \mod U_L^{n+1}. \end{aligned}$$

Somit gilt

$$x \equiv \left(\prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \not| j}}^{n} (1 + \alpha_k T^j)^{\tilde{z}_{jk}} \right) \mod U_L^{n+1}.$$

2. Fall $p \mid n$: Dann gibt es eindeutig bestimmte $l, \tilde{j} \in \mathbb{N}$ mit $p^l \tilde{j} = n$ und $p \not| \tilde{j}$. Da die Abbildung $a \longmapsto a^{p^l}$ auf $\mathbb{F}_q$ ein $\mathbb{F}_p$- Automorphismus ist, muß die Menge $\{\alpha_1^{p^l}, \ldots, \alpha_h^{p^l}\}$ ebenfalls eine $\mathbb{F}_p$-Basis

von $\mathbb{F}_q$ sein. Daraus folgt die Existenz von $\lambda_1, \dots, \lambda_h \in \{0, \dots, p-1\}$ mit $a_n = \sum_{k=1}^h \lambda_k \alpha_k^{p^l}$. Für alle $k = 1, \dots, h$ wähle man

$$\tilde{z}_{jk} := \begin{cases} z_{jk} & \text{für alle } j = 1, \dots, n \text{ mit } p \not| j \text{ und } j \neq \tilde{j} \\ z_{\tilde{j}k} + \lambda_k p^l & \text{für } j = \tilde{j}. \end{cases}$$

Damit erhält man

$$\begin{aligned} x\left(\prod_{k=1}^h \prod_{\substack{j=1 \\ p \not| j}}^n (1+\alpha_k T^j)^{\tilde{z}_{jk}}\right)^{-1} &= x\left(\prod_{k=1}^h \prod_{\substack{j=1 \\ p \not| j \\ j \neq \tilde{j}}}^{n-1} (1+\alpha_k T^j)^{z_{jk}}\right)^{-1} \left(\prod_{k=1}^h (1+\alpha_k T^n)^{z_{jk}+\lambda_k p^l}\right)^{-1} \\ &= x\left(\prod_{k=1}^h \prod_{\substack{j=1 \\ p \not| j}}^{n-1} (1+\alpha_k T^j)^{z_{jk}}\right)^{-1} \left(\prod_{k=1}^h (1+\alpha_k^{p^l} T^n)^{\lambda_k}\right)^{-1} \\ &\equiv (1+a_n T^n)\left(1+\sum_{k=1}^h \lambda_k \alpha_k^{p^l} T^n\right)^{-1} \mod U_L^{n+1} \\ &\equiv 1 \mod U_L^{n+1}. \end{aligned}$$

Somit gilt

$$x \equiv \left(\prod_{k=1}^h \prod_{\substack{j=1 \\ p \not| j}}^n (1+\alpha_k T^j)^{\tilde{z}_{jk}}\right) \mod U_L^{n+1}.$$

□

Korollar 2.2.10 *Unter den Voraussetzungen des Satzes 2.2.9 ist es für alle $k = 1, \dots, h$ und $j = 1, \dots, n-1$ mit $p \not| j$ möglich, die z_{jk} in $\{0, 1, \dots, p^{M(j,n)} - 1\}$ zu wählen.*

Beweis: Sei $k \in \{1, \dots, h\}$ und $j \in \{1, \dots, n-1\}$ mit $p \not| j$. Dann gilt wegen $jp^{M(j,n)} > n-1$ die Bedingung

$$\left(1+\alpha_k T^j\right)^{p^{M(j,n)}} = 1 + \alpha_k^{p^{M(j,n)}} T^{jp^{M(j,n)}} \equiv 1 \mod U_L^n.$$

Also ist die Ordnung von $\left(1+\alpha_k T^j\right) U_L^n \in \hat{G}_L^n$ kleiner oder gleich $p^{M(j,n)}$. Somit muß es ein $\hat{z}_{jk} \in \{0, 1, \dots, p^{M(j,n)} - 1\}$ geben mit

$$\left(1+\alpha_k T^j\right)^{z_{jk}} \equiv \left(1+\alpha_k T^j\right)^{\hat{z}_{jk}} \mod U_L^n.$$

Damit folgt die Aussage des Korollars. □

Korollar 2.2.11 *Seien die Voraussetzungen von Satz 2.2.9 erfüllt. Wählt man nun gemäß Korollar 2.2.10 für alle $k = 1, \dots, h$ und $j = 1, \dots, n-1$ mit $p \not| j$ die $z_{jk} \in \{0, 1, \dots, p^{M(j,n)} - 1\}$, so sind sie eindeutig bestimmt.*

Beweis: Angenommen, für alle $k = 1, \dots, h$ und $j = 1, \dots, n-1$ mit $p \not| j$ gäbe es jeweils Zahlen $z_{jk}^{(1)}, z_{jk}^{(2)} \in \{0, 1, \dots, p^{M(j,n)} - 1\}$, so daß für mindestens ein (j,k) die Ungleichheit $z_{jk}^{(1)} \neq z_{jk}^{(2)}$ gilt und trotzdem die Bedingung

$$x \equiv \prod_{k=1}^h \prod_{\substack{j=1 \\ p \not| j}}^{n-1} (1+\alpha_k T^j)^{z_{jk}^{(1)}} \mod U_L^n \equiv \prod_{k=1}^h \prod_{\substack{j=1 \\ p \not| j}}^{n-1} (1+\alpha_k T^j)^{z_{jk}^{(2)}} \mod U_L^n$$

erfüllt ist. Dann folgte

$$\begin{aligned}\#\hat{G}_L^n &< \#\{(z_{jk})_{\substack{j=1,\ldots,n-1 \ mit \ p \nmid j \\ k=1,\ldots,h}} \mid z_{jk} \in \{0,1,\ldots,p^{M(j,n)}-1\}\} \\ &= \prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \nmid j}}^{n-1} p^{M(j,n)}.\end{aligned}$$

Das ist ein Widerspruch zu

$$\hat{G}_L^n \cong \prod_{k=1}^{h} \left(\prod_{\substack{j=1 \\ p \nmid j}}^{n-1} \mathbb{Z}/p^{M(j,n)}\mathbb{Z} \right)_k .$$

Daraus folgt die Eindeutigkeit der Zahlen $z_{jk} \in \{0,1,\ldots,p^{M(j,n)}-1\}$. □

Satz 2.2.12 *(i) Die Menge*

$$\{(1+\alpha_k T^j)U_L^n \mid k=1,\ldots,h \ \ und \ \ j=1,\ldots,n-1 \ \ mit \ \ p \nmid j\}$$

ist ein minimales Erzeugendensystem der Gruppe $\hat{G}_L^n$.

(ii) Die Menge

$$\{\alpha U_L^n\} \cup \{(1+\alpha_k T^j)U_L^n \mid k=1,\ldots,h \ \ und \ \ j=1,\ldots,n-1 \ \ mit \ \ p \nmid j\}$$

ist ein minimales Erzeugendensystem der Gruppe G_L^n.

Beweis: Die Aussage (i) ergibt sich aus Satz 2.2.9 und der Isomorphie

$$\hat{G}_L^n \cong \prod_{k=1}^{h} \left(\prod_{\substack{j=1 \\ p \nmid j}}^{n-1} \mathbb{Z}/p^{M(j,n)}\mathbb{Z} \right)_k .$$

Die Aussage (ii) ergibt sich aus der Aussage (i), der Isomorphie $G_L^n \cong \mathbb{F}_q^* \times \hat{G}_L^n$ sowie der Tatsache, daß $\alpha U_L^n \notin \hat{G}_L^n$ und $\mathrm{ord}(\alpha U_L^n) = q-1$ gilt. □

2.3 Die Struktur der Einseinheitengruppe U_L^1

Ähnlich wie die $\hat{G}_L^n$ läßt sich auch U_L^1 als $\mathbb{Z}$-Modul auffassen. Allerdings stellt sich heraus, daß $\mathbb{Z}$ nicht „groß" genug ist, um die Struktur von U_L^1 richtig zu erfassen. Deshalb „erweitert" man $\mathbb{Z}$ zum Ring der p-adischen Zahlen $\mathbb{Z}_p$. Dieser ist definiert durch $\mathbb{Z}_p := \{\sum_{i=0}^{\infty} a_i p^i \mid a_0, a_1, \ldots \in \{0,\ldots,p-1\}\}$, wobei die Elemente von $\mathbb{Z}_p$ zunächst als *rein formale Symbole* aufzufassen sind. Die Addition ist erklärt durch $\sum_{i=0}^{\infty} a_i p^i + \sum_{i=0}^{\infty} b_i p^i = \sum_{i=0}^{\infty} c_i p^i$, wobei die $c_i \in \{0,\ldots,p-1\}$ so gewählt sind, daß in $\mathbb{Z}$ für alle $n \in \mathbb{N}$ die Kongruenzen

$$\sum_{i=0}^{n-1} a_i p^i + \sum_{i=0}^{n-1} b_i p^i \equiv \sum_{i=0}^{n-1} c_i p^i \mod p^n\mathbb{Z}$$

gelten. Ähnlich verhält es sich mit der Multiplikation $\left(\sum_{i=0}^{\infty} a_i p^i\right) \cdot \left(\sum_{i=0}^{\infty} b_i p^i\right) = \sum_{i=0}^{\infty} d_i p^i$, wobei hier die d_i so gewählt sind, daß für alle $n \in \mathbb{N}$ die Kongruenzen

$$\left(\sum_{i=0}^{n-1} a_i p^i\right) \cdot \left(\sum_{i=0}^{n-1} b_i p^i\right) \equiv \sum_{i=0}^{n-1} d_i p^i \mod p^n\mathbb{Z}$$

gelten. Eine genauere Beschreibung von $\mathbb{Z}_p$ findet sich in [7].

Bezeichnung 2.3.1 *Sei $r = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ beliebig und $n \in \mathbb{N}$. Dann sei $r_n := \sum_{i=0}^{n-1} a_i p^i$.*

Seien nun $r, s \in \mathbb{Z}_p$. Dann folgt unmittelbar aus der Definition der Addition und der Multiplikation auf $\mathbb{Z}_p$, daß für alle $n \in \mathbb{N}$ die Kongruenzen $(r+s)_n \equiv s_n + r_n \mod p^n\mathbb{Z}$ und $(r \cdot s)_n \equiv s_n \cdot r_n \mod p^n\mathbb{Z}$ gelten.

Lemma 2.3.2 *Sei $r = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ und $j \in \mathbb{N}$ sowie $x \in U_L^j$. Dann konvergiert die Folge $\{x_n := x^{r_n}\}_{n\in\mathbb{N}}$, und für den Grenzwert $x' \in U_L^j$ gilt $x' \equiv x_n \mod U_L^{jp^n}$ für alle $n \in \mathbb{N}$.*

Beweis: Offensichtlich ist x von der Form $x = 1 + \tilde{x}T^j$ mit $\tilde{x} := T^{-j}(x-1)$. Wegen $x - 1 \in \mathfrak{m}_L^j$ folgt $\tilde{x} \in B_L$. Damit erhält man für alle $n \in \mathbb{N}$ die Kongruenz

$$x_{n+1} = x_n(1+\tilde{x}T^j)^{a_n p^n} = x_n(1+\tilde{x}^{p^n}T^{jp^n})^{a_n} \equiv x_n \mod U_L^{jp^n}.$$

Nach Lemma 1.3.1.4 folgt $x_{n+1} \equiv x_n \mod \mathfrak{m}_L^{jp^n}$ und damit $\nu_L(x_{n+1} - x_n) \geq jp^n$. Die Anwendung von Lemma 1.3.1.13 liefert die Konvergenz der Folge $\{x_n\}_{n\in\mathbb{N}}$, so daß für den Grenzwert $x' \in U_L^j$ für alle $n \in \mathbb{N}$ die Bedingung $\nu_L(x' - x_n) \geq jp^n$ erfüllt ist. Daraus folgt $x' \equiv x_n \mod \mathfrak{m}_L^{jp^n}$ und damit $x' \equiv x_n \mod U_L^{jp^n}$. □

Definition 2.3.3 (Skalarmultiplikation auf U_L^1) *Man definiere die Abbildung $\varrho : \mathbb{Z}_p \times U_L^1 \longrightarrow U_L^1$ durch $(r, x) \longmapsto x^r := \lim_{n\to\infty} x^{r_n}$.*

Lemma 2.3.4 *Seien $x, y \in U_L^1$ und $r \in \mathbb{Z}_p$. Dann gilt $y = x^r$ genau dann, wenn für alle $n \in \mathbb{N}$ die Kongruenzbedingung $y \equiv x^{r_n} \mod U_L^{p^n}$ erfüllt ist.*

Beweis: Daß aus $y = x^r$ für alle $n \in \mathbb{N}$ die Kongruenz $x^r \equiv x^{r_n} \mod U_L^{p^n}$ folgt, ist Gegenstand von Lemma 2.3.2. Sind nun umgekehrt für alle $n \in \mathbb{N}$ die Kongruenzen $y \equiv x^{r_n} \mod U_L^{p^n}$ erfüllt, dann folgt $y \equiv x^{r_n} \mod \mathfrak{m}_L^{p^n}$ und damit $\nu_l(y - x^{r_n}) \geq p^n$. Wegen $\lim_{n\to\infty} p^n = \infty$ erhält man $y = x^r$. □

Satz 2.3.5 *Die Gruppe U_L^1 läßt sich vermöge ϱ als $\mathbb{Z}_p$-Modul auffassen.*

Beweis: Seien $x, y \in U_L$ und $r, s \in \mathbb{Z}_p$. Unter Verwendung von Lemma 2.3.4 lassen sich nun die Axiome nachrechnen.
Unitarität: Für alle $n \in \mathbb{N}$ gilt $x \equiv x^{1_n} \mod U_L^{p^n}$. Daraus folgt $x = x^1$.
Assoziativität: Für alle $n \in \mathbb{N}$ gilt

$$(x^r)^s \equiv (x^{r_n})^{s_n} \mod U_L^{p^n} \equiv x^{r_n s_n} \mod U_L^{p^n} \equiv x^{(rs)_n} \mod U_L^{p^n}.$$

Daraus folgt $(x^r)^s = x^{rs}$.
1. Distributivregel: Für alle $n \in \mathbb{N}$ gilt

$$x^r x^s \equiv x^{r_n} x^{s_n} \mod U_L^{p^n} \equiv x^{r_n + s_n} \mod U_L^{p^n} \equiv x^{(r+s)_n} \mod U_L^{p^n}.$$

Daraus folgt $x^r x^s = x^{r+s}$.
2. Distributivregel: Für alle $n \in \mathbb{N}$ gilt

$$x^r y^r \equiv x^{r_n} y^{r_n} \mod U_L^{p^n} \equiv (xy)^{r_n} \mod U_L^{p^n}.$$

Daraus folgt $x^r y^r = (xy)^r$. □

Für die folgenden Betrachtungen sei $\{\alpha_1, \ldots, \alpha_h\}$ eine festgewählte $\mathbb{F}_p$-Basis von $\mathbb{F}_q$.

Lemma 2.3.6 *Für alle $k \in \{1,\dots,h\}$ und $j \in \mathbb{N}$ mit $p \nmid j$ sei $r(k,j) \in \mathbb{Z}_p$. Außerdem setze man $x_n := \prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \nmid n}}^{n-1} (1+\alpha_k T^j)^{r(k,j)}$ für alle $n \in \mathbb{N}$. Dann konvergiert die Folge $\{x_n\}_{n\in\mathbb{N}}$, und der Grenzwert x erfüllt für alle $n \in \mathbb{N}$ die Kongruenzen $x \equiv x_n \mod U_L^n$.*

Beweis: Für den Fall $p \mid n$ gilt $x_{n+1} = x_n$. Falls nun $p \nmid n$ gilt, folgt

$$x_{n+1} = x_n \prod_{k=1}^{n} (1+\alpha_k T^n)^{r(k,n)}.$$

Damit erhält man $x_{n+1} \equiv x_n \mod U_L^n$ bzw. $x_{n+1} \equiv x_n \mod \mathfrak{m}_L^n$ und damit $\nu_L(x_{n+1} - x_n) \geq n$. Mit Lemma 1.3.1.13 folgt die Konvergenz von $\{x_n\}_{n\in\mathbb{N}}$, so daß für x die Kongruenz $x \equiv x_n \mod U_L^n$ für alle $n \in \mathbb{N}$ gilt. $\square$

Bezeichnung 2.3.7 *Für alle $k \in \{1,\dots,h\}$ und $j \in \mathbb{N}$ mit $p \nmid j$ seien $r(k,j) \in \mathbb{Z}_p$. Dann ist*

$$\prod_{k=1}^{h} \prod_{\substack{j\in\mathbb{N} \\ p \nmid j}} (1+\alpha_k T^j)^{r(k,j)} := \lim_{n\to\infty} \prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \nmid j}}^{n-1} (1+\alpha_k T^j)^{r(k,j)}$$

Satz 2.3.8 *Sei $x \in U_L^1$. Dann gibt es für alle $k \in \{1,\dots,h\}$ und $j \in \mathbb{N}$ mit $p \nmid j$ eindeutig bestimmte $r(k,j) \in \mathbb{Z}_p$ mit*

$$x = \prod_{k=1}^{h} \prod_{\substack{j\in\mathbb{N} \\ p \nmid j}} (1+\alpha_k T^j)^{r(k,j)}.$$

Beweis: *Existenz:* Nach Satz 2.2.9 gibt es für alle $n \in \mathbb{N}$, $k \in \{1,\dots,h\}$ und $j = 1,\dots,n-1$ mit $p \nmid j$ ganze Zahlen $r(n,k,j) \in \mathbb{Z}$, so daß gilt

$$x \equiv \prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \nmid j}}^{n-1} (1+\alpha_k T^j)^{r(n,k,j)} \mod U_L^n.$$

Seien nun $k \in \{1,\dots,h\}$ und $j \in \mathbb{N}$ mit $p \nmid j$ festgewählt. Man betrachte die Folge $\{\tilde{r}(n)\}_{\substack{n\in\mathbb{N} \\ n\geq j}}$, wobei $\tilde{r}(n) := r(n,k,j)$ für alle $n \in \mathbb{N}$ mit $n \geq j$ ist. Für ein beliebiges $n \in \mathbb{N}$ mit $n \geq j$ gibt es nun eindeutig bestimmte $a_0,\dots,a_{M(j,n)-1} \in \{0,1,\dots,p-1\}$, so daß

$$\tilde{r}(n) \equiv \sum_{i=0}^{M(j,n)-1} a_i p^i \mod p^{M(j,n)}\mathbb{Z}$$

gilt (p-adische Entwicklung). Nach Korollar 2.2.11 folgt nun

$$\tilde{r}(n+1) \equiv \tilde{r}(n) \mod p^{M(j,n)}\mathbb{Z}$$

für alle $n \in \mathbb{N}$ mit $n \geq j$. Da die Folge $\{M(n,j)\}_{\substack{n\in\mathbb{N} \\ n\geq j}}$ monoton wachsend ist und $\lim_{n\to\infty} M(j,n) = \infty$ gilt, folgt die Existenz einer Folge $\{a_i\}_{i\in\mathbb{N}} \subset \{0,1,\dots,p-1\}$ mit

$$\tilde{r}(n) \equiv \sum_{i=0}^{M(j,n)-1} a_i p^i \mod p^{M(j,n)}\mathbb{Z}$$

für alle $n \in \mathbb{N}$ mit $n \geq j$. Setze nun $r(k,j) := \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$.

Nach Lemma 2.3.2 folgt nun für alle $k \in \{1, \ldots, h\}$ und $j \in \mathbb{N}$ mit $p \not| j$ sowie $n \in \mathbb{N}$ mit $n \geq j$ die Kongruenz

$$\begin{aligned}
(1+\alpha_k T^j)^{r(k,j)} &\equiv (1+\alpha_k T^j)^{(r(k,j))_{M(j,n)}} \mod U_L^{jp^{M(j,n)}} \\
&\equiv (1+\alpha_k T^j)^{(r(n,k,j))_{M(j,n)}} \mod U_L^{jp^{M(j,n)}} \\
&\equiv (1+\alpha_k T^j)^{r(n,k,j)} \mod U_L^{jp^{M(j,n)}} \\
&\equiv (1+\alpha_k T^j)^{r(n,k,j)} \mod U_L^{n}.
\end{aligned}$$

Man beachte dazu, daß $jp^{M(j,n)} > n-1$ nach Definition von $M(j,n)$ gilt. Insgesamt erhält man damit

$$x \equiv \prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \not| j}}^{n-1} (1+\alpha_k T^j)^{r(k,j)} \mod U_L^n$$

für alle $n \in \mathbb{N}$. Daraus folgt

$$x = \prod_{k=1}^{h} \prod_{\substack{j \in \mathbb{N} \\ p \not| j}} (1+\alpha_k T^j)^{r(k,j)}.$$

Eindeutigkeit: Seien $r(k,j), s(k,j) \in \mathbb{Z}_p$ für alle $k = 1, \ldots, h$ und $j \in \mathbb{N}$ mit $p \not| j$, so daß

$$\prod_{k=1}^{h} \prod_{\substack{j \in \mathbb{N} \\ p \not| j}} (1+\alpha_k T^j)^{r(k,j)} = x = \prod_{k=1}^{h} \prod_{\substack{j \in \mathbb{N} \\ p \not| j}} (1+\alpha_k T^j)^{s(k,j)}$$

gilt. Nach Lemma 2.3.6 gelten für alle $n \in \mathbb{N}$ die Kongruenzen

$$\prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \not| j}}^{n-1} (1+\alpha_k T^j)^{r(k,j)} \equiv \prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \not| j}}^{n-1} (1+\alpha_k T^j)^{s(k,j)} \mod U_L^n.$$

Weil $jp^{M(j,n)} \geq n$ gilt, ergeben sich nach Lemma 2.3.2 die Kongruenzen

$$\prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \not| j}}^{n-1} (1+\alpha_k T^j)^{(r(k,j))_{M(j,n)}} \equiv \prod_{k=1}^{h} \prod_{\substack{j=1 \\ p \not| j}}^{n-1} (1+\alpha_k T^j)^{s((k,j))_{M(j,n)}} \mod U_L^n.$$

Wegen $(r(k,j))_{M(j,n)}, (s(k,j))_{M(j,n)} \in \{0, 1, \ldots, p^{M(j,n)}-1\}$ folgt nach Korollar 2.2.11 die Gleichheit $(r(k,j))_{M(j,n)} = (s(k,j))_{M(j,n)}$ für alle $k \in \{1, \ldots, h\}$ und $j \in \mathbb{N}$ mit $p \not| j$ sowie $n \in \mathbb{N}$ mit $n > j$. Seien nun $k \in \{1, \ldots, h\}$ und $j \in \mathbb{N}$ mit $p \not| j$ festgewählt. Dann gilt für alle $m \in \mathbb{N}$ die Gleichung $M(j, jp^{m-1}) = m$ und damit $(r(k,j))_m = (s(k,j))_m$. Daraus folgt $r(k,j) = s(k,j)$. □

Satz 2.3.9 *Durch die Abbildung*

$$\theta : \prod_{k=1}^{h} \left(\prod_{\substack{j \in \mathbb{N} \\ p \not| j}} (\mathbb{Z}_p)_j \right)_k \longrightarrow U_L^1, \qquad (r(k,j))_{\substack{k=1,\ldots,h \\ j \in \mathbb{N}, p \not| j}} \longmapsto \prod_{k=1}^{h} \prod_{\substack{j \in \mathbb{N} \\ p \not| j}} (1+\alpha_k T^j)^{r(k,j)}$$

ist ein $\mathbb{Z}_p$-Modulisomorphismus gegeben.

Beweis: Die Bijektivität von θ folgt direkt aus Satz 2.3.8. Die Homomorphismuseigenschaften von θ rechnet man wie folgt nach.

Additivität: Seien

$$r = (r(k,j))_{\substack{k=1,\dots,h \\ j\in\mathbb{N},\, p\nmid j}},\, s = (s(k,j))_{\substack{k=1,\dots,h \\ j\in\mathbb{N},\, p\nmid j}} \in \prod_{k=1}^{h} \left(\prod_{\substack{j\in\mathbb{N} \\ p\nmid j}} (\mathbb{Z}_p)_j \right)_k .$$

Dann gelten für alle $n \in \mathbb{N}$ die Kongruenzen

$$\begin{aligned}
\theta(r+s) &= \prod_{k=1}^{h} \prod_{\substack{j\in\mathbb{N} \\ p\nmid j}} (1+\alpha_k T^j)^{r(k,j)+s(k,j)} \\
&\equiv \prod_{k=1}^{h} \prod_{\substack{j=1 \\ p\nmid j}}^{n-1} (1+\alpha_k T^j)^{r(k,j)+s(k,j)} \mod U_L^n \\
&\equiv \left(\prod_{k=1}^{h} \prod_{\substack{j=1 \\ p\nmid j}}^{n-1} (1+\alpha_k T^j)^{r(k,j)} \right) \left(\prod_{k=1}^{h} \prod_{\substack{j=1 \\ p\nmid j}}^{n-1} (1+\alpha_k T^j)^{s(k,j)} \right) \mod U_L^n \\
&\equiv \left(\prod_{k=1}^{h} \prod_{\substack{j\in\mathbb{N} \\ p\nmid j}} (1+\alpha_k T^j)^{r(k,j)} \right) \left(\prod_{k=1}^{h} \prod_{\substack{j\in\mathbb{N} \\ p\nmid j}} (1+\alpha_k T^j)^{s(k,j)} \right) \mod U_L^n \\
&\equiv \theta(r)\cdot\theta(s) \mod U_L^n.
\end{aligned}$$

Daraus folgt $\theta(r+s) = \theta(r) + \theta(s)$.

Homogenität: Sei

$$r = (r(k,j))_{\substack{k=1,\dots,h \\ j\in\mathbb{N},\, p\nmid j}} \in \prod_{k=1}^{h} \left(\prod_{\substack{j\in\mathbb{N} \\ p\nmid j}} (\mathbb{Z}_p)_j \right)_k$$

und $\lambda \in \mathbb{Z}_p$. Dann gelten für alle $n \in \mathbb{N}$ die Kongruenzen

$$\begin{aligned}
\theta(\lambda r) &= \prod_{k=1}^{h} \prod_{\substack{j\in\mathbb{N} \\ p\nmid j}} (1+\alpha_k T^j)^{\lambda s(k,j)} \\
&\equiv \prod_{k=1}^{h} \prod_{\substack{j=1 \\ p\nmid j}}^{n-1} (1+\alpha_k T^j)^{\lambda s(k,j)} \mod U_L^n \\
&\equiv \left(\prod_{k=1}^{h} \prod_{\substack{j=1 \\ p\nmid j}}^{n-1} (1+\alpha_k T^j)^{s(k,j)} \right)^{\lambda} \mod U_L^n \\
&\equiv \left(\prod_{k=1}^{h} \prod_{\substack{j=1 \\ p\nmid j}}^{n-1} (1+\alpha_k T^j)^{\lambda s(k,j)} \right)^{\lambda_n} \mod U_L^n \\
&\equiv \left(\prod_{k=1}^{h} \prod_{\substack{j\in\mathbb{N} \\ p\nmid j}} (1+\alpha_k T^j)^{\lambda s(k,j)} \right)^{\lambda_n} \mod U_L^n \\
&\equiv \left(\prod_{k=1}^{h} \prod_{\substack{j\in\mathbb{N} \\ p\nmid j}} (1+\alpha_k T^j)^{\lambda s(k,j)} \right)^{\lambda} \mod U_L^n.
\end{aligned}$$

Daraus folgt $\theta(\lambda r) = (\theta(r))^{\lambda}$. □

Zum Abschluß dieses Kapitels soll noch kurz beschrieben werden, wie man die Isomorphie

$$U_D^1 \cong \prod_{k=1}^{h} \left(\prod_{\substack{j\in\mathbb{N} \\ p\nmid j}} (\mathbb{Z}_p)_j \right)_k$$

auch mit dem Formalismus des projektiven Limes herleiten kann. Dazu ist es notwendig projektive Systeme und projektive Limiten in der Kategorie der $\mathbb{Z}_p$-Moduln zu definieren. Dies geschieht dadurch, daß man in den Definitionen 1.3.2.1 und 1.3.2.3 alle Gruppen durch $\mathbb{Z}_p$-Moduln und alle Gruppenhomomorphismen durch $\mathbb{Z}_p$-Modulhomomorphismen ersetzt. Analog zum Beweis von Satz 1.3.2.4 kann man zeigen, daß auch in der Kategorie der $\mathbb{Z}_p$-Moduln der projektive Limes existiert und bis auf Isomorphie eindeutig bestimmt ist. Die Faktorgruppen $\hat{G}_L^n$ lassen sich vermöge der Abbildung $\rho_n : \mathbb{Z}_p \longrightarrow \hat{G}_L^n, r \longmapsto x^r U_L^n$ für alle $n \in \mathbb{N}$ als $\mathbb{Z}_p$-Moduln auffassen. Außerdem läßt sich leicht zeigen, daß durch die Abbildungen $\vartheta_m^n : \hat{G}_L^m \longrightarrow \hat{G}_L^n, xU_L^m \longmapsto xU_L^n$ für alle $m \geq n$ ein projektives System von $\mathbb{Z}_p$-Modulhomomorphismen gegeben ist. Ähnlich wie in Satz 1.3.2.5 läßt sich nun das System der kanonischen Homomorphismen $\left(\hat{\vartheta}_l : U_L^1 \longrightarrow \hat{G}_L^l\right)_{l\in\mathbb{N}}$ als projektiver Limes von $\left(\hat{\vartheta}_m^n : \hat{G}_L^m \longrightarrow \hat{G}_L^n\right)_{m\geq n\in\mathbb{N}}$ auffassen. Definiert man nun $M(j,n) := 0$ für alle $i \geq n \in \mathbb{N}$, so kann man gemäß Satz 2.2.8 die Faktorgruppen $\hat{G}^n$ mit

$$\prod_{k=1}^{h}\left(\prod_{\substack{j\in\mathbb{N}\\ p\not| j}} \mathbb{Z}/p^{M(j,n)}\mathbb{Z}\right)_k \cong \prod_{k=1}^{h}\left(\prod_{\substack{j\in\mathbb{N}\\ p\not| j}}^{n-1} \mathbb{Z}/p^{M(j,n)}\mathbb{Z}\right)_k$$

identifizieren. Die $\mathbb{Z}_p$-Modulhomomorphismen $\hat{\vartheta}_m^n$ bekommen dann für alle $m \geq n \in \mathbb{N}$ die Form

$$\hat{\vartheta}_m^n = \prod_{k=1}^{h}\left(\prod_{\substack{j\in\mathbb{N}\\ p\not| j}} \delta(j,m,n)\right)_k : \prod_{k=1}^{h}\left(\prod_{\substack{j\in\mathbb{N}\\ p\not| j}} \mathbb{Z}/p^{M(j,m)}\mathbb{Z}\right)_k \longrightarrow \prod_{k=1}^{h}\left(\prod_{\substack{j\in\mathbb{N}\\ p\not| j}} \mathbb{Z}/p^{M(j,n)}\mathbb{Z}\right)_k ,$$

wobei die Abbildung $\delta(j,m,n) : \mathbb{Z}/p^{M(j,m)}\mathbb{Z} \longrightarrow \mathbb{Z}/p^{M(j,n)}\mathbb{Z}$ für alle $m \geq n \in \mathbb{N}$ und $j \in \mathbb{N}$ mit $p \not| j$ durch die Vorschrift $x\left(p^{M(j,m)}\mathbb{Z}\right) \longmapsto x\left(p^{M(j,n)}\mathbb{Z}\right)$ definiert sind. Weiter kann man leicht zeigen, daß durch $\left(\delta(j,m,n) : \mathbb{Z}/p^{M(j,m)}\mathbb{Z} \longrightarrow \mathbb{Z}/p^{M(j,n)}\mathbb{Z}\right)_{m\geq n\in\mathbb{N}}$ für alle $j \in \mathbb{N}$ ein projektives System gegeben ist. Als projektiven Limes erhält man das System $\left(\Delta_l^j : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^{M(j,l)}\mathbb{Z}\right)_{l\in\mathbb{N}}$, wobei für alle $l \in \mathbb{N}$ der $\mathbb{Z}_p$-Modulhomomorphismus Δ_l^j durch die Vorschrift $r \longmapsto r_{M(j,l)}$ definiert ist. Allgemein kann man nun zeigen, daß die kartesischen Produkte von projektiven Systemen wieder projektive Systeme definieren. Für den projektiven Limes erhält man dann das kartesische Produkt der projektiven Limiten der einzelnen Komponenten. Auf diese Weise ergibt sich dann die Isomorphie

$$U_D^1 \cong \prod_{k=1}^{h}\left(\prod_{\substack{j\in\mathbb{N}\\ p\not| j}} (\mathbb{Z}_p)_j\right)_k .$$

Kapitel 3

Die Konjugationsklassen von G_n

Nach Satz 1.3.1.5 ist

$$V_n := \{\sum_{i=0}^{n-1} a_i\tau^i \mid a_0, \ldots, a_{n-1} \in \mathbb{F}_{q^2} \;\; mit \;\; a_0 \neq 0\}$$

ein Repräsentantensystem der Faktorgruppe G_n. Für ein $x = \sum_{i=0}^{\infty} a_i\tau^i \in U$ ist $\sum_{i=0}^{n-1} a_i\tau^i \in V_n$ der Repräsentant von $xU_n \in G_n$. Der Übergang von U nach G_n vollzieht sich also dadurch, daß man nur noch die ersten n Koeffizienten betrachtet. In diesem Kapitel wird nun ein Repräsentantensystem für die Konjugationsklassen von G_n sowie deren Länge bestimmt.

3.1 Allgemeine Zusammenhänge

In diesem Abschnitt geht es darum, einen Überblick zu erlangen, welche verschiedenen Typen von Konjugationsklassen es gibt, und welche strukturellen Gemeinsamkeiten es zwischen diesen verschiedenen Typen gibt.

Bezeichnung 3.1.1 *(i) Für zwei Elemente xU_n und yU_n der Faktorgruppe G_n wählt man das Symbol „$xU_n \sim yU_n$“, wenn xU_n und yU_n konjugiert sind.*

(ii) Die Elemente $x, y \in U$ heißen konjugiert modulo U_n, *wenn $xU_n \sim yU_n$ gilt. Zur Kennzeichnung dieses Sachverhaltes schreibt man „$x \sim_n y$“.*

(iii) Sei $x \in U_n$. Mit $[x]_n$ bezeichnet man die Konjugationsklasse von xU_n in G_n.

Diese Bezeichnung macht es möglich, für ein *festes* $x \in U$ zwischen den Konjugationsklassen, die $xU_n \in G_n$ für *verschiedene* $n \in \mathbb{N}$ repräsentiert, zu unterscheiden.

Definition 3.1.2 *Sei $x = \sum_{i=0}^{\infty} a_i\tau^i \in U$. Dann heißt*

$$\mathrm{SP}(x) := \begin{cases} \min\{j \in \mathbb{N}_0 \mid \sum\limits_{i=0}^{j} a_i\tau^i \notin L\} & \text{falls } x \notin L \\ \infty & \text{falls } x \in L \end{cases}$$

die Sprungstelle von x.

Diese Definition ist ein Spezialfall der Definition von Sprungstellen aus [9] und ist von großer Bedeutung für die folgenden Betrachtungen.

Bemerkung 3.1.3 Sei $x = \sum_{i=0}^{\infty} a_i\tau^i \in U$. Dann gilt:

(i) Es existiert die Zerlegung $x := \sum_{i=0}^{\mathrm{SP}(x)-1}{}'' a_i\tau^i + x'\tau^{\mathrm{SP}(x)}$, wobei $x' = \sum_{i=\mathrm{SP}(x)}^{\infty} a_i\tau^{i-\mathrm{SP}(x)} \in U$ eindeutig bestimmt ist und $\sum_{i=0}^{\mathrm{SP(x)}-1}{}'' a_i\tau^i$ in L liegt.

(ii) Für alle $n \in \mathbb{N}$ mit $n \geq \mathrm{SP}(x)$ liegt die Restklasse xU_n im Zentrum von G_n.

Lemma 3.1.4 *Seien $n \in \mathbb{N}$ und $x, y \in U$ mit $x \equiv y \mod U_n$. Dann gilt:*

(i) Die Bedingung $\mathrm{SP}(x) \geq n$ ist genau dann erfüllt, wenn $\mathrm{SP}(y) \geq n$ gilt.

(ii) Aus $\mathrm{SP}(x) < n$ folgt $\mathrm{SP}(x) = \mathrm{SP}(y)$.

Beweis: Wegen $x \equiv y \mod U_n$ muß es Elemente $x', y' \in (\tau^n)$ sowie $a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_{q^2}$ geben, so daß

$$x = \sum_{i=0}^{n-1} a_i\tau^i + x' \text{ und } y = \sum_{i=0}^{n-1} a_i\tau^i + y'$$

gilt. Offensichtlich gelten die Bedingungen $\mathrm{SP}(x) \geq n$ bzw. $\mathrm{SP}(y) \geq n$ genau dann, wenn $\sum_{i=0}^{n-1} a_i\tau^i$ in L liegt. Daraus folgt die Aussage (i). Falls $\mathrm{SP}(x) < n$ ist, gilt $\mathrm{SP}(x) = \min\{j \in \{1, 2, \ldots n-1\} \mid \sum_{i=0}^{j} a_i\tau^i \notin L\} = \mathrm{SP}(y)$. Damit ist die Aussage (ii) gezeigt. □

Für den gesamten Rest dieser Arbeit wird nun für alle $n \in \mathbb{Z}$ mit $g(n)$ bzw. $u(n)$ die größte gerade bzw. ungerade ganze Zahl bezeichnet, die echt kleiner ist als n. Damit läßt sich folgende Unterteilung von G_n vornehmen.

Definition 3.1.5 *Sei $n \in \mathbb{N}$ und $m \in \{1, 2, \ldots, n\}$. Dann wählt man die Bezeichnung*

$$G_n^{(m)} := \begin{cases} \{xU_n \in G_n \mid \mathrm{SP}(x) = m\} & \text{falls } m < n \\ \{xU_n \in G_n \mid \mathrm{SP}(x) > n\} & \text{falls } m = n \end{cases}$$

Falls $m \neq 0$ ist, definiert man für alle $a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q$ mit $a_0 \neq 0$ die Menge

$$G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)}) := \{xU_n \in G_n^{(m)} \mid x \equiv \sum_{i=0}^{g(m)}{}'' a_i\tau^i \mod U_m\}.$$

Man beachte, daß aus Lemma 3.1.4 die Wohldefiniertheit von $G_n^{(m)}$ folgt.

Bemerkung 3.1.6 (i) Die Menge $G_n^{(n)}$ liegt im Zentrum von G_n.

(ii) Es existiert die disjunkte Vereinigung

$$G_n = \biguplus_{m=0}^{n} G_n^{(m)}.$$

Für alle $m = 1, 2, \ldots, n$ gilt außerdem

$$G_n^{(m)} = \biguplus_{\substack{a_0, a_2, \ldots, a_{g(m)} \\ a_0 \neq 0}} G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)}).$$

Die Definition 3.1.5 liefert also eine disjunkte Unterteilung der Faktorgruppe G_n. Inwiefern es sinnvoll ist, G_n auf diese Art zu unterteilen, geht aus dem folgenden Lemma hervor.

Lemma 3.1.7 *Sei $n \in \mathbb{N}$ und $x \in U$. Dann gilt:*

(i) Entweder ist $[x]_n \subset G_n^{(0)}$ *oder* $[x]_n \cap G_n^{(0)} = \emptyset$.

(ii) Für alle $m = 1, 2, \ldots, n$ *und* $a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q$ *mit* $a \neq 0$ *ist entweder*

$$[x]_n \subset G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$$

oder

$$[x]_n \cap G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)}) = \emptyset.$$

Beweis: (i) Es reicht aus zu zeigen, daß für alle $xU_n \in G_n^{(0)}$ die Beziehung $[x]_n \subset G_n^{(0)}$ gilt. Sei also $xU_n \in G_n^{(0)}$. Dann gilt $\mathrm{SP}(x) = 0$. Also muß es ein $a_0 \in \mathbb{F}_{q^2} - \mathbb{F}_q$ geben mit $x \equiv a_0 \mod U_1$. Sei nun $yU_n \in [x]_n$. Dann gibt es ein $z \in U$ mit $y \equiv zxz^{-1} \mod U_m$. Da $G_1 \cong \mathbb{F}_{q^2}^*$ abelsch ist, folgt $y \equiv x \mod U_1$. Nach Lemma 3.1.4 erhält man $\mathrm{SP}(y) = 0$ und damit $yU_n \in [x]_n$.

(ii) Für $m = n$ ist die Aussage trivial, da $G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$ nach Bemerkung 3.1.6 im Zentrum von G_n liegt. Sei also $m < n$. Auch hier reicht es aus zu zeigen, daß für alle $xU_n \in G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$ die Beziehung $[x]_n \subset G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$ gilt. Sei also $xU_n \in G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$. Dann gilt $\mathrm{SP}(x) = m$ und $x \equiv \sum_{i=0}^{g(m)}{}'' a_i \tau^i \mod U_m$. Sei nun $yU_n \in [x]_n$. Dann gibt es ein $z \in U$ mit $y \equiv zxz^{-1} \mod U_n$. Da xU_m im Zentrum von G_m liegt, folgt

$$y \equiv x \mod U_m \equiv \sum_{i=0}^{g(m)}{}'' a_i \tau^i \mod U_m.$$

Dies bedeutet insbesondere $\mathrm{SP}(x) \geq m$. Damit ist nur noch $\mathrm{SP}(x) \leq m$ zu zeigen. Angenommen, es gälte $\mathrm{SP}(x) > m$. Dann folgte $y \equiv x \mod U_{m+1}$, was nach Lemma 3.1.5 im Widerspruch zu $\mathrm{SP}(x) = m$ steht. Damit erhält man $yU_n \in [x]_n$. $\square$

Mit Lemma 3.1.7 ist gezeigt, daß die Einteilung von G_n gemäß Definition 3.1.5 die Einteilung in Konjugationsklassen respektiert. Damit vereinfacht sich nun das Problem der Bestimmung der Konjugationsklassen von G_n in die Teilprobleme der Bestimmung der Konjugationsklassen auf $G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$.

Lemma 3.1.8 *Sei* $m \in \mathbb{N}$ *und* $a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q$ *mit* $a_0 \neq 0$ *sowie* $x' \in U$.

(i) Falls m *gerade ist, gilt die Bedingung* $\mathrm{SP}(\sum_{i=0}^{g(m)}{}'' a_i \tau^i + x'\tau^m) = m$ *genau dann, wenn* $\mathrm{SP}(x') = 0$ *ist.*

(ii) Falls m *ungerade ist, gilt die Bedingung* $\mathrm{SP}(\sum_{i=0}^{g(m)}{}'' a_i \tau^i + x'\tau^m) = m$ *genau dann, wenn* $\mathrm{SP}(a_0 + x'\tau) = 1$ *ist.*

Beweis: Sei $a_m \in \mathbb{F}_{q^2}^*$ mit $x' \equiv a_m \mod U_1$.

(i) Falls m gerade ist, gilt $\mathrm{SP}(\sum_{i=0}^{g(m)}{}'' a_i \tau^i + x'\tau^m) = m$ genau dann, wenn $a_m \notin \mathbb{F}_q$ ist. Das wiederum ist äquivalent zu $\mathrm{SP}(x') = 0$.

(ii) Falls m ungerade ist, gilt $\mathrm{SP}(\sum_{i=0}^{g(m)}{}'' a_i \tau^i + x'\tau^m) = m$ genau dann, wenn $a_m \neq 0$ ist. Das wiederum ist äquivalent zu $\mathrm{SP}(a_0 + x'\tau) = 1$. $\square$

Damit läßt sich nun der folgende wichtige Satz beweisen, mit dem sich das Problem auf die Bestimmung der Konjugationsklassen auf $G_n^{(0)}$ bzw. $G_n^{(1)}(a_0)$ für alle $a_0 \in \mathbb{F}_q^*$ reduziert.

Hauptsatz 3.1.9 *Seien $n, m \in \mathbb{N}$ mit $1 \leq m < n$ und $a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q$ mit $a_0 \neq 0$. Dann gilt:*

(i) Falls m gerade ist, gibt es eine bijektive Abbildung

$$\phi_0 : G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)}) \longrightarrow G_{n-m}^{(0)}$$

mit der Eigenschaft, daß für alle $xU_n, yU_n \in G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$ die Bedingung $xU_n \sim yU_n$ in G_n genau dann erfüllt ist, wenn $\phi_0(xU_n) \sim \phi_0(yU_n)$ in G_{n-m} gilt.

(ii) Falls m ungerade ist, gibt es eine bijektive Abbildung

$$\phi_1 : G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)}) \longrightarrow G_{n-m+1}^{(1)}(a_0)$$

mit der Eigenschaft, daß für alle $xU_n, yU_n \in G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$ die Bedingung $xU_n \sim yU_n$ in G_n genau dann erfüllt ist, wenn $\phi_1(xU_n) \sim \phi_1(yU_n)$ in G_{n-m+1} gilt.

Beweis: *Vorbemerkung:* Nach Lemma 3.1.8 folgt, daß ein Element xU_n von G_n genau dann in $G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$ liegt, wenn x von der Form $x = \sum_{i=0}^{g(m)}{}'' a_i\tau^i + x'\tau^m$ mit $x' \in U$ ist und $\mathrm{SP}(x') = 0$ im Fall m gerade bzw. $\mathrm{SP}(a_0 + x'\tau) = 1$ im Fall m ungerade gilt.

(i) Sei m gerade. Man definiere

$$\phi_0 : G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)}) \longrightarrow G_{n-m}^{(0)}$$
$$\left(\sum_{i=0}^{g(m)}{}'' a_i\tau^i + x'\tau^m\right) U_n \longmapsto x'U_{n-m}.$$

Weil nun für alle $x', y' \in U$ mit $\mathrm{SP}(x') = \mathrm{SP}(y') = 0$ die Bedingung

$$\sum_{i=0}^{g(m)}{}'' a_i\tau^i + x'\tau^m \equiv \sum_{i=0}^{g(m)}{}'' a_i\tau^i + y'\tau^m \mod U_n$$

genau dann erfüllt ist, wenn $x' \equiv y' \mod U_{n-m}$ gilt, folgt zusammen mit der Vorbemerkung, daß ϕ_0 wohldefiniert und injektiv ist. Sei nun $x'U_{n-m} \in G_{n-m}^{(0)}$ beliebig. Man setze $x := \sum_{i=0}^{g(m)}{}'' a_i\tau^i + x'\tau^m$. Dann gilt $\mathrm{SP}(x') = 0$ und damit $\mathrm{SP}(x) = m$. Außerdem ist $\phi_0(xU_n) = x'U_{n-m}$. Also ist ϕ_0 auch surjektiv. Für alle $xU_n = \left(\sum_{i=0}^{g(m)}{}'' a_i\tau^i + x'\tau^m\right) U_n$ und $yU_n = \left(\sum_{i=0}^{g(m)}{}'' a_i\tau^i + y'\tau^m\right) U_n$ in $G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$ gilt die Bedingung $xU_n \sim yU_n$ genau dann, wenn es ein $z \in U$ gibt mit

$$\begin{aligned}\sum_{i=0}^{g(m)}{}'' a_i\tau^i + x'\tau^m &\equiv z\left(\sum_{i=0}^{g(m)}{}'' a_i\tau^i + y'\tau^m\right) z^{-1} \mod U_n \\ &\equiv \sum_{i=0}^{g(m)}{}'' a_i\tau^i + zxz^{-1}\tau^m \mod U_n.\end{aligned}$$

Das ist äquivalent dazu, daß es ein $z \in U$ gibt mit $x' \equiv zy'z^{-1} \mod U_{n-m}$. Das wiederum besagt nichts anderes, als daß $\phi_0(xU_n) \sim \phi_0(yU_n)$ in G_{n-m} ist. Damit ist die Aussage (i) bewiesen.

(ii) Sei m ungerade. Man definiere

$$\phi_1 : G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)}) \longrightarrow G_{n-m+1}^{(1)}(a_0)$$

$$\left(\sum_{i=0}^{g(m)}{}'' a_i\tau^i + x'\tau^m\right) U_n \longmapsto (a_0 + x'\tau)U_{n-m+1}.$$

Weil nun für alle $x', y' \in U$ mit $\mathrm{SP}(a_0 + x'\tau) = \mathrm{SP}(a_0 + y'\tau) = 1$ die Bedingung

$$\sum_{i=0}^{g(m)}{}'' a_i\tau^i + x'\tau^m \equiv \sum_{i=0}^{g(m)}{}'' a_i\tau^i + y'\tau^m \mod U_n$$

genau dann erfüllt ist, wenn $x' \equiv y' \mod U_{n-m}$ gilt, was wiederum äquivalent ist zu $a_0 + x'\tau \equiv a_0 + y'\tau \mod U_{n-m+1}$, folgt zusammen mit der Vorbemerkung, daß ϕ_1 wohldefiniert und injektiv ist. Sei nun $(a_0 + x'\tau)U_{n-m+1} \in G^{(1)}_{n-m+1}(a_0)$ beliebig. Setze $x := \sum_{i=0}^{g(m)}{}'' a_i\tau^i + x'\tau^m$. Dann gilt $\mathrm{SP}(a_0 + x'\tau) = 1$ und damit $\mathrm{SP}(x) = m$. Außerdem ist $\phi_1(xU_n) = (a_0 + x'\tau)U_{n-m+1}$. Also ist ϕ_1 auch surjektiv. Für alle $xU_n = \left(\sum_{i=0}^{g(m)}{}'' a_i\tau^i + x'\tau^m\right) U_n$ und $yU_n = \left(\sum_{i=0}^{g(m)}{}'' a_i\tau^i + y'\tau^m\right) U_n$ in $G^{(m)}_n(a_0, a_2, \ldots, a_{g(m)})$ gilt die Bedingung $xU_n \sim yU_n$ genau dann, wenn es ein $z \in U$ gibt mit

$$\begin{aligned}\sum_{i=0}^{g(m)}{}'' a_i\tau^i + x'\tau^m &\equiv z\left(\sum_{i=0}^{g(m)}{}'' a_i\tau^i + y'\tau^m\right) z^{-1} \mod U_n\\ &\equiv \sum_{i=0}^{g(m)}{}'' a_i\tau^i + zx\tau z^{-1}\tau^{m-1} \mod U_n.\end{aligned}$$

Das ist äquivalent dazu, daß es ein $z \in U$ gibt mit

$$\begin{aligned}a_0 + x'\tau &\equiv a_0 + zy'\tau z^{-1} \mod U_{n-m+1}\\ &\equiv z(a_0 + y'\tau)z^{-1} \mod U_{n-m+1}.\end{aligned}$$

Das wiederum besagt nichts anderes, als daß $\phi_1(xU_n) \sim \phi_1(yU_n)$ in $G_{n-m+1}(a_0)$ ist. Damit ist die Aussage (ii) bewiesen. □

Korollar 3.1.10 *Seien $n, m \in \mathbb{N}$ mit $1 \le m < n$ und $a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q$ mit $a_0 \neq 0$.*

(i) Sei m gerade und $V \subset \{x \in U \mid \mathrm{SP}(x) = 0\}$ mit $G^{(0)}_{n-m} = \biguplus_{x\in V} [x]_{n-m}$. Dann gilt

$$G^{(m)}_n(a_0, a_2, \ldots, a_{g(m)}) = \biguplus_{x \in \sum_{i=0}^{g(m)}{}'' a_i\tau^i + V\tau^m} [x]_n.$$

Außerdem erhält man für die Länge der Konjugationsklassen

$$\#[x]_{n-m} = \#[\sum_{i=0}^{g(m)}{}'' a_i\tau^i + x\tau^m]_n$$

für alle $x \in V$.

(ii) Sei m ungerade und $V \subset \{x \in U \mid \mathrm{SP}(a_0 + x\tau) = 1\}$ mit $G^{(1)}_{n-m+1}(a_0) = \biguplus_{x\in a_0+V\tau} [x]_{n-m+1}$. Dann gilt

$$G^{(m)}_n(a_0, a_2, \ldots, a_{g(m)}) = \biguplus_{x \in \sum_{i=0}^{g(m)}{}'' a_i\tau^i + V\tau^m} [x]_n.$$

Außerdem erhält man für die Länge der Konjugationsklassen

$$\#[a_0 + x\tau]_{n-m+1} = \#[\sum_{i=0}^{g(m)}{}'' a_i\tau^i + x\tau^m]_n$$

für alle $x \in V$.

Beweis: (i) Sei ϕ_0 die Abbildung aus dem Beweis von Satz 3.1.9(i). Dann gilt für alle $x \in V$, daß $\phi_0^{-1}(xU_{n-m}) = \left(\sum_{i=0}^{g(m)}{}'' a_i\tau^i + x\tau^m\right) U_n$ ist. Aus den Eigenschaften von ϕ_0 folgen nun sofort die beiden Aussagen von (i).

(ii) Sei ϕ_1 die Abbildung aus dem Beweis von Satz 3.1.9(ii). Dann gilt für alle $x \in V$, daß $\phi_1^{-1}((a_0 + x\tau)U_{n-m+1}) = \left(\sum_{i=0}^{g(m)}{}'' a_i\tau^i + x\tau^m\right) U_n$ ist. Aus den Eigenschaften von ϕ_1 folgen nun sofort die beiden Aussagen von (ii). □

Damit sind nun nur noch für alle $n \in \mathbb{N}$ und $a_0 \in \mathbb{F}_q$ entsprechende V anzugeben die, den Bedingungen von Korollar 3.1.10(i) bzw. (ii) genügen.

3.2 Bestimmung der Konjugationsklassen auf $G_n^{(0)}$

Um die Konjugationsklassen auf $G_n^{(0)}$ zu bestimmen, versucht man für alle $x \in U$ mit $\mathrm{SP}(x) = 0$ für die Konjugationsklasse $[x]_n$ einen Repräsentanten zu finden, bei dem alle ungeraden Koeffizienten verschwinden. Der Sinn dieser Vorgehensweise besteht darin, daß man mit diesem Repräsentanten leichter rechnen kann.

Lemma 3.2.1 *Sei* $n \in \mathbb{N}$ ungrade *und* $x, y \in U$ *mit* $\mathrm{SP}(x) = \mathrm{SP}(y) = 0$ *und* $x \equiv y \mod U_n$. *Dann gilt* $x \sim_{n+1} y$.

Beweis: Wegen $x \equiv y \mod U_n$ muß es $a_0, a_1, \ldots, a_{n-1}, a_n, b_n \in \mathbb{F}_{q^2}$ geben mit

$$x \equiv \sum_{i=0}^{n} a_i\tau^i \mod U_{n+1} \text{ und } y \equiv \sum_{i=0}^{n-1} a_i\tau^i + b_n\tau^n \mod U_{n+1}.$$

Aus $\mathrm{SP}(x) = \mathrm{SP}(y) = 0$ folgt $a_0 \notin \mathbb{F}_q$ und damit $a_0 - a_0^q \neq 0$. Man setze nun $c := \frac{b_n - a_n}{a_0^q - a_0}$. Für $z := 1 + c\tau^n$ gilt nun $(1 + c\tau^n)(1 - c\tau^n) \equiv 1 \mod U_{n+1}$. Also ist $z^{-1} \equiv 1 - c\tau^n \mod U_{n+1}$. Damit erhält man

$$\begin{aligned}
zxz^{-1} &\equiv (1 + c\tau^n)\left(\sum_{i=0}^{n} a_i\tau^i\right)(1 - c\tau^n) \mod U_{n+1} \\
&\equiv \left(\sum_{i=0}^{n} a_i\tau^i + ca_0^q\tau^n\right)(1 - c\tau^n) \mod U_{n+1} \\
&\equiv \sum_{i=0}^{n} a_i\tau^i + (ca_0^q - ca_0)\tau^n \mod U_{n+1} \\
&\equiv \sum_{i=0}^{n} a_i\tau^i + (b_n - a_n)\tau^n \mod U_{n+1} \\
&\equiv y \mod U_{n+1}.
\end{aligned}$$

Daraus folgt $x \sim_{n+1} y$. □

Satz 3.2.2 *Sei* $n \in \mathbb{N}$ *mit* $x \in U$ *und* $\mathrm{SP}(x) = 0$. *Dann gibt es Elemente* $a_0, a_2, \ldots, a_{g(n)} \in \mathbb{F}_{q^2}$ *mit* $a_0 \notin \mathbb{F}_q$, *so daß gilt*

$$x \sim_n \sum_{i=0}^{g(n)}{}'' a_i\tau^i.$$

Beweis: Man zeigt die Aussage des Satzes durch Induktion über alle $n \in \mathbb{N}$. Für $n = 1$ wähle man $a_0 \in \mathbb{F}_{q^2}^*$, so daß $x \equiv a_0 \mod U_1$ ist. Wegen $\mathrm{SP}(x) = 0$ folgt $a_0 \notin \mathbb{F}_q$. Außerdem gilt trivialerweise $x \sim_1 \sum_{i=0}^{g(1)}{}'' a_i\tau^i$. Sei nun $n \in \mathbb{N}$ beliebig. Nach Induktionsannahme gibt es Elemente $a_0, a_2, \ldots, a_{g(n)} \in \mathbb{F}_{q^2}$ mit $a_0 \notin \mathbb{F}_q$, so daß $x \sim_n \sum_{i=0}^{g(n)}{}'' a_i\tau^i$ gilt. Es gibt nun ein $a_n \in \mathbb{F}_{q^2}$ mit $x \sim_{n+1} \sum_{i=0}^{g(n)}{}'' a_i\tau^i + a_n\tau^n$. Falls n gerade ist, gilt $g(n+1) = n$ und damit $x \sim_{n+1} \sum_{i=0}^{g(n+1)}{}'' a_i\tau^i$. Sei nun n ungerade. Dann gilt $g(n+1) = g(n)$ und damit $x \sim_{n+1} \sum_{i=0}^{g(n+1)}{}'' a_i\tau^i + a_n\tau^n$. Wegen $a_0 \notin \mathbb{F}_q$ folgt nach Lemma 3.2.1 die Relationen $\sum_{i=0}^{g(n+1)}{}'' a_i\tau^i + a_n\tau^n \sim_{n+1} \sum_{i=0}^{g(n+1)}{}'' a_i\tau^i$ bzw. $x \sim_{n+} \sum_{i=0}^{g(n+1)}{}'' a_i\tau^i$. □

Bemerkung 3.2.3 Der Satz 3.2.2 liefert für alle $n \in \mathbb{N}$ die folgende Aussage

$$G_n^{(0)} = \bigcup_{\substack{a_0, a_2, \ldots, a_{g(n)} \in \mathbb{F}_{q^2} \\ mit\ a_0 \notin \mathbb{F}_q}} [\sum_{i=0}^{g(n)}{}'' a_i\tau^i]_n.$$

Um nun zu zeigen, daß diese Vereinigung disjunkt ist, bestimmt man nun für alle $x \in U$ mit $\mathrm{SP}(x) = 0$ eine untere Schranke für die Elementanzahl des Zentralisators $\mathrm{Z}(xU_n)$ von xU_n in G_n (das ist die Menge aller Elemente von G_n, die mit xU_n kommutieren). Es sei an dieser Stelle daran erinnert, daß für ein beliebiges Element einer endlichen Gruppe das Produkt aus der Länge seiner Konjugationsklasse und der Elementanzahl seines Zentralisators gleich der Mächtigkeit der Gruppe ist.

Lemma 3.2.4 *Seien $n \in \mathbb{N}$ und $a_0, a_2, \ldots, a_{g(n)} \in \mathbb{F}_{q^2}$ mit $a_0 \notin \mathbb{F}_q$. Man setze $x := \sum_{i=0}^{g(n)}{}'' a_i\tau^i$. Dann gilt für die Elementanzahl des Zentralisators von xU_n in G_n die Abschätzung*

$$\#\mathrm{Z}(xU_n) \geq (q^2-1)q^{g(n)}.$$

Beweis: Man beachte, daß x mit allen Elementen der Form $\sum_{i=0}^{g(n)}{}'' a_i\tau^i$ mit $a_0, a_2, \ldots, a_{g(n)} \in \mathbb{F}_{q^2}$ und $a_0 \neq 0$ kommutiert. Offensichtlich gibt es von dieser Form genau

$$(q^2-1)(q^2)^{\#\{2,4,\ldots,g(n)\}} = (q^2-1)q^{g(n)}$$

Elemente, die modulo U_n paarweise nicht kongruent sind. Daraus folgt sofort

$$\#\mathrm{Z}(xU_n) \geq (q^2-1)q^{g(n)}.$$

□

Bemerkung 3.2.5 Unter den Voraussetzungen von Lemma 3.2.4 gilt für die Länge von $[x]_n$ die folgende Abschätzung

$$\#[x]_n = \frac{\#G_n}{\#\mathrm{Z}(xU_n)} \leq \frac{(q^2-1)(q^2)^{n-1}}{(q^2-1)q^{g(n)}} = q^{2n-g(n)-2}.$$

Satz 3.2.6 *Sei $n \in \mathbb{N}$. Dann gilt:*

(i) Für $G_n^{(0)}$ existiert die Zerlegung

$$G_n^{(0)} = \biguplus_{\substack{a_0,a_2,\ldots,a_{g(n)}\in\mathbb{F}_{q^2}\\ mit\ a_0\notin\mathbb{F}_q}} [\sum_{i=0}^{g(n)}{}'' a_i\tau^i]_n.$$

(ii) Für alle $xU_n \in G_n^{(0)}$ gilt $\#[x]_n = q^{2n-g(n)-2}$.

Beweis: Wegen Bemerkung 3.2.3 und Bemerkung 3.2.5 reicht es aus zu zeigen, daß die Vereinigung in (i) disjunkt ist und in (ii) die Ungleichung $\#[x]_n \geq q^{2n-g(n)-2}$ gilt.

Angenommen, die Vereinigung in (i) wäre nicht disjunkt oder es gäbe ein $xU_n \in G_n^{(0)}$ mit $\#[x]_n < q^{2n-g(n)-2}$. Dann folgte

$$(q^2-1)(q^2)^{n-1} < \sum_{\substack{a_0,a_2,\ldots,a_{g(n)}\in\mathbb{F}_{q^2}\\ mit\ a_0\notin\mathbb{F}_q}} \#[\sum_{i=0}^{g(n)}{}'' a_i\tau^i]_n \leq (q^2-1)q^{g(n)}\cdot q^{2n-g(n)-2}.$$

Damit erhielte man jedoch $(q^2-1)(q^2)^{n-1} < (q^2-1)q^{2n-2}$, was offensichtlich ein Widerspruch ist. Damit ist die Ausage des Satzes bewiesen. □

3.3 Bestimmung der Konjugationsklassen auf $G_n^{(1)}(a_0)$

Aus technischen Gründen bestimmt man in diesem Abschnitt zunächst die Länge der Konjugationsklassen. Dies geschieht ähnlich wie im letzten Abschnitt, indem man für alle $xU_n \in G_n^{(1)}(a_0)$ wieder die Elementanzahl des Zentralisators $\mathrm{Z}(xU_n)$ ausrechnet.

Satz 3.3.1 *Seien $n \in \mathbb{N}$ und $x = \sum_{i=0}^{\infty} a_i\tau^i \in U$ mit $\mathrm{SP}(x) = 1$. Dann gilt für die Elementanzahl des Zentralisators*

$$\#\mathrm{Z}(xU_n) = \begin{cases} q^2-1 & \text{falls } n = 1 \\ (q-1)q^n & \text{falls } n > 1. \end{cases}$$

Beweis: Falls $n = 1$ ist, wird die Aussage trivial, da G_1 abelsch ist und genau q^2-1 Elemente enthält. Sei also $n > 1$. Für ein beliebiges $y = \sum_{i=0}^{\infty} b_i\tau^i \in U$ ist die Bedingung $yU_n \in \mathrm{Z}(xU_n)$ genau dann erfüllt, wenn $xy = yx \mod U_n$ ist. Das ist äquivalent zu

$$\sum_{k=0}^{n-1}\left(\sum_{j=0}^{k} a_j b_{k-j}^{q^j}\right)\tau^k \equiv \sum_{k=0}^{n-1}\left(\sum_{j=0}^{k} b_j a_{k-j}^{q^j}\right)\tau^k \mod U_n.$$

Das wiederum ist gleichbedeutend damit, daß für alle $k = 0,1,\ldots,n-1$ die Gleichung

$$\sum_{j=0}^{k} a_j b_{k-j}^{q^j} = \sum_{j=0}^{k} b_j a_{k-j}^{q^j} \qquad (\mathbf{S_k})$$

erfüllt ist. Für alle $k \in \mathbb{N}$ läßt sich $\mathbf{S_k}$ als polynomiale Gleichung in den Variablen $b_0, b_1, \ldots, b_k$ auffassen. Man sieht nun leicht, daß die Gleichung $\mathbf{S_0}$ trivial ist, d.h. immer erfüllt ist. Damit läßt sich jedem Element $yU_n \in \mathrm{Z}(xU_n)$ *eineindeutig* ein n-Tupel $(b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_{q^2}^* \times (\mathbb{F}_{q^2})^{n-1}$ zu ordnen, das die Gleichungen $\mathbf{S_1}, \mathbf{S_2}, \ldots, \mathbf{S_{n-1}}$ erfüllt. Demnach reicht es aus zu zeigen, daß es für alle $n \in \mathbb{N}$ mit $n > 2$ genau $(q-1)q^n$ verschiedene n-Tupel $(b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_{q^2}^* \times (\mathbb{F}_{q^2})^{n-1}$ gibt, die den Gleichungen $\mathbf{S_0}, \mathbf{S_1}, \ldots, \mathbf{S_{n-1}}$ genügen. Dies geschieht durch Induktion über n. Dazu verwendet man die folgenden Hilfsbehauptungen, die das Lösungsverhalten der Gleichungen $\mathbf{S_k}$ beschreiben und anschließend bewiesen werden:

(H1) Es gibt genau $(q-1)q^2$ verschiedene Paare $(b_0, b_1) \in \mathbb{F}_{q^2}^* \times \mathbb{F}_{q^2}$, die der Gleichung $\mathbf{S_1}$ genügen.

(H2) Für alle $k \in \mathbb{N}$ mit $k > 2$ läßt sich $\mathbf{S_k}$ als polynomiale Gleichung in den Variablen $b_0, b_1, \ldots, b_{k-1}$ auffassen. Die Variable b_k ist frei wählbar.

(H3) Sei $k \in \mathbb{N}$ mit $k > 2$. Dann gibt es für alle $k-1$-Tupel $(b_0, b_1, \ldots, b_{k-2}) \in \mathbb{F}_{q^2}^* \times (\mathbb{F}_{q^2})^{k-2}$, die den Gleichungen $\mathbf{S_1}, \mathbf{S_2}, \ldots, \mathbf{S_{k-1}}$ genügen, genau q verschiedene $b_{k-1} \in \mathbb{F}_{q^2}$, so daß $(b_0, b_1, \ldots, b_{k-1})$ die Gleichung $\mathbf{S_k}$ erfüllt.

Damit entspricht der Induktionsanfang $n = 2$ der Hilfsbehauptung **(H1)**. Sei nun $n \in \mathbb{N}$ mit $n \geq 2$ beliebig. Dann gibt es nach Induktionsannahme gibt es genau $(q-1)q^n$ verschiedene $(b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_{q^2}^* \times (\mathbb{F}_{q^2})^{n-1}$, die den Gleichungen $\mathbf{S_1}, \mathbf{S_2}, \ldots, \mathbf{S_{n-1}}$ genügen. Nach **(H2)** folgt, daß es genau $(q-1)q^{n-2}$ verschiedene $n-1$-Tupel $(b_0, b_1, \ldots, b_{n-2}) \in \mathbb{F}_{q^2}^* \times (\mathbb{F}_{q^2})^{n-2}$ gibt, die ebenfalls den Gleichungen $\mathbf{S_1}, \mathbf{S_2}, \ldots, \mathbf{S_{n-1}}$ genügen. Nach **(H3)** gibt es nun genau $(q-1)q^{n-1}$ verschiedene $(b_0, b_1, \ldots, b_{n-1}) \in \mathbb{F}_{q^2}^* \times (\mathbb{F}_{q^2})^{n-1}$, so daß die Gleichungen $\mathbf{S_1}, \mathbf{S_2}, \ldots, \mathbf{S_n}$ gelten. Daraus folgt nun, daß es $(q-1)q^{n+1}$ verschiedene $n+1$-Tupel $(b_0, b_1, \ldots, b_n) \in \mathbb{F}_{q^2}^* \times (\mathbb{F}_{q^2})^n$, die die Gleichungen $\mathbf{S_1}, \mathbf{S_2}, \ldots, \mathbf{S_n}$ erfüllen.

Damit bleiben nun die Aussagen **(H1)**, **(H2)** und **(H3)** zu zeigen. Die Gleichung $\mathbf{S_1}$ lautet $a_0 b_1 + a_1 b_0^q = b_0 a_1 + b_1 a_0^q$. Wegen der Voraussetzung $\mathrm{SP}(x) = 1$ muß nun $a_0 \in \mathbb{F}_q$ und $a_1 \neq 0$ gelten. Damit wird $\mathbf{S_1}$ äquivalent zu der Gleichung $b_0 = b_0^q$. Das bedeutet, daß $b_1 \in \mathbb{F}_{q^2}$ frei wählbar ist und b_0 in $\mathbb{F}_q^*$ liegt. Also gibt es genau $(q-1)q^2$ verschiedene Paare $(b_0, b_1) \in \mathbb{F}_{q^2}^* \times \mathbb{F}_{q^2}$, die der Gleichung $\mathbf{S_1}$ genügen. Somit ist **(H1)** gezeigt. Um die Aussagen **(H2)** und **(H3)** zu zeigen, ist es notwendig, die Gleichungen $\mathbf{S_k}$ umzuformen. Hierbei unterscheidet man die Fälle k gerade und k ungerade. Falls k gerade ist, läßt sich die rechte Seite der Gleichung $\mathbf{S_k}$ folgendermaßen umformen

$$\sum_{j=0}^{k} b_j a_{k-j}^{q^j} = \sum_{j=0}^{k} b_{k-j} a_j^{q^{k-j}} = \sum_{j=0}^{k} b_{k-j} a_j^{q^j}.$$

Hierbei ist lediglich zu beachten, daß $k-j$ genau dann gerade ist, wenn j gerade ist. Somit ist $\mathbf{S_k}$ äquivalent zur Gleichung

$$\begin{aligned}
0 &= \sum_{j=0}^{k} (a_j b_{k-j}^{q^j} - b_{k-j} a_j^{q^j}) \\
&= \sum_{j=1}^{k-1}{}' (a_j b_{k-j}^q - b_{k-j} a_j^q) \\
&= a_1 b_{k-1}^q - a_1^q b_{k-1} + \sum_{j=1}^{k-3}{}' (a_j b_{k-j}^q - b_{k-j} a_j^q). \\
&= a_1 b_{k-1}^q - a_1^q b_{k-1} + \sum_{j=1}^{k-3}{}' (a_{k-j} b_j^q - b_j a_{k-j}^q).
\end{aligned}$$

Das wiederum ist gleichbedeutend mit der Gleichung

$$a_1 b_{k-1}^q - a_1^q b_{k-1} = -\sum_{j=1}^{k-3}{}' (a_{k-j} b_j^q - b_j a_{k-j}^q) \qquad (\mathbf{S'_k}).$$

Falls k ungerade ist, läßt sich die linke Seite der Gleichung $\mathbf{S_k}$ folgendermaßen umformen

$$\sum_{j=0}^{k} a_j b_{k-j}^{q^j} = \sum_{j=0}^{k} a_{k-j} b_j^{q^{k-j}} = \sum_{j=0}^{k} a_{k-j} b_j^{q^{j+1}}.$$

Hierbei ist lediglich zu beachten, daß $k-j$ genau dann gerade ist, wenn $j+1$ gerade ist. Somit ist $\mathbf{S_k}$ äquivalent zur Gleichung

$$\begin{aligned} 0 &= \sum_{j=0}^{k}(a_{k-j}b_j^{q^{j+1}} - b_j a_{k-j}^{q^j}) \\ &= \sum_{j=1}^{k}{}' b_j(a_{k-j} - a_{k-j}^q) + \sum_{j=0}^{k-1}{}'' a_{k-j}(b_j^q - b_j) \\ &= b_k(a_0 - a_0^q) + \sum_{j=1}^{k-2}{}' b_j(a_{k-j} - a_{k-j}^q) + \sum_{j=0}^{k-3}{}'' a_{k-j}(b_j^q - b_j) + a_1(b_{k-1}^q - b_{k-1}). \end{aligned}$$

Wegen $a_0 \in \mathbb{F}_q$ und $a_1 \neq 0$ erhält man daraus durch einfache Äquivalenzumformungen die Gleichung

$$b_{k-1}^q - b_{k-1} = \frac{1}{a_1}\left(-\sum_{j=1}^{k-2}{}' b_j(a_{k-j} - a_{k-j}^q) - \sum_{j=0}^{k-3}{}'' a_{k-j}(b_j^q - b_j)\right) \qquad (\mathbf{S'_k}).$$

Da nun in den zu $(\mathbf{S_k})$ äquivalenten Gleichungen $(\mathbf{S'_k})$ die Variable b_k nicht mehr auftritt, folgt die Behauptung **(H2)**.

Für den Beweis von **(H3)** sei $(b_0, b_1, \ldots, b_{k-2}) \in \mathbb{F}_{q^2}^* \times (\mathbb{F}_{q^2})^{k-2}$ ein $k-1$-Tupel, das die Gleichungen $\mathbf{S_1}, \mathbf{S_2}, \ldots, \mathbf{S_{k-1}}$ löst. Es bleibt zu zeigen, daß die Gleichung $\mathbf{S'_k}$ genau q verschiedene Lösungen b_{k-1} hat. Falls k gerade ist, reicht es aus, die Gleichung $\mathbf{S'_k}$ genauer zu betrachten. Weil $a_j b_{k-j}^q - b_{k-j}a_j^q = (a_j^q b_{k-j})^q - a_j^q b_{k-j}$ für alle $j = 1, 3, \ldots, k-3$ nach Satz 1.1.4 in $(\alpha - \alpha^q)\mathbb{F}_q$ liegt, ist der Ausdruck der gesamten rechten Seite in $(\alpha - \alpha^q)\mathbb{F}_q$. Wegen $a_1 \neq 0$ folgt aus Korollar 1.1.5, daß es genau q verschiedene b_{k-1} gibt, die die Gleichung $\mathbf{S'_k}$ lösen.

Der Fall k ungerade gestaltet sich dagegen wesentlich schwieriger. Auch hier reicht es nach Satz 1.1.4 zu zeigen, daß die rechte Seite von $\mathbf{S'_k}$ in $(\alpha - \alpha^q)\mathbb{F}_q$ liegt. Dazu geht man in 2 Schritten vor. Im ersten Schritt zeigt man unter Verwendung von $\mathbf{S'_1}, \mathbf{S'_3}, \ldots, \mathbf{S'_{k-2}}$, daß die rechte Seite von $\mathbf{S'_k}$ von der Form

$$\sum_{i=2}^{k-1}{}'' \Phi_{k-i}(a_i^q - a_i)$$

ist, wobei die $\Phi_1, \Phi_3, \ldots, \Phi_{k-2} \in \mathbb{F}_{q^2}$ unabhängig von $b_0, b_2, \ldots, b_{k-1}$ sind. Im zweiten Schritt zeigt man unter Verwendung von $\mathbf{S'_2}, \mathbf{S'_4}, \ldots, \mathbf{S'_{k-1}}$, daß die $\Phi_1, \Phi_3, \ldots, \Phi_{k-2}$ in $\mathbb{F}_q$ liegen, womit dann die Behauptung folgt. Bevor es nun so richtig los geht, führt man noch die Abkürzung

$$\Psi_{i-1} := \frac{1}{a_1}\left(-\sum_{j=1}^{i-2}{}' b_j(a_{i-j} - a_{i-j}^q) - \sum_{j=0}^{i-3}{}'' a_{i-j}(b_j^q - b_j)\right)$$

für alle ungeraden natürlichen Zahlen i ein. Mit dieser Abkürzung bekommt dann die Gleichung $\mathbf{S'_i}$ die einfache Form $b_i^q - b_i = \Psi_i$.

<u>1. Schritt:</u> Man setze $\Phi_1 := \frac{b_1}{a_1}$. Weiter definiere man induktiv

$$\Phi_{i+2} := \frac{1}{a_1}(b_{i+1} - \sum_{j=0}^{i-1}{}'' a_{i+2-j}\Phi_{j+1})$$

für alle ungeraden $i \in \mathbb{N}$. Durch Induktion über alle ungeraden $k \in \mathbb{N}$ mit $k \geq 3$ zeigt man nun die folgende Behauptung: Sind die Gleichungen $\mathbf{S'_1}, \mathbf{S'_3}, \ldots, \mathbf{S'_{k-2}}$ erfüllt, so gilt

$$\Psi_{k-1} = \sum_{i=2}^{k-1}{}'' \Phi_{k-i}(a_i^q - a_i).$$

Induktionsanfang $k = 3$: Nach der Definition von Ψ_2 gilt

$$\Psi_2 = \frac{1}{a_1}(-b_1(a_2 - a_2^q) - a_3(b_0^q - b_0)).$$

Aus $\mathbf{S_1'}$ folgt nun $b_0 = b_0^q$ (vgl. Beweis von **(H1)**). Damit erhält man

$$\Psi_2 = \frac{b_1}{a_1}(a_2^q - a_2) = \sum_{i=2}^{2}{}'' \Phi_{k-i}(a_i^q - a_i).$$

Induktionsschritt $k \longmapsto k+2$: Es seien die Gleichungen $\mathbf{S_1'}, \mathbf{S_3'}, \ldots \mathbf{S_k'}$ erfüllt. Nach Induktionsannahme gilt nun

$$\Psi_{i-1} = \sum_{j=2}^{i-1}{}'' \Phi_{i-j}(a_j^q - a_j)$$

für alle $i = 3, 5, \ldots, k$. Daraus folgt

$$\begin{aligned}
\Psi_{k+1} &= \tfrac{1}{a_1}\left(-\sum_{i=1}^{k-2}{}' b_i(a_{k-i} - a_{k-i}^q) - \sum_{i=0}^{k-3}{}'' a_{k-i}\Psi_i\right)\\
&= \tfrac{1}{a_1}\left(\sum_{i=1}^{k-2}{}' b_i(a_{k-i}^q - a_{k-i}) - \sum_{i=0}^{k-3}{}'' a_{k-i}\sum_{j=2}^{i}{}'' \Phi_{i+1-j}(a_j^q - a_j)\right)\\
&= \tfrac{1}{a_1}\left(\sum_{i=2}^{k-1}{}'' b_{k-i}(a_i^q - a_i) - \sum_{i=2}^{k-3}{}'' \sum_{j=2}^{i}{}'' a_{k-i}\Phi_{i+1-j}(a_j^q - a_j)\right)\\
&= \tfrac{1}{a_1}\left(\sum_{j=2}^{k-1}{}'' b_{k-j}(a_j^q - a_j) - \sum_{j=2}^{k-3}{}'' \sum_{i=j}^{k-3}{}'' a_{k-i}\Phi_{i+1-j}(a_j^q - a_j)\right)\\
&= \tfrac{1}{a_1}\left(b_1(a_{k-1}^q - a_{k-1}) + \sum_{j=2}^{k-3}{}'' b_{k-j}(a_j^q - a_j) - \sum_{j=2}^{k-3}{}'' \sum_{i=j}^{k-3}{}'' a_{k-i}\Phi_{i+1-j}(a_j^q - a_j)\right)\\
&= \tfrac{b_1}{a_1}(a_{k-1}^q - a_{k-1}) + \sum_{j=2}^{k-3}{}'' \tfrac{1}{a_1}\left(b_{k-j} - \sum_{i=j}^{k-3}{}'' a_{k-i}\Phi_{i+1-j}\right)(a_j^q - a_j)\\
&= \tfrac{b_1}{a_1}(a_{k-1}^q - a_{k-1}) + \sum_{j=2}^{k-3}{}'' \tfrac{1}{a_1}\left(b_{k-j} - \sum_{i=0}^{k-3-j}{}'' a_{k-i-j}\Phi_{i+1}\right)(a_j^q - a_j)\\
&= \Phi_1(a_{k-1}^q - a_{k-1}) + \sum_{j=2}^{k-3}{}'' \Phi_{k-j}(a_j^q - a_j)\\
&= \sum_{j=2}^{k-1}{}'' \Phi_{k-j}(a_j^q - a_j).
\end{aligned}$$

<u>2. Schritt:</u> Durch Induktion über alle ungeraden $k \in \mathbb{N}$ mit $k \geq 3$ zeigt man die folgende Behauptung: Sind die Gleichungen $\mathbf{S_2'}, \mathbf{S_4'}, \ldots, \mathbf{S_{k-1}'}$ erfüllt, so liegt ϕ_{k-2} in $\mathbb{F}_q$.

Induktionsanfang $k = 3$: Die Gleichung $\mathbf{S_2'}$ lautet $a_1 b_1^q - a_1^q b_1 = 0$. Daraus folgt $\frac{b_1}{a_1} = \left(\frac{b_1}{a_1}\right)^q$. Somit ist $\Phi_1 = \frac{b_1}{a_1} \in \mathbb{F}_q$.

Induktionsschritt $k \longmapsto k+2$: Es seien die Gleichungen $\mathbf{S_2'}, \mathbf{S_4'}, \ldots, \mathbf{S_{k+1}'}$ erfüllt. Nach Induktionsannahme gilt nun $\Phi_1, \Phi_3, \ldots, \Phi_{k-2} \in \mathbb{F}_q$. Damit erhält man

$$\begin{aligned}
\Phi_k &= \tfrac{1}{a_1}\left(b_k - \sum_{i=0}^{k-3}{}'' a_{k-i}\Phi_{i+1}\right)\\
&= \tfrac{1}{a^{q+1}}\left(b_k a_1^q - \sum_{i=0}^{k-3}{}'' a_{k-i}(a_1\Phi_{i+1})^q\right)\\
&= \tfrac{1}{a^{q+1}}\left(b_k a_1^q - \sum_{i=0}^{k-3}{}'' a_{k-i}\left(b_{i+1} - \sum_{j=0}^{i-2}{}'' a_{i+1-j}\Phi_{j+1}\right)^q\right)\\
&= \tfrac{1}{a^{q+1}}\left(b_k a_1^q - \sum_{i=0}^{k-3}{}'' a_{k-i}b_{i+1}^q + \sum_{i=0}^{k-3}{}'' \sum_{j=0}^{i-2}{}'' a_{k-i}a_{i+1-j}^q\Phi_{j+1}\right)\\
&= \tfrac{1}{a^{q+1}}\left(b_k a_1^q - \sum_{i=1}^{k-2}{}' a_{k+1-i}b_i^q + \sum_{j=0}^{k-3}{}'' \left(\sum_{i=j+2}^{k-3}{}'' a_{k-i}a_{i+1-j}^q\right)\Phi_{j+1}\right).
\end{aligned}$$

Die Gleichung $\mathbf{S'_{k+1}}$ lautet nun $a_1 b_k^q - a_1^q b_k = -\sum\limits_{j=0}^{k-2}{}'(a_{k+1-j}b_j^q - b_j a_{k+1-j}^q)$. Damit erhält man

$$\left(b_k a_1^q - \sum_{i=0}^{k-2}{}' a_{k+1-i} b_i^q\right)^q = b_k^q a_1 - \sum_{i=0}^{k-2}{}' a_{k+1-i}^q b_i = b_k a_1^q - \sum_{i=0}^{k-2}{}' a_{k+1-i} b_i^q.$$

Somit liegt $b_k a_1^q - \sum\limits_{i=0}^{k-2}{}' a_{k+1-i} b_i^q$ in $\mathbb{F}_q$. Wegen $\frac{1}{a_1^{q+1}} \in \mathbb{F}_q$ bleibt lediglich zu zeigen, daß der Ausdruck

$$\sum_{j=0}^{k-3}{}'' \left(\sum_{i=j+2}^{k-3}{}'' a_{k-i} a_{i+1-j}^q \right) \Phi_{j+1}$$

in $\mathbb{F}_q$ liegt. Dazu reicht es aus, $\sum\limits_{i=j+2}^{k-3}{}'' a_{k-i} a_{i+1-j}^q \in \mathbb{F}_q$ für alle $j = 0, 2, \ldots, k-3$ zu zeigen. Dies geschieht durch folgende einfache Rechnung:

$$\begin{aligned}\left(\sum_{i=j+2}^{k-3}{}'' a_{k-i} a_{i+1-j}^q\right)^q &= \left(a_{k-j-2} a_3^q + a_{k-j-4} a_5^q + \ldots + a_5 a_{k-j-4}^q + a_3 a_{k-j-2}^q\right)^q \\ &= a_{k-j-2}^q a_3 + a_{k-j-4}^q a_5 + \ldots + a_5^q a_{k-j-4} + a_3^q a_{k-j-2} \\ &= \sum_{i=j+2}^{k-3}{}'' a_{k-i} a_{i+1-j}^q.\end{aligned}$$

Damit ist $\Phi_k \in \mathbb{F}_q$ gezeigt.

Insgesamt nun folgt nun die Aussage **(H3)**. □

Mit diesem Satz läßt sich nun die Länge aller Konjugationsklassen auf $G_n^{(1)}$ angeben.

Korollar 3.3.2 *Sei $n \in \mathbb{N}$. Für alle $xU_n \in G_n^{(1)}$ gilt dann*

$$\#[x]_n = \begin{cases} 1 & \textit{falls } n = 1 \\ (q+1)q^{n-2} & \textit{falls } n > 1. \end{cases}$$

Beweis: Im Fall $n = 1$ gilt $\#[x]_n = 1$, da $G_1 \cong \mathbb{F}_{q^2}^*$ abelsch ist. Falls $n \neq 1$ ist, liefert Satz 3.3.1 die Gleichung

$$\#[x]_n = \frac{\#G_n}{\#\mathrm{N}(xU_n)} = \frac{(q^2-1)(q^2)^{n-1}}{(q-1)q^n} = (q+1)q^{n-2}.$$

□

Im folgenden wird nun die Frage behandelt, wie für ein $x \in U$ mit $\mathrm{SP}(x) = 1$ die Konjugationsklassen $[x]_n$ und $[x]_{n+1}$ zusammenhängen. Dazu wähle man die Bezeichnung $\mathbb{S}_{q^2} := \{\alpha^{q-1}, \alpha^{2(q-1)}, \ldots, \alpha^{q(q-1)}, 1\}$. Offensichtlich ist dann $\mathbb{S}_{q^2}$ eine Untergruppe von $\mathbb{F}_{q^2}^*$, und es gilt $\#\mathbb{S}_{q^2} = q + 1$.

Lemma 3.3.3 *Sei $n \in \mathbb{N}$. Seien weiter $x = \sum_{i=0}^{\infty} a_i \tau^i, y \in U$ mit $\mathrm{SP}(x) = 1$ sowie $b_n \in \mathbb{F}_{q^2}$ mit $y \equiv \sum_{i=1}^{n-1} a_i \tau^i + b_n \tau^n \mod U_{n+1}$. Dann gilt:*

(i) Falls $n = 1$ ist, folgt aus $b_1 \in a_1 \mathbb{S}_{q^2}$ die Relation $x \sim_2 y$.

(ii) Falls n gerade ist, folgt aus $b_n \in a_n + (\alpha - \alpha^q)\mathbb{F}_q$ die Relation $x \sim_{n+1} y$

(iii) Falls $n \neq 1$ und n ungerade ist, folgt aus $b_n \in a_n + a_1(\alpha - \alpha^q)\mathbb{F}_q$ die Relation $x \sim_{n+1} y$.

Beweis: (i) Aus $b_1 \in a_1 \mathbb{S}_{q^2}$ folgt, daß es ein $s \in \{1, 2, \ldots, q+1\}$ gibt mit $b_1 = a_1 \alpha^{s(q-1)}$. Damit erhält man

$$\begin{aligned} \alpha^{-s} x (\alpha^{-s})^{-1} &\equiv \alpha^{-s}(a_0 + a_1\tau)\alpha^s \mod U_2 \\ &\equiv a_0 + a_1 \alpha^{s(q-1)}\tau \mod U_2 \\ &\equiv a_0 + b_1\tau \mod U_2. \end{aligned}$$

Daraus folgt $x \sim_2 y$.

(ii) Aus $b_n \in a_n + (\alpha - \alpha^q)\mathbb{F}_q$ folgt $b_n - a_n \in (\alpha - \alpha^q)\mathbb{F}_q$. Nach Korollar 1.1.5 gibt es nun ein $c \in \mathbb{F}_{q^2}$ mit $a_1^q c - a_1 c^q = b_n - a_n$. Damit erhält man

$$\begin{aligned} (1 + c\tau^{n-1}) x (1 + c\tau^{n-1})^{-1} &\equiv (1 + c\tau^{n-1}) \left(a_0 + \sum_{i=1}^n a_i\tau^i \right) (1 + c\tau^{n-1})^{-1} \mod U_{n+1} \\ &\equiv a_0 + (1 + c\tau^{n-1}) \left(\sum_{i=1}^n a_i\tau^i \right) (1 - c\tau^{n-1}) \mod U_{n+1} \\ &\equiv a_0 + (1 + c\tau^{n-1}) \left(\sum_{i=1}^n a_i\tau^i - a_1 c^q \tau^n \right) \mod U_{n+1} \\ &\equiv a_0 + \left(\sum_{i=1}^n a_i\tau^i + (a_1^q c - a_1 c^q)\tau^n \right) \mod U_{n+1} \\ &\equiv a_0 + \left(\sum_{i=1}^n a_i\tau^i + (b_n - a_n)\tau^n \right) \mod U_{n+1} \\ &\equiv y \mod U_{n+1}. \end{aligned}$$

Daraus folgt $x \sim_{n+1} y$.

(iii) Aus $b_n \in a_n + a_1(\alpha - \alpha^q)\mathbb{F}_q$ folgt $\frac{b_n - a_n}{a_1} \in (\alpha - \alpha^q)\mathbb{F}_q$. Nach Satz 1.1.4 gibt es nun ein $c \in \mathbb{F}_{q^2}$ mit $\frac{b_n - a_n}{a_1} = c^q - c$. Damit erhält man

$$\begin{aligned} (1 - c\tau^{n-1}) x (1 - c\tau^{n-1})^{-1} &\equiv (1 - c\tau^{n-1}) \left(a_0 + \sum_{i=1}^n a_i\tau^i \right) (1 - c\tau^{n-1})^{-1} \mod U_{n+1} \\ &\equiv a_0 + (1 - c\tau^{n-1}) \left(\sum_{i=1}^n a_i\tau^i \right) (1 + c\tau^{n-1}) \mod U_{n+1} \\ &\equiv a_0 + (1 - c\tau^{n-1}) \left(\sum_{i=1}^n a_i\tau^i + a_1 c^q \tau^n \right) \mod U_{n+1} \\ &\equiv a_0 + \sum_{i=1}^n a_i\tau^i + (a_1 c^q - a_1 c)\tau^n \mod U_{n+1} \\ &\equiv a_0 + \sum_{i=1}^n a_i\tau^i + (b_n - a_n)\tau^n \mod U_{n+1} \\ &\equiv y \mod U_{n+1}. \end{aligned}$$

Daraus folgt $x \sim_{n+1} y$. $\square$

Lemma 3.3.4 *Sei $n \in \mathbb{N}$ und $x \in U$ mit* $\mathrm{SP}(x) = 1$. *Dann gibt es im Fall $\left\{ {n=1 \atop n>1} \right\}$ genau $\left\{ {q+1 \atop q} \right\}$ verschiedene $yU_n \in G_n$ mit $x \equiv y \mod U_n$ und $x \sim_n y$.*

Beweis: (i) Daß es im Fall $\left\{ {n=1 \atop n>1} \right\}$ *mindestens* $\left\{ {q+1 \atop q} \right\}$ verschiedene $yU_n \in G_n$ mit $x \equiv y \mod U_n$ und $x \sim_n y$ gibt, folgt wegen $\#\mathbb{S}_{q^2} = q + 1$ und $\#(\alpha - \alpha^q)\mathbb{F}_q = q$ direkt aus Lemma 3.3.3. Im Fall $n = 1$ führt die Annahme, daß es *mehr* als $q + 1$ verschiedene $yU_2 \in G_2$ mit $x \equiv y \mod U_1$ und $x \sim_2 y$ gäbe, wegen $\#[x]_2 = q + 1$ zum Widerspruch mit Korollar 3.3.2. Sei also nun $n > 1$. Angenommen, es gäbe *mehr* als q verschiedene $yU_n \in G_n$ mit $x \equiv y \mod U_n$ und $x \sim_n y$. Dann folgte nach Korollar 3.3.2 die Ungleichung $\#[x]_{n+1} > (q+1)q^{n-1}$, die gleichzeitig im Widerspruch zu Korollar 3.3.2 steht. $\square$

Aus den Lemmata 3.3.3 und 3.3.4 ergibt sich wegen $\#\mathbb{S}_{q^2} = q + 1$ und $\#(\alpha - \alpha^q)\mathbb{F}_q = q$ sofort die folgende Aussage.

Satz 3.3.5 *Sei $n \in \mathbb{N}$. Seien weiter $x = \sum_{i=0}^{\infty} a_i \tau^i, y \in U$ mit $\mathrm{SP}(x) = 1$ sowie $b_n \in \mathbb{F}_{q^2}$ mit $y \equiv \sum_{i=1}^{n-1} a_i \tau^i + b_n \tau^n \mod U_{n+1}$.*

(i) Falls $n = 1$ ist, gilt die Relation $x \sim_2 y$ genau dann, wenn die Bedingung $b_1 \in a_1 \mathbb{S}_{q^2}$ erfüllt ist.

(ii) Falls n gerade ist, gilt die Relation $x \sim_{n+1} y$ genau dann, wenn die Bedingung $b_n \in a_n + (\alpha - \alpha^q)\mathbb{F}_q$ erfüllt ist.

(iii) Falls $n \neq 1$ und n ungerade ist, gilt die Relation $x \sim_{n+1} y$ genau dann, wenn die Bedingung $b_n \in a_n + a_1(\alpha - \alpha^q)\mathbb{F}_q$ erfüllt ist.

Damit ist nun die Frage, wie $[x]_n$ und $[x]_{n+1}$ zusammenhängen vollständig beantwortet. Mit Satz 3.3.5 läßt sich nun wie folgt ein Repräsentantensystem für die Konjugationsklassen auf $G_n^{(1)}(a_0)$ angeben.

Satz 3.3.6 *Sei $n \in \mathbb{N}$ und $a_0 \in \mathbb{F}_q$. Seien weiter*

- *$\{\alpha_1, \ldots, \alpha_{q-1}\}$ ein Repräsentantensystem der multiplikativen Faktorgruppe $\mathbb{F}_{q^2}^* / \mathbb{S}_{q^2}$,*
- *$\{\beta_1, \ldots, \beta_q\}$ ein Repräsentantensystem der additiven Faktorgruppe $\mathbb{F}_{q^2}/(\alpha - \alpha^q)\mathbb{F}_q$ und*
- *$\{\gamma_1^{(k)}, \ldots, \gamma_q^{(k)}\}$ für alle $k = 1, 2, \ldots, q-1$ ein Repräsentantensystem der additiven Faktorgruppe $\mathbb{F}_{q^2}/\alpha_k(\alpha - \alpha^q)\mathbb{F}_q$.*

Dann gilt

$$G_n^{(1)}(a_0) = \biguplus_{\substack{k \in \{1,\ldots,q-1\} \\ l_i \in \{1,\ldots,q\} \\ \text{für } i=2,\ldots,n-1}} [a_0 + \alpha_k \tau + \sum_{i=2}^{g(n)}{}'' \beta_{l_i} \tau^i + \sum_{i=3}^{u(n)}{}' \gamma_{l_i}^{(k)} \tau^i]_n.$$

Beweis: Für $n = 1$ wird die Aussage trivial. Sei also $n > 1$. Zuerst zeigt man, daß die Vereinigung auf der rechten Seite disjunkt ist. Seien dazu

$$\begin{aligned} x &= a_0 + \alpha_k \tau + \sum_{i=2}^{n-1}{}'' \beta_{l_i} \tau^i + \sum_{i=3}^{n-1}{}' \gamma_{l_i}^{(k)} \tau^i \quad \text{und} \\ y &= a_0 + \alpha_{k'} \tau + \sum_{i=2}^{n-1}{}'' \beta_{l'_i} \tau^i + \sum_{i=3}^{n-1}{}' \gamma_{l'_i}^{(k')} \tau^i \end{aligned}$$

mit $k, k' \in \{1, \ldots, q-1\}$ und $l_i, l'_i \in \{1, \ldots, q\}$ für alle $i = 2, \ldots, n-1$, so daß $x \sim_n y$ gilt. Nach Satz 3.3.5(i) folgt $\alpha_{k'} \in \alpha_k \mathbb{S}_{q^2}$ und damit $\alpha_{k'} = \alpha_k$. Also ist $k = k'$. Daraus ergibt sich $x \equiv y \mod U_2$. Angenommen, es gäbe $x \not\equiv y \mod U_n$. Sei $m \in \{2, \ldots, n-1\}$ die kleinste Zahl mit $x \not\equiv y \mod U_{m+1}$. Falls m gerade ist, folgt nach Satz 3.3.5(ii), daß $\beta_{l'_m} \in \beta_{l_m} + (\alpha - \alpha^q)\mathbb{F}_q$ und damit $\beta_{l'_m} = \beta_{l_m}$ gilt. Da dies ein Widerspruch zu $x \equiv y \mod U_{m+1}$ ist, muß m gerade sein. In diesem Fall folgt aber nach Satz 3.3.5(iii), daß $\gamma_{l'_m}^{(k')} \in \gamma_{l_m}^{(k)} + \alpha_k(\alpha - \alpha^q)\mathbb{F}_q$ ist. Wegen $k = k'$ erhält man daraus $\gamma_{l_m}^{(k)} = \gamma_{l'_m}^{(k')}$, was wiederum einen Widerspruch zu $x \not\equiv y \mod U_{m+1}$ darstellt. Damit ist gezeigt, daß die Vereinigung auf der rechten Seite disjunkt ist. Da diese offensichtlich eine Teilmenge von $G_n^{(1)}(a_0)$ ist, bleibt lediglich zu zeigen, daß die Anzahl der Konjugationsklassen auf beiden Seiten gleich ist. Für die Anzahl der Konjugationsklassen auf der rechten Seite erhält man

$$\#\{(k, l_2, l_3, \ldots, l_{n-1}) \mid k \in \{1, \ldots, q-1\}, l_i \in \{1, \ldots, q\} \text{ für } i = 2, \ldots, n-1\} = (q-1)q^{n-2}.$$

Für die Elementanzahl von $G_n^{(1)}(a_0)$ ergibt sich

$$\begin{aligned} \#G_n^{(1)}(a_0) &= \#\{(a_0 + \sum_{i=1}^{n-1} a_i \tau^i) U_n \mid a_1, \ldots, a_{n-1} \in \mathbb{F}_{q^2} \text{ mit } a_1 \neq 0\} \\ &= (q^2-1)(q^2)^{n-2}. \end{aligned}$$

Da jede Konjugationsklasse nach Korollar 3.3.2 genau $(q+1)q^{n-2}$ Elemente enthält, folgt, daß es auf $G_n^{(1)}(a_0)$ ebenfalls genau

$$\frac{(q^2-1)(q^2)^{n-1}}{(q+1)q^{n-2}} = (q-1)q^{n-2}$$

verschiedene Konjugationsklassen gibt. Damit folgt die Gleichheit. □

3.4 Folgerungen aus den Ergebnissen der Abschnitte 3.1-3.3

Für die folgenden Betrachtungen sei

- $\{\alpha_1, \ldots, \alpha_{q-1}\}$ ein Repräsentantensystem der multiplikativen Faktorgruppe $\mathbb{F}_{q^2}^*/\mathbb{S}_{q^2}$,
- $\{\beta_1, \ldots, \beta_q\}$ ein Repräsentantensystem der additiven Faktorgruppe $\mathbb{F}_{q^2}/(\alpha - \alpha^q)\mathbb{F}_q$ und
- $\{\gamma_1^{(k)}, \ldots, \gamma_q^{(k)}\}$ für alle $k = 1, 2, \ldots, q-1$ ein Repräsentantensystem der additiven Faktorgruppe $\mathbb{F}_{q^2}/\alpha_k(\alpha - \alpha^q)\mathbb{F}_q$.

Außerdem sei

$$V_n' := \{\alpha_k + \sum_{i=2}^{g(n)}{}''\beta_{l_i}\tau^{i-1} + \sum_{i=3}^{u(n)}{}'\gamma_{l_i}^{(k)}\tau^{i-1} \mid k \in \{1, \ldots, q-1\}, l_i \in \{1, \ldots, q\} \textit{ für } i = 2, \ldots, n-1\}$$

für alle $n \in \mathbb{N}$. Damit lassen sich nun folgende Teilmengen von V_n definieren.

Definition 3.4.1 *Sei $n \in \mathbb{N}$.*

(i) Man setze $V_n^{(0)} := \{\sum_{i=0}^{g(n)}{}''a_i\tau^i \mid a_0, a_2, \ldots, a_{g(n)} \in \mathbb{F}_{q^2}$ *mit* $a_0 \notin \mathbb{F}_q\}$

(ii) Für alle $m \in \mathbb{N}$ mit $m < n$ und $a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q$ mit $a_0 \neq 0$ sei

$$V_n^{(m)}(a_0, a_2, \ldots, a_{g(m)}) := \sum_{i=0}^{g(m)}{}''a_i\tau^i + \begin{cases} V_{n-m}^{(0)}\tau^m & \textit{falls } m \textit{ gerade} \\ V_{n-m+1}'\tau^{m+1} & \textit{falls } m \textit{ ungerade} \end{cases}$$

(iii) Für alle $a_0, a_2, \ldots, a_{g(n)} \in \mathbb{F}_q$ mit $a_0 \neq 0$ sei

$$V_n^{(n)}(a_0, a_2, \ldots, a_{g(n)}) := \{\sum_{i=0}^{g(n)}{}''a_i\tau^i\}.$$

Mit diesen Teilmengen läßt sich nun die Einteilung von G_n in Konjugationsklassen vollständig beschreiben.

Satz 3.4.2 *Sei $n \in \mathbb{N}$.*

(i) Es gilt $G_n^{(0)} = \biguplus_{x \in V_n^{(0)}} [x]_n$. *Dabei ist* $\#[x]_n = q^{2n-g(n)-2}$ *für alle* $x \in V_n^{(0)}$.

(ii) Für alle $m \in \{1, \ldots, n-1\}$ und $a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q$ mit $a_0 \neq 0$ gilt

$$G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)}) = \biguplus_{x \in V_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})} [x]_n.$$

Dabei haben die Konjugationsklassen die Länge

$$\#[x]_n = \begin{cases} q^{2(n-m)-g(n-m)-2} & \text{falls } m \text{ gerade} \\ (q+1)q^{n-m-1} & \text{falls } m \text{ ungerade} \end{cases}$$

für alle $x \in V_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$.

(iii) Für alle $a_0, a_2, \ldots, a_{g(n)} \in \mathbb{F}_q$ *mit* $a_0 \neq 0$ *gilt*

$$G_n^{(n)}(a_0, a_2, \ldots, a_{g(n)}) = \biguplus_{x \in V_n^{(n)}(a_0, a_2, \ldots, a_{g(n)})} [x]_n.$$

Dabei ist $\#[x]_n = 1$ *für alle* $x \in V_n^{(n)}(a_0, a_2, \ldots, a_{g(n)})$.

Beweis: (i) Die Aussage entspricht exakt der Aussage von Satz 3.2.6.

(ii) Für $n = 1$ ist die Aussage leer. Sei also $n \neq 1$ und $m \in \{1, \ldots, n-1\}$. Falls m gerade ist ergibt sich die Aussage unmittelbar aus Teil(i) und Korollar 3.1.10(i). Falls m ungerade ist, gilt

$$G_{n-m+1}^{(1)}(a_0) = \biguplus_{x \in a_0 + V'_{n-m+1}\tau} [x]_n$$

nach Satz 3.3.6. Dabei ist nach Korollar 3.3.2 $\#[x]_n = (q+1)q^{n-m-1}$ für alle $x \in a_0 + V'_{n-m+1}\tau$. Mit Korollar 3.1.10(ii) erhält man nun die gewünschte Aussage.

(iii) Nach Bemerkung 3.1.6 ist $G_n^{(n)}(a_0, a_2, \ldots, a_{g(n)}) = \{(\sum_{i=0}^{g(n)}{}'' a_i \tau^i) U_n\} \subset G_n^{(n)}$ Teilmenge des Zentrums von G_n. Damit folgt auch die Aussage von Teil (iii). □

Damit läßt sich nun zusammenfassend die Länge der Konjugationsklassen wie folgt beschreiben.

Korollar 3.4.3 *Sei* $n \in \mathbb{N}$ *und* $m \in \{1, \ldots, n\}$. *Dann hat jede Konjugationsklasse* $[x]_n$ *von* G_n, *die in* $G_n^{(m)}$ *liegt, die Länge*

$$\#[x]_n = \begin{cases} q^{2(n-m)-g(n-m)-2} & \text{falls } m \text{ ungerade und } m \neq n \\ (q+1)q^{n-m-1} & \text{falls } m \text{ gerade und } m \neq n \\ 1 & \text{falls } m = n. \end{cases}$$

Beweis: Für den Fall $m = 0$ folgt die Aussage aus Teil (i) von Satz 3.4.2. Sei nun $m \neq 0$. Wegen

$$G_n^{(m)} = \biguplus_{\substack{a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q \\ a_0 \neq 0}} G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$$

nach Bemerkung 3.1.6 muß es Elemente $a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q$ mit $a_0 \neq 0$ geben, so daß $[x]_n \subset G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$ gilt. Damit folgt nun die Aussage aus Satz 3.4.2(ii), falls $m \neq n$ ist, und aus Satz 3.4.2(iii), falls $m = n$ ist. □

Als eine einfache Folgerung läßt sich nun das Zentrum von G_n bestimmen.

Korollar 3.4.4 (Zentrum von G_n) *Sei* $n \in \mathbb{N}$. *Dann gilt für das Zentrum von* G_n *die Relation*

$$Z(G_n) = \begin{cases} G_n^{(n)} & \text{falls } n \text{ ungerade} \\ G_n^{(n-1)} \cup G_n^{(n)} & \text{falls } n \text{ gerade.} \end{cases}$$

Beweis: Nach Korollar 3.4.3 gilt für alle $m \in \{0, \ldots, n\}$, daß die Konjugationsklassen von $G_n^{(m)}$ alle die gleiche Länge haben. Daraus folgt, daß entweder $G_n^{(m)} \subset Z(G_n)$ ist, falls alle Konjugationsklassen von $G_n^{(m)}$ die Länge 1 haben, oder $G_n^{(m)} \cap Z(G_n) = \emptyset$. Nach Korollar 3.4.3 gilt $G_n^{(m)} \subset Z(G_n)$ genau dann, wenn

$$1 = \begin{cases} q^{2(n-m)-g(n-m)-2} & \text{falls } m \text{ ungerade und } m \neq n \\ (q+1)q^{n-m-1} & \text{falls } m \text{ gerade und } m \neq n \\ 1 & \text{falls } m = n \end{cases}$$

ist. Das ist im Fall n gerade äquivalent zu $m = n$ und im Fall n ungerade zu $m = n$ oder $m = n-1$. Damit folgt die Aussage des Korollares. □

Korollar 3.4.5 (Konjugationsklassen von G_n) *Sei $n \in \mathbb{N}$. Man setze*

$$V_n^{(m)} := \bigcup_{\substack{a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q \\ a_0 \neq 0}} V_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})$$

für alle $m \in \{1, \ldots, n\}$ und $V_n^* := \bigcup_{m=0}^{n} V_n^{(m)}$. Dann gilt

$$G_n = \biguplus_{x \in V_n^*} [x]_n.$$

Beweis: Nach Bemerkung 3.1.6 und Satz 3.4.2 gilt

$$\begin{aligned} G_n &= G_n^{(0)} \uplus \biguplus_{m=1}^{n} \left(\biguplus_{\substack{a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q \\ a_0 \neq 0}} G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)}) \right) \\ &= G_n^{(0)} \uplus \biguplus_{m=1}^{n} \left(\biguplus_{\substack{a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q \\ a_0 \neq 0}} \left(\biguplus_{x \in V_n^{(m)}(a_0, a_2, \ldots, a_{g(m)})} [x]_n \right) \right) \\ &= G_n^{(0)} \uplus \biguplus_{m=1}^{n} \left(\biguplus_{x \in V_n^{(m)}} [x]_n \right) \\ &= \biguplus_{m=0}^{n} \left(\biguplus_{x \in V_n^{(m)}} [x]_n \right) \\ &= \biguplus_{x \in V_n^*} [x]_n. \end{aligned}$$

□

Korollar 3.4.6 *Sei $n \in \mathbb{N}$ und s_n die Klassenzahl von G_n. Dann gilt*

$$s_n = (q-1) \begin{cases} 2q^{n-1} + q^{n-2} - q^{\frac{1}{2}n-1} & \textit{falls } n \textit{ gerade} \\ q^n + 2q^{n-1} - q^{\frac{1}{2}n-\frac{1}{2}} & \textit{falls } n \textit{ ungerade.} \end{cases}$$

Beweis: Da die Vereinigung

$$G_n = G_n^{(0)} \uplus \biguplus_{m=1}^{n} \left(\biguplus_{\substack{a_0, a_2, \ldots, a_{g(m)} \in \mathbb{F}_q \\ a_0 \neq 0}} G_n^{(m)}(a_0, a_2, \ldots, a_{g(m)}) \right)$$

disjunkt ist, muß auch die Vereinigung

$$V_n^* = V_n^{(0)} \uplus \biguplus_{m=1}^{n} \left(\biguplus_{\substack{a_0,a_2,\ldots,a_{g(m)}\in\mathbb{F}_q \\ a_0\neq 0}} V_n^{(m)}(a_0,a_2,\ldots,a_{g(m)}) \right)$$

disjunkt sein (vgl. dazu den Beweis von Korollar 3.4.5). Daraus folgt nun

$$s_n = \#V_n^* = \#V_n^{(0)} + \sum_{m=1}^{n} \left(\sum_{\substack{a_0,a_2,\ldots,a_{g(m)}\in\mathbb{F}_q \\ a_0\neq 0}} \#V_n^m(a_0,a_2,\ldots,a_{g(m)}) \right).$$

Dabei gilt $\#V_n^{(0)} = (q^2-q)(q^2)^{\#\{2,4,\ldots,g(n)\}} = (q^2-q)q^{g(n)}$. Sei nun $m \in \{1,\ldots,n\}$ und $a_0,a_2,\ldots,a_{g(m)} \in \mathbb{F}_q$ mit $a_0 \neq 0$ beliebig. Falls m gerade und $n \neq m$ ist, gilt

$$\#V_n^{(m)}(a_0,a_2,\ldots,a_{g(m)}) = \#V_{n-m}^{(0)} = (q^2-q)q^{g(n-m)}.$$

Falls m ungerade und $n \neq m$ ist, gilt

$$\#V_n^{(m)}(a_0,a_2,\ldots,a_{g(m)}) = \#V'_{n-m+1} = (q-1)q^{\#\{2,3,\ldots,n-m\}} = (q-1)q^{n-m-1}.$$

Falls $n = m$ ist, gilt $\#V_n^{(m)}(a_0,a_2,\ldots,a_{g(m)}) = 1$. Weil es nun für jedes $m \in \{1,\ldots,n\}$ genau $(q-1)q^{\#\{2,4,\ldots,g(m)\}} = (q-1)q^{\frac{1}{2}g(m)}$ verschiedene Tupel $(a_0,a_2,\ldots,a_{g(m)})$ mit $a_0,a_2,\ldots,a_{g(m)} \in \mathbb{F}_q$ und $a_0 \neq 0$ gibt, erhält man

$$s_n = (q^2-q)q^{g(n)} + {\sum_{m=1}^{u(n)}}'(q-1)q^{\frac{1}{2}g(m)}(q-1)q^{n-m-1} + {\sum_{m=2}^{g(n)}}''(q-1)q^{\frac{1}{2}g(m)}(q^2-q)q^{g(n-m)} + (q-1)q^{\frac{1}{2}g(n)}.$$

Daraus folgt $s_1 = (q^2-q)+q-1 = (q-1)(q+1)$ sowie $s_2 = (q^2-q)+(q-1)(q-1)+q-1 = (q-1)2q$. Damit verifiziert man leicht die Aussage des Korollares für den Fall $n \leq 2$. Sei nun $n > 2$. Dann ist

$$s_n = (q^2-q)q^{g(n)} + (q-1)^2 q^{n-1} {\sum_{m=1}^{u(n)}}' q^{\frac{1}{2}g(m)-m} + (q-1)^2 q {\sum_{m=2}^{g(n)}}'' q^{\frac{1}{2}g(m)+g(n-m)} + (q-1)q^{\frac{1}{2}g(n)}.$$

Dabei gilt nun

$$\begin{aligned}
(q-1){\sum_{m=1}^{u(n)}}' q^{\frac{1}{2}g(m)-m} &= {\sum_{m=1}^{u(n)}}' q^{\frac{1}{2}g(m-2)-(m-2)} - {\sum_{m=1}^{u(n)}}' q^{\frac{1}{2}g(m)-m} \\
&= {\sum_{m=-1}^{u(n)-2}}' q^{\frac{1}{2}g(m)-m} - {\sum_{m=1}^{u(n)}}' q^{\frac{1}{2}g(m)-m} \\
&= q^{\frac{1}{2}g(-1)+1} - q^{\frac{1}{2}g(u(n))-\frac{1}{2}u(n)} \\
&= 1 - q^{-\frac{1}{2}u(n)-\frac{1}{2}}
\end{aligned}$$

sowie

$$\begin{aligned}
(q-1){\sum_{m=2}^{g(n)}}'' q^{\frac{1}{2}g(m)+g(n-m)} &= {\sum_{m=2}^{g(n)}}'' q^{\frac{1}{2}g(m-2)+g(n-(m-2))} - {\sum_{m=2}^{g(n)}}'' q^{\frac{1}{2}g(m)+g(n-m)} \\
&= {\sum_{m=0}^{g(n)-2}}'' q^{\frac{1}{2}g(m)+g(n-m)} - {\sum_{m=2}^{g(n)}}'' q^{\frac{1}{2}g(m)+g(n-m)} \\
&= q^{\frac{1}{2}g(0)+g(n)} - q^{\frac{1}{2}g(g(n))+g(n-g(n))} \\
&= q^{g(n)-1} - q^{\frac{1}{2}g(n)-1}.
\end{aligned}$$

Damit erhält man schließlich

$$
\begin{aligned}
s_n &= (q^2-q)q^{g(n)} + (q-1)q^{n-1}(1-q^{-\frac{1}{2}u(n)-\frac{1}{2}}) + (q-1)(q^{g(n)} - q^{\frac{1}{2}g(n)}) + (q-1)q^{\frac{1}{2}g(n)} \\
&= (q-1)(q^{g(n)+1} + q^{n-1} - q^{n-\frac{1}{2}u(n)-\frac{3}{2}} + q^{g(n)} - q^{\frac{1}{2}g(n)} + q^{\frac{1}{2}g(n)}) \\
&= (q-1)(q^{g(n)+1} + q^{n-1} - q^{n-\frac{1}{2}u(n)-\frac{3}{2}} + q^{g(n)}) \\
&= (q-1)\begin{cases} 2q^{n-1} + q^{n-2} - q^{\frac{1}{2}n-1} & \text{falls } n \text{ gerade} \\ q^n + 2q^{n-1} - q^{\frac{1}{2}n-\frac{1}{2}} & \text{falls } n \text{ ungerade.} \end{cases}
\end{aligned}
$$

□

Kapitel 4

Allgemeine Kommutatorrelationen auf U

Ziel dieses Kapitels ist die Charakterisierung der Kommutatorgruppen $[U_i, U_j]$ für alle $i, j \in \mathbb{N}_0$.

4.1 Grundlegendes über Elemente der Form $xyx^{-1}y^{-1}$

In diesem Abschnitt wird die Frage behandelt, wie der Kommutator $xyx^{-1}y^{-1}$ von 2 Elementen $x, y \in U$ reagiert, wenn x bzw. y „geringfügig" abgeändert werden. Dabei ist das folgende Lemma grundlegend für fast alle späteren Rechnungen.

Lemma 4.1.1 *Seien $x, y \in U$ und $n, m \in \mathbb{N}$.*

(i) Falls es Elemente $a_0 \in \mathbb{F}_{q^2}^*$ und $b_m \in \mathbb{F}_{q^2}$ gibt, so daß die Kongruenzbedingungen

$$x \equiv a_0 \mod U_1 \text{ und } y \equiv 1 + b_m\tau^m \mod U_{m+1}$$

erfüllt sind, gelten die Kongruenzen

$$\begin{aligned} xy &\equiv (1 + b_m(a_0^{1-q^m} - 1)\tau^m)yx \mod U_{m+1} \\ &\equiv yx(1 + b_m(1 - a_0^{q^m-1})\tau^m) \mod U_{m+1}. \end{aligned}$$

sowie

$$\begin{aligned} yx &\equiv (1 + b_m(1 - a_0^{1-q^m})\tau^m)xy \mod U_{m+1} \\ &\equiv xy(1 + b_m(a_0^{q^m-1} - 1)\tau^m) \mod U_{m+1}. \end{aligned}$$

(ii) Falls es Elemente $a_n, b_m \in \mathbb{F}_{q^2}$ gibt, so daß die Kongruenzbedingungen

$$x \equiv 1 + a_n\tau^n \mod U_{n+1} \text{ und } y \equiv 1 + b_m\tau^m \mod U_{m+1}$$

erfüllt sind, gilt

$$\begin{aligned} xy &\equiv yx(1 + (a_n b_m^{q^n} - b_m a_n^{q^m})\tau^{n+m} \mod U_{n+m+1} \\ &\equiv (1 + (a_n b_m^{q^n} - b_m a_n^{q^m})\tau^{n+m}yx \mod U_{n+m+1}. \end{aligned}$$

Beweis: (i) Die Elemente x und y lassen sich in der Form $x = \sum_{i=0}^{\infty} a_i \tau^i$ und $y = 1 + \sum_{i=m}^{\infty} b_i \tau^i$ schreiben. Damit erhält man

$$\begin{aligned} xy &\equiv \left(\sum_{i=0}^{m} a_i \tau^i\right)(1 + b_m \tau^m) \mod U_{m+1} \\ &\equiv \sum_{i=0}^{m} a_i \tau^i + a_0 b_m \tau^m \mod U_{m+1} \\ &\equiv (1 + b_m a_0^{1-q^m} \tau^m) \left(\sum_{i=0}^{m} a_i \tau^i\right) \mod U_{m+1} \\ &\equiv (1 + b_m (a_0^{1-q^m} - 1)\tau^m)(1 + b_m \tau^m) \left(\sum_{i=0}^{m} a_i \tau^i\right) \mod U_{m+1} \\ &\equiv (1 + b_m (a_0^{1-q^m} - 1)\tau^m) yx \mod U_{m+1} \end{aligned}$$

sowie

$$\begin{aligned} xy &\equiv \sum_{i=0}^{m} a_i \tau^i + a_0 b_m \tau^m \mod U_{m+1} \\ &\equiv \left(\sum_{i=0}^{m} a_i \tau^i + b_m a_0^{q^m} \tau^m\right) \left(1 + b_m (1 - a_0^{q^m - 1})\tau^m\right) \mod U_{m+1} \\ &\equiv (1 + b_m \tau^m) \left(\sum_{i=0}^{m} a_i \tau^i\right) \left(1 + b_m (1 - a_0^{q^m - 1})\tau^m\right) \mod U_{m+1} \\ &\equiv yx \left(1 + b_m (1 - a_0^{q^m - 1})\tau^m\right) \mod U_{m+1}. \end{aligned}$$

Wegen

$$(1 + b_m (a_0^{1-q^m} - 1)\tau^m)^{-1} \equiv 1 + b_m (1 - a_0^{1-q^m})\tau^m \mod U_{m+1}$$

und

$$((1 + b_m (1 - a_0^{q^m - 1})\tau^m)^{-1} \equiv 1 + b_m (a_0^{q^m - 1} - 1)\tau^m \mod U_{m+1}$$

folgt außerdem die Kongruenz

$$\begin{aligned} yx &\equiv (1 + b_m (1 - a_0^{1-q^m})\tau^m) xy \mod U_{m+1} \\ &\equiv xy (1 + b_m (a_0^{q^m - 1} - 1)\tau^m) \mod U_{m+1}. \end{aligned}$$

(ii) Die Elemente x und y lassen sich in der Form $x = 1 + \sum_{i=n}^{\infty} a_i \tau^i$ und $y = 1 + \sum_{i=m}^{\infty} b_i \tau^i$ schreiben. Damit erhält man

$$\begin{aligned} xy &\equiv \left(1 + \sum_{i=n}^{n+m} a_i \tau^i\right) \left(1 + \sum_{i=m}^{n+m} b_i \tau^i\right) \mod U_{n+m+1} \\ &\equiv 1 + \sum_{i=n}^{n+m} a_i \tau^i + \sum_{i=m}^{n+m} b_i \tau^i + a_n b_m^{q^n} \tau^{n+m} \mod U_{n+m+1} \\ &\equiv \left(1 + \sum_{i=n}^{n+m} a_i \tau^i + \sum_{i=m}^{n+m} b_i \tau^i + b_m a_n^{q^m} \tau^{n+m}\right) \left(1 + (a_n b_m^{q^n} - b_m a_n^{q^m})\tau^{n+m}\right) \mod U_{n+m+1} \\ &\equiv \left(1 + \sum_{i=n}^{n+m} a_i \tau^i\right) \left(1 + \sum_{i=m}^{n+m} b_i \tau^i\right) \left(1 + (a_n b_m^{q^n} - b_m a_n^{q^m})\tau^{n+m}\right) \mod U_{n+m+1} \\ &\equiv yx \left(1 + (a_n b_m^{q^n} - b_m a_n^{q^m})\tau^{n+m}\right) \mod U_{n+m+1}. \end{aligned}$$

Wegen $yx \equiv 1 \mod U_1$ folgt nach Teil(i) die Kongruenz

$$xy \equiv \left(1 + (a_n b_m^{q^n} - b_m a_n^{q^m})\tau^{n+m}\right) yx \mod U_{n+m+1}.$$

□

Seien $x, y, z \in U$ mit $z \equiv xyx^{-1}y^{-1} \mod U_n$. Dann gibt es ein $c \in \mathbb{F}_{q^2}$ mit $z \equiv xyx^{-1}y^{-1}(1 + c\tau^n) \mod U_{n+1}$. Die nächsten 3 Lemmata befassen sich nun mit der Frage, welche Bedingungen man an c stellen muß, damit man Elemente $\tilde{x}, \tilde{y} \in U$ finden kann, so daß $z \equiv \tilde{x}\tilde{y}\tilde{x}^{-1}\tilde{y}^{-1} \mod U_{n+1}$ gilt. Dieses Problem spielt bei der Charakterisierung der Kommutatorgruppe $[U, U]$ eine große Rolle.

Lemma 4.1.2 *Seien $n, m \in \mathbb{N}$ mit m* ungerade. *Man wähle die Elemente $x, y \in U$ sowie $a_0 \in \mathbb{F}_{q^2} - \mathbb{F}_q$ und $b_m \in \mathbb{F}_{q^2}^*$ so daß die Bedingungen $x \equiv a_0 \mod U_1$ und $y \equiv 1 + b_m\tau^m \mod U_{m+1}$ gelten.*

(i) Sei n gerade *und $c \in \mathbb{F}_{q^2}$. Dann gibt es ein $b \in \mathbb{F}_{q^2}$, so daß für alle $\tilde{y} \in U$ mit $\tilde{y} \equiv y(1 + b\tau^{n+m}) \mod U_{m+n+1}$ die Kongruenz*

$$x\tilde{y}x^{-1}\tilde{y}^{-1} \equiv xyx^{-1}y^{-1}(1 + c\tau^{n+m}) \mod U_{m+n+1}$$

gilt.

(ii) Sei n ungerade *und $c \in (\alpha - \alpha^q)\mathbb{F}_q$. Dann gibt es ein $a \in \mathbb{F}_{q^2}$, so daß für alle $\tilde{x} \in U$ mit $\tilde{x} \equiv x(1 + a\tau^n) \mod U_{n+1}$ die Kongruenz*

$$\tilde{x}y\tilde{x}^{-1}y^{-1} \equiv xyx^{-1}y^{-1}(1 + c\tau^{n+m}) \mod U_{m+n+1}$$

gilt.

Beweis: (i) Wegen $a_0 \notin \mathbb{F}_q$ gilt $a_0^{1-q} \neq 1$. Man setze $b := \frac{c}{a_0^{1-q}-1}$. Sei nun $\tilde{y} \in U$ mit $\tilde{y} \equiv y(1 + b\tau^{n+m}) \mod U_{m+n+1}$. Für $y' := y^{-1}\tilde{y}$ gilt dann $y' \equiv 1 + b\tau^{n+m} \mod U_{m+n+1}$. Weil außerdem $x^{-1} \equiv a_0^{-1} \mod U_1$ gilt, folgt nach Lemma 4.1.1 die Kongruenz

$$\begin{aligned}
x\tilde{y}x^{-1}\tilde{y}^{-1} &= xyy'x^{-1}\tilde{y}^{-1} \\
&\equiv xyx^{-1}y'(1 + b((a_0^{-1})^{q^{n+m}-1} - 1)\tau^{n+m})\tilde{y}^{-1} \mod U_{m+n+1} \\
&\equiv xyx^{-1}y'\tilde{y}^{-1}(1 + b(a_0^{1-q} - 1)\tau^{n+m}) \mod U_{m+n+1} \\
&= xyx^{-1}y^{-1}(1 + c\tau^{n+m}).
\end{aligned}$$

(ii) Weil auch $-c$ in $(\alpha - \alpha^q)\mathbb{F}_q$ liegt, folgt nach Korollar 1.1.5, daß es ein $a \in \mathbb{F}_{q^2}$ gibt mit $b_m a^q - b_m^q a = -c$. Daraus folgt $ab_m^{q^n} - b_m a^{q^m} = c$. Sei nun $\tilde{x} \in U$ mit $\tilde{x} \equiv x(1 + a\tau^n) \mod U_{n+1}$. Für $x' := x^{-1}\tilde{x}$ gilt dann $x' \equiv 1 + a\tau^n \mod U_{n+1}$. Weil außerdem $\tilde{x}^{-1}y^{-1} \equiv a_0^{-1} \mod U_1$ gilt, folgt nach Lemma 4.1.1 die Kongruenz

$$\begin{aligned}
\tilde{x}y\tilde{x}^{-1}y^{-1} &= xx'y\tilde{x}^{-1}y^{-1} \\
&\equiv xyx'(1 + (ab_m^{q^n} - b_m a^{q^m})\tau^{n+m})\tilde{x}^{-1}y^{-1} \mod U_{m+n+1} \\
&= xyx'(1 + c\tau^{n+m})\tilde{x}^{-1}y^{-1} \\
&\equiv xyx'\tilde{x}^{-1}y^{-1}(1 + c\tau^{n+m})(1 + c((a_0^{-1})^{q^{m+n}-1} - 1)\tau^{n+m}) \mod U_{m+n+1} \\
&= xyx^{-1}y^{-1}(1 + c\tau^{n+m}).
\end{aligned}$$

□

Lemma 4.1.3 *Seien $i, j, n, m \in \mathbb{N}$ mit i* gerade, *j* ungerade *und $i + j = m$. Man wähle die Elemente $x, y \in U$ sowie $a_i \in \mathbb{F}_{q^2} - \mathbb{F}_q$ und $b_j \in \mathbb{F}_q^*$, so daß die Bedingungen $x \equiv 1 + a_i\tau^i \mod U_{i+1}$ und $y \equiv 1 + b_j\tau^j \mod U_{j+1}$ gelten.*

(i) Sei n gerade *und $c \in \mathbb{F}_{q^2}$. Dann gibt es ein $b \in \mathbb{F}_{q^2}$, so daß für alle $\tilde{y} \in U$ mit $\tilde{y} \equiv y(1 + b\tau^{j+n}) \mod U_{j+n+1}$ die Kongruenz*

$$x\tilde{y}x^{-1}\tilde{y}^{-1} \equiv xyx^{-1}y^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1}$$

gilt.

(ii) Sei n ungerade *und $c \in (\alpha - \alpha^q)\mathbb{F}_q$. Dann gibt es ein $a \in \mathbb{F}_{q^2}$, so daß für alle $\tilde{x} \in U$ mit $\tilde{x} \equiv x(1 + a\tau^{i+n}) \mod U_{i+n+1}$ die Kongruenz*

$$\tilde{x}y\tilde{x}^{-1}y^{-1} \equiv xyx^{-1}y^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1}$$

gilt.

Beweis: (i) Wegen $a_i \notin \mathbb{F}_q$ gilt $a_i \neq a_i^q$. Man setze $b := \frac{c}{a_i - a_i^q}$. Sei nun $\tilde{y} \in U$ mit $\tilde{y} \equiv y(1 + b\tau^{j+n}) \mod U_{j+n+1}$. Für $y' := y^{-1}\tilde{y}$ gilt dann $y' \equiv (1 + b\tau^{j+n}) \mod U_{j+n+1}$. Weil außerdem $x^{-1} \equiv 1 - a_i\tau^i \mod U_{i+1}$, und $y^{-1} \equiv 1 \mod U_1$ gilt, folgt nach Lemma 4.1.1 die Kongruenz

$$\begin{aligned}
x\tilde{y}x^{-1}\tilde{y}^{-1} &= xyy'x^{-1}\tilde{y}^{-1} \\
&\equiv xyx^{-1}y'(1 + b((-a_i)^{q^{j+n}} - (-a_i)b^{q^i})\tau^{n+m})\tilde{y}^{-1} \mod U_{n+m+1} \\
&\equiv xyx^{-1}y'\tilde{y}^{-1}(1 + b(a_i - a_i^q)\tau^{n+m}) \mod U_{n+m+1} \\
&= xyx^{-1}y^{-1}(1 + c\tau^{n+m}).
\end{aligned}$$

(ii) Weil auch $-c$ in $(\alpha - \alpha^q)\mathbb{F}_q$ liegt, folgt nach Korollar 1.1.5, daß es ein $a \in \mathbb{F}_{q^2}$ gibt mit $b_j a^q - b_j^q a = -c$. Daraus folgt $ab_j^{q^{i+n}} - b_j a^{q^j} = c$. Sei nun $\tilde{x} \in U$ mit $\tilde{x} \equiv x(1 + a\tau^{i+n}) \mod U_{n+i+1}$. Für $x' := x^{-1}\tilde{x}$ gilt dann $\tilde{x} \equiv 1 + a\tau^{i+n} \mod U_{n+i+1}$. Weil außerdem $\tilde{x}^{-1}y^{-1} \equiv 1 \mod U_1$ gilt, folgt nach Lemma 4.1.1 die Kongruenz

$$\begin{aligned}
\tilde{x}y\tilde{x}^{-1}y^{-1} &= xx'y\tilde{x}^{-1}y^{-1} \\
&\equiv xyx'(1 + (ab_j^{q^{i+n}} - b_j a^{q^j})\tau^{n+m})\tilde{x}^{-1}y^{-1} \mod U_{n+m+1} \\
&\equiv xyx'\tilde{x}^{-1}y^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1} \\
&= xyx^{-1}y^{-1}(1 + c\tau^{n+m}).
\end{aligned}$$

□

Lemma 4.1.4 *Seien $i, j, n, m \in \mathbb{N}$ mit i* und j ungerade *sowie $i + j = m$. Man wähle die Elemente $x, y \in U$ sowie $a_i, b_j \in \mathbb{F}_{q^2}^*$, so daß die Bedingungen $x \equiv 1 + a_i\tau^i \mod U_{i+1}$ und $x \equiv 1 + b_j\tau^j \mod U_{j+1}$ gelten.*

(i) Sei n gerade *und $c \in (\alpha - \alpha^q)\mathbb{F}_q$. Dann gibt es ein $b \in \mathbb{F}_{q^2}$, so daß für alle $\tilde{y} \in U$ mit $\tilde{y} \equiv y(1 + b\tau^{j+n}) \mod U_{j+n+1}$ die Kongruenz*

$$x\tilde{y}x^{-1}\tilde{y}^{-1} \equiv xyx^{-1}y^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1}$$

gilt.

(ii) Sei n ungerade *sowie $c \in \mathbb{F}_{q^2}$ und außerdem $\{a_i, b_j\}$ eine $\mathbb{F}_q$-Basis von $\mathbb{F}_{q^2}$. Dann gibt es Elemente $a, b \in \mathbb{F}_{q^2}$, so daß für $\tilde{x} := x(1 + a\tau^{i+n})$ und $\tilde{y} := y(1 + b\tau^{j+n})$ die Kongruenz*

$$\tilde{x}\tilde{y}\tilde{x}^{-1}\tilde{y}^{-1} \equiv xyx^{-1}y^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1}$$

gilt.

(iii) Sei n ungerade *und q* ungerade *sowie $c \in \mathbb{F}_{q^2}$ und außerdem $\{a_i, b_j\}$ eine $\mathbb{F}_q$-Basis von $\mathbb{F}_{q^2}$. Dann gibt es Elemente $a, b \in (\alpha - \alpha^q)\mathbb{F}_q$, so daß für alle $\tilde{x}, \tilde{y} \in U$ mit $\tilde{x} \equiv x(1 + a\tau^{i+n}) \mod U_{i+n+1}$ und $\tilde{y} \equiv y(1 + b\tau^{j+n}) \mod U_{j+n+1}$ die Kongruenz*

$$\tilde{x}\tilde{y}\tilde{x}^{-1}\tilde{y}^{-1} \equiv xyx^{-1}y^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1}$$

gilt.

Beweis: (i) Wegen $c \in (\alpha - \alpha^q)\mathbb{F}_q$ folgt nach Korollar 1.1.5, daß es ein $b \in \mathbb{F}_{q^2}$ gibt mit $a_i b^q - a_i^q b = c$. Daraus folgt $b(-a_i)^{q^{j+n}} - (-a_i)b^{q^i} = c$. Sei nun $\tilde{y} \in U$ mit $\tilde{y} \equiv y(1 + b\tau^{j+n}) \mod U_{j+n+1}$. Für $y' := y^{-1}\tilde{y}$ gilt dann $\tilde{y} \equiv 1 + b\tau^{j+n} \mod U_{j+n+1}$. Weil außerdem $x^{-1} \equiv 1 - a_i\tau^i \mod U_{i+1}$ und $\tilde{y}^{-1} \equiv 1 \mod U_1$ ist, folgt nach Lemma 4.1.1 die Kongruenz

$$\begin{aligned}
x\tilde{y}x^{-1}\tilde{y}^{-1} &= xyy'x^{-1}\tilde{y}^{-1} \\
&\equiv xyx^{-1}y'(1 + (b(-a_i)^{q^{j+n}} - (-a_i)b^{q^i})\tau^{n+m})\tilde{y}^{-1} \mod U_{n+m+1} \\
&\equiv xyx^{-1}y'\tilde{y}^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1} \\
&= xyx^{-1}y^{-1}(1 + c\tau^{n+m}).
\end{aligned}$$

(ii) Man wähle $\tilde{a}, \tilde{b} \in \mathbb{F}_q$, so daß $a_i\tilde{b}+b_j\tilde{a} = \frac{c}{\alpha-\alpha^q}$ ist, und setze $a := \tilde{a}\alpha$ und $b := -\tilde{b}\alpha$. Dann gilt $b_j(a-a^q)+a_i(b^q-b) = c$. Weiter setze man $x' := x^{-1}\tilde{x} = 1+a_i\tau^{i+n}$ und $y' := y^{-1}\tilde{y} = 1+b_j\tau^{j+n}$. Weil $x^{-1} \equiv 1-a_i\tau^i \mod U_{i+1}$ und ${x'}^{-1}x^{-1}y', \tilde{y}^{-1} \equiv 1 \mod U_1$ gilt, folgt nach Lemma 4.1.1 die Kongruenz

$$\begin{aligned}
\tilde{x}\tilde{y}\tilde{x}^{-1}\tilde{y}^{-1} &= xx'yy'{x'}^{-1}x^{-1}\tilde{y}^{-1} \\
&\equiv xyx'(1+(ab_j^{q^{i+n}} - b_j a^{q^j})\tau^{n+m}){x'}^{-1}x^{-1}y' \\
&\quad (1+(b(-a_i)^{q^{j+n}} - (-a_i)b^{q^i})\tau^{n+m})\tilde{y}^{-1} \mod U_{n+m+1} \\
&\equiv xyx'{x'}^{-1}y'\tilde{y}^{-1}(1+(b_j(a-a^q)+a_i(b-b^q))\tau^{n+m}) \mod U_{n+m+1} \\
&= xyx^{-1}y^{-1}(1+c\tau^{n+m})
\end{aligned}$$

(iii) Da q ungerade ist, gilt $2 \neq 0$. Man wähle $\tilde{a}, \tilde{b} \in \mathbb{F}_q$, so daß $a_i\tilde{b} + b_j\tilde{a} = \frac{c}{2(\alpha-\alpha^q)}$ ist, und setze $a := \tilde{a}(\alpha-\alpha^q) \in (\alpha-\alpha^q)\mathbb{F}_q$ und $b := -\tilde{b}(\alpha-\alpha^q) \in (\alpha-\alpha^q)\mathbb{F}_q$. Dann gilt $b_j(a-a^q) + a_i(b^q-b) = c$. Seien nun $\tilde{x}, \tilde{y} \in U$ mit $\tilde{x} \equiv x(1+a\tau^{i+n}) \mod U_{i+n+1}$ und $\tilde{y} \equiv y(1+b\tau^{j+n}) \mod U_{j+n+1}$. Für $x' := x^{-1}\tilde{x}$ und $y' := y^{-1}\tilde{y}$ gilt dann $x' \equiv 1+a\tau^{i+n} \mod U_{i+n+1}$ sowie $y' \equiv 1+b\tau^{j+n} \mod U_{j+n+1}$. Weil außerdem $x^{-1} \equiv 1-a_i\tau^i \mod U_{i+1}$ und ${x'}^{-1}x^{-1}y', \tilde{y}^{-1} \equiv 1 \mod U_1$ gilt, folgt nach Lemma 4.1.1 ähnlich wie in Teil (ii) die Kongruenz.

$$\tilde{x}\tilde{y}\tilde{x}^{-1}\tilde{y}^{-1} = xyx^{-1}y^{-1}(1+c\tau^{n+m}).$$

□

4.2 Grundlegendes über die Kommutatorrelation $[U, U]$

In diesem Abschnitt geht es darum, den Zusammenhang zwischen den beiden Faktorgruppen $([U,U]\cdot U_n)/U_n$ und $([U,U]\cdot U_{n+1})/U_{n+1}$ zu beschreiben. Dabei ist folgende Fragestellung von Interesse: Sei $x = \sum_{i=0}^{\infty} a_i\tau^i, y = \sum_{i=0}^{\infty} b_i\tau^i \in [U,U]$, so daß $a_i = b_i$ für alle $i = 0, \ldots, n-1$ gilt. Dann ist $x \equiv y(1+(a_n-b_n)\tau^n) \mod U_{n+1}$. Was kann man über $a_n - b_n$ sagen?

Lemma 4.2.1 *Es gilt $[U,U] \subset U_1$.*

Beweis: Wegen $G_1 \cong \mathbb{F}_{q^2}^*$ gilt $xyx^{-1}y^{-1} \equiv 1 \mod U_1$ für alle $x, y \in U$. Da U_1 einen Untergruppe von U ist, folgt $[U,U] \subset U_1$. □

Dieses Lemma bildet die Voraussetzung dafür, $[U,U]$ mit dem folgenden Formalismus zu charakterisieren.

Definition 4.2.2 *Sei $\mathfrak{U}$ eine Untergruppe von U_1 und $n \in \mathbb{N}$. Dann heißt*

$$F_n(\mathfrak{U}) := \{a \in \mathbb{F}_{q^2} \mid \textit{Es gibt ein } x \in \mathfrak{U} \textit{ mit } x \equiv 1+a\tau^n \mod U_{n+1}\}$$

die n-te Koeffizientenvariation von $\mathfrak{U}$.

Bemerkung 4.2.3 Seien $\mathfrak{U}, \mathfrak{V}$ Untergruppen von U_1 mit $\mathfrak{U} \subset \mathfrak{V}$. Dann folgt direkt aus Definition 4.2.1 die Teilmengenbeziehung $F_n(\mathfrak{U}) \subset F_n(\mathfrak{V})$ für alle $n \in \mathbb{N}$.

Lemma 4.2.4 *Sei $\mathfrak{U}$ eine Untergruppe von U_1 und $n \in \mathbb{N}$. Dann ist $F_n(\mathfrak{U})$ eine additive Untergruppe von $\mathbb{F}_{q^2}$.*

Beweis: Offensichtlich gilt $F_n(\mathfrak{U}) \subset \mathbb{F}_{q^2}$. Da $\mathbb{F}_{q^2}$ endlich ist, reicht es aus, die additive Abgeschlossenheit von $F_n(\mathfrak{U})$ zu zeigen. Seien dazu $a, b \in F_n(\mathfrak{U})$. Dann gibt es Elemente $x, y \in \mathfrak{U}$ mit $x \equiv 1+a\tau^n \mod U_{n+1}$ und $y \equiv 1+b\tau^n \mod U_{n+1}$. Daraus folgt $xy \equiv 1+(a+b)\tau^n \mod U_{n+1}$

und damit $a+b \in F_n(\mathfrak{U})$. $\square$

Sind nun $x = \sum_{i=0}^{\infty} a_i\tau^i, y = \sum_{i=0}^{\infty} b_i\tau^i \in [U,U]$ wie oben gewählt, dann gilt $a_n - b_n \in F_n([U,U])$. Damit kann man die eingangs gestellte Frage präzisieren: Wie lautet für ein beliebiges $n \in \mathbb{N}$ die n-te Koeffizientenvariation von $[U,U]$?

Lemma 4.2.5 *Sei $n \in \mathbb{N}$.*

(i) Falls n ungerade ist, gilt $F_n([U,U]) = \mathbb{F}_{q^2}$

(ii) Falls n gerade ist, gilt $F_n([U,U]) \supset (\alpha - \alpha^q)\mathbb{F}_q$.

Beweis: (i) Sei $c \in \mathbb{F}_{q^2}$ beliebig. Man wähle $a \in \mathbb{F}_{q^2} - \mathbb{F}_q$. Dann gilt $a^{1-q} - 1 \neq 0$. Weiter setze man $b := \frac{c}{a^{1-q}-1}$. Für $x := a$ und $y := 1 + b\tau^n$ gilt nach Lemma 4.1.1 die Kongruenz

$$xy \equiv (1 + b(a^{1-q^n} - 1)\tau^n)yx \mod U_{n+1}.$$

Daraus folgt

$$xyx^{-1}y^{-1} \equiv 1 + c\tau^n \mod U_{n+1}.$$

Also ist $c \in F_n([U,U])$. Damit ist $F_n([U,U]) = \mathbb{F}_{q^2}$ gezeigt.

(ii) Sei $c \in (\alpha - \alpha^q)\mathbb{F}_q$. Dann gibt es nach Satz 1.1.4 ein $a \in \mathbb{F}_{q^2}$ mit $a^q - a = c$. Für $x := 1 - a\tau^{n-1}$ und $y := 1 + \tau$ gilt nach Lemma 4.1.1 die Kongruenz

$$\begin{aligned} xy &\equiv (1 + (-a1^{q^{n-1}} - 1(-a)^q)\tau^n)yx \mod U_{n+1} \\ &\equiv (1 + (a^q - a)\tau^n)yx \mod U_{n+1}. \end{aligned}$$

Daraus folgt

$$xyx^{-1}y^{-1} \equiv 1 + c\tau^n \mod U_{n+1}.$$

Also ist $c \in F_n([U,U])$. Damit ist $F_n([U,U]) \supset (\alpha - \alpha^q)\mathbb{F}_q$ gezeigt. $\square$

Damit ist $F_n([U,U])$ für den Fall n ungerade bestimmt. Um nun im Fall n ungerade die Beziehung $F_n([U,U]) \subset (\alpha - \alpha^q)\mathbb{F}_q$ zeigen zu können, benötigt man eine Untergruppe von U_1, die $[U,U]$ enthält und von der man leicht zeigen kann, daß ihre n-te Koeffizientenvariation im Fall n ungerade eine Untergruppe von $(\alpha - \alpha^q)\mathbb{F}_q$ ist. Dazu führt man folgende Abkürzung ein.

Bezeichnung 4.2.6 *Für alle $n \in \mathbb{N}$ sei $E_n := \{z \in U_n \mid \mathrm{N}(x) = 1\}$.*

Bemerkung 4.2.7 Wegen $E_n = U_n \cap \mathrm{Kern}(\mathrm{N})$ (vgl. Lemma 1.2.3.6) folgt für alle $n \in \mathbb{N}$, daß E_n eine Untergruppe von U ist.

Lemma 4.2.8 *Der Kommutator $[U,U]$ ist eine Untergruppe von E_1.*

Beweis: Für alle $x, y \in U$ gilt nach Lemma 1.2.3.6 die Gleichung

$$\begin{aligned} \mathrm{N}(xyx^{-1}y^{-1}) &= \mathrm{N}(x)\mathrm{N}(y)\mathrm{N}(x^{-1})\mathrm{N}(y^{-1}) \\ &= \mathrm{N}(x)\mathrm{N}(y)(\mathrm{N}(x))^{-1}(\mathrm{N}(y))^{-1} \\ &= 1 \end{aligned}$$

Also liegen alle Elemente der Form $xyx^{-1}y^{-1}$ in E_1. Nach Bemerkung 4.2.7 folgt, daß $[U,U]$ eine Untergruppe von E_1 ist. $\square$

Satz 4.2.9 *Sei $n \in \mathbb{N}$ mit n gerade. Dann gilt $F_n(E_1) \subset (\alpha - \alpha^q)\mathbb{F}_q$.*

Beweis: Sei $a \in F_n(E_1)$ beliebig. Dann gibt es ein $x \in E_1$ mit $x \equiv 1 + a\tau^n \mod U_{n+1}$. Wegen $\mathrm{N}(x) = 1$ folgt nach Lemma 1.2.3.2 die Kongruenz

$$1 = x\overline{x} \equiv (1 + a\tau^n)(1 + a^q\tau^n) \mod U_{n+1} \equiv 1 + (a + a^q)\tau^n \mod U_{n+1}.$$

Also muß die Gleichung $0 = a + a^q$ erfüllt sein. Das ist nach Satz 1.1.3 genau dann der Fall, wenn $a \in (\alpha - \alpha^q)\mathbb{F}_q$ ist. Daraus folgt die Aussage des Satzes. □

Zusammen mit Lemma 4.2.5 und Bemerkung 4.2.3 ergibt sich nun das folgende Resultat.

Korollar 4.2.10 *Sei $n \in \mathbb{N}$. Dann gilt*

$$F_n([U, U]) = \begin{cases} \mathbb{F}_{q^2} & \textit{falls } n \textit{ ungerade} \\ (\alpha - \alpha^q)\mathbb{F}_q & \textit{falls } n \textit{ gerade.} \end{cases}$$

4.3 Charakterisierung der Kommutatorgruppen $[U_i, U_j]$ für alle $i, j \in \mathbb{N}_0$

Nachdem im vorigen Abschnitt mit Korollar 4.2.10 alle Koeffizientenvariationen von $[U, U]$ bestimmt wurden, werden in diesem Abschnitt explizite Gleichungen angegeben, denen die Koeffizienten eines Elementes $x = \sum_{i=0}^{\infty} a_i\tau^i \in U$ genügen müssen, damit $x \in [U, U]$ gilt. Darüberhinaus ergibt sich als Nebenprodukt auch eine vollständige Charakterisierung der Kommutatorgruppen $[U_i, U_j]$ für alle $i, j \in \mathbb{N}_0$. Alle wesentlichen Ergebnisse dieses Abschnitts sind schon in dem folgenden Satz enthalten.

Hauptsatz 4.3.1 *Sei $\mathfrak{U}$ eine Untergruppe von U_1 mit $\mathfrak{U} \supset [U, U]$ und $F_n(\mathfrak{U}) \subset (\alpha - \alpha^q)\mathbb{F}_q$ für alle geraden $n \in \mathbb{N}$. Seien weiter $i, j \in \mathbb{N}_0$, wobei j ungerade sei. Man setze $m_0 := i + j$. Dann gibt es für alle $z \in U_{m_0} \cap \mathfrak{U}$ ein $x \in U_i$ und ein $y \in U_j$ mit $z = xyx^{-1}y^{-1}$.*

Beweis: Sei $z \in \mathfrak{U} \cap U_{m_0}$. Falls $z = 1$ ist, wird die Aussage trivial (man wähle $x = y = 1$). Sei also $z \neq 1$. Setze $m := \max\{k \in \mathbb{N} \mid z \equiv 1 \mod U_k\}$. Dann gibt es ein $c_m \in \mathbb{F}_{q^2}$ mit $c_m \neq 0$, so daß $z \equiv 1 + c_m\tau^m \mod U_{m+1}$ gilt. Man zeigt nun durch Induktion über n, daß es ein $i' \in \mathbb{N}_0$ gibt, so daß Folgen $\{x_n\}_{n\in\mathbb{N}} \subset U_{i'}$ und $\{y_n\}_{n\in\mathbb{N}} \subset U_j$ existieren, die für alle $n \in \mathbb{N}$ folgenden Bedingungen genügen:

(Bed 1) Falls $n \neq 1$ ist, gilt $x_n \equiv x_{n-1} \mod U_{i'+n-1}$ sowie $x_n \equiv x_{n-1} \mod U_{j+n-1}$.

(Bed 2) Es gilt $x_n y_n x_n^{-1} y_n^{-1} \equiv z \mod U_{n+m.}$

Aus **(Bed 1)** folgt, daß $\{x_n\}_{n\in\mathbb{N}} \subset U_{i'} \subset U_i$ und $\{y_n\}_{n\in\mathbb{N}} \subset U_j$ Cauchyfolgen und damit konvergent sind. Man setze nun $x := \lim_{n\to\infty} x_n$ und $y := \lim_{n\to\infty} y_n$. Wegen der topologischen Abgeschlossenheit von $U_{i'}$ und U_j nach Lemma 1.3.1.9 folgt $x \in U_{i'}$ und $y \in U_j$. Aus **(Bed 2)** folgt weiter, daß die Folge $\{x_n y_n x_n^{-1} y_n^{-1}\}_{n\in\mathbb{N}}$ gegen z konvergiert. Mit Satz 1.3.1.10 erhält man

$$z = \lim_{n\to\infty}(x_n y_n x_n^{-1} y_n^{-1}) = xyx^{-1}y^{-1}$$

und damit die Aussage von Satz 4.3.1.

Zur Existenz der Folgen $\{x_n\}_{n\in\mathbb{N}} \subset U_{i'}$ und $\{y_n\}_{n\in\mathbb{N}} \subset U_j$
<u>1. Fall $m = j$</u>: Es folgt, daß $i = 0$ und m ungerade ist. Man setze $i' := i = 0$.

Induktionsanfang n=1: Man setze $x_1 := a_0$ mit $a_0 \in \mathbb{F}_{q^2} - \mathbb{F}_q$ beliebig sowie $y_1 := 1 + b_j\tau^j$ mit $b_j := \frac{c_m}{a_0^{1-q}-1}$. Dann gilt $x_1 \in U_{i'}$ und $y_1 \in U_j$. Wegen $n = 1$ ist **(Bed 1)** trivialerweise erfüllt. Außerdem gilt nach Lemma 4.1.1 die Kongruenz

$$x_1 y_1 \equiv (1 + b_m(a_0^{1-q} - 1)\tau^m)y_1 x_1 \mod U_{m+1}.$$

Daraus folgt

$$\begin{aligned} x_1 y_1 x_1^{-1} y_1^{-1} &\equiv (1 + b_m(a_0^{1-q} - 1)\tau^m) \mod U_{m+1} \\ &\equiv 1 + c_m \tau^m \mod U_{m+1} \\ &\equiv z \mod U_{m+1}. \end{aligned}$$

Also ist auch **(Bed 2)** erfüllt.

Induktionsschritt $n \longmapsto n+1$: Nach Induktionsannahme gibt es ein $x_n \in U_{i'}$ und ein $y_n \in U_j$ mit $x_n y_n x_n^{-1} y_n^{-1} \equiv z \mod U_{n+m}$. Daraus folgt, daß es ein $c \in \mathbb{F}_{q^2}$ geben muß mit

$$z \equiv x_n y_n x_n^{-1} y_n^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1}.$$

Falls n gerade ist, gibt es nach Lemma 4.1.2(i) ein $b \in \mathbb{F}_{q^2}$, so daß für $x_{n+1} := x_n \in U_{i'}$ und $y_{n+1} := y_n(1 + b\tau^{n+m}) \in U_j$ die Kongruenz

$$\begin{aligned} x_{n+1} y_{n+1} x_{n+1}^{-1} y_{n+1}^{-1} &\equiv x_n y_n x_n^{-1} y_n^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1} \\ &\equiv z \mod U_{n+m+1} \end{aligned}$$

gilt. Damit sind die beiden Bedingungen **(Bed 1)** und **(Bed 2)** erfüllt.

Falls n ungerade ist, folgt wegen $z(x_n y_n x_n^{-1} y_n^{-1})^{-1} \in \mathfrak{U}$, daß c in $F_{n+m}(\mathfrak{U}) \subset (\alpha - \alpha^q)\mathbb{F}_q$ liegt. Nach Lemma 4.1.2(ii) gibt es nun ein $a \in \mathbb{F}_{q^2}$, so daß für $y_{n+1} := y_n \in U_j$ und $x_{n+1} := x_n(1 + a\tau^{n+i'}) \in U_{i'}$ die Kongruenz

$$\begin{aligned} x_{n+1} y_{n+1} x_{n+1}^{-1} y_{n+1}^{-1} &\equiv x_n y_n x_n^{-1} y_n^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1} \\ &\equiv z \mod U_{n+m+1} \end{aligned}$$

gilt. Damit sind die beiden Bedingungen **(Bed 1)** und **(Bed 2)** erfüllt.

2. Fall $m > j$ und m ungerade: Man setze $i' := m - j$. Dann ist i' gerade, und es gilt $i' + j = m$ sowie $i' \geq i$.

Induktionsanfang $n = 1$: Man setze $x_1 := 1 + a_{i'}\tau^{i'}$ mit $a_{i'} \in \mathbb{F}_{q^2} - \mathbb{F}_q$ beliebig und $y_1 := 1 + b_j \tau^j$ mit $b_j = \frac{c_m}{a_{i'} - a_{i'}^q}$. Dann gilt $x_1 \in U_{i'}$ und $y_1 \in U_j$. Wegen $n = 1$ ist **(Bed 1)** trivialerweise erfüllt. Außerdem gilt nach Lemma 4.1.1 die Kongruenz

$$\begin{aligned} x_1 y_1 &\equiv (1 + (a_{i'} b_j^{q^{i'}} - b_j a_{i'}^{q^j})\tau^m) y_1 x_1 \mod U_{m+1} \\ &\equiv (1 + b_j(a_{i'} - a_{i'}^q)\tau^m) y_1 x_1 \mod U_{m+1}. \end{aligned}$$

Daraus folgt

$$x_1 y_1 x_1^{-1} y_1^{-1} \equiv 1 + c_m \tau^m \mod U_{m+1} \equiv z \mod U_{m+1}.$$

Also ist auch **(Bed 2)** erfüllt.

Induktionsschritt $n \longmapsto n+1$: Nach Induktionsannahme gibt es ein $x_n \in U_{i'}$ und ein $y_n \in U_j$ mit $x_n y_n x_n^{-1} y_n^{-1} \equiv z \mod U_{n+m}$. Daraus folgt, daß es ein $c \in \mathbb{F}_{q^2}$ geben muß mit

$$z \equiv x_n y_n x_n^{-1} y_n^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1}.$$

Falls n gerade ist, gibt es nach Lemma 4.1.3(i) ein $b \in \mathbb{F}_{q^2}$, so daß für $x_{n+1} := x_n \in U_{i'}$ und $y_{n+1} := y_n(1 + b\tau^{n+j}) \in U_j$ die Kongruenz

$$\begin{aligned} x_{n+1} y_{n+1} x_{n+1}^{-1} y_{n+1}^{-1} &\equiv x_n y_n x_n^{-1} y_n^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1} \\ &\equiv z \mod U_{n+m+1} \end{aligned}$$

gilt. Damit sind die beiden Bedingungen **(Bed 1)** und **(Bed 2)** erfüllt.

Falls n ungerade ist, folgt wegen $z(x_ny_nx_n^{-1}y_n^{-1})^{-1} \in \mathfrak{U}$, daß c in $F_{n+m}(\mathfrak{U}) \subset (\alpha-\alpha^q)\mathbb{F}_q$ liegt. Nach Lemma 4.1.3(ii) gibt es nun ein $a \in \mathbb{F}_q$, so daß für $y_{n+1} := y_n \in U_j$ und $x_{n+1} := x_n(1+a\tau^{n+i'}) \in U_{i'}$ die Kongruenz

$$\begin{aligned} x_{n+1}y_{n+1}x_{n+1}^{-1}y_{n+1}^{-1} &\equiv x_ny_nx_n^{-1}y_n^{-1}(1+c\tau^{n+m}) \mod U_{n+m+1} \\ &\equiv z \mod U_{n+m+1} \end{aligned}$$

gilt. Damit sind die beiden Bedingungen **(Bed 1)** und **(Bed 2)** erfüllt.

3.Fall m gerade: Man setze $i' := m-j$. Dann ist i' ungerade, und es gilt $i'+j=m$ sowie $i' \geq i$.

Induktionsanfang $n=1$: Da m gerade ist, muß $c_m \in (\alpha-\alpha^q)\mathbb{F}_q$ gelten. Nach Satz 1.1.4 folgt, daß es ein $b_j \in \mathbb{F}_{q^2}$ gibt mit $b_j^q - b_j = c_m$. Man setze nun $x_1 := 1+\tau^{i'}$ und $y_1 := 1+b_j\tau^j$. Dann gilt $x_1 \in U_{i'}$ und $y_1 \in U_j$. Wegen $n=1$ ist **(Bed 1)** trivialerweise erfüllt. Außerdem gilt nach Lemma 4.1.1 die Kongruenz

$$\begin{aligned} x_1y_1 &\equiv (1+(1b_j^{q^{i'}} - b_j1^{q^j})\tau^m)y_1x_1 \mod U_{m+1} \\ &\equiv (1+(b_j^q-b_j)\tau^m)y_1x_1 \mod U_{m+1}. \end{aligned}$$

Daraus folgt

$$x_1y_1x_1^{-1}y_1^{-1} \equiv 1+c_m\tau^m \mod U_{m+1} \equiv z \mod U_{m+1}.$$

Also ist auch **(Bed 2)** erfüllt.

Induktionsschritt $n \longmapsto n+1$: Nach Induktionsannahme gibt es ein $x_n \in U_{i'}$ und ein $y_n \in U_j$ mit $x_ny_nx_n^{-1}y_n^{-1} \equiv z \mod U_{n+m}$. Daraus folgt, daß es ein $c \in \mathbb{F}_{q^2}$ geben muß mit

$$z \equiv x_ny_nx_n^{-1}y_n^{-1}(1+c\tau^{n+m}) \mod U_{n+m+1}.$$

Falls n gerade ist, folgt wegen $z(x_ny_nx_n^{-1}y_n^{-1})^{-1} \in \mathfrak{U}$, daß c in $F_{n+m}(\mathfrak{U}) \subset (\alpha-\alpha^q)\mathbb{F}_q$ liegt. Nach Lemma 4.1.4(i) gibt es nun ein $a \in \mathbb{F}_q$, so daß für $x_{n+1} := x_n \in U_j$ und $y_{n+1} := y_n(1+a\tau^{n+i'}) \in U_{i'}$ die Kongruenz

$$\begin{aligned} x_{n+1}y_{n+1}x_{n+1}^{-1}y_{n+1}^{-1} &\equiv x_ny_nx_n^{-1}y_n^{-1}(1+c\tau^{n+m}) \mod U_{n+m+1} \\ &\equiv z \mod U_{n+m+1} \end{aligned}$$

gilt. Damit sind die beiden Bedingungen **(Bed 1)** und **(Bed 2)** erfüllt.

Sei nun n ungerade. Wegen $b_j^q - b_j = c_m \neq 0$ gilt $b_j \notin \mathbb{F}_q$. Also ist $\{1, b_j\}$ eine $\mathbb{F}_q$-Basis von $\mathbb{F}_{q^2}$. Nach Lemma 4.1.4(ii) folgt, daß es Elemente $a, b \in \mathbb{F}_{q^2}$ gibt, so daß für $x_{n+1} := x_n(1+a\tau^{i'+n}) \in U_{i'}$ und $y_{n+1} := y_n(1+b\tau^{j+n}) \in U_j$ die Kongruenz

$$\begin{aligned} x_{n+1}y_{n+1}x_{n+1}^{-1}y_{n+1}^{-1} &\equiv x_ny_nx_n^{-1}y_n^{-1}(1+c\tau^{n+m}) \mod U_{n+m+1} \\ &\equiv z \mod U_{n+m+1} \end{aligned}$$

gilt. Damit sind die beiden Bedingungen **(Bed 1)** und **(Bed 2)** erfüllt. □

Aus diesem Satz ergibt sich nun eine ganze Reihe von Folgerungen.

Korollar 4.3.2 *Seien $i, j \in \mathbb{N}_0$. Man setze*

$$m_0 := \begin{cases} i+j+1 & \textit{falls } i \textit{ und } j \textit{ gerade sind} \\ i+j & \textit{falls } i \textit{ oder } j \textit{ ungerade ist.} \end{cases}$$

Dann gilt $[U_i, U_j] = U_{m_0} \cap [U, U]$.

Beweis: Sei $z \in U_{m_0} \cap [U,U]$. Falls i oder j ungerade ist, kann man wegen $[U_i,U_j] = [U_j,U_i]$ ohne Einschränkung j ungerade annehmen. Wegen $m_0 = i+j$ folgt nach Satz 4.3.1, daß es ein $x \in U_i$ und ein $y \in U_j$ gibt mit $z = xyx^{-1}y^{-1}$. Falls i und j gerade sind, gilt $m_0 = i+j+1$, wobei $j+1$ ungerade ist. Nach Satz 4.3.1 gibt es nun ein $y \in U_{j+1} \subset U_j$ und ein $y \in U_i$ mit $z = xyx^{-1}y^{-1}$. Somit gilt $z \in [U_i,U_j]$ in beiden Fällen. Folglich gilt $[U_i,U_j] \supset U_{m_0} \cap [U,U]$. Weil $[U_i,U_j] \subset [U,U]$ ist, bleibt nur noch $[U_i,U_j] \subset U_{m_0}$ zu zeigen. Wegen $[U_i,U_j] = [U_j,U_i]$ kann man ohne Einschräkung $j \geq i$ annehmen. Falls $j = 0$ ist gilt $[U_i,U_j] = [U,U] \subset U_{m_0} = U_1$ nach Lemma 4.2.1. Sei nun $j \neq 0$. Man unterscheidet die folgenden Fälle.

1.Fall i=0: Seien $x \in U_i$ und $y \in U_j$ beliebig. Dann gibt es ein $a_0 \in \mathbb{F}_{q^2}^*$ und $b_j \in \mathbb{F}_{q^2}$ mit $x \equiv a_0 \mod U_1$ und $y \equiv 1 + b_j\tau^j \mod U_{j+1}$. Nach Lemma 4.1.1 gilt nun

$$\begin{aligned} xy &\equiv (1 + b_j(a_0^{1-q^j} - 1)\tau^j)yx \mod U_{j+1} \\ &\equiv \begin{cases} yx \mod U_j & \text{falls } j \text{ ungerade} \\ yx \mod U_{j+1} & \text{falls } j \text{ gerade} \end{cases} \\ &\equiv xy \mod U_{m_0}. \end{aligned}$$

Daraus ergibt sich $xyx^{-1}y^{-1} \in U_{m_0}$. Da U_{m_0} eine Untergruppe von U ist, folgt $[U_i,U_j] \subset U_{m_0}$.

2.Fall $i \neq 0$: Seien $x \in U_i$ und $y \in U_j$ beliebig. Dann gibt es Elemente $a_i, b_j \in \mathbb{F}_{q^2}$ mit $x \equiv 1 + a_i\tau^i \mod U_{i+1}$ und $y \equiv 1 + b_j\tau^j \mod U_{j+1}$ Nach Lemma 4.1.1 gilt nun

$$\begin{aligned} xy &\equiv (1 + (a_i b_j^{q^i} - b_j a_i^{q^j})\tau^{i+j})yx \mod U_{i+j+1} \\ &\equiv \begin{cases} yx \mod U_{i+j+1} & \text{falls } i \text{ und } j \text{ gerade} \\ yx \mod U_{i+j} & \text{falls } j \text{ oder } j \text{ ungerade} \end{cases} \\ &\equiv xy \mod U_{m_0}. \end{aligned}$$

Daraus ergibt sich $xyx^{-1}y^{-1} \in U_{m_0}$. Da U_{m_0} eine Untergruppe von U ist, folgt $[U_i,U_j] \subset U_{m_0}$. □

Mit diesem Korollar ist nun das Problem der Charakterisierung von $[U_i,U_j]$ auf das Problem der Charakterisierung von $[U,U]$ zurückgeführt worden.

Korollar 4.3.3 *Seien $i,j \in \mathbb{N}_0$. Dann gilt*

$$[U_i,U_j] = \{xyx^{-1}y^{-1} \mid x \in U_i \ \textit{und} \ y \in U_j\}.$$

Beweis: Da „$\supset$“ trivial ist, bleibt lediglich „$\subset$“ zu zeigen. Dazu setze man

$$m_0 := \begin{cases} i+j+1 & \text{falls } i \text{ und } j \text{ gerade} \\ i+j & \text{falls } i \text{ oder } j \text{ ungerade.} \end{cases}$$

Sei nun $z \in [U_i,U_j] = U_{m_0} \cap [U,U]$. Falls i und j gerade sind, gilt $m_0 = i+j+1$, wobei $j+1$ ungerade ist. Nach Satz 4.3.1 gibt es nun ein $y \in U_j$ und ein $y \in U_i$ mit $z = xyx^{-1}y^{-1}$. Somit gilt $z \in \{xyx^{-1}y^{-1} \mid x \in U_i \ \textit{und} \ y \in U_j\}$. Falls j ungerade ist, gibt es nach Satz 4.3.1 ein $y \in U_j$ und ein $x \in U_i$ mit $z = xyx^{-1}y^{-1}$. Sei nun j gerade und i ungerade. Wegen $z^{-1} \in [U_i,U_j]$ gibt es nach Satz 4.3.1 ein $y \in U_j$ und ein $x \in U_i$ mit $z^{-1} = yxy^{-1}x^{-1}$. Damit erhält man $z = xyx^{-1}y^{-1}$. Somit gilt in beiden Fällen $z \in \{xyx^{-1}y^{-1} \mid x \in U_i \ \textit{und} \ y \in U_j\}$. □

Korollar 4.3.4 *Seien $i,j \in \mathbb{N}$. Dann ist $[U_i,U_j]$ topologisch abgeschlossen.*

Beweis: Die Aussage dieses Korollares folgt direkt aus Korollar 4.3.3 und Korollar 1.3.1.11. □

Das folgende Korollar verschärft nun die Aussage von Lemma 4.2.8.

Korollar 4.3.5 *Seien $i, j \in \mathbb{N}_0$. Man setze*

$$m_0 := \begin{cases} i+j+1 & \textit{falls } i \textit{ und } j \textit{ gerade} \\ i+j & \textit{falls } i \textit{ oder } j \textit{ ungerade.} \end{cases}$$

Dann gilt $[U_i, U_j] = E_{m_0}$.

Beweis: Offensichtlich gilt $E_{m_0} = U_{m_0} \cap E_1$. Wegen $[U_i, U_j] = U_{m_0} \cap [U, U]$ nach Korollar 4.3.2 und $E_1 \supset [U, U]$ nach Lemma 4.2.8 bleibt nur noch $E_1 \subset [U, U]$ zu zeigen. Sei hierzu $z \in E_1$. Weil nach Satz 4.2.9 für alle geraden $n \in \mathbb{N}$ die Bedingung $F_n(E_1) \subset (\alpha - \alpha^q)\mathbb{F}_q$ erfüllt ist, folgt mit Satz 4.3.1, daß es ein $x \in U_0$ und ein $y \in U_1$ gibt, so daß $z = xyx^{-1}y^{-1}$ gilt. Also ist $E_1 \subset [U, U]$. Somit ist $[U_i, U_j] = E_{m_0}$ gezeigt. □

Korollar 4.3.6 *Sei $m \in \mathbb{N}$. Dann ist E_m topologisch abgeschlossen.*

Beweis: Es gilt $E_m = [U_{m-1}, U_1]$ nach Korollar 4.3.5. Mit Korollar 4.3.4 folgt, daß E_m topologisch abgeschlossen ist. □

Damit man nun $[U, U] = \{x \in U_1 \mid \mathrm{N}(x) = 1\}$ charakterisieren kann, ist es von Interesse, die Norm eines beliebigen Elementes x von U zu berechnen.

Lemma 4.3.7 *Sei $x = \sum_{i=0}^{\infty} a_i \tau^i \in U$. Dann gilt*

$$\mathrm{N}(x) = a_0^{q+1} + \sum_{i=2}^{\infty}{}'' \left(\sum_{k=0}^{i} (-1)^k a_k a_{i-k}^q \right) \tau^i.$$

Beweis: Nach Lemma 1.2.3.2 gilt

$$\begin{aligned} \mathrm{N}(x) &= \left(\sum_{i=0}^{\infty} a_i \tau^i \right) \left(\sum_{i=0}^{\infty} (-1)^i a_i^{q^{i+1}} \tau^i \right) \\ &= \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k \left((-1)^{i-k} a_{i-k}^{q^{i-k+1}} \right)^{q^k} \right) \tau^i \\ &= \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} (-1)^{i-k} a_k a_{i-k}^{q^{i+1}} \right) \tau^i. \end{aligned}$$

Wegen $\mathrm{N}(x) \in L$ müssen alle ungeraden Koeffizienten verschwinden. Daraus ergibt sich

$$\begin{aligned} \mathrm{N}(x) &= \sum_{i=0}^{\infty}{}'' \left(\sum_{k=0}^{i} (-1)^{i-k} a_k a_{i-k}^{q^{i+1}} \right) \tau^i \\ &= a_0^{q+1} + \sum_{i=2}^{\infty}{}'' \left(\sum_{k=0}^{i} (-1)^k a_k a_{i-k}^q \right) \tau^i. \end{aligned}$$

□

Damit läßt sich nun angeben, welchen Gleichungen die Koeffizienten eines Elementes x von U genügen müssen, damit x in $[U, U]$ liegt.

Satz 4.3.8 *Sei $j \in \mathbb{N}$ und $x = 1 + \sum_{i=1}^{\infty} a_i \tau^i \in U_1$. Dann gilt $\mathrm{N}(x) \equiv 1 \mod U_j$ genau dann, wenn für alle geraden $n \in \mathbb{N}$ mit $n < j$ die Gleichung*

$$a_n + a_n^q = \sum_{k=1}^{n-1} (-1)^{k+1} a_k a_{n-k}^q$$

erfüllt ist.

Beweis: Nach Lemma 4.3.7 gilt

$$\mathrm{N}(x) = 1 + \sum_{i=2}^{\infty}{}'' \left(\sum_{k=0}^{i} (-1)^k a_k a_{i-k}^{q^i} \right) \tau^i.$$

Damit ist $\mathrm{N}(x) \equiv 1 \mod U_j$ genau dann erfüllt, wenn für alle geraden $i \in \mathbb{N}$ mit $i < j$ die Gleichung

$$0 = \sum_{k=0}^{i} (-1)^k a_k a_{i-k}^q = a_i^q + \sum_{k=1}^{i-1} (-1)^k a_k a_{i-k}^q + a_i$$

bzw.

$$a_i + a_i^q = -\sum_{k=1}^{i-1} (-1)^k a_k a_{i-k}^q = \sum_{k=1}^{i-1} (-1)^{k+1} a_k a_{i-k}^q$$

gilt. Indem man nun i durch n ersetzt, erhält man die Aussage des Satzes. □

Korollar 4.3.9 *Sei $x = \sum_{i=0}^{\infty} a_i \tau^i \in U$. Dann liegt x genau dann in $[U,U]$, wenn $a_0 = 1$ ist und für alle geraden $n \in \mathbb{N}$ die Gleichung $a_n + a_n^q = \sum_{k=1}^{n-1} (-1)^{k+1} a_k a_{n-k}^q$ gilt.*

Beweis: Wegen $[U,U] = E_1$ nach Korollar 4.3.5 gilt $x \in [U,U]$ genau dann, wenn $x \in U_1$ und $\mathrm{N}(x) = 1$ ist. Offensichtlich ist $x \in U_1$ äquivalent zu $a_0 = 1$, und die Bedingung $\mathrm{N}(x) = 1$ ist genau dann erfüllt, wenn $\mathrm{N}(x) \equiv 1 \mod U_{j+1}$ für alle $n \in \mathbb{N}$ gilt. Durch Anwendung von Satz 4.3.8 folgt nun, daß x genau dann in $[U,U]$ liegt, wenn $a_0 = 1$ ist und für alle geraden $n \in \mathbb{N}$ die Gleichung $a_n + a_n^q = \sum_{k=1}^{n-1} (-1)^{k+1} a_k a_{n-k}^q$ gilt. □

Dieses Ergebnis ist bemerkenswert. Hier erfolgt die Charakterisierung von $[U,U]$ durch $\mathbb{F}_q$-lineare Gleichungen. Für ein gegebenes x in U ist es sofort möglich zu entscheiden, ob x in $[U,U]$ liegt. Für spätere Anwendungen ist noch die folgende Aussage über die Existenz von Elementen in $[U,U]$ zu vorgegebenen Anfangskoeffizienten von Bedeutung.

Satz 4.3.10 *Sei $x = 1 + \sum_{i=1}^{\infty} a_i \tau^i \in U_1$ und $j \in \mathbb{N}$, so daß $\mathrm{N}(x) \equiv 1 \mod U_{j+1}$ gilt. Dann gibt es ein $y \in [U,U]$ mit $y \equiv x \mod U_{g(j+3)}$ und $x - y \in Q_0$.*

Beweis: *Vorbemerkung:* Sei $n \in \mathbb{N}$ gerade und seien $b_1, \ldots, b_{n-1} \in \mathbb{F}_{q^2}$ beliebig. Man setze $b_0 := 1$ und $b_i := 0$ für alle $i \in \mathbb{N}$ mit $i \geq n$. Für $y := \sum_{i=0}^{\infty} b_i \tau^i \in U_1$ gilt dann $\mathrm{N}(y) := 1 + \sum_{i=2}^{\infty}{}'' \left(\sum_{k=0}^{i} (-1)^k b_k b_{i-k}^q \right) \tau^i$ nach Lemma 4.3.7. Wegen $\mathrm{N}(y) \in L$ nach Lemma 1.2.3.6 muß

$$\sum_{k=0}^{n} (-1)^k b_k b_{n-k}^q = \sum_{k=1}^{n-1} b_k b_{n-k}^q$$

in $\mathbb{F}_q$ liegen. Damit folgt nach Satz 1.1.3, daß es ein $\tilde{b}_n \in \mathbb{F}_{q^2}$ gibt, das die Gleichung

$$\tilde{b}_n + \tilde{b}_n^q = \sum_{k=1}^{n-1} b_k b_{n-k}^q$$

löst.

Man setze $l := g(j+1)$. Dann ist l die größte gerade natürliche Zahl, die kleiner oder gleich j ist. Weiter setze man $b_i := a_i$ für alle $i = 1, \ldots, l$ und $i = l+1, l+3, l+5, \ldots$. Aus der Vorbemerkung folgt nun die Existenz einer Folge $\{b_n\}_{n=l+2,l+4,\ldots} \in \mathbb{F}_{q^2}$ die den Bedingungen $b_n + b_n^q = \sum_{k=1}^{n-1} b_k b_{n-k}^q$ für alle $n = l+2, l+4, \ldots$ genügt. Aus den Voraussetzungen an x sowie aus Satz 4.3.8 folgt, daß $b_n + b_n^q = \sum_{k=1}^{n-1} b_k b_{n-k}^q$ auch für alle $n = 2, 4, \ldots, l$ gilt. Nach Korollar 4.3.9 liegt nun $y := 1 + \sum_{i=1}^{\infty} b_i \tau^i$ in $[U, U]$. Wegen $a_i = b_i$ für $i = 1, \ldots, l+1$ gilt $x \equiv y \mod U_{l+2}$. Zusammen mit $a_i = b_i$ für $i = l+2, l+4 \ldots$ folgt $x - y \in Q_0$. Weil $l + 2 = g(j+3)$ gilt, ist damit die Aussage des Satzes bewiesen. □

4.4 Die Kommutatorgruppe $[E_j, U]$ für alle $j \in \mathbb{N}$

Um später die abgeleitete Reihe bzw. die absteigende Zentralreihe von U_n angeben zu können, ist es erforderlich die Kommutatorgruppen der Form $[E_j, E_i]$ und $[E_j, U_n]$ für alle $i, j \in \mathbb{N}_0$ zu bestimmen. Für die Charakterisierung von $[E_j, E_i]$ und $[E_j, U_n]$ im Fall $n \neq 0$ sind die Fälle q gerade und q ungerade zu unterscheiden. Diese werden in den Kapiteln 5 und 6 behandelt. Nur falls $n = 0$ ist, verhält sich der Kommutator von $[E_j, U_0]$ für alle q einheitlich. Um nun $[E_j, U_0]$ bestimmen zu können, ist es zunächst erforderlich die Koeffizientenvariationen von E_j zu berechnen.

Lemma 4.4.1 *Seien $n, m \in \mathbb{N}$. Dann gilt*

$$F_n(E_m) = \begin{cases} \{0\} & \textit{falls } n < m \\ (\alpha - \alpha^q)\mathbb{F}_q & \textit{falls } n \geq m \textit{ und } n \textit{ gerade} \\ \mathbb{F}_{q^2} & \textit{falls } n \geq m \textit{ und } n \textit{ ungerade.} \end{cases}$$

Beweis: Wegen $E_m \subset U_m$ folgt $F_n(E_m) = \{0\}$ für den Fall $n < m$. Sei nun $n \geq m$. Wegen $E_m \subset [U, U]$ folgt

$$F_n(E_m) \subset \begin{cases} (\alpha - \alpha^q)\mathbb{F}_q & \text{falls } n \text{ gerade} \\ \mathbb{F}_{q^2} & \text{falls } n \text{ ungerade} \end{cases}$$

nach Korollar 4.2.10 und Bemerkung 4.2.3. Falls n gerade ist, gibt es für alle $a \in (\alpha - \alpha^q)\mathbb{F}_q$ ein $x \in [U, U]$ mit $x \equiv 1 + a\tau^n \mod U_{n+1}$. Wegen $n \geq m$ gilt auch $x \in E_m = U_m \cap [U, U]$. Somit ist $a \in F_n(E_m)$. Also gilt $(\alpha - \alpha^q)\mathbb{F}_q \subset F_n(E_m)$. Falls n ungerade ist, gibt es für alle $a \in \mathbb{F}_{q^2}$ ein $x \in [U, U]$ mit $x \equiv 1 + a\tau^n \mod U_{n+1}$. Wegen $n \geq m$ gilt auch $x \in E_m = U_m \cap [U, U]$. Somit ist $a \in F_n(E_m)$. Also gilt $\mathbb{F}_{q^2} \subset F_n(E_m)$. Insgesamt folgt damit die Aussage des Lemmas □

Satz 4.4.2 *Sei $j \in \mathbb{N}$ mit j ungerade sowie $c_j \in \mathbb{F}_{q^2}^*$. Dann gibt es für alle $z \in E_j$ mit $z \equiv 1 + c_j\tau^j \mod U_{j+1}$ ein $x \in U$ und ein $y \in E_j$, so daß $z = xyx^{-1}y^{-1}$ gilt.*

Beweis: Man zeigt durch Induktion über n, daß es Folgen $\{x_n\}_{n\in\mathbb{N}} \subset U$ und $\{y_n\}_{n\in\mathbb{N}} \subset E_j$ gibt, die für alle $n \in \mathbb{N}$ folgenden Bedingungen genügen:

- **(Bed 1)** Falls $n \neq 1$ ist, gilt $x_n \equiv x_{n-1} \mod U_{n-1}$ sowie $x_n \equiv x_{n-1} \mod U_{j+n-1}$.
- **(Bed 2)** Es gilt $x_n y_n x_n^{-1} y_n^{-1} \equiv z \mod U_{n+j}$.

Aus **(Bed 1)** folgt, daß $\{x_n\}_{n\in\mathbb{N}} \subset U$ und $\{y_n\}_{n\in\mathbb{N}} \subset E_j$ Cauchyfolgen und damit konvergent sind. Man setze nun $x := \lim_{n\to\infty} x_n$ und $y := \lim_{n\to\infty} y_n$. Wegen der topologischen Abgeschlossenheit von U nach Lemma 1.3.1.9 und von E_j nach Korollar 4.3.6 folgt $x \in U$ und $y \in E_j$. Aus **(Bed 2)** folgt weiter, daß die Folge $\{x_n y_n x_n^{-1} y_n^{-1}\}_{n\in\mathbb{N}}$ gegen z konvergiert. Mit Satz 1.3.1.10 erhält man

$$z = \lim_{n\to\infty} (x_n y_n x_n^{-1} y_n^{-1}) = xyx^{-1}y^{-1}$$

und damit die Aussage von Satz 4.4.2.

Zur Existenz der Folgen $\{x_n\}_{n\in\mathbb{N}} \subset U$ und $\{y_n\}_{n\in\mathbb{N}} \subset U_j$

Induktionsanfang $n = 1$: Man setze $x_1 := a_0$ mit $a_0 \in \mathbb{F}_{q^2} - \mathbb{F}_q$ beliebig. Weiter setze man $b_j := \frac{c_j}{a_0^{1-q}-1}$. Dann gibt es wegen $F_j(E_j) = \mathbb{F}_{q^2}$ ein $y_1 \in E_j$ mit $y_1 \equiv 1 + b_j\tau^j \mod U_{j+1}$. Da $n = 1$ ist, gilt **(Bed 1)** trivialerweise. Außerdem erhält man nach Lemma 4.1.1 die Kongruenz

$$x_1y_1 \equiv (1 + b_j(a_0^{1-q} - 1)\tau^j)y_1x_1 \mod U_{j+1}.$$

Daraus folgt

$$\begin{aligned} x_1y_1x_1^{-1}y_1^{-1} &\equiv (1 + b_j(a_0^{1-q} - 1)\tau^j) \mod U_{j+1} \\ &\equiv 1 + c_j\tau^j \mod U_{j+1} \\ &\equiv z \mod U_{j+1}. \end{aligned}$$

Also ist auch **(Bed 2)** erfüllt.

Induktionsschritt $n \longmapsto n + 1$: Nach Induktionsannahme gibt es ein $x_n \in U$ und ein $y_n \in E_j$ mit $x_ny_nx_n^{-1}y_n^{-1} \equiv z \mod U_{j+n}$. Daraus folgt, daß es ein $c \in \mathbb{F}_{q^2}$ geben muß mit

$$z \equiv x_ny_nx_n^{-1}y_n^{-1}(1 + c\tau^{n+j}) \mod U_{n+j+1}.$$

Falls n gerade ist, gilt $F_{n+j}(E_j) = \mathbb{F}_{q^2}$. Also existiert für alle $b \in \mathbb{F}_{q^2}$ ein $y(b) \in E_j$ mit $y(b) \equiv 1+b\tau^{j+n} \mod U_{n+j+1}$. Nach Lemma 4.1.2(i) gibt es ein $b \in \mathbb{F}_{q^2}$, so daß für $x_{n+1} := x_n \in U$ und $y_{n+1} := y_ny(b) \in E_j$ die Kongruenz

$$\begin{aligned} x_{n+1}y_{n+1}x_{n+1}^{-1}y_{n+1}^{-1} &\equiv x_ny_nx_n^{-1}y_n^{-1}(1 + c\tau^{j+n}) \mod U_{j+n+1} \\ &\equiv z \mod U_{j+n+1} \end{aligned}$$

gilt. Damit sind die beiden Bedingungen **(Bed 1)** und **(Bed 2)** erfüllt.

Falls n ungerade ist, folgt wegen $z(x_ny_nx_n^{-1}y_n^{-1})^{-1} \in E_1$, daß c in $F_{j+n}(E_1) = (\alpha - \alpha^q)\mathbb{F}_q$ liegt. Nach Lemma 4.1.2(ii) gibt es nun ein $a \in \mathbb{F}_{q^2}$, so daß für $y_{n+1} := y_n \in E_j$ und $x_{n+1} := x_n(1 + a\tau^n) \in U$ die Kongruenz

$$\begin{aligned} x_{n+1}y_{n+1}x_{n+1}^{-1}y_{n+1}^{-1} &\equiv x_ny_nx_n^{-1}y_n^{-1}(1 + c\tau^{n+j}) \mod U_{j+n+1} \\ &\equiv z \mod U_{j+n+1} \end{aligned}$$

gilt. Damit sind die beiden Bedingungen **(Bed 1)** und **(Bed 2)** erfüllt. □

Mit diesem Satz läßt sich nun der Kommutator $[U, E_j]$ bestimmen.

Korollar 4.4.3 *: Sei $j \in \mathbb{N}$ beliebig. Man setze*

$$m_0 := \begin{cases} j + 1 & \textit{falls } j \textit{ gerade} \\ j & \textit{falls } j \textit{ ungerade.} \end{cases}$$

Dann gilt $[U, E_j] = E_{m_0}$.

Beweis: Wegen $E_j \subset U_j$ folgt $[U, E_j] \subset [U, U_j] = E_{m_0}$ nach Korollar 4.3.5. Damit bleibt $[U, E_j] \supset E_{m_0}$ zu zeigen. Sei dazu $z \in E_{m_0}$. Falls $z = 1$ ist, wird die Aussage trivial. Falls j ungerade ist, gilt $m_0 = j$. Sei also $z \neq 1$. Man setze $m := \max\{k \in \mathbb{N} \mid z \equiv 1 \mod U_k\}$. Dann gibt es ein $c_m \in F_m(E_j)$ mit $c_m \neq 0$, so daß $z \equiv 1 + c_m\tau^m \mod U_{m+1}$ gilt. Falls nun m ungerade ist, folgt $z \in [U, E_m] \subset [U, E_j]$ nach Satz 4.4.2. Sei nun m gerade. Dann ist $m - 1$ ungerade. Wegen $m - 1 \geq m_0$ gibt es ein $\tilde{z} \in E_{m_0}$ mit $\tilde{z} \equiv 1 + \tau^{m-1} \mod U_m$. Damit gilt auch $z\tilde{z} \equiv 1 + \tau^{m-1} \mod U_m$. Da nach Satz 4.4.2 sowohl $z\tilde{z}$ als auch $\tilde{z}$ in $[U, E_j]$ liegen, folgt $z = (z\tilde{z})\tilde{z}^{-1} \in [U, E_j]$. Damit ist die Aussage des Korollares bewiesen. □

Kapitel 5

Die höheren Kommutatorgruppen im Fall q ungerade

Für dieses gesamte Kapitel sei vereinbart, daß q ungerade ist.

5.1 Der Hauptsatz über die Kommutatorgruppe $[E_i, E_j]$ für alle $i, j \in \mathbb{N}$

Für alle $i, j \in \mathbb{N}$ lassen sich die Kommutatorgruppen der Form $[E_i, E_j]$ ähnlich charakterisieren wie die der Form $[U_i, U_j]$.

Hauptsatz 5.1.1 *Seien $i, j \in \mathbb{N}$ mit j ungerade sowie $m_0 := i + j$. Dann gibt es für alle $z \in E_{m_0}$ ein $x \in E_i$ und ein $y \in E_j$, so daß $z = xyx^{-1}y^{-1}$ gilt.*

Beweis: Sei $z \in E_{m_0}$. Falls $z = 1$ ist, wird die Aussage trivial (man wähle $x = y = 1$). Sei also $z \neq 1$. Man setze $m := \max\{k \in \mathbb{N} \mid z \equiv 1 \mod U_k\}$. Dann gibt es ein $c_m \in \mathbb{F}_{q^2}$ mit $c_m \neq 0$, so daß $z \equiv 1 + c_m \tau^m \mod U_{m+1}$ gilt. Man zeigt nun durch Induktion über n, daß es ein $i' \in \mathbb{N}_0$ mit $i' \geq i$ gibt, so daß Folgen $\{x_n\}_{n \in \mathbb{N}} \subset E_{i'}$ und $\{y_n\}_{n \in \mathbb{N}} \subset E_j$ existieren, die für alle $n \in \mathbb{N}$ folgenden Bedingungen genügen:

(Bed 1) Falls $n \neq 1$ ist, gilt $x_n \equiv x_{n-1} \mod U_{i'+n-1}$ sowie $x_n \equiv x_{n-1} \mod U_{j+n-1}$.

(Bed 2) Es gilt $x_n y_n x_n^{-1} y_n^{-1} \equiv z \mod U_{n+m}$.

Aus **(Bed 1)** folgt, daß $\{x_n\}_{n \in \mathbb{N}} \subset E_{i'} \subset E_i$ und $\{y_n\}_{n \in \mathbb{N}} \subset E_j$ Cauchyfolgen und damit konvergent sind. Man setze nun $x := \lim_{n \to \infty} x_n$ und $y := \lim_{n \to \infty} y_n$. Wegen der topologischen Abgeschlossenheit von $E_{i'}$ und E_j nach Korollar 4.3.6 folgt $x \in E_{i'}$ und $y \in E_j$. Aus **(Bed 2)** folgt weiter, daß die Folge $\{x_n y_n x_n^{-1} y_n^{-1}\}_{n \in \mathbb{N}}$ gegen z konvergiert. Mit Satz 1.3.1.10 erhält man

$$z = \lim_{n \to \infty} (x_n y_n x_n^{-1} y_n^{-1}) = xyx^{-1}y^{-1}$$

und damit die Aussage von Satz 5.1.1.

Zur Existenz der Folgen $\{x_n\}_{n \in \mathbb{N}} \subset E_{i'}$ und $\{y_n\}_{n \in \mathbb{N}} \subset E_j$

1. Fall m ungerade: Man setze $i' := m - j$. Dann ist i' gerade, und es gilt $i' + j = m$ sowie $i' \geq i$.

Induktionsanfang $n = 1$: Sei $a_{i'} \in (\alpha - \alpha^q)\mathbb{F}_q - \{0\}$ Dann gilt $a_{i'}^q = -a_{i'} \neq a_{i'}$. Man setze nun $b_j := \frac{c_m}{a_{i'} - a_{i'}^q}$. Da $F_{i'}(E_{i'}) = (\alpha - \alpha^q)\mathbb{F}_q$ und $F_j(E_j) = \mathbb{F}_{q^2}$ ist, gibt es ein $x_1 \in E_{i'}$ mit

$x_1 \equiv 1 + a_{i'}\tau^{i'} \mod U_{i'+1}$ und ein $y_1 \in E_j$ mit $y_1 \equiv 1 + b_j\tau^j \mod U_{j+1}$. Wegen $n = 1$ ist **(Bed 1)** trivialerweise erfüllt. Außerdem gilt nach Lemma 4.1.1 die Kongruenz

$$\begin{aligned} x_1y_1 &\equiv (1 + (a_{i'}b_j^{q^{i'}} - b_j a_{i'}^{q^j})\tau^m)y_1x_1 \mod U_{m+1} \\ &\equiv (1 + b_j(a_{i'} - a_{i'}^q)\tau^m)y_1x_1 \mod U_{m+1}. \end{aligned}$$

Daraus folgt

$$x_1y_1x_1^{-1}y_1^{-1} \equiv 1 + c_m\tau^m \mod U_{m+1} \equiv z \mod U_{m+1}.$$

Also ist auch **(Bed 2)** erfüllt.

Induktionsschritt $n \longmapsto n+1$: Nach Induktionsannahme gibt es ein $x_n \in E_{i'}$ und ein $y_n \in E_j$ mit $x_ny_nx_n^{-1}y_n^{-1} \equiv z \mod U_{n+m}$. Daraus folgt, daß es ein $c \in \mathbb{F}_{q^2}$ geben muß mit

$$z \equiv x_ny_nx_n^{-1}y_n^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1}.$$

Falls n gerade ist, gilt $F_{j+n}(E_j) = \mathbb{F}_{q^2}$. Also gibt es für alle $b \in \mathbb{F}_{q^2}$ ein $y(b) \in E_j$ mit $y(b) \equiv 1 + b\tau^{j+n} \mod U_{j+n+1}$. Nach Lemma 4.1.3(i) gibt es nun ein $b \in \mathbb{F}_{q^2}$, so daß für $x_{n+1} := x_n \in E_{i'}$ und $y_{n+1} := y_ny(b) \in E_j$ die Kongruenz

$$\begin{aligned} x_{n+1}y_{n+1}x_{n+1}^{-1}y_{n+1}^{-1} &\equiv x_ny_nx_n^{-1}y_n^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1} \\ &\equiv z \mod U_{n+m+1} \end{aligned}$$

gilt. Damit sind die beiden Bedingungen **(Bed 1)** und **(Bed 2)** erfüllt.

Falls n ungerade ist, folgt wegen $z(x_ny_nx_n^{-1}y_n^{-1})^{-1} \in E_1$, daß c in $F_{n+m}(E_1) = (\alpha - \alpha^q)\mathbb{F}_q$ liegt. Da $F_{i'+n}(E_{i'}) = \mathbb{F}_{q^2}$ ist, gibt es für alle $a \in \mathbb{F}_{q^2}$ ein $x(a) \in E_{i'}$ mit $x(a) \equiv 1 + a\tau^{i'+n} \mod U_{i'+n+1}$. Nach Lemma 4.1.3(ii) gibt es nun ein $a \in \mathbb{F}_{q^2}$, so daß für $x_{n+1} := x_nx(a) \in E_{i'}$ und $y_{n+1} := y_n \in E_j$ die Kongruenz

$$\begin{aligned} x_{n+1}y_{n+1}x_{n+1}^{-1}y_{n+1}^{-1} &\equiv x_ny_nx_n^{-1}y_n^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1} \\ &\equiv z \mod U_{n+m+1} \end{aligned}$$

gilt. Damit sind die beiden Bedingungen **(Bed 1)** und **(Bed 2)** erfüllt.

2. Fall m gerade: Man setze $i' := m - j$. Dann ist i' ungerade, und es gilt $m = i' + j$ sowie $i' \geq i$.

Induktionsanfang $n = 1$: Da m gerade ist, gilt $c_m \in F_m(E_{m_0}) = (\alpha - \alpha^q)\mathbb{F}_q$. Nach Satz 1.1.4 folgt, daß es ein $b_j \in \mathbb{F}_{q^2}$ gibt mit $b_j^q - b_j = c_m$. Wegen $F_{i'}(E_{i'}) = F_j(E_j) = \mathbb{F}_{q^2}$ gibt es nun ein $x_1 \in E_{i'}$ mit $x_1 \equiv 1 + \tau^{i'} \mod U_{i'+1}$ und ein $y_1 \in E_j$ mit $y_1 \equiv 1 + b_j\tau^j \mod U_{j+1}$. Wegen $n = 1$ ist **(Bed 1)** trivialerweise erfüllt. Außerdem gilt nach Lemma 4.1.1 die Kongruenz

$$\begin{aligned} x_1y_1 &\equiv (1 + (1b_j^{q^{i'}} - b_j1^{q^j})\tau^m)y_1x_1 \mod U_{m+1} \\ &\equiv (1 + (b_j^q - b_j)\tau^m)y_1x_1 \mod U_{m+1}. \end{aligned}$$

Daraus folgt

$$x_1y_1x_1^{-1}y_1^{-1} \equiv 1 + c_m\tau^m \mod U_{m+1} \equiv z \mod U_{m+1}.$$

Also ist auch **(Bed 2)** erfüllt.

Induktionsschritt $n \longmapsto n+1$: Nach Induktionsannahme gibt es ein $x_n \in E_{i'}$ und ein $y_n \in E_j$ mit $x_ny_nx_n^{-1}y_n^{-1} \equiv z \mod U_{n+m}$. Daraus folgt, daß es ein $c \in \mathbb{F}_{q^2}$ geben muß mit

$$z \equiv x_ny_nx_n^{-1}y_n^{-1}(1 + c\tau^{n+m}) \mod U_{n+m+1}.$$

Falls n gerade ist, folgt wegen $z(x_ny_nx_n^{-1}y_n^{-1})^{-1} \in E_1$, daß c in $F_{n+m}(E_1) = (\alpha - \alpha^q)\mathbb{F}_q$ liegt. Da $F_{j+n}(E_j) = \mathbb{F}_{q^2}$ ist, gibt es für alle $b \in \mathbb{F}_{q^2}$ ein $y(b) \in E_j$ mit $y(b) \equiv 1 + b\tau^{j+n} \mod U_{j+n+1}$.

Nach Lemma 4.1.4(i) gibt es nun ein $b \in \mathbb{F}_{q^2}$, so daß für $x_{n+1} := x_n \in E_{i'}$ und $y_{n+1} := y_n y(b) \in E_j$ die Kongruenz

$$\begin{aligned} x_{n+1}y_{n+1}x_{n+1}^{-1}y_{n+1}^{-1} &\equiv x_n y_n x_n^{-1} y_n^{-1}(1+c\tau^{n+m}) \mod U_{n+m+1} \\ &\equiv z \mod U_{n+m+1} \end{aligned}$$

gilt. Damit sind die beiden Bedingungen **(Bed 1)** und **(Bed 2)** erfüllt.

Sei nun n ungerade. Wegen $b_j^q - b_j = c_m \neq 0$ gilt $b_j \notin \mathbb{F}_q$. Also ist $\{1, b_j\}$ eine $\mathbb{F}_q$-Basis von $\mathbb{F}_{q^2}$. Für alle $a, b \in (\alpha - \alpha^q)\mathbb{F}_q = F_{i'+n}(E_{i'+n}) = F_{j+n}(E_{j+n})$ gibt es nun ein $x(a) \in E_{i'}$ mit $x(a) \equiv 1 + a\tau^{i'+n} \mod U_{i'+n+1}$ und ein $y(b) \in E_j$ mit $y(b) \equiv 1 + b\tau^{j+n} \mod U_{j+n+1}$. Nach Lemma 4.1.4(iii) gibt es nun Elemente $a, b \in (\alpha - \alpha^q)\mathbb{F}_q$, so daß für $x_{n+1} := x_n x(a) \in E_{i'}$ und $y_{n+1} := y_n y(b) \in E_j$ die Kongruenz

$$\begin{aligned} x_{n+1}y_{n+1}x_{n+1}^{-1}y_{n+1}^{-1} &\equiv x_n y_n x_n^{-1} y_n^{-1}(1+c\tau^{n+m}) \mod U_{n+m+1} \\ &\equiv z \mod U_{n+m+1} \end{aligned}$$

gilt. Damit sind die beiden Bedingungen **(Bed 1)** und **(Bed 2)** erfüllt. □

Korollar 5.1.2 *Seien $i, j \in \mathbb{N}$ und*

$$m_0 := \begin{cases} i+j+1 & \textit{falls } i \textit{ und } j \textit{ gerade} \\ i+j & \textit{falls } i \textit{ oder } j \textit{ ungerade.} \end{cases}$$

Dann gilt $[E_i, E_j] = E_{m_0}$.

Beweis: Nach Korollar 4.3.5 gilt $[E_i, E_j] \subset [U_i, U_j] = E_{m_0}$. Damit bleibt nur noch $[E_i, E_j] \supset E_{m_0}$ zu zeigen. Sei hierzu $z \in E_{m_0}$. Falls i oder j ungerade ist, kann man wegen $[E_i, E_j] = [E_j, E_i]$ ohne Einschränkung annehmen, daß j ungerade ist. Da $m_0 = i + j$ ist, folgt nach Satz 5.1.1, daß es ein $x \in E_i$ und ein $y \in E_j$ gibt mit $z = xyx^{-1}y^{-1}$. Somit ist $z \in E_{m_0}$. Falls i und j ungerade sind, gilt $m_0 = i + j + 1$, wobei $j + 1$ ungerade ist. Nach Satz 5.1.1 folgt, daß es ein $x \in E_i$ und ein $y \in E_{j+1} \subset E_j$ gibt mit $z = xyx^{-1}y^{-1}$. Somit ist $z \in E_{m_0}$. Damit folgt die Aussage des Korollares. □

Korollar 5.1.3 *Seien $i, j \in \mathbb{N}$ sowie*

$$m_0 := \begin{cases} i+j+1 & \textit{falls } i \textit{ und } j \textit{ gerade} \\ i+j & \textit{falls } i \textit{ oder } j \textit{ ungerade.} \end{cases}$$

Dann gilt $[E_i, U_j] = E_{m_0}$.

Beweis: Nach Korollar 4.3.5 und Korollar 5.1.2 gilt

$$E_{m_0} = [E_i, E_j] \subset [E_i, U_j] \subset [U_i, U_j] = E_{m_0}.$$

Daraus folgt $[E_i, U_j] = E_{m_0}$. □

Mit den letzten beiden Korollaren läßt sich nun sowohl die abgleitete Reihe als auch die absteigende Zentralreihe von U_n auf einfache Weise explizit angeben. Das folgende Korollar ist rein theoretischen Interesses.

Korollar 5.1.4 *Seien $i, j \in \mathbb{N}$. Dann gilt*

$$[E_i, E_j] = \{xyx^{-1}y^{-1} \mid x \in E_i \textit{ und } y \in E_j\}.$$

Beweis: Da „$\supset$" trivial ist, bleibt lediglich „$\subset$" zu zeigen. Dazu setze man

$$m_0 := \begin{cases} i+j+1 & \text{falls } i \text{ und } j \text{ gerade} \\ i+j & \text{falls } i \text{ oder } j \text{ ungerade.} \end{cases}$$

Sei nun $z \in [E_i, E_j] = E_{m_0}$. Falls i und j gerade sind, gilt $m_0 = i+j+1$, wobei $j+1$ ungerade ist. Nach Satz 4.3.1 gibt es nun ein $y \in E_j$ und ein $y \in E_i$ mit $z = xyx^{-1}y^{-1}$. Somit gilt $z \in \{xyx^{-1}y^{-1} \mid x \in E_i \;\; und \;\; y \in E_j\}$. Falls j ungerade ist, gibt es nach Satz 4.3.1 ein $y \in E_j$ und ein $y \in E_i$ mit $z = xyx^{-1}y^{-1}$. Somit gilt $z \in \{xyx^{-1}y^{-1} \mid x \in E_i \;\; und \;\; y \in E_j\}$. Sei nun j gerade und i ungerade. Wegen $z^{-1} \in [E_i, E_j]$ gibt es nach Satz 4.3.1 ein $y \in E_j$ und ein $x \in E_i$ mit $z^{-1} = yxy^{-1}x^{-1}$. Damit erhält man $z = xyx^{-1}y^{-1}$. Somit gilt $z \in \{xyx^{-1}y^{-1} \mid x \in E_i \;\; und \;\; y \in E_j\}$. $\square$

5.2 Folgerungen aus dem Hauptsatz

Für den gesamten Rest dieser Arbeit wählt man folgende Bezeichnungen. Für eine beliebige Gruppe G sei $\{Z^k(G)\}_{k \in \mathbb{N}_0}$ die *absteigende Zentralreihe von* G und $\{D^k(G)\}_{k \in \mathbb{N}_0}$ die *abgeleitete Reihe von* G. Es sei daran erinnert, daß die absteigende Zentralreihe durch $Z^0(G) = G$ sowie $Z^{k+1}(G) = [Z^k(G), G]$ und die abgeleitete Reihe durch $D^0(G) = G$ sowie $D^{k+1}(G) = [D^k(G), D^k(G)]$ für alle $k \in \mathbb{N}_0$ definiert ist. Aus formalen Gründen wählt man die Bezeichnungen $Z^\infty(G)$ bzw. $D^\infty(G)$ für diejenige Untergruppe von G, die nur aus dem neutralen Element besteht. Es sei darauf hingewiesen, daß für einen beliebigen Normalteiler N von G die Relationen $Z^k(G/N) = (Z^k(G) \cdot N)/N$ und $D^k(G/N) = (D^k(G) \cdot N)/N$ für alle $k \in \mathbb{N}_0$ gelten. Auf diese Weise erhält man z. B. die abgeleitete Reihe bzw. die absteigende Zentralreihe von G_n aus der abgeleiteten Reihe bzw. absteigenden Zentralreihe von U_n. Weiter sei $l_{auf}(G) := \min\{l \in \mathbb{N} \cup \{\infty\} \mid D^l(G) = D^\infty(G)\}$ *die auflösbare Länge von* G und $l_{nil}(G) := \min\{l \in \mathbb{N} \cup \{\infty\} \mid Z^l(G) = Z^\infty(G)\}$ *die nilpotente Länge von* G. Diese beiden Zahlenwerte sind deshalb von Interesse, weil sie ein Maß für die Nichtkommutativität von G sind. In diesem Abschnitt werden nun für alle $n \in \mathbb{N}_0$ die absteigende Zentralreihe sowie die abgeleitete Reihe von U_n bestimmt. Daraus läßt sich sofort die abgeleitete Reihe bzw. die absteigende Zentralreihe und damit die auflösbare bzw. nilpotente Länge von einer beliebigen Faktorgruppe der Form U_m/U_n für alle $n \geq m \in \mathbb{N}_0$ bestimmen. Das Hauptinteresse gilt dabei der auflösbaren Länge von G_n sowie der nilpotenten Länge der Faktorgruppe U_1/U_n, da diese sich als die einzige p-Sylowuntergruppe von G_n auffassen läßt und G_n selbst im Fall $n > 1$ nicht nilpotent ist. Für diese Faktorgruppe U_1/U_n wählt man die Bezeichnung $\hat{G}_n$.

5.2.1 Die absteigende Zentralreihe von U_n

Satz 5.2.1.1 *Seien $n \in \mathbb{N}_0$ und $k \in \mathbb{N}$. Dann gilt für die absteigende Zentralreihe von U_n*

$$Z^k(U_n) = \begin{cases} E_{(k+1)n} & \textit{falls } n \textit{ ungerade} \\ E_{(k+1)n+1} & \textit{falls } n \textit{ gerade.} \end{cases}$$

Beweis: Die Aussage wird durch Induktion über alle $k \in \mathbb{N}$ gezeigt. Für $k = 1$ gilt nach Korollar 4.3.5 die Identität

$$Z^1(U_n) := [U_n, U_n] = \begin{cases} E_{2n} & \text{falls } n \text{ ungerade} \\ E_{2n+1} & \text{falls } n \text{ gerade.} \end{cases}$$

Für ein beliebiges $k \in \mathbb{N}$ gilt nach Induktionsannahme

$$Z^k(U_n) = \begin{cases} E_{(k+1)n} & \text{falls } n \text{ ungerade} \\ E_{(k+1)n+1} & \text{falls } n \text{ gerade.} \end{cases}$$

Für $n = 0$ erhält man $Z^{k+1}(U) = [Z^k(U_0), U_0] = [E_1, U_0] = E_1$ nach Korollar 4.4.3. Falls $n \neq 0$ ist folgt

$$Z^{k+1}(U_n) = \begin{cases} [E_{(k+1)n}, U_n] & \text{falls } n \text{ ungerade} \\ [E_{(k+1)n+1}, U_n] & \text{falls } n \text{ gerade} \end{cases} = \begin{cases} E_{(k+2)n} & \text{falls } n \text{ ungerade} \\ E_{(k+2)n+1} & \text{falls } n \text{ gerade} \end{cases}$$

nach Korollar 5.1.3. □

Korollar 5.2.1.2 *Sei $n \in \mathbb{N}$. Dann gilt:*

(i) Die Faktorgruppe G_n ist genau dann nilpotent, wenn $n = 1$ ist. Dabei gilt $l_{nil}(G_1) = 1$.

(ii) Die Faktorgruppe $\hat{G}_n$ ist nilpotent der Länge $n - 1$.

Beweis: (i) Für $n = 1$ ist $G_1 \cong \mathbb{F}_{q^2}^*$ abelsch und damit nilpotent der Länge 1. Sei nun $n \neq 1$. Dann gilt $Z^k(G_n) = (Z^k(U) \cdot U_n)/U_n = (E_1 \cdot U_n)/U_n$ nach Satz 5.2.1.1. Wegen $E_1 \not\subset U_n$ gilt $Z^k(G_n) \neq \{1 \cdot U_n\}$ für alle $k \in \mathbb{N}$. Somit ist G_n nicht nilpotent.

(ii) Offensichtlich besteht $\hat{G}_1$ nur aus dem neutralen Element und ist folglich nilpotent der Länge 0. Weiter gilt $\hat{G}_2 \neq \{1 \cdot U_2\}$ sowie $Z^1(\hat{G}_2) = (E_2 \cdot U_2)/U_2 = \{1 \cdot U_2\}$. Damit ist die Aussage im Fall $n = 1$ und $n = 2$ gezeigt. Sei nun $n > 2$. Dann gilt $Z^{n-2}(\hat{G}_n) = (E_{n-1} \cdot U_n)/U_n$ sowie $Z^{n-1}(\hat{G}_n) = (E_n \cdot U_n)/U_n$ nach Satz 5.2.1.1. Wegen $E_{n-1} \not\subset U_n$ und $E_n \subset U_n$ folgt, daß $\hat{G}_n$ nilpotent der Länge $n - 1$ ist. □

5.2.2 Die abgeleitete Reihe von U_n

Satz 5.2.2.1 *Seien $n \in \mathbb{N}_0$ und $k \in \mathbb{N}$. Dann gilt $D^k(U_n) = E_{f(n,k)}$, wobei*

$$f(n,k) := \begin{cases} n2^k + \frac{2^{k+1}}{3} - \frac{1}{2} - \frac{(-1)^k}{6} & \textit{falls } n \textit{ gerade} \\ n2^k + \frac{2^k}{3} - \frac{1}{2} - \frac{(-1)^{k+1}}{6} & \textit{falls } n \textit{ ungerade} \end{cases}$$

ist.

Beweis: Durch Induktion über k zeigt man für alle $n \in \mathbb{N}_0$ die folgende weitergehende Aussage : Der Ausdruck $f(n,k)$ liegt in $\mathbb{N}$, ist genau dann gerade, wenn k und n entweder beide gerade oder beide ungerade sind, und es gilt $D^k(U_n) = E_{f(n,k)}$.

<u>1. Fall n gerade:</u> Für $k = 1$ ist $f(1,n) = 2n + \frac{4}{3} - \frac{1}{2} + \frac{1}{6} = 2n + 1 \in \mathbb{N}$ ungerade. Außerdem gilt $D^1(U_n) = [U_n, U_n] = E_{2n+1}$ nach Korollar 4.3.5. Sei nun $k \in \mathbb{N}$ beliebig. Nach Induktionsannahme ist $f(n,k) \in \mathbb{N}$ genau dann gerade, wenn k gerade ist, und es gilt $D^k(U_n) = E_{f(n,k)}$.

Falls k gerade ist, erhält man, daß

$$f(k+1,n) = n2^{k+1} + \frac{2^{k+2}}{3} - \frac{2}{6} = 2(n2^k + \frac{2^{k+1}}{3} - \frac{1}{2} - \frac{1}{6}) + 1 = 2f(k,n) + 1$$

ungerade ist. Da $f(k,n)$ gerade ist, folgt $D^{k+1}(U_n) = [E_{f(k,n)}, E_{f(k,n)}] = E_{f(k+1,n)}$ nach Korollar 5.1.2.

Falls k ungerade ist, erhält man, daß

$$f(k+1,n) = n2^{k+1} + \frac{2^{k+2}}{3} - \frac{4}{6} = 2(n2^k + \frac{2^{k+1}}{3} - \frac{1}{2} + \frac{1}{6}) = 2f(k,n)$$

gerade ist. Da $f(k,n)$ ungerade ist, folgt $D^{k+1}(U_n) = [E_{f(k,n)}, E_{f(k,n)}] = E_{f(k+1,n)}$ nach Korollar 5.1.2.

2. Fall n ungerade: Für $k=1$ ist $f(1,n)=2n+\frac{2}{3}-\frac{1}{2}-\frac{1}{6}=2n\in\mathbb{N}$ ungerade. Außerdem gilt $D^1(U_n)=[U_n,U_n]=E_{2n+1}$ nach Korollar 4.3.5. Sei nun $k\in\mathbb{N}$ beliebig. Nach Induktionsannahme ist $f(n,k)\in\mathbb{N}$ genau dann gerade, wenn k ungerade ist, und es gilt $D^k(U_n)=E_{f(n,k)}$.

Falls k gerade ist, erhält man, daß

$$f(k+1,n)=n2^{k+1}+\frac{2^{k+1}}{3}-\frac{4}{6}=2(n2^k+\frac{2^k}{3}-\frac{1}{2}+\frac{1}{6})=2f(k,n)$$

gerade ist. Da $f(k,n)$ ungerade ist, folgt $D^{k+1}(U_n)=[E_{f(k,n)},E_{f(k,n)}]=E_{f(k+1,n)}$ nach Korollar 5.1.2.

Falls k ungerade ist, erhält man, daß

$$f(k+1,n)=n2^{k+1}+\frac{2^{k+1}}{3}-\frac{2}{6}=2(n2^k+\frac{2^k}{3}-\frac{1}{2}-\frac{1}{6})+1=2f(k,n)+1$$

ungerade ist. Da $f(k,n)$ gerade ist, folgt $D^{k+1}(U_n)=[E_{f(k,n)},E_{f(k,n)}]=E_{f(k+1,n)}$ nach Korollar 5.1.2. □

Um nun die auflösbare Länge von G_n anzugeben, verwendet man die folgende Abkürzung.

Bezeichnung 5.2.2.2 *Für alle $k\in\mathbb{N}_0$ setze man*

$$f_q(k):=\frac{2^{k+1}}{3}-\frac{1}{2}-\frac{(-1)^k}{6}$$

Unter der Voraussetzungen von Satz 5.2.2.1 gilt $f_q(k)=f(0,k)$.

Korollar 5.2.2.3 *Die Faktorgruppe G_n ist für alle $n\in\mathbb{N}$ auflösbar. Die auflösbare Länge $l=l_{auf}(G_n)$ ist eindeutig bestimmt durch die Bedingung*

$$l\in\mathbb{N}\ \textit{und}\ f_q(l-1)<n\leq f_q(l).$$

Beweis: Aus Satz 5.2.2.1 folgt $D^k(G_n)=(D^k(U_0)\cdot U_n)/U_n=(E_{f_q(l)}\cdot U_n)/U_n$. Die notwendige und hinreichende Bedingung dafür, daß $D^k(G_n)=\{1\cdot U_0\}$ ist, lautet $E_{f_q(k)}\subset U_n$. Das ist äquivalent zu $f_q(k)\geq n$. Wegen $\lim_{k\to\infty}f_q(k)=\infty$ folgt die Auflösbarkeit von G_n. Für die auflösbare Länge l gilt dabei

$$l=\min\{k\in\mathbb{N}\mid f_q(k)\geq n\}.$$

Für alle $k\in\mathbb{N}_0$ gilt nun

$$\begin{aligned} f_q(k+1)-f_q(k) &= \tfrac{2^{k+2}}{3}-\tfrac{1}{2}-\tfrac{(-1)^{k+1}}{6}-\left(\tfrac{2^{k+1}}{3}-\tfrac{1}{2}-\tfrac{(-1)^k}{6}\right)\\ &\geq \tfrac{2^{k+1}}{3}-\tfrac{1}{3}>0. \end{aligned}$$

Also ist $\{f_q(k)\}_{k\in\mathbb{N}_0}$ *streng* monoton wachsend. Wegen $f_q(0)=0$ und $n>0$ folgt, daß l eindeutig bestimmt ist durch die Bedingung

$$l\in\mathbb{N}\ \text{und}\ f_q(l-1)<n\leq f_q(l).$$

□

5.2.3 Asymptotisches Verhalten der auflösbaren Länge von G_n

Nach Korollar 5.2.2.3 erhält man für die auflösbare Länge l von G_n die Bedingung

$$\frac{2^l}{3} - \frac{1}{2} - \frac{(-1)^{l-1}}{6} < n \leq \frac{2^{l+1}}{3} - \frac{1}{2} - \frac{(-1)^l}{6}.$$

Das ist äquivalent zu

$$\frac{1}{3} + \frac{1}{2^l}\left(-\frac{1}{2} - \frac{(-1)^{l-1}}{6}\right) < \frac{n}{2^l} \leq \frac{2}{3} + \frac{1}{2^l}\left(-\frac{1}{2} - \frac{(-1)^l}{6}\right).$$

Für $n \longrightarrow \infty$ muß nun auch $l \longrightarrow \infty$ gehen. Wegen

$$\lim_{l\to\infty} \frac{1}{2^l}\left(-\frac{1}{2} - \frac{(-1)^{l-1}}{6}\right) = \lim_{l\to\infty} \frac{1}{2^l}\left(-\frac{1}{2} - \frac{(-1)^l}{6}\right) = 0$$

läßt sich der Zusammenhang zwischen n und l für „große“ n näherungsweise durch die Beziehung $\frac{1}{3} < \frac{n}{2^l} \leq \frac{2}{3}$ beschreiben, was äquivalent ist zu $2^l < 3n \leq 2^{l+1}$. Die Ausnutzung der Monotonie der Logarithmusfunktion liefert $\ln(2)l < \ln(3n) \leq \ln(2)(l+1)$ bzw. $l < \frac{\ln(3n)}{\ln(2)} \leq l+1$. Damit erhält man für l näherungsweise

$$l = \left[\frac{\ln(3n)}{\ln(2)}\right].$$

Kapitel 6

Die höheren Kommutatorrelationen im Fall q gerade

Um für den Fall, daß q gerade ist, die abgeleitete Reihe bzw. die absteigende Zentralreihe von U_n bestimmen zu können, ist es notwendig, die Eigenschaften von speziellen Untergruppen von $[U, U]$, die dafür in Frage kommen, zu untersuchen und auf möglichst einfache Weise zu charakterisieren. Dazu wird im ersten Abschnitt der Begriff der „Gutartigkeit“ eingeführt. Im 2. Abschnitt werden dann die Kommutatorrelationen gutartiger Untergruppen von $[U, U]$ bestimmt, um dann im 3. Abschnitt die abgeleitete Reihe bzw. die absteigende Zentralreihe von U_n zu charakterisieren. Dabei sei für das ganze Kapitel vereinbart, daß q gerade ist.

6.1 Definition und Eigenschaften gutartiger Untergruppen von $[U, U]$

Um bestimmte Untergruppen von $[U, U]$ charakterisieren zu können, wird zunächst eine Charakterisierung von Elementen von $U_1 \supset [U, U]$ benötigt.

Definition 6.1.1 *Sei* $x = 1 + \sum\limits_{i=1}^{\infty} a_i \tau^i \in U_1$. *Dann bezeichne*

(i) $R(x) := \begin{cases} \infty & \text{falls } a_i = 0 \text{ für alle ungeraden } i \in \mathbb{N} \\ \min\{i \in \mathbb{N} \mid i \text{ ungerade und } a_i \neq 0\} & \text{sonst} \end{cases}$

(ii) $S(x) := \begin{cases} \infty & \text{falls } a_i = 0 \text{ für alle geraden } i \in \mathbb{N} \\ \min\{i \in \mathbb{N} \mid i \text{ gerade und } a_i \neq 0\} & \text{sonst} \end{cases}$

(iii) $T(x) := \begin{cases} \infty & \text{falls } a_i \in \mathbb{F}_q \text{ für alle geraden } i \in \mathbb{N} \\ \min\{i \in \mathbb{N} \mid i \text{ gerade und } a_i \notin \mathbb{F}_q\} & \text{sonst} \end{cases}$

Der Sinn dieser Definition läßt sich besser verstehen, wenn man die Graduierung von $Q = Q_0 \bigoplus Q_1$ betrachtet und $x \in U_1$ in die entsprechenden Anteile zerlegt. Dazu sei $\tau^\infty := 0$.

Bemerkung 6.1.2 Sei $x = 1 + \sum_{i=1}^{\infty} a_i \tau^i \in U_1$. Für die Zerlegung von $x = x_0 + x_1$ mit $x_0 = 1 + \sum\limits_{i=2}^{\infty}{}'' a_i \tau^i \in Q_0$ und $x_1 = \sum\limits_{i=1}^{\infty}{}' a_i \tau^i \in Q_1$ erhält man folgende Aussagen:

(i) Es gilt $R(x) = \max\{R \in \mathbb{N} \mid x_1 \equiv 0 \mod (\tau^R)\}$. Das bedeutet daß $R(x)$ die Bewertung von x_1 angibt.

(ii) Es gilt $S(x) = \max\{S \in \mathbb{N} \mid x_0 \equiv 1 \mod (\tau^S)\}$. Das bedeutet daß $S(x)$ die Bewertung von $x_0 - 1$ angibt.

(iii) Es gilt $T(x) = \max\{T \in \mathbb{N} \mid \exists y \in L \cap U \ \mathit{mit}\ y \equiv x_0 \mod (\tau^T)\}$. Das bedeutet, daß $T(x)$ den „Abstand, den x_0 vom Zentrum L hat“ angibt.

Elemente von U_1 lassen sich in folgender Weise „abschätzen“.

Bemerkung 6.1.3 Sei $x = 1 + \sum_{i=1}^{\infty} a_i \tau^i \in U_1$ mit $x \neq 1$. Dann gilt

$$\max\{i \in \mathbb{N} \mid x \in U_i\} = \min\{i \in \mathbb{N} \mid a_i \neq 0\} = \min\{R(x), S(x)\}.$$

Die Definition 6.1.1 läßt sich nun in folgender Weise auf Untergruppen von U_1 übertragen.

Definition 6.1.4 *Sei $\mathfrak{U}$ eine Untergruppe von U_1. Dann heißt*

(i) $R(\mathfrak{U}) = \min\{R(x) \mid x \in \mathfrak{U}\}$ *der* ungerade Charakterisierungsindex von $\mathfrak{U}$,

(ii) $S(\mathfrak{U}) = \min\{S(x) \mid x \in \mathfrak{U}\}$ *der* gerade Charakterisierungsindex von $\mathfrak{U}$ *und*

(iii) $T(\mathfrak{U}) = \min\{T(x) \mid x \in \mathfrak{U}\}$ *der* Verzögerungsindex von $\mathfrak{U}$.

Für spätere Anwendungen ist das folgende Lemma von Bedeutung.

Lemma 6.1.5 *Sei $\mathfrak{U} \leq U_1$. Dann gilt* $\min\{R(\mathfrak{U}), S(\mathfrak{U})\} = \max\{i \in \mathbb{N} \mid \mathfrak{U} \subset U_i\}$.

Beweis: Für alle $x \in \mathfrak{U}$ gilt $\max\{i \in \mathbb{N} \mid x \in U_i\} = \min\{R(x), S(x)\} \geq \min\{R(\mathfrak{U}), S(\mathfrak{U})\}$. Daraus folgt $\max\{i \in \mathbb{N} \mid \mathfrak{U} \subset U_i\} \geq \min\{R(\mathfrak{U}), S(\mathfrak{U})\}$. Andererseits gibt es ein $x \in \mathfrak{U}$ mit $\min\{R(x), S(x)\} = \min\{R(\mathfrak{U}), S(\mathfrak{U})\}$. Daraus folgt $\min\{R(\mathfrak{U}), S(\mathfrak{U})\} = \max\{i \in \mathbb{N} \mid x \in U_i\} \geq \max\{i \in \mathbb{N} \mid \mathfrak{U} \subset U_i\}$. Damit folgt die Aussage des Lemmas. □

Es geht nun darum, eine Teilmenge der Menge aller Untergruppen von $[U, U]$ zu finden, die sowohl die abgeleitete Reihe als auch die absteigende Zentralreihe aller U_n umfaßt. In dieser Menge müssen nun alle E_m mit $m \in \mathbb{N}$ enthalten sein. Deshalb ist es von Interesse, die E_m zu charakterisieren.

Lemma 6.1.6 *Seien $n, m \in \mathbb{N}$. Dann gilt*

$$F_n(E_m) = \begin{cases} \{0\} & \textit{falls } n < m \\ \mathbb{F}_q & \textit{falls } n \geq m \textit{ und } n \textit{ gerade} \\ \mathbb{F}_{q^2} & \textit{falls } n \geq m \textit{ und } n \textit{ ungerade.} \end{cases}$$

Beweis: Dieses Lemma ist ein Spezialfall von Lemma 4.4.1. Es ist lediglich zu beachten, daß wegen $\mathrm{char}(\mathbb{F}_{q^2}) = 2$ das Element $\alpha - \alpha^q = \alpha + \alpha^q$ in $\mathbb{F}_q$ liegt. Damit folgt $(\alpha - \alpha^q)\mathbb{F}_q = \mathbb{F}_q$. □

Es ist nun naheliegend, eine Menge von Untergruppen von $[U, U]$ zu definieren, deren Koeffizientenvariationen sich ähnlich verhalten wie die von E_n. Man betrachte dazu die Untergruppen von $[U, U]$, deren n-te Koeffizientenvariation für kleine n verschwindet und für große gerade n den Wert $\mathbb{F}_{q^2}$ sowie für große ungerade n den Wert $\mathbb{F}_q$ annimmt, wobei es jeweils einen scharfen Übergang geben soll. Die geschieht durch die folgende Definition.

Definition 6.1.7 *Sei $\mathfrak{U}$ einen Untergruppe von $[U, U]$. Dann heißt $\mathfrak{U}$ gutartig, wenn die folgenden 3 Bedingungen erfüllt sind.*

(i) $R(\mathfrak{U}), S(\mathfrak{U}) < \infty$.

(ii) *Für alle ungeraden* $n \in \mathbb{N}$ *mit* $n \geq R(\mathfrak{U})$ *gilt* $F_n(\mathfrak{U}) = \mathbb{F}_{q^2}$.

(iii) *Für alle geraden* $n \in \mathbb{N}$ *mit* $n \geq S(\mathfrak{U})$ *gilt* $F_n(\mathfrak{U}) = \mathbb{F}_q$.

Wie sinnvoll diese Definition ist, hängt zum einen davon ab, ob es genügend viele gutartige Untergruppen von $[U, U]$ gibt, zum anderen davon, ob durch die Angabe von $R(\mathfrak{U})$ und $S(\mathfrak{U})$ eine gutartige Untergruppe $\mathfrak{U}$ von $[U, U]$ hinreichend genau beschrieben wird. Im folgenden wird zunächst die Frage nach der Existenz von gutartigen Untergruppen von $[U, U]$ behandelt. Ein Kriterium für Gutartigkeit stellt das folgende Lemma dar.

Lemma 6.1.8 *Sei* $\mathfrak{U}$ *eine Untergruppe von* $[U, U]$ *und seien* R, S *natürliche Zahlen, wobei* R *ungerade und* S *gerade ist, so daß die folgenden Bedingungen erfüllt sind:*

(i) *Für alle* $x \in \mathfrak{U}$ *gilt* $R(x) \geq R$ *und* $S(x) \geq S$.

(ii) *Für alle ungeraden* $n \in \mathbb{N}$ *mit* $n \geq R$ *gilt* $F_n(\mathfrak{U}) = \mathbb{F}_{q^2}$.

(iii) *Für alle geraden* $n \in \mathbb{N}$ *mit* $n \geq S$ *gilt* $F_n(\mathfrak{U}) \supset \mathbb{F}_q$.

Dann ist $\mathfrak{U}$ *gutartig mit* $R(\mathfrak{U}) = R$ *und* $S(\mathfrak{U}) = S$.

Beweis: Aus (i) folgt $R(\mathfrak{U}) \geq R$ und $S(\mathfrak{U}) \geq S$. Wegen (ii) gilt $F_R(\mathfrak{U}) = \mathbb{F}_{q^2}$. Also muß es ein $x \in \mathfrak{U}$ geben mit $x \equiv 1 + \tau^R \mod U_{R+1}$. Daraus folgt $R(x) = R = R(\mathfrak{U}) < \infty$. Wegen (iii) gilt $F_R(\mathfrak{U}) \supset \mathbb{F}_q$. Also muß es ein $y \in \mathfrak{U}$ geben mit $y \equiv 1 + \tau^S \mod U_{S+1}$. Daraus folgt $S(y) = S = S(\mathfrak{U}) < \infty$. Damit ist die Voraussetzung (i) von Definition 6.1.7 erfüllt. Da (ii) mit Voraussetzung (ii) von Definition 6.1.7 identisch ist, bleibt nur noch Bedingung (iii) zu prüfen. Sei dazu $n \in \mathbb{N}$ mit $n \geq S$. Dann gilt $F_n(\mathfrak{U}) \supset \mathbb{F}_q$ nach (iii). Wegen $\mathfrak{U} \leq [U, U]$ muß auch $F_n(\mathfrak{U}) \subset \mathbb{F}_q$ gelten. Damit ist die Aussage des Lemmas gezeigt. $\square$

Beispiel 6.1.9 *Sei* $m \in \mathbb{N}$. *Dann ist* E_m *gutartig mit*

$$R(E_m) = \begin{cases} m+1 & \textit{falls } m \textit{ gerade} \\ m & \textit{falls } m \textit{ ungerade} \end{cases}$$

und

$$S(E_m) = \begin{cases} m & \textit{falls } m \textit{ gerade} \\ m+1 & \textit{falls } m \textit{ ungerade.} \end{cases}$$

Beweis: Offensichtlich ist E_m eine Untergruppe von $[U, U] = E_1$. Man setze nun

$$R := \left\{ \begin{array}{ll} m+1 & \text{falls } m \text{ gerade} \\ m & \text{falls } m \text{ ungerade} \end{array} \right\} \text{ und } S := \left\{ \begin{array}{ll} m & \text{falls } m \text{ gerade} \\ m+1 & \text{falls } m \text{ ungerade} \end{array} \right\}.$$

Dann ist R ungerade und S gerade. Für alle $x \in E_m \subset U_m$ gilt nun $R(x) \geq R$ und $S(x) \geq S$. Weiter gilt $F_n(E_m) = \mathbb{F}_{q^2}$ für alle ungeraden $n \in \mathbb{N}$ mit $n \geq R \geq m$ und $F_n(E_m) = \mathbb{F}_q$ für alle geraden $n \in \mathbb{N}$ mit $n \geq S \geq m$ (vgl. Lemma 6.1.6). Mit Lemma 6.1.8 folgt nun, daß E_m gutartig ist mit $R(E_m) = R$ und $S(E_m) = S$, was der Aussage dieses Beispiels entspricht. $\square$

Die folgenden Lemmata werden benötigt, um weitere gutartige Untergruppen von $[U, U]$ zu konstruieren.

Lemma 6.1.10 *Seien* $R, S \in \mathbb{N}$ *mit* $S \leq 2R$ *sowie* R *ungerade und* S *gerade. Dann gelten für alle* $x, y \in U_1$ *mit* $R(x), R(y) \geq R$ *und* $S(x), S(y) \geq S$, *die Bedingungen* $R(xy) \geq R$ *und* $S(xy) \geq S$.

Beweis: Für $x, y \in U_1$ existieren die Zerlegungen $x = x_0 + x_1$ bzw. $y = y_0 + y_1$ mit $x_0, y_0 \in Q_0$ und $x_1, y_1 \in Q_1$. Daraus folgt $xy = (x_0 + x_1)(y_0 + y_1) = x_0y_0 + x_1y_0 + x_0y_1 + x_1y_1 = z_1 + z_2$, wobei $z_0 := x_0y_0 + x_1y_1 \in Q_0$ und $z_1 := x_0y_1 + x_1y_0 \in Q_1$ gilt. Mit Bemerkung 6.1.2 erhält man nun die Kongruenzen

$$x_0, y_0 \equiv 1 \mod (\tau^S) \text{ sowie } x_1, y_1 \equiv 0 \mod (\tau^R).$$

Daraus folgt zum einen $x_0y_1, x_1y_0 \equiv 0 \mod (\tau^R)$ und damit $z_1 \equiv 0 \mod (\tau^R)$. Zum anderen gilt $x_0y_0 \equiv 1 \mod (\tau^S)$ sowie $x_1y_1 \equiv 0 \mod (\tau^{2R})$, woraus wegen $2R \geq S$ die Kongruenz $z_0 \equiv 1 \mod (\tau^R)$ folgt. Damit erhält man $R(xy) \geq R$ und $S(xy) \geq S$. □

Lemma 6.1.11 *Sei $x \in [U, U]$. Dann gilt $R(x^{-1}) = R(x)$ und $S(x^{-1}) = S(x)$.*

Beweis: Sei $x = 1 + \sum_{i=1}^{\infty} a_i\tau^i \in [U, U]$. Dann gilt $x^{-1} = \overline{x} = 1 + \sum_{i=1}^{\infty} a_i^{q^{i+1}} \tau^i$ nach Lemma 1.2.3.2. Da für alle $i \in \mathbb{N}$ die Bedingungen $a_i = 0$ und $a_i^{q^{i+1}} = 0$ äquivalent sind, folgt sofort $R(x^{-1}) = R(x)$ und $S(x^{-1}) = S(x)$. □

Damit läßt sich nun die Frage klären, für welche $R, S \in \mathbb{N}$ mit R ungerade und S gerade es eine gutartige Untergruppe $\mathfrak{U}$ von $[U, U]$ gibt, so daß $R(\mathfrak{U}) = R$ und $S(\mathfrak{U}) = S$ gilt.

Lemma 6.1.12 *Sei $\mathfrak{U} \leq [U, U]$ gutartig. Dann gilt $S(\mathfrak{U}) \leq 2R(\mathfrak{U})$.*

Beweis: Man setze $n := R(\mathfrak{U})$. Wegen $F_n(\mathfrak{U}) = \mathbb{F}_{q^2}$ gibt es ein $x \in \mathfrak{U}$ mit $x \equiv 1 + \tau^n \mod U_{n+1}$. Weiter existieren nun $a_{n+1}, a_{n+2}, \ldots, a_{2n} \in \mathbb{F}_{q^2}$ mit $x \equiv 1 + \tau^n + \sum_{i=n+1}^{2n} a_i\tau^i \mod U_{2n+1}$. Daraus folgt

$$\begin{aligned} x^2 &\equiv \left(1 + \tau^n + \sum_{i=n+1}^{2n} a_i\tau^i\right)\left(1 + \tau^n + \sum_{i=n+1}^{2n} a_i\tau^i\right) \mod U_{2n+1} \\ &\equiv 1 + \tau^n + \sum_{i=n+1}^{2n} a_i\tau^i + \tau^n + \tau^{2n} + \sum_{i=n+1}^{2n} a_i\tau^i \mod U_{2n+1} \\ &\equiv 1 + \tau^{2n} \mod U_{2n+1}. \end{aligned}$$

Also ist $S(x^2) = 2n$. Folglich gilt $S(\mathfrak{U}) \leq 2n = 2R(\mathfrak{U})$. □

Lemma 6.1.13 *Sei $\mathfrak{U} \leq [U, U]$ gutartig. Dann gilt für den Verzögerungsindex*

$$T(\mathfrak{U}) = \min\{2R(\mathfrak{U}), 2S(\mathfrak{U})\}.$$

Beweis: Man verwendet die Abkürzung $T := \min\{2R(\mathfrak{U}), 2S(\mathfrak{U})\}$ und zeigt $T(\mathfrak{U}) = T$.

Sei $x = 1 + \sum_{i=1}^{\infty} a_i\tau^i \in \mathfrak{U}$ beliebig. Man setze $m := \frac{1}{2}T - 1$. Dann gilt $m < R(\mathfrak{U}), S(\mathfrak{U})$ und damit $a_1, a_2, \ldots, a_m = 0$. Für alle $n \in \{2, 4, \ldots, T-2\}$ folgt nun wegen $\frac{1}{2}n \leq m$ nach Korollar 4.3.9 die Gleichung

$$a_n + a_n^q = \sum_{k=1}^{n-1} a_k a_{n-k}^q = \sum_{k=1}^{\frac{1}{2}n} \underbrace{a_k}_{=0} a_{n-k}^q + \sum_{k=\frac{1}{2}n+1}^{n-1} a_k \underbrace{a_{n-k}^q}_{=0} = 0.$$

Damit ergibt sich $a_n = a_n^q$ bzw. $a_n \in \mathbb{F}_q$. Also gilt $T(x) \geq T$. Da $x \in \mathfrak{U}$ beliebig gewählt war, erhält man $T(\mathfrak{U}) \geq T$.

Wegen $F_{\frac{1}{2}T}(\mathfrak{U}) \supset \mathbb{F}_q$ muß es ein $x \in \mathfrak{U}$ geben mit $x \equiv 1 + \tau^{\frac{1}{2}T} \mod U_{\frac{1}{2}T+1}$. Das heißt, x ist von der Form $x = 1 + \sum_{i=1}^{\infty} a_i\tau^i$ mit $a_1, a_2, \ldots, a_{\frac{1}{2}T-1} = 0$ und $a_{\frac{1}{2}T} = 1$. Nach Korollar 4.3.9 folgt nun

$$a_T + a_T^q = \sum_{k=1}^{T-1} a_k a_{T-k}^q = \sum_{k=1}^{\frac{1}{2}T-1} \underbrace{a_k}_{=0} a_{T-k}^q + a_{\frac{1}{2}T} a_{\frac{1}{2}T}^q + \sum_{k=\frac{1}{2}T+1}^{T-1} a_k \underbrace{a_{T-k}^q}_{=0} = 1 \neq 0.$$

Damit ergibt sich $a_T \neq a_T^q$ bzw. $a_T \notin \mathbb{F}_q$. Also gilt $T(x) \leq T$ und damit $T(\mathfrak{U}) \leq T$. □

Satz 6.1.14 *Sei $\mathfrak{U} \leq [U, U]$ gutartig. Dann gilt:*

(i) Es gibt eine gutartige Untergruppe $\tilde{\mathfrak{U}}$ von $\mathfrak{U}$ mit $S(\tilde{\mathfrak{U}}) = S(\mathfrak{U})$ und $R(\tilde{\mathfrak{U}}) = R(\mathfrak{U}) + 2$.

(ii) Falls $S(\mathfrak{U}) + 2 \leq 2R(\mathfrak{U})$ ist, gibt es eine gutartige Untergruppe $\tilde{\mathfrak{U}}$ von $\mathfrak{U}$ mit $S(\tilde{\mathfrak{U}}) = S(\mathfrak{U}) + 2$ und $R(\tilde{\mathfrak{U}}) = R(\mathfrak{U})$.

Beweis: (i) Man setze $\tilde{\mathfrak{U}} := \{x \in \mathfrak{U} \mid R(x) \geq R(\mathfrak{U}) + 2\}$. Wegen $R(1) = \infty > R(\mathfrak{U}) + 2$ folgt $1 \in \tilde{\mathfrak{U}}$. Seien $x, y \in \tilde{\mathfrak{U}} \subset \mathfrak{U}$. Dann gilt $x^{-1}, xy \in \mathfrak{U}$. Wegen $R(x^{-1}) = R(x) \geq R(\mathfrak{U}) + 2$ nach Lemma 6.1.11, folgt $x^{-1} \in \tilde{\mathfrak{U}}$. Weiter gilt $2(R(\mathfrak{U}) + 2) > 2R(\mathfrak{U}) \geq S(\mathfrak{U})$ nach Lemma 6.1.12. Mit Lemma 6.1.10 ergibt sich daraus $R(xy) \geq R(\mathfrak{U}) + 2$. Also gilt auch $xy \in \tilde{\mathfrak{U}}$. Somit ist gezeigt, daß $\tilde{\mathfrak{U}}$ eine Untergruppe von $\mathfrak{U}$ ist.

Um nun die Gutartigkeit von $\tilde{\mathfrak{U}}$ zu zeigen, prüft man die Voraussetzungen von Lemma 6.1.8. Offensichtlich ist $\tilde{\mathfrak{U}}$ eine Untergruppe von $[U, U]$. Außerdem sind für alle $x \in \tilde{\mathfrak{U}}$ die Bedingungen $R(x) \geq R(\mathfrak{U}) + 2$ und $S(x) \geq S(\mathfrak{U})$ erfüllt, wobei $R(\mathfrak{U}) + 2$ ungerade und $S(\mathfrak{U})$ gerade ist. Sei nun $n \in \mathbb{N}$ mit n ungerade und $n \geq R(\mathfrak{U}) + 2$. Dann gibt es für alle $a \in \mathbb{F}_{q^2} = F_n(\mathfrak{U})$ ein $x \in \mathfrak{U}$ mit $x \equiv 1 + a\tau^n \mod U_{n+1}$. Daraus folgt $R(x) \geq n \geq R(\mathfrak{U}) + 2$ bzw. $x \in \tilde{\mathfrak{U}}$. Somit gilt $a \in F_n(\tilde{\mathfrak{U}})$. Damit ist $F_n(\tilde{\mathfrak{U}}) = \mathbb{F}_{q^2}$ gezeigt. Sei nun $n \in \mathbb{N}$ mit n gerade und $n \geq S(\mathfrak{U}) + 2$. Dann gibt es für alle $a_n \in \mathbb{F}_q = F_n(\mathfrak{U})$ ein $x \in \mathfrak{U}$ mit $x \equiv 1 + a_n\tau^n \mod U_{n+1}$. Falls $R(x) > R(\mathfrak{U})$ gilt, folgt $x \in \tilde{\mathfrak{U}}$ und damit $a_n \in F_n(\tilde{\mathfrak{U}})$. Man betrachte nun den Fall, daß $R(x) = R(\mathfrak{U})$ ist. Dann hat x die Form

$$x = 1 + \sum_{i=n}^{\infty}{}'' a_i\tau^i + \sum_{i=R(\mathfrak{U})}^{\infty}{}' a_i\tau^i,$$

wobei $R(\mathfrak{U}) \geq n+1$ gelten muß. Für $a_{R(\mathfrak{U})} \in \mathbb{F}_{q^2}$ gibt es nun ein $y \in \mathfrak{U}$, das die Kongruenzbedingung $y \equiv 1 + a_{R(\mathfrak{U})}\tau^{R(\mathfrak{U})} \mod U_{R(\mathfrak{U})+1}$ erfüllt. Damit erhält man

$$yx \equiv 1 + \sum_{i=n}^{R(\mathfrak{U})+1}{}'' a_i\tau^i \mod U_{R(\mathfrak{U})+2} \equiv 1 + a_n\tau^n \mod U_{n+1}.$$

Daraus folgt $R(yx) \geq R(\mathfrak{U}) + 2$ bzw. $yx \in \tilde{\mathfrak{U}}$. Somit ist $a_n \in F_n(\tilde{\mathfrak{U}})$. Damit ist $F_n(\tilde{\mathfrak{U}}) \supset \mathbb{F}_q$ gezeigt.

(ii) Man setze $\tilde{\mathfrak{U}} := \{x \in \mathfrak{U} \mid S(x) \geq S(\mathfrak{U}) + 2\}$. Wegen $S(1) = \infty > S(\mathfrak{U}) + 2$ folgt $1 \in \tilde{\mathfrak{U}}$. Seien $x, y \in \tilde{\mathfrak{U}} \subset \mathfrak{U}$ Dann gilt $x^{-1}, xy \in \mathfrak{U}$. Wegen $S(x^{-1}) = S(x) \geq S(\mathfrak{U}) + 2$ nach Lemma 6.1.11, folgt $x^{-1} \in \tilde{\mathfrak{U}}$. Da nach Voraussetzung $2R(\mathfrak{U}) \geq S(\mathfrak{U}) + 2$ ist, folgt $S(xy) \geq S(\mathfrak{U}) + 2$ nach Lemma 6.1.10. Also gilt auch $xy \in \tilde{\mathfrak{U}}$. Somit ist gezeigt, daß $\tilde{\mathfrak{U}}$ eine Untergruppe von $\mathfrak{U}$ ist.

Um nun die Gutartigkeit von $\tilde{\mathfrak{U}}$ zu zeigen, prüft man wieder die Voraussetzungen von Lemma 6.1.8. Offensichtlich ist $\tilde{\mathfrak{U}}$ eine Untergruppe von $[U, U]$. Außerdem sind für alle $x \in \tilde{\mathfrak{U}}$ die Bedingungen $R(x) \geq R(\mathfrak{U})$ und $S(x) \geq S(\mathfrak{U}) + 2$ erfüllt, wobei $R(\mathfrak{U})$ ungerade und $S(\mathfrak{U}) + 2$ gerade ist. Sei nun $n \in \mathbb{N}$ mit n ungerade und $n \geq R(\mathfrak{U})$. Dann gibt es für alle $a_n \in \mathbb{F}_{q^2} = F_n(\mathfrak{U})$ ein $x \in \mathfrak{U}$ mit $x \equiv 1 + a_n\tau^n \mod U_{n+1}$. Falls $S(x) > S(\mathfrak{U})$ gilt, folgt $x \in \tilde{\mathfrak{U}}$ und damit $a_n \in F_n(\tilde{\mathfrak{U}})$. Man betrachte nun den Fall, daß $S(x) = S(\mathfrak{U})$ ist. Dann hat x die Form

$$x = 1 + \sum_{i=S(\mathfrak{U})}^{\infty}{}'' a_i\tau^i + \sum_{i=n}^{\infty}{}' a_i\tau^i,$$

wobei $S(\mathfrak{U}) \geq n + 1$ gelten muß. Wegen der Voraussetzung $2R(\mathfrak{U}) \geq S(\mathfrak{U}) + 2$ folgt nach Lemma 6.1.13, daß $T(x) \geq T(\mathfrak{U}) = \min\{2R(\mathfrak{U}), 2S(\mathfrak{U})\} \geq S(\mathfrak{U})$ ist. Somit gilt $a_{S(\mathfrak{U})} \in \mathbb{F}_q = F_{S(\mathfrak{U})}(\mathfrak{U})$. Also gibt es ein $y \in \mathfrak{U}$ mit $y \equiv 1 + a_{S(\mathfrak{U})}\tau^{S(\mathfrak{U})} \mod U_{S(\mathfrak{U})+1}$. Damit erhält man

$$yx \equiv 1 + \sum_{i=n}^{S(\mathfrak{U})+1}{}' a_i\tau^i \mod U_{S(\mathfrak{U})+2} \equiv 1 + a_n\tau^n \mod U_{n+1}.$$

Daraus folgt $S(yx) \geq S(\mathfrak{U})+2$ bzw. $yx \in \tilde{\mathfrak{U}}$. Somit gilt $a_n \in F_n(\tilde{\mathfrak{U}})$. Damit ist $F_n(\tilde{\mathfrak{U}}) = \mathbb{F}_{q^2}$ gezeigt. Sei nun $n \in \mathbb{N}$ mit n gerade und $n \geq S(\mathfrak{U}) + 2$. Dann gibt es für alle $a \in \mathbb{F}_q = F_n(\mathfrak{U})$ ein $x \in \mathfrak{U}$ mit $x \equiv 1 + a\tau^n \mod U_{n+1}$. Daraus folgt $S(x) \geq n \geq S(\mathfrak{U}) + 2$ bzw. $x \in \tilde{\mathfrak{U}}$. Somit gilt $a \in F_n(\tilde{\mathfrak{U}})$. Damit ist $F_n(\tilde{\mathfrak{U}}) \supset \mathbb{F}_q$ gezeigt. □

Korollar 6.1.15 *Seien $R, S \in \mathbb{N}$ mit R ungerade und S gerade. Eine gutartige Untergruppe $\mathfrak{U}_{R,S}$ von $[U,U]$ mit $R(\mathfrak{U}_{R,S}) = R$ und $S(\mathfrak{U}_{R,S}) = S$ existiert genau dann, wenn $S \leq 2R$ ist.*

Beweis: Daß es für den Fall $S > 2R$ keine gutartige Untergruppe $\mathfrak{U}_{R,S}$ von $[U,U]$ gibt mit $R(\mathfrak{U}_{R,S}) = R$ und $S(\mathfrak{U}_{R,S}) = S$, folgt aus Lemma 6.1.12. Die umgekehrte Richtung, daß es für alle ungeraden $R \in \mathbb{N}$ und alle geraden $S \in \mathbb{N}$ mit $S \leq R$ eine gutartige Untergruppe $\mathfrak{U}_{R,S}$ von $[U,U]$ mit $R(\mathfrak{U}_{R,S}) = R$ und $S(\mathfrak{U}_{R,S}) = S$ gibt, zeigt man durch Induktion über alle ungeraden $R \in \mathbb{N}$.

Induktionsanfang $R = 1$: Sei $S \in \mathbb{N}$ mit S gerade und $S \leq R$. Dann folgt $S = 2$. Man setze $\mathfrak{U}_{1,2} := E_1$. Dann ist gilt $\mathfrak{U}_{1,2}$ gutartig, und es gilt $R(\mathfrak{U}_{1,2}) = 1$ sowie $S(\mathfrak{U}_{1,2}) = 2$ (vgl. Beispiel 6.1.9).

Induktionsschritt $R \longrightarrow R + 2$: Nach Induktionsannahme gibt es für alle geraden $S \in \mathbb{N}$ mit $S \leq 2R$ eine gutartige Untergruppe $\mathfrak{U}_{R,S}$ von $[U,U]$ mit $R(\mathfrak{U}_{R,S}) = R$ und $S(\mathfrak{U}_{R,S}) = S$. Nach Satz 6.1.14(i) gibt es nun für alle geraden $S \in \mathbb{N}$ mit $S \geq 2R$ eine gutartige Untergruppe $\mathfrak{U}_{R,S}$ von $\mathfrak{U}_{R+2,S}$ mit $R(\mathfrak{U}_{R+2,S}) = R+2$ und $S(\mathfrak{U}_{R+2,S}) = S$. Wegen $2R+2, 2R+4 \leq 2(R+2)$ liefert die Anwendung von Satz 6.1.14(ii) die Existenz von gutartigen Untergruppen $\mathfrak{U}_{R+2,2R+4} \leq \mathfrak{U}_{R+2,2R+2} \leq \mathfrak{U}_{R+2,2R}$ mit $R(\mathfrak{U}_{R+2,2R+2}) = R + 2$ und $S(\mathfrak{U}_{R+2,2R+2}) = 2R + 2$ sowie $R(\mathfrak{U}_{R+2,2R+4}) = R + 2$ und $S(\mathfrak{U}_{R+2,2R+4}) = 2R + 4$. Da für alle geraden $S \in \mathbb{N}$ mit $S \leq 2(R + 2)$ entweder $S \leq 2R$ oder $S = 2R + 2$ oder $S = 2R + 4$ gilt, folgt damit die Aussage des Korollares. □

Für spätere Anwendungen ist noch der folgende Sachverhalt von Bedeutung.

Korollar 6.1.16 *Sei $\mathfrak{U} \leq [U,U]$ gutartig und $n \in \mathbb{N}_0$. Dann gibt es eine gutartige Untergruppe $\mathfrak{U}_n \leq \mathfrak{U}$ mit $S(\mathfrak{U}_n) = S(\mathfrak{U})$ und $R(\mathfrak{U}_n) = R(\mathfrak{U}) + 2n$.*

Beweis: Der Beweis erfolgt durch Induktion über alle $n \in \mathbb{N}_0$. Für $n = 0$ setze man $\mathfrak{U}_0 = \mathfrak{U}$. Damit wird die Aussage trivial. Sei nun $n \in \mathbb{N}_0$. Dann gibt es nach Induktionsannahme eine gutartige Untergruppe $\mathfrak{U}_n \leq \mathfrak{U}$ mit $S(\mathfrak{U}) = S(\mathfrak{U})$ und $R(\mathfrak{U}) = R(\mathfrak{U}) + 2n$. Nach Satz 6.1.14(i) folgt die Existenz einer gutartigen Untergruppe $\mathfrak{U}_{n+1} \leq \mathfrak{U}_n \leq \mathfrak{U}$ mit $S(\mathfrak{U}_{n+1}) = S(\mathfrak{U})$ und $R(\mathfrak{U}_{n+1}) = R(\mathfrak{U}_n) + 2 = R(\mathfrak{U}) + 2(n-1)$. □

Im folgenden wird nun die Frage behandelt, wie genau eine gutartige Untergruppe $\mathfrak{U}$ von $[U,U]$ durch ihre Charakterisierungsindizes beschrieben wird.

Definition 6.1.17 *Sei $\mathfrak{U}$ eine Untergruppe von U_1 und $n \in \mathbb{N}$. Dann sei*

$$\mathfrak{U}^{(n)} := \{x \in U_1 \mid \exists y \in \mathfrak{U} \textit{ mit } x \equiv y \mod U_{n+1}\}.$$

Lemma 6.1.18 *(i) Für alle $n \in \mathbb{N}$ gilt $\mathfrak{U}^{(n)} = \mathfrak{U} \cdot U_{n+1}$.*

(ii) Es gilt $\overline{\mathfrak{U}} = \bigcap_{n \in \mathbb{N}} \mathfrak{U}^{(n)}$, wobei $\overline{\mathfrak{U}}$ der topologische Abschluß von $\mathfrak{U}$ ist.

Beweis: (i) Für alle $x_1, x_2 \in \mathfrak{U}^{(n)}$ gibt es nun Elemente $y_1, y_2 \in \mathfrak{U}$ mit $x_1 \equiv y_1 \mod U_{n+1}$ und $x_2 \equiv y_2 \mod U_{n+1}$. Daraus folgt $x_1 x_2^{-1} \equiv y_1 y_2^{-1} \mod U_{n+1}$ und damit $x_1 x_2^{-1} \in \mathfrak{U}^{(n)}$. Wegen $\mathfrak{U}^{(n)} \neq \emptyset$ folgt, daß $\mathfrak{U}^{(n)}$ eine Untergruppe von U_1 ist. Da nun für alle $x \in \mathfrak{U}$ und $y \in U_{n+1}$ das Element xy in $\mathfrak{U}^{(n)}$ liegt, muß $\mathfrak{U} \cdot U_{n+1}$ einen Untergruppe von $\mathfrak{U}^{(n)}$ sein. Sei nun $x \in \mathfrak{U}^{(n)}$. Dann gibt es ein $y \in \mathfrak{U}$ mit $x \equiv y \mod U_{n+1}$. Daraus folgt $xy^{-1} \in U_{n+1}$ und damit $x \in \mathfrak{U} \cdot U_{n+1}$. Damit ist $\mathfrak{U}^{(n)} = \mathfrak{U} \cdot U_{n+1}$ gezeigt.

(ii) Sei $x \in \overline{\mathfrak{U}}$. Dann gibt es eine konvergente Folge $\{x_n\}_{n\in\mathbb{N}} \subset \mathfrak{U}$ mit $\lim_{n\to\infty} x_n = x$. Für alle $n \in \mathbb{N}$ gibt es nun ein $n \in \mathbb{N}$ mit $x \equiv x_n \mod U_{n+1}$. Damit gilt $x \in \mathfrak{U}^{(n)}$ für alle $n \in \mathbb{N}$. Daraus folgt $x \in \bigcap_{n\in\mathbb{N}} \mathfrak{U}^{(n)}$. Damit ist $\overline{\mathfrak{U}} \subset \bigcap_{n\in\mathbb{N}} \mathfrak{U}^{(n)}$ gezeigt. Sei nun $x \in \bigcap_{n\in\mathbb{N}} \mathfrak{U}^{(n)}$. Dann gilt $x \in \mathfrak{U}^{(n)}$ für alle $n \in \mathbb{N}$. Damit gibt es für alle $n \in \mathbb{N}$ ein $x_n \in \mathfrak{U}$ mit $x \equiv x_n \mod U_{n+1}$. Daraus folgt, daß die Folge $\{x_n\}_{n\in\mathbb{N}} \subset \mathfrak{U}$ konvergent ist mit $\lim_{n\to\infty} x_n = x$. Also gilt $x \in \overline{\mathfrak{U}}$. Damit ist auch $\overline{\mathfrak{U}} \supset \bigcap_{n\in\mathbb{N}} \mathfrak{U}^{(n)}$ gezeigt. □

Satz 6.1.19 *Seien $\mathfrak{U}, \mathfrak{V} \leq [U,U]$ gutartig mit $S(\mathfrak{U}) = S(\mathfrak{V}) = S$ und $R(\mathfrak{U}) = R(\mathfrak{V}) = R$. Dann gilt $\mathfrak{U}^{(n)} = \mathfrak{V}^{(n)}$ für alle $n \in \mathbb{N}$.*

Beweis: Der Beweis erfolgt durch Induktion über alle $n \in \mathbb{N}$.

Für den Induktionsanfang $n = 1$ ist $\mathfrak{U}^{(1)} = \mathfrak{V}^{(1)}$ zu zeigen. Sei dazu $x = 1 + \sum_{i=1}^{\infty} a_i\tau^i \in \mathfrak{U}^{(1)} \subset U_1$. Falls nun $R = 1$ ist, gilt $F_1(\mathfrak{V}) = \mathbb{F}_{q^2}$. Daraus folgt, daß es ein $y \in \mathfrak{V}$ gibt mit $y \equiv 1 + a_1\tau \mod U_2 \equiv x \mod U_2$. Somit gilt $x \in \mathfrak{V}^{(1)}$. Falls $R > 1$ ist, gilt $x \equiv 1 \mod U_2$. Wegen $1 \in \mathfrak{V}$ folgt $x \in \mathfrak{V}^{(1)}$. Damit ist $\mathfrak{U}^{(1)} \subset \mathfrak{V}^{(1)}$ gezeigt. Die andere Inklusion $\mathfrak{U}^{(1)} \supset \mathfrak{V}^{(1)}$ zeigt man analog.

Induktionsschritt $n \longrightarrow n+1$: Nach Induktionsannahme gilt $\mathfrak{U}^{(n)} = \mathfrak{V}^{(n)}$. Zu zeigen ist $\mathfrak{U}^{(n+1)} = \mathfrak{V}^{(n+1)}$. Aus Symmetriegründen reicht es, wenn man dabei die Inklusion in nur einer Richtung beweist.

1. Fall ($n+1$ gerade und $n+1 < S$) oder ($n+1$ ungerade und $n+1 < R$)
Es gilt für alle $y = 1+\sum_{i=1}^{\infty} b_i\tau^i \in \mathfrak{U}$ (bzw. $\mathfrak{V}$), daß $b_{n+1} = 0$ ist. Sei nun $x \in \mathfrak{U}^{(n+1)} \subset \mathfrak{U}^{(n)} = \mathfrak{V}^{(n)}$. Dann gibt es sowohl ein $y_1 \in \mathfrak{U}$ mit $x \equiv y_1 \mod U_{n+2}$ als auch ein $y_2 \in \mathfrak{V}$ mit $x \equiv y_2 \mod U_{n+1}$. Daraus ergibt sich $y_1 \equiv y_2 \mod U_{n+1}$. Da nun sowohl der $n+1$-te Koeffizient von $y_1 \in \mathfrak{U}$ als auch der $n+1$-te Koeffizient von $y_2 \in \mathfrak{V}$ verschwindet, gilt sogar $y_1 \equiv y_2 \mod U_{n+2}$. Daraus folgt $x \equiv y_2 \mod U_{n+2}$ und damit $x \in \mathfrak{U}^{(n+1)}$. Somit gilt $\mathfrak{U}^{(n+1)} \subset \mathfrak{V}^{(n+1)}$.

2. Fall $n+1$ ungerade und $n+1 \geq R$
Es gilt $F_{n+1}(\mathfrak{U}) = F_{n+1}(\mathfrak{V}) = \mathbb{F}_{q^2}$. Sei nun $x \in \mathfrak{U}^{(n+1)} \subset \mathfrak{U}^{(n)} = \mathfrak{V}^{(n)}$. Dann gibt es ein $y \in \mathfrak{V}$ mit $y \equiv x \mod U_{n+1}$ bzw. $xy^{-1} \equiv 1 \mod U_{n+1}$. Das bedeutet, daß es ein $a \in \mathbb{F}_{q^2}$ gibt mit $xy^{-1} \equiv 1 + a\tau^{n+1} \mod U_{n+2}$. Folglich gibt es auch ein $z \in \mathfrak{V}$ mit $xy^{-1} \equiv z \mod U_{n+2}$ bzw. $x \equiv zy \mod U_{n+2}$. Wegen $zy \in \mathfrak{V}$ folgt $x \in \mathfrak{V}^{(n+1)}$. Somit gilt $\mathfrak{U}^{(n+1)} \subset \mathfrak{V}^{(n+1)}$.

3. Fall $n+1$ gerade und $n+1 \geq S$
Es gilt $F_{n+1}(\mathfrak{U}) = F_{n+1}(\mathfrak{V}) = \mathbb{F}_q$. Sei nun $x \in \mathfrak{U}^{(n+1)} \subset \mathfrak{U}^{(n)} = \mathfrak{V}^{(n)}$. Dann gibt es sowohl ein $y_1 \in \mathfrak{U}$ mit $x \equiv y_1 \mod U_{n+2}$ als auch ein $y_2 \in \mathfrak{V}$ mit $x \equiv y_2 \mod U_{n+1}$. Wegen $y_1y_2^{-1} \in [U,U] = E_1$ folgt nach Lemma 6.1.6, daß es ein $a \in \mathbb{F}_q$ gibt mit $xy_2^{-1} \equiv y_1y_2^{-1} \mod U_{n+2} \equiv 1 + a\tau^{n+1} \mod U_{n+2}$. Damit muß es ein $z \in \mathfrak{V}$ geben mit $z \equiv xy_2^{-1} \mod U_{n+2}$ bzw. $x \equiv zy_2 \mod U_{n+2}$. Wegen $zy_2 \in \mathfrak{V}$ folgt $x \in \mathfrak{V}^{(n+1)}$. Somit gilt $\mathfrak{U}^{(n+1)} \subset \mathfrak{V}^{(n+1)}$. □

Zusammen mit Lemma 6.1.18 ergibt sich die folgende Aussage.

Korollar 6.1.20 *Seien $\mathfrak{U}, \mathfrak{V} \leq [U,U]$ gutartig mit $R(\mathfrak{U}) = R(\mathfrak{V})$ und $S(\mathfrak{U}) = S(\mathfrak{V})$. Dann haben $\mathfrak{U}$ und $\mathfrak{V}$ den gleichen topologischen Abschluß.*

Damit ist nun gezeigt, daß eine gutartige Untergruppe von $[U,U]$ durch Angabe ihres geraden und ihres ungeraden Indizes hinreichend gut charakterisiert ist.

Das folgende Lemma gibt Auskunft auf die Frage, wie „dicht" eine gutartige Untergruppe von $[U,U]$ in $[U,U]$ liegt.

Lemma 6.1.21 *Sei $\mathfrak{U} \leq [U,U]$ gutartig und $x \in [U,U]$ mit $S(x) \geq S(\mathfrak{U})$ und $R(x) \geq R(\mathfrak{U})$. Dann gilt $x \in \mathfrak{U}^{(n)}$ für alle $n \in \mathbb{N}$.*

Beweis: Das Element x ist von der Form $x = 1 + \sum_{i=1}^{\infty} a_i\tau^i$, wobei die Anfangskoeffizienten den Bedingungen $a_1, a_3, \ldots, a_{R(\mathfrak{U})-2} = 0$ und $a_2, a_4, \ldots, a_{S(\mathfrak{U})-2} = 0$ genügen.Durch Induktion über n zeigt man nun, daß $x \in \mathfrak{U}^{(n)}$ für alle $n \in \mathbb{N}$ gilt.

Induktionsanfang $n = 1$: Falls $R(\mathfrak{U}) > 1$ ist, gilt $a_1 = 0$ und damit $x \equiv 1 \mod U_2$. Wegen $1 \in \mathfrak{U}$ folgt $x \in \mathfrak{U}^{(1)}$. Falls $R(\mathfrak{U}) = 1$ ist, gilt $F_1(\mathfrak{U}) = \mathbb{F}_{q^2}$. Also gibt es ein $y \in \mathfrak{U}$ mit $y \equiv 1 + a_1\tau \mod U_2 \equiv x \mod U_2$. Daraus folgt $x \in \mathfrak{U}^{(1)}$.

Induktionsschritt $n \longrightarrow n+1$: Nach Induktionsannahme gilt $x \in \mathfrak{U}^{(n)}$. Also gibt es ein $y = 1 + \sum_{i=1}^{\infty} b_i\tau^i \in \mathfrak{U}$ mit $x \equiv y \mod U_{n+1}$.

1. Fall ($n+1$ gerade und $n+1 < S(\mathfrak{U})$) oder ($n+1$ ungerade und $n+1 < R(\mathfrak{U})$): Es gilt $a_{n+1} = 0$. Wegen $y \in \mathfrak{U}$ folgt $b_{n+1} = 0$. Daraus ergibt sich $x \equiv y \mod U_{n+2}$ und damit $x \in \mathfrak{U}^{(n+1)}$.

2. Fall $n+1$ ungerade und $n+1 \geq R(\mathfrak{U})$: Es gilt $F_{n+1}(\mathfrak{U}) = \mathbb{F}_{q^2}$. Außerdem muß es ein $a \in \mathbb{F}_{q^2}$ geben mit $xy^{-1} \equiv 1 + a\tau^{n+1} \mod U_{n+2}$. Daraus folgt, daß es ein $z \in \mathfrak{U}$ gibt mit $z \equiv xy^{-1} \mod U_{n+2}$ bzw. $x \equiv zy \mod U_{n+2}$. Wegen $zy \in \mathfrak{U}$ folgt $x \in \mathfrak{U}^{(n+1)}$.

3. Fall $n+1$ gerade und $n+1 \geq S(\mathfrak{U})$: Es gilt $F_{n+1}(\mathfrak{U}) = \mathbb{F}_q$. Außerdem muß es ein $a \in \mathbb{F}_{q^2}$ geben mit $xy^{-1} \equiv 1 + a\tau^{n+1} \mod U_{n+2}$. Wegen $xy^{-1} \in [U,U] = E_1$ gilt nach Lemma 6.1.6 sogar $a \in \mathbb{F}_q$. Daraus folgt, daß es ein $z \in \mathfrak{U}$ gibt mit $z \equiv xy^{-1} \mod U_{n+2}$ bzw. $x \equiv zy \mod U_{n+2}$. Wegen $zy \in \mathfrak{U}$ folgt $x \in \mathfrak{U}^{(n+1)}$. □

Der folgende Satz macht nun eine Aussage, wann eine gutartige Untergruppe von $[U,U]$ zu vorgegebenen Anfangskoeffizienten $a_1, a_2, \ldots, a_j \in \mathbb{F}_{q^2}$ ein Element der Form $x = 1 + \sum_{i=1}^{\infty} a_i\tau^i$ enthält.

Satz 6.1.22 *Sei $\mathfrak{U} \leq [U,U]$. Seien weiter $j \in \mathbb{N}$ und $\tilde{x} \in U_1$, so daß $\mathrm{N}(\tilde{x}) \equiv 1 \mod U_{j+1}$ ist und die Bedingungen $R(\tilde{x}) \geq R(\mathfrak{U})$ und $S(\tilde{x}) \geq S(\mathfrak{U})$ gelten. Dann gibt es für alle $n \in \mathbb{N}$ ein $x^* \in (\tau^{g(j+3)}) \cap Q_0$ und ein $x \in \mathfrak{U}$ mit $x \equiv \tilde{x} + x^* \mod U_n$.*

Beweis: Man setze $k := \min\{2R(\tilde{x}), S(\tilde{x})\}$. Dann gibt es Elemente $a_{R(\tilde{x})}, a_{R(\tilde{x})+2}, \cdots, a_{k-1} \in \mathbb{F}_{q^2}$ mit $\tilde{x} \equiv 1 + \sum_{i=R(\tilde{x})}^{k-1}{}'' a_i\tau^i \mod U_k$. Daraus folgt

$$N(x) \equiv (1 + \sum_{i=R(\tilde{x})}^{k-1}{}'' a_i\tau^i)(1 + \sum_{i=R(\tilde{x})}^{k-1}{}'' a_i\tau^i) \mod U_k \equiv 1 \mod U_k.$$

Also kann man ohne Einschränkung $j \geq k-1$ annehmen. Da nun

$$k \geq \min\{2R(\mathfrak{U}), S(\mathfrak{U})\} = S(\mathfrak{U})$$

gilt, erhält man $g(j+3) \geq S(\mathfrak{U})$. Nach Satz 4.3.10 gibt es ein $x' \in [U,U]$ mit $x' \equiv \tilde{x} \mod U_{g(j+3)}$ und $x' + \tilde{x} \in Q_0$. Man setze $x^* := x' + \tilde{x}$. Dann gilt $x^* \in (\tau^{g(j+3)}) \cap Q_0$. Außerdem folgt wegen $R(\tilde{x}) \geq R(\mathfrak{U})$ und $S(\tilde{x}) \geq S(\mathfrak{U})$, daß $R(x') \geq R(\mathfrak{U})$ und $S(x') \geq S(\mathfrak{U})$ gilt. Damit folgt nach Lemma 6.1.21, daß x' in $\mathfrak{U}^{(n)}$ liegt. Also muß es ein $x \in \mathfrak{U}$ geben mit

$$x \equiv x' \mod U_n \equiv \tilde{x} + x^* \mod U_n.$$

□

6.2 Die Hauptsätze über Kommutatorrelationen gutartiger Untergruppen von $[U,U]$.

Ziel dieses Abschnittes ist es, zu zeigen, daß für gutartige Untergruppen $\mathfrak{U}$ und $\mathfrak{V}$ von $[U,U]$ sowie $n \in \mathbb{N}$ die Kommutatorgruppen $[\mathfrak{U},\mathfrak{V}]$ und $[\mathfrak{U},U_n]$ selbst wieder gutartig sind, und deren Charakterisierungsindizes zu bestimmen.

6.2.1 Der Kommutator zweier gutartiger Untergruppen von $[U,U]$ im Fall $q \neq 2$

Zuerst versucht man $R([\mathfrak{U},\mathfrak{V}])$ und $S([\mathfrak{U},\mathfrak{V}])$ nach unten abzuschätzen. Dazu wird das folgende Lemma benötigt.

Lemma 6.2.1.1 *Sei $x \in U_1$ und $T \in \mathbb{N}$ mit $T \leq T(x)$. Dann gilt* $\mathrm{Tr}(x) \in L \cap (\tau^T)$.

Beweis: Wegen $\mathrm{Tr}(x) \in L$ nach Lemma 1.2.3.5 bleibt lediglich $\mathrm{Tr}(x) \in (\tau^T)$ zu zeigen. Dazu schreibt man x in der Form $x = 1 + \sum_{i=1}^{\infty} a_i\tau^i$. Nach Lemma 1.2.3.2 gilt

$$\mathrm{Tr}(x) = x + \overline{x} = 1 + \sum_{i=1}^{\infty} a_i\tau^i + 1 + \sum_{i=1}^{\infty} a_i^{q^{i+1}}\tau^i = {\sum_{i=1}^{\infty}}''(a_i + a_i^q)\tau^i$$

Wegen $a_i \in \mathbb{F}_q$ folgt $a_i + a_i^q = 0$ für alle geraden $i \in \mathbb{N}$ mit $i < T$. Also gilt $\mathrm{Tr}(x) \in (\tau^T)$. □

Satz 6.2.1.2 *Seien $x, y \in U_1$ und $R_1, T_1, R_2, T_2 \in \mathbb{N}$ mit $R_1 \leq R(x)$, $R_2 \leq R(y)$, $T_1 \leq T(x)$ und $T_2 \leq T(y)$. Man setze $\tilde{S} := \min\{T_1 + 2R_2, T_2 + 2R_1, R_1 + R_2\}$ und $\tilde{R} := \min\{T_1 + R_2, T_2 + R_1, 2R_1 + R_2, R_1 + 2R_2\}$. Dann gilt $S(xyx^{-1}y^{-1}) \geq \tilde{S}$ und $R(xyx^{-1}y^{-1}) \geq \tilde{R}$.*

Beweis: Gemäß Lemma 1.2.4.1 existieren eindeutig bestimmte Elemente $x_0, y_0 \in Q_0$ und $x_1, y_1 \in Q_1$ mit $x = x_0 + x_1$ und $y = y_0 + y_1$. Dabei müssen nach Bemerkung 6.1.2 die Bedingungen $x_1 \in (\tau^{R_1})$, $y_1 \in (\tau^{R_2})$ sowie $x_0 \equiv 1 \mod (\tau^{T_1})$ und $y_0 \equiv 1 \mod (\tau^{T_2})$ gelten. Wegen $x^{-1} = \frac{1}{\mathrm{N}(x)}\overline{x}$ und $y^{-1} = \frac{1}{\mathrm{N}(y)}\overline{y}$ erhält man

$$\begin{aligned} xyx^{-1}y^{-1} &= \tfrac{1}{\mathrm{N}(xy)}xy\overline{x}\,\overline{y} \\ &= \tfrac{1}{\mathrm{N}(xy)}(x_0 + x_1)(y_0 + y_1)(\overline{x}_0 + \overline{x}_1)(\overline{y}_0 + \overline{y}_1) \\ &= \tfrac{1}{\mathrm{N}(xy)} \sum_{i,j,k,l \in \{0,1\}} x_iy_j\overline{x}_k\overline{y}_l \\ &= z_0 + z_1, \end{aligned}$$

wobei

$$z_0 := \frac{1}{\mathrm{N}(xy)} \sum_{\substack{i,j,k,l \in \{0,1\} \\ i+j+k+l \ \text{gerade}}} x_iy_j\overline{x}_k\overline{y}_l$$

und

$$z_1 := \frac{1}{\mathrm{N}(xy)} \sum_{\substack{i,j,k,l \in \{0,1\} \\ i+j+k+l \ \text{ungerade}}} x_iy_j\overline{x}_k\overline{y}_l$$

ist. Nach Satz 1.2.4.2 folgt nun $z_0 \in Q_0$ und $z_1 \in Q_1$.

Wegen $x_0y_0\overline{x}_1\overline{y}_1, x_0y_1\overline{x}_1\overline{y}_0, x_1y_0\overline{x}_0\overline{y}_1, x_1y_1\overline{x}_0\overline{y}_0, x_1y_1\overline{x}_1\overline{y}_1 \in (\tau^{R_1+R_2})$ erhält man für z_0 die Kongruenz

$$\begin{aligned} \mathrm{N}(xy)z_0 &\equiv x_0y_0\overline{x}_0\overline{y}_0 + x_0y_1\overline{x}_0\overline{y}_1 + x_1y_0\overline{x}_1\overline{y}_0 \mod (\tau^{\tilde{S}}) \\ &= x_0\overline{x}_0y_0\overline{y}_0 + x_0x_0y_1y_1 + x_1x_1\overline{y}_0\overline{y}_0. \end{aligned}$$

Die Anwendung von Korollar 1.2.4.3 liefert nun

$$\begin{aligned} \mathrm{N}(xy)z_0 &\equiv (\mathrm{N}(x) + x_1x_1)(\mathrm{N}(y) + y_1y_1) + x_0x_0y_1y_1 + x_1x_1\overline{y}_0\overline{y}_0 \mod (\tau^{\tilde{S}}) \\ &\equiv \mathrm{N}(xy) + \mathrm{N}(x)y_1y_1 + x_1x_1\mathrm{N}(y) + x_0x_0y_1y_1 + x_1x_1\overline{y}_0\overline{y}_0 \mod (\tau^{\tilde{S}}) \\ &= \mathrm{N}(xy) + (\mathrm{N}(x) + x_0x_0)y_1y_1 + x_1x_1(\mathrm{N}(y) + \overline{y}_0\overline{y}_0) \\ &= \mathrm{N}(xy) + (x_0\overline{x}_0 + x_1x_1 + x_0x_0)y_1y_1 + x_1x_1(y_0\overline{y}_0 + y_1y_1 + \overline{y}_0\overline{y}_0) \\ &= \mathrm{N}(xy) + x_0(x_0 + \overline{x}_0)y_1y_1 + x_1x_1(y_0 + \overline{y}_0)\overline{y}_0. \end{aligned}$$

Wegen $x_0+\overline{x}_0 \in (\tau^{T_1})$ und $y_0+\overline{y}_0 \in (\tau^{T_2})$ nach Lemma 6.2.1.1 folgt $x_0(x_0+\overline{x}_0)y_1y_1 \in (\tau^{T_1+2R_2})$ und $x_1x_1(y_0+\overline{y}_0)\overline{y}_0 \in (\tau^{T_2+2R_1})$. Damit erhält man

$$\mathrm{N}(xy)z_0 \equiv \mathrm{N}(xy) \mod (\tau^{\tilde{S}}) \text{ bzw. } z_0 \equiv 1 \mod (\tau^{\tilde{S}}).$$

Das aber bedeutet nichts anderes, als daß die Ungleichung

$$S(xyx^{-1}y^{-1}) \geq \tilde{S}$$

gilt.

Wegen $x_0y_1\overline{x}_1\overline{y}_1, x_1y_1\overline{x}_0\overline{y}_1 \in (\tau^{R_1+2R_2})$ und $x_1y_0\overline{x}_1\overline{y}_1, x_1y_1\overline{x}_1\overline{y}_0 \in (\tau^{2R_1+R_2})$ erhält man für z_1 die Kongruenz

$$\begin{aligned}
\mathrm{N}(xy)z_1 &\equiv x_0y_0\overline{x}_0\overline{y}_1 + x_0y_0\overline{x}_1\overline{y}_0 + x_0y_1\overline{x}_0\overline{y}_0 + x_1y_0\overline{x}_0\overline{y}_0 \mod (\tau^{\tilde{R}}) \\
&= x_0y_0\overline{x}_0y_1 + x_0y_0x_1\overline{y}_0 + x_0y_1\overline{x}_0\overline{y}_0 + x_1y_0\overline{x}_0\overline{y}_0 \\
&= x_0\overline{x}_0y_0y_1 + x_1\overline{x}_0\overline{y}_0\overline{y}_0 + x_0x_0y_0y_1 + x_1\overline{x}_0y_0\overline{y}_0 \\
&= x_0(\overline{x}_0+x_0)y_0y_1 + x_1\overline{x}_0(\overline{y}_0+y_0)\overline{y}_0.
\end{aligned}$$

Wegen $x_0+\overline{x}_0 \in (\tau^{T_1})$ und $y_0+\overline{y}_0 \in (\tau^{T_2})$ nach Lemma 6.2.1.1 folgt $x_0(\overline{x}_0+x_0)y_0y_1 \in (\tau^{T_1+R_2})$ und $x_1\overline{x}_0(\overline{y}_0+y_0) \in (\tau^{T_2+R_1})$. Damit erhält man

$$\mathrm{N}(xy)z_1 \equiv 0 \mod (\tau^{\tilde{R}}) \text{ bzw. } z_1 \equiv 0 \mod (\tau^{\tilde{R}}).$$

Das aber bedeutet nichts anderes, als daß die Ungleichung

$$R(xyx^{-1}y^{-1}) \geq \tilde{R}$$

gilt. □

Korollar 6.2.1.3 *Seien $\mathfrak{U}, \mathfrak{V} \leq [U,U]$ gutartig mit $R_1 := R(\mathfrak{U})$, $R_2 := R(\mathfrak{V})$, $S_1 := S(\mathfrak{U})$ und $S_2 := S(\mathfrak{V})$. Man setze $\tilde{S} := \min\{2S_1+2R_2, 2S_2+2R_1, R_1+R_2\}$ und $\tilde{R} := \min\{2S_1+R_2, 2S_2+R_1, 2R_1+R_2, R_1+2R_2\}$. Dann gelten für alle $z \in [\mathfrak{U},\mathfrak{V}]$ die Ungleichungen $R(z) \geq \tilde{R}$ und $S(z) \geq \tilde{S}$.*

Beweis: Man setze $T_1 := T(\mathfrak{U})$ und $T_2 := T(\mathfrak{V})$. Mit Lemma 6.1.13 erhält man

$$\tilde{S} = \min\{T_1+2R_2, T_2+2R_1, R_1+R_2\}$$

sowie

$$\tilde{R} = \min\{T_1+R_2, T_2+R_1, 2R_1+R_2, R_1+R_2\}.$$

Man definiere $W_1 := \{xyx^{-1}y^{-1} \mid x \in \mathfrak{U}, y \in \mathfrak{V}\}$ und $W_2 := \{yxy^{-1}x^{-1} \mid x \in \mathfrak{U}, y \in \mathfrak{V}\}$. Sei nun $w_1 = xyx^{-1}y^{-1} \in W_1$ beliebig mit $x \in \mathfrak{U}$ und $y \in \mathfrak{V}$. Wegen $R(x) \geq R_1$ und $R(y) \geq R_2$ sowie $T(x) \geq T_1$ und $T(y) \geq T_2$ folgt aus Satz 6.2.1.2, daß $R(w_1) \geq \tilde{R}$ und $S(w_1) \geq \tilde{S}$ gilt. Ebenso zeigt man $R(w_2) \geq \tilde{R}$ und $S(w_2) \geq \tilde{S}$ für alle $w_2 \in W_2$, so daß man insgesamt $R(w) \geq \tilde{R}$ und $S(w) \geq \tilde{S}$ für alle $w \in W_1 \cup W_2$ erhält. Sei nun $z \in [\mathfrak{U},\mathfrak{V}]$ beliebig. Dann läßt sich z als *endliches* Produkt $z = w^{(1)} \cdot \ldots \cdot w^{(n)}$ von Elementen $w^{(1)}, \ldots, w^{(n)} \in W_1 \cup W_2$ schreiben. Wegen

$$2\tilde{R} = \min\{4S_1+2R_2, 4S_2+2R_1, 4R_1+2R_2, 2R_1+4R_2\} \geq \tilde{S}$$

folgt durch fortlaufende Anwendung von Lemma 6.1.10, daß $S(z) \geq \tilde{S}$ und $R(z) \geq \tilde{R}$ gilt. □

Damit hat man nun für alle gutartigen Untergruppen $\mathfrak{U}, \mathfrak{V}$ von $[U,U]$ die Charakterisierungsindizes des Kommutators $[\mathfrak{U},\mathfrak{V}]$ nach unten abgeschätzt. Im folgenden bestimmt man nun das Verhalten von $F_n([\mathfrak{U},\mathfrak{V}])$ für große n.

Lemma 6.2.1.4 *Seien $\mathfrak{U}, \mathfrak{V} \leq [U,U]$ gutartig mit $R_1 := R(\mathfrak{U})$ und $R_2 := R(\mathfrak{V})$. Dann gilt für alle geraden $n \in \mathbb{N}$ mit $n \geq R_1 + R_2$ die Inklusion $F_n([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$.*

Beweis: Man setze $i := R_1$ und $j := n - i$. Dann sind i und j ungerade mit $j \geq R_2$, und es gilt $i + j = n$.

Sei nun $g \in \mathbb{F}_q$. Dann gibt es nach Satz 1.1.3 ein $a \in \mathbb{F}_{q^2}$ mit $a^q + a = g$. Wegen $F_i(\mathfrak{U}) = \mathbb{F}_{q^2} = F_j(\mathfrak{V})$ gibt es ein $x \in \mathfrak{U}$ mit $x \equiv 1 + a\tau^i \mod U_{i+1}$ und ein $y \in \mathfrak{V}$ mit $x \equiv 1 + \tau^j \mod U_{j+1}$. Daraus folgt nach Lemma 4.1.1 die Kongruenz

$$\begin{aligned} xy &\equiv (1 + (a1^{q^i} + 1a^{q^j})\tau^n)yx \mod U_{n+1} \\ &\equiv (1 + (a + a^q)\tau^n)yx \mod U_{n+1}. \end{aligned}$$

Damit erhält man

$$\begin{aligned} xyx^{-1}y^{-1} &\equiv 1 + (a + a^q)\tau^n \mod U_{n+1} \\ &\equiv 1 + g\tau^n \mod U_{n+1}. \end{aligned}$$

Wegen $xyx^{-1}y^{-1} \in [\mathfrak{U}, \mathfrak{V}]$ folgt $g \in F_n([\mathfrak{U}, \mathfrak{V}])$. Somit ist $F_n([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$ gezeigt. □

Lemma 6.2.1.5 *Seien $\mathfrak{U}, \mathfrak{V} \leq [U,U]$ gutartig mit $R_1 := R(\mathfrak{U}) \neq 1$ und $S_2 := S(\mathfrak{V})$. Man setze $n := 2R_1 + 2R_2$. Dann gilt $F_n([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$ und $F_{n+2}([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$.*

Beweis: Man setze $i := R_1$ und $j := R_2$. Dann gilt $n = 2i + 2j$, wobei i ungerade und $i \geq 3$ sowie j gerade ist.

Für $\tilde{y} := 1 + \tau^j$ gilt nun

$$\mathrm{N}(\tilde{y}) = (1 + \tau^j)(1 + \tau^j) \equiv 1 \mod U_{2j}.$$

Außerdem sind die Bedingungen $R(\tilde{y}) = \infty > R(\mathfrak{U})$ und $S(\tilde{y}) = j = S(\mathfrak{V})$ erfüllt. Damit folgt nach Satz 6.1.22, daß es ein $y^* \in (\tau^{2j}) \cap Q_0$ und ein $y \in \mathfrak{V}$ gibt mit $y \equiv \tilde{y} + y^* \mod U_{n+3}$. Seien nun $a, b \in \mathbb{F}_{q^2}$ beliebig. Man setze $\tilde{x} := 1 + a\tau^i + b\tau^{i+2}$. Dann gilt die Kongruenz

$$\mathrm{N}(\tilde{x}) = (1 + a\tau^i + b\tau^{i+2})(1 + a\tau^i + b\tau^{i+2}) \equiv 1 \mod U_{2i}.$$

Außerdem sind die Bedingungen $R(\tilde{x}) \geq i = R(\mathfrak{U})$ und $S(\tilde{x}) = \infty > S(\mathfrak{U})$ erfüllt. Damit folgt nach Satz 6.1.22, daß es ein $x^* \in (\tau^{2i}) \cap Q_0 \subset (\tau^{i+3}) \cap Q_0$ und ein $x \in \mathfrak{U}$ gibt mit $x \equiv \tilde{x} + x^* \mod U_{n+3}$. Man definiere nun $z(a,b) = xyx^{-1}y^{-1}$. Dann gilt nach Satz 1.2.4.2 die Kongruenz

$$\begin{aligned} z(a,b) &= xy\overline{x}\,\overline{y} \\ &\equiv xy(1 + a\tau^i + b\tau^{i+2} + \overline{x}^*)\overline{y} \mod U_{n+3} \\ &\equiv x\left(y\overline{y}(1 + \overline{x}^*) + yy(a\tau^i + b\tau^{i+2})\right) \mod U_{n+3} \\ &\equiv x\left(1 + \overline{x}^* + (1 + \tau^j + y*)^2(a\tau^i + b\tau^{i+2})\right) \mod U_{n+3} \\ &= x\left(1 + \overline{x}^* + a\tau^i + b\tau^{i+2} + (\tau^{2j} + (y*)^2)(a\tau^i + b\tau^{i+2})\right) \\ &\equiv 1 + x(\tau^{2j} + (y*)^2)(a\tau^i + b\tau^{i+2}) \mod U_{n+3} \\ &\equiv 1 + (1 + a\tau^i + b\tau^{i+2} + x^*)(a\tau^{i+2j} + b\tau^{i+2j+2} + (y^*)^2a\tau^i + (y^*)^2b\tau^{i+2}) \mod U_{n+3}. \end{aligned}$$

Wegen $y^* \in (\tau^{2j})$ und $x^* \in (\tau^{i+3})$ sowie $n = 2i + 2j$ erhält man

$$\begin{aligned} z(a,b) &\equiv 1 + a\tau^{i+2j} + b\tau^{i+2j+2} + (y^*)^2a\tau^i + (y^*)^2b\tau^{i+2} \\ &\quad + a^{q+1}\tau^n + ab^q\tau^{n+2} + ba^q\tau^{n+2} \mod U_{n+3} \\ &\equiv 1 + ay_1 + by_2 + a^{q+1}\tau^n + (ab^q + ba^q)\tau^{n+2} \mod U_{n+3}, \end{aligned}$$

wobei $y_1 := \tau^{i+2j} + (y^*)^2\tau^i, y_2 := \tau^{i+2j+2} + (y^*)^2\tau^{i+2} \in (\tau^{i+2j})$ *unabhängig* von a und b sind. Man setze nun für alle $a_1, a_2, b_1, b_2 \in \mathbb{F}_{q^2}$ beliebig

$$w(a_1, b_1, a_2, b_2) := z(a_1, b_1) \cdot z(a_2, b_2) \cdot z(a_1 + a_2, b_1 + b_2).$$

Wegen $2(i+2j) = 2i + 4j \geq 2i + 2j + 4 > n + 3$ folgt die Kongruenz

$$\begin{aligned} w(a_1, b_1, a_2, b_2) &\equiv (1 + (a_1 + a_2)y_1 + (b_1 + b_2)y_2 + (a_1^{q+1} + a_2^{q+1})\tau^n \\ &+ (a_1 b_1^q + b_1 a_1^q + a_2 b_2^q + b_2 a_2^q)\tau^{n+2}) \cdot z(a_1 + a_2, b_1 + b_2) \mod U_{n+3} \\ &\equiv 1 + (a_1^{q+1} + a_2^{q+1} + (a_1 + a_2)^{q+1})\tau^n + (a_1 b_1^q + b_1 a_1^q + a_2 b_2^q + b_2 a_2^q + \\ &(a_1 + a_2)(b_1 + b_2)^q + (b_1 + b_2)(a_1 + a_2)^q)\tau^{n+2} \mod U_{n+3} \\ &\equiv 1 + (a_1 a_2^q + a_2 a_1^q)\tau^n + (a_1 b_2^q + a_1 b_2^q + b_1 a_2^q + b_2 a_1^q)\tau^{n+2} \mod U_{n+3}. \end{aligned}$$

Sei nun $g \in \mathbb{F}_q$ beliebig. Dann gibt es nach Satz 1.1.3 ein $a_1 \in \mathbb{F}_{q^2}$ mit $a_1^q + a_1 = g$. Damit erhält man die Kongruenz

$$w(a_1, 0, 1, 0) \equiv 1 + (a_1 + a_1^q)\tau^n \mod U_{n+1} \equiv 1 + g\tau^n \mod U_{n+1}.$$

Wegen $w(a_1, 0, 1, 0) \in [\mathfrak{U}, \mathfrak{V}]$ folgt hiermit $g \in F_n([\mathfrak{U}, \mathfrak{V}])$. Außerdem gilt die Kongruenz

$$w(a_1, 0, 0, 1) \equiv 1 + (a_1 + a_1^q)\tau^{n+2} \mod U_{n+3} \equiv 1 + g\tau^{n+2} \mod U_{n+3}.$$

Wegen $w(a_1, 0, 0, 1) \in [\mathfrak{U}, \mathfrak{V}]$ folgt hiermit $g \in F_{n+2}([\mathfrak{U}, \mathfrak{V}])$. Da $g \in \mathbb{F}_q$ beliebig gewählt war, gilt somit $F_n([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$ und $F_{n+2}([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$. □

Lemma 6.2.1.6 *Seien $\mathfrak{U}, \mathfrak{V} \leq [U, U]$ gutartig mit $R(\mathfrak{U}) = 1$ und $S_2 := S(\mathfrak{V})$. Man setze $n := 2 + 2S_2$. Dann gilt $F_n([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$ und $F_{n+2}([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$.*

Beweis: Man setze $j := S_2$. Dann gilt $n = 2j + 2$, wobei j gerade ist.

Für $\tilde{y} := 1 + \tau^j$ gilt nun die Kongruenz

$$\mathrm{N}(\tilde{y}) = (1 + \tau^j)(1 + \tau^j) \equiv 1 \mod U_{2j}.$$

Außerdem sind die Bedingungen $R(\tilde{y}) = \infty > R(\mathfrak{V})$ und $S(\tilde{y}) = j = S(\mathfrak{V})$ erfüllt. Damit folgt nach Satz 6.1.22, daß es ein $y^* \in (\tau^{2j}) \cap Q_0$ und ein $y \in \mathfrak{V}$ gibt mit $y \equiv \tilde{y} + y^* \mod U_{n+3}$. Seien nun $a, c \in \mathbb{F}_{q^2}$ beliebig. Wegen $a^{q+1} \in \mathbb{F}_q$ gibt es nach Satz 1.1.3 ein $b \in \mathbb{F}_{q^2}$ mit $b^q + b = a^{q+1}$. Man setze nun $\tilde{x} := 1 + a\tau + b\tau^2 + c\tau^3$. Dann gilt die Kongruenz

$$\begin{aligned} \mathrm{N}(\tilde{x}) &= (1 + a\tau + b\tau^2 + c\tau^3)(1 + a\tau + b^q\tau^2 + c\tau^3) \\ &\equiv 1 + (b + a^{q+1} + b^q)\tau^2 \mod U_4 \\ &\equiv 1 \mod U_4. \end{aligned}$$

Außerdem sind die Bedingungen $R(\tilde{x}) \geq 1 = R(\mathfrak{U})$ und $S(\tilde{x}) \geq 2 = 2R(\mathfrak{U}) \geq S(\mathfrak{U})$ nach Lemma 6.1.12 erfüllt. Damit folgt nach Satz 6.1.22, daß es ein $x^* \in (\tau^4) \cap Q_0$ und ein $x \in \mathfrak{U}$ gibt mit $x \equiv \tilde{x} + x^* \mod U_{n+3}$. Man definiere nun $\tilde{z}(a, c) = xyx^{-1}y^{-1}$. Dann gilt nach Satz 1.2.4.2 die Kongruenz

$$\begin{aligned} \tilde{z}(a, c) &= xy\overline{x}\,\overline{y} \\ &\equiv xy(1 + a\tau + b^q\tau^2 + c\tau^3 + \overline{x}^*)\overline{y} \mod U_{n+3} \\ &\equiv x(y\overline{y}(1 + b^q\tau^2 + \overline{x}^*) + yy(a\tau + c\tau^3)) \mod U_{n+3} \\ &\equiv x(1 + b^q\tau^2 + \overline{x}^* + (1 + \tau^j + y^*)^2(a\tau + c\tau^3)) \mod U_{n+3} \\ &= x(1 + b^q\tau^2 + \overline{x}^* + a\tau + c\tau^3 + (\tau^{2j} + (y^*)^2)(a\tau + c\tau^3)) \\ &\equiv 1 + x(\tau^{2j} + (y^*)^2)(a\tau + c\tau^3) \mod U_{n+3} \\ &\equiv 1 + x\tau^{2j}(a\tau + c\tau^3) + x(y^*)^2(a\tau + c\tau^3) \mod U_{n+3}. \end{aligned}$$

Wegen $(y^*)^2 \in (\tau^4)$ und $4j \geq 2j + 4 = n + 2$ folgt $(y^*)^2(a\tau + c\tau^3) \in (\tau^{n+3})$. Damit erhält man

$$\begin{aligned} \tilde{z}(a, c) &\equiv 1 + (1 + a\tau + b\tau^2 + c\tau^3)(a\tau^{n-1} + c\tau^{n+1}) \mod U_{n+3} \\ &= 1 + a\tau^{n-1} + a^{q+1}\tau^n + (ba + c)\tau^{n+1} + (ac^q + ca^q)\tau^{n+2}. \end{aligned}$$

Man setze nun $z(a,c) := \tilde{z}(a,c) \cdot z(0, ba+c)$. Wegen $n = 2j+2 \geq 6$ folgt $2(n-1) > n+3$. Damit erhält man

$$z(a,c) \equiv 1 + a\tau^{n-1} + a^{q+1}\tau^n + (ca^q + ac^q)\tau^{n+2} \mod U_{n+3}.$$

Man definiere nun für alle $a_1, a_2, c_1, c_2 \in \mathbb{F}_{q^2}$ beliebig

$$w(a_1, c_1, a_2, c_2) := z(a_1, c_1) \cdot z(a_2, c_2) \cdot z(a_1 + a_2, c_1 + c_2).$$

Dann gilt die Kongruenz

$$\begin{aligned} w(a_1, c_1, a_2, c_2) &\equiv (1 + (a_1 + a_2)\tau^{n-1} + (a_1^{q+1} + a_2^{q+1})\tau^n + (c_1 a_1^q + a_1 c_1^q + a_2 c_2^q + c_2 a_2^q)\tau^{n+1}) \\ &\quad z(a_1 + a_2, c_1 + c_2) \mod U_{n+3} \\ &\equiv 1 + (a_1^{q+1} + a_2^{q+1} + (a_1 + a_2)^{q+1})\tau^n + (c_1 a_1^q + a_1 c_1^q + a_2 c_2^q + c_2 a_2^q + \\ &\quad (c_1 + c_2)(a_1 + a_2)^q + (a_1 + a_2)(c_1 + c_2)^q)\tau^{n+2} \mod U_{n+3} \\ &= 1 + (a_2 a_1^q + a_2 a_1^q)\tau^n + (c_2 a_1^q + c_1 a_2^q + a_2 c_1^q + a_1 c_2^q)\tau^{n+2} \end{aligned}$$

Sei nun $g \in \mathbb{F}_q$ beliebig. Dann gibt es nach Satz 1.1.3 ein $a_1 \in \mathbb{F}_{q^2}$ mit $a_1^q + a_1 = g$. Damit erhält man die Kongruenz

$$w(a_1, 0, 1, 0) \equiv 1 + (a_1 + a_1^q)\tau^n \mod U_{n+1} \equiv 1 + g\tau^n \mod U_{n+1}.$$

Wegen $w(a_1, 0, 1, 0) \in [\mathfrak{U}, \mathfrak{V}]$ folgt hiermit $g \in F_n([\mathfrak{U}, \mathfrak{V}])$. Außerdem gilt die Kongruenz

$$w(a_1, 0, 0, 1) \equiv 1 + (a_1 + a_1^q)\tau^{n+2} \mod U_{n+3} \equiv 1 + g\tau^{n+2} \mod U_{n+3}.$$

Wegen $w(a_1, 0, 0, 1) \in [\mathfrak{U}, \mathfrak{V}]$ folgt hiermit $g \in F_{n+2}([\mathfrak{U}, \mathfrak{V}])$. Da $g \in \mathbb{F}_q$ beliebig gewählt war, gilt somit $F_n([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$ und $F_{n+2}([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$. □

Satz 6.2.1.7 *Seien $\mathfrak{U}, \mathfrak{V} \leq [U,U]$ gutartig mit $R_1 := R(\mathfrak{U})$ und $S_2 := S(\mathfrak{V})$. Dann gilt für alle geraden $n \in \mathbb{N}$ mit $n \geq 2R_1 + 2S_2$, daß $F_n([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$ ist.*

Beweis: Man setze $m := \max\{\tilde{m} \in \mathbb{N} \mid \tilde{m} \text{ ist ungerade und } n \geq 2\tilde{m} + 2S_2\}$. Dann ist $m \geq R_1$ und es gilt entweder $n = 2m + 2S_2$ oder $n = 2m + 2S_2{+}2$. Falls $m = 1$ ist, folgt $R_1 = 1$ und damit $F_n([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$ nach Lemma 6.2.1.6. Sei nun $m > 1$. Man setze $\tilde{n} := \frac{1}{2}(m - R_1)$. Dann gilt $m = R_1 + 2\tilde{n}$ und mit Korollar 6.1.16 folgt, daß es eine gutartige Untergruppe $\tilde{\mathfrak{U}}$ von $\mathfrak{U}$ gibt mit $S(\tilde{\mathfrak{U}}) = S(\mathfrak{U})$ und $R(\tilde{\mathfrak{U}}) = m$. Mit Lemma 6.2.1.5 folgt nun $F_n([\tilde{\mathfrak{U}}, \mathfrak{V}]) \supset \mathbb{F}_q$. Wegen $[\tilde{\mathfrak{U}}, \mathfrak{V}] \subset [\mathfrak{U}, \mathfrak{V}]$ erhält man schließlich $F_n([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$. □

Lemma 6.2.1.8 *Seien $\mathfrak{U}, \mathfrak{V} \leq [U.U]$ gutartig mit $R_1 := R(\mathfrak{U})$ und $S_2 := S(\mathfrak{V})$. Dann gilt für alle ungeraden $n \in \mathbb{N}$ mit $n \geq R_1 + 2S_2$, daß $F_n([\mathfrak{U}, \mathfrak{V}]) = \mathbb{F}_{q^2}$ ist.*

Beweis: Man setze $i := S_2$ und $j := n - 2i$. Dann gilt $n = 2i + 2j$, wobei i gerade ist mit $i \geq S(\mathfrak{V})$ und j ungerade mit $j \geq R(\mathfrak{U})$.

Sei nun $g \in \mathbb{F}_{q^2}$ beliebig. Man wähle $b \in \mathbb{F}_q^*$. Dann gibt es nach Satz 1.1.3 ein $c \in \mathbb{F}_{q^2}$ mit $c^q + c = b^{q+1} \neq 0$. Weiter setze man $a := \frac{g}{c^q + c}$. Für $\tilde{x} := 1 + a\tau^j$ gilt dann die Kongruenz

$$\mathrm{N}(\tilde{x}) = (1 + a\tau^j)(1 + a\tau^j) \equiv 1 \mod U_{2j}.$$

Außerdem sind die Bedingungen $R(\tilde{x}) \geq j \geq R(\mathfrak{U})$ und $S(\tilde{x}) = \infty \geq S(\mathfrak{U})$ erfüllt. Damit folgt nach Satz 6.1.22, daß es ein $x^* \in (\tau^{2j}) \cap Q_0$ und $x \in \mathfrak{U}$ gibt mit $x \equiv \tilde{x} + x^* \mod U_{n+1}$. Für $\tilde{y} := 1 + b\tau^i + c\tau^{2i}$ gilt nun die Kongruenz

$$\begin{aligned} \mathrm{N}(\tilde{y}) &= (1 + b\tau^i + c\tau^{2i})(1 + b\tau^i + c^q\tau^{2i}) \\ &\equiv 1 + (c + b^{q+1} + c^q)\tau^{2i} \mod U_{2i+1} \\ &\equiv 1 \mod U_{2i+1}. \end{aligned}$$

Außerdem sind die Bedingungen $R(\tilde{y}) = \infty > R(\mathfrak{V})$ und $S(\tilde{y}) = i \geq S(\mathfrak{V})$ erfüllt. Damit folgt nach Satz 6.1.22, daß es ein $y^* \in (\tau^{2i+2}) \cap Q_0$ und ein $y \in \mathfrak{V}$ gibt mit $y \equiv \tilde{y} + y^* \mod U_{n+1}$. Wegen $n := 2i + j$ erhält man nun die Kongruenzen

$$\begin{aligned} yx &\equiv (1 + b\tau^i + c\tau^{2i} + y^*)(1 + a\tau^j + x^*) \mod U_{n+1} \\ &\equiv 1 + b\tau^i + c\tau^{2i} + a\tau^j + ba\tau^{i+j} + x^* + y^* + b\tau^i x^* + ac\tau^n \mod U_{n+1} \end{aligned}$$

sowie

$$\begin{aligned} xy &\equiv (1 + a\tau^j + x^*)(1 + b\tau + c\tau^{2i} + y^*) \mod U_{n+1} \\ &\equiv 1 + b\tau^i + c\tau^{2i} + a\tau^j + ba\tau^{i+j} + x^* + y^* + b\tau^i x^* + ac^q\tau^n \mod U_{n+1}. \end{aligned}$$

Daraus folgt

$$xy \equiv (1 + (ac^q + ca)\tau^n)yx \mod U_{n+1}.$$

Hieraus ergibt sich

$$\begin{aligned} xyx^{-1}y^{-1} &\equiv 1 + a(c + c^q)\tau^n \mod U_{n+1} \\ &\equiv 1 + g\tau \mod U_{n+1}. \end{aligned}$$

Wegen $xyx^{-1}y^{-1} \in [\mathfrak{U}, \mathfrak{V}]$ folgt nun $g \in F_n([\mathfrak{U}, \mathfrak{V}])$. Da $g \in \mathbb{F}_{q^2}$ beliebig gewählt war, ist damit $F_n([\mathfrak{U}, \mathfrak{V}]) = \mathbb{F}_{q^2}$ gezeigt. □

Satz 6.2.1.9 *Seien $\mathfrak{U}, \mathfrak{V} \leq [U, U]$ gutartig und $R_1, R_2 \in \mathbb{N}$ mit R_1 und R_2 ungerade, $R_1 \neq R_2$ sowie $R_1 \geq R(\mathfrak{U})$ und $R_2 \geq R(\mathfrak{V})$. Dann gilt für alle ungeraden $n \in \mathbb{N}$ mit $n \geq R_1 + 2R_2$, daß $F_n([\mathfrak{U}, \mathfrak{V}]) = \mathbb{F}_{q^2}$ ist.*

Beweis: Wegen $[\mathfrak{U}, \mathfrak{V}] = [\mathfrak{V}, \mathfrak{U}]$ kann man ohne Einschränkung $R_1 > R_2$ annehmen. Man setze $j := R_2$ und $i = n - 2j$. Dann gilt $n = i + 2j$, wobei i und j ungerade sind mit $i \geq R_2$ sowie $i > j$.

Sei nun $g \in \mathbb{F}_{q^2}$ beliebig. Nach Lemma 1.1.6 gibt es nun Elemente $a, b \in \mathbb{F}_{q^2}$ mit $ab^q + ba^q = 0$ und $g = ab^{q+1}$. Wegen $b^{q+1} \in \mathbb{F}_q$ folgt nach Satz 1.1.3, daß es ein $c \in \mathbb{F}_{q^2}$ gibt mit $c^q + c = b^{q+1}$. Für $\tilde{x} := 1 + a\tau^i$ gilt nun Kongruenz

$$\mathrm{N}(\tilde{x}) = (1 + a\tau^i)(1 + a\tau^i) \equiv 1 \mod U_{2i}.$$

Außerdem sind die Bedingungen $R(\tilde{x}) \geq i \geq R(\mathfrak{U})$ und $S(\tilde{x}) = \infty > S(\mathfrak{U})$ erfüllt. Damit folgt nach Satz 6.1.22, daß es ein $x^* \in (\tau^{2i}) \cap Q_0$ und $x \in \mathfrak{U}$ gibt mit $x \equiv \tilde{x} + x^* \mod U_{n+1}$. Für $\tilde{y} := 1 + b\tau^j + c\tau^{2j}$ gilt nun die Kongruenz

$$\begin{aligned} \mathrm{N}(\tilde{y}) &= (1 + b\tau^j + c\tau^{2j})(1 + b\tau^j + c^q\tau^{2j}) \\ &\equiv 1 + (c + b^{q+1} + c^q)\tau^{2j} \mod U_{2j+1} \\ &\equiv 1 \mod U_{2j+1}. \end{aligned}$$

Außerdem sind die Bedingungen $R(\tilde{y}) \geq j \geq R(\mathfrak{V})$ und $S(\tilde{y}) \geq 2j = 2R(\mathfrak{V}) \geq S(\mathfrak{V})$ nach Lemma 6.1.12 erfüllt. Damit folgt nach Satz 6.1.22, daß es ein $y^* \in (\tau^{2j+2}) \cap Q_0$ und ein $y \in \mathfrak{V}$ gibt mit $y \equiv \tilde{y} + y^* \mod U_{n+1}$.

Wegen $n := i + 2j$ erhält man nun die Kongruenzen

$$\begin{aligned} yx &\equiv (1 + b\tau^j + c\tau^{2j} + y^*)(1 + a\tau^i + x^*) \mod U_{n+1} \\ &\equiv 1 + b\tau^j + c\tau^{2j} + a\tau^i + ba^q\tau^{i+j} + x^* + y^* + ac\tau^n \mod U_{n+1} \end{aligned}$$

sowie

$$\begin{aligned} xy &\equiv (1 + a\tau^i + x^*)(1 + b\tau^j + c\tau^{2j} + y^*) \mod U_{n+1} \\ &\equiv 1 + b\tau^j + c\tau^{2j} + a\tau^i + ba^q\tau^{i+j} + x^* + y^* + ac^q\tau^n \mod U_{n+1}. \end{aligned}$$

Daraus folgt

$$xy \equiv (1 + a(c^q + c)\tau^n)yx \mod U_{n+1}.$$

Hieraus ergibt sich

$$\begin{aligned} xyx^{-1}y^{-1} &\equiv 1 + ab^{q+1}\tau^n \mod U_{n+1}. \\ &\equiv 1 + g\tau \mod U_{n+1} \end{aligned}$$

Wegen $xyx^{-1}y^{-1} \in [\mathfrak{U}, \mathfrak{V}]$ folgt nun $g \in F_n([\mathfrak{U}, \mathfrak{V}])$. Da $g \in \mathbb{F}_{q^2}$ beliebig gewählt war, ist damit $F_n([\mathfrak{U}, \mathfrak{V}]) = \mathbb{F}_{q^2}$ gezeigt. □

Korollar 6.2.1.10 *Seien $\mathfrak{U}, \mathfrak{V} \leq [U, U]$ gutartig mit $R_1 := R(\mathfrak{U})$ und $R_2 := R(\mathfrak{V})$.*

(i) Falls $R_1 \neq R_2$ ist, gilt für alle ungeraden $n \in \mathbb{N}$ mit $n \geq R_1 + 2R_2$, daß $F_n([\mathfrak{U}, \mathfrak{V}]) = \mathbb{F}_{q^2}$ ist.

(ii) Falls $R_1 = R_2$ ist, gilt für alle ungeraden $n \in \mathbb{N}$ mit $n \geq R_1 + 2R_2 + 2$, daß $F_n([\mathfrak{U}, \mathfrak{V}]) = \mathbb{F}_{q^2}$ ist.

Beweis: (i) Die Aussage folgt direkt aus Satz 6.2.1.9

(ii) Die Aussage folgt wegen $R_1 + 2 \neq R_2$ sowie $R_1 + 2 \geq R(\mathfrak{U})$ und $R_2 \geq R(\mathfrak{V})$ aus Satz 6.2.1.9. □

Satz 6.2.1.11 *Sei $q \neq 2$. Seien weiter $\mathfrak{U}, \mathfrak{V} \leq [U, U]$ gutartig mit $R(\mathfrak{U}) = R(\mathfrak{V}) = n$. Dann gilt $F_{3n}([\mathfrak{U}, \mathfrak{V}]) = \mathbb{F}_{q^2}$.*

Beweis: Sei $g \in \mathbb{F}_{q^2}$ beliebig. Dann gibt es nach Lemma 1.1.7 ein $r \in \mathbb{N}$ sowie Elemente $g_1, \ldots, g_r \in \mathbb{F}_{q^2}$ mit $g = g_1 + \ldots + g_r$, so daß es für alle $i = 1, \ldots, r$ Elemente $a_i, b_i \in \mathbb{F}_{q^2}$ gibt mit $a_i b_i^q + a_i b_i^q = 0$ und $g_i = a_i b_i^{q+1} + a_i^{q+1} b_i$. Sei nun $i \in \{1, \ldots, r\}$ festgewählt und $a, b \in \mathbb{F}_{q^2}$ mit $ab^q + ab^q = 0$ und $g_i = ab^{q+1} + a^{q+1}b$. Wegen $a^{q+1}, b^{q+1} \in \mathbb{F}_q$ gibt es nach Satz 1.1.3 Elemente $c, d \in \mathbb{F}_{q^2}$ mit $c^q + c = a^{q+1}$ und $d^q + d = b^{q+1}$. Für $\tilde{x} := 1 + a\tau^n + c\tau^{2n}$ gilt nun die Kongruenz

$$\begin{aligned} \mathrm{N}(\tilde{x}) &= (1 + a\tau^n + c\tau^{2n})(1 + a\tau^n + c^q\tau^{2n}) \\ &\equiv 1 + (c^q + a^{q+1} + c)\tau^{2n} \mod U_{3n+1} \\ &\equiv 1 \mod U_{3n+1}. \end{aligned}$$

Außerdem sind die Bedingungen $R(\tilde{x}) \geq n \geq R(\mathfrak{U})$ und $S(\tilde{x}) \geq 2n = 2R(\mathfrak{U}) \geq S(\mathfrak{U})$ nach Lemma 6.1.12 erfüllt. Damit folgt nach Satz 6.1.22, daß es ein $x^* \in (\tau^{3n+1}) \cap Q_0$ und ein $x \in \mathfrak{U}$ gibt mit $x \equiv \tilde{x} + x^* \mod U_{3n+1}$. Für $\tilde{y} := 1 + b\tau^n + d\tau^{2n}$ gilt nun die Kongruenz

$$\begin{aligned} \mathrm{N}(\tilde{y}) &= (1 + b\tau^n + d\tau^{2n})(1 + b\tau^n + d^q\tau^{2n}) \\ &\equiv 1 + (d^q + b^{q+1} + d)\tau^{2n} \mod U_{3n+1} \\ &\equiv 1 \mod U_{3n+1}. \end{aligned}$$

Außerdem sind die Bedingungen $R(\tilde{y}) \geq n \geq R(\mathfrak{V})$ und $S(\tilde{y}) \geq 2n = 2R(\mathfrak{V}) \geq S(\mathfrak{V})$ nach Lemma 6.1.12 erfüllt. Damit folgt nach Satz 6.1.22, daß es ein $x^* \in (\tau^{3n+1}) \cap Q_0$ und ein $y \in \mathfrak{V}$ gibt mit $y \equiv \tilde{y} + y^* \mod U_{3n+1}$. Damit erhält man nun die Kongruenzen

$$\begin{aligned} xy &\equiv (1 + a\tau^n + c\tau^{2n} + x^*)(1 + b\tau^n + d\tau^{2n}) \mod U_{3n+1} \\ &\equiv 1 + (a + b)\tau^n + (d + ab^q + c)\tau^{2n} + (ad^q + cb)\tau^{3n} \mod U_{3n+1} \end{aligned}$$

sowie

$$\begin{aligned} yx &\equiv (1 + b\tau^n + d\tau^{2n})(1 + a\tau^n + c\tau^{2n} + x^*) \mod U_{3n+1} \\ &\equiv 1 + (a + b)\tau^n + (d + ba^q + c)\tau^{2n} + (bc^q + da)\tau^{3n} \mod U_{3n+1}. \end{aligned}$$

Wegen $ab^q = ba^q$ folgt daraus

$$xy \equiv (1 + (ad^q + cb + da + bc^q)\tau^{3n})yx \mod U_{3n+1}.$$

Damit erhält man nun

$$\begin{aligned} xyx^{-1}y^{-1} &\equiv 1 + (a(d + d^q) + b(c + c^q))\tau^{3n} \mod U_{3n+1} \\ &\equiv 1 + (ab^{q+1} + ba^{q+1})\tau^{3n} \mod U_{3n+1} \\ &\equiv 1 + g_i\tau^{3n} \mod U_{3n+1}. \end{aligned}$$

Wegen $xyx^{-1}y^{-1} \in [\mathfrak{U}, \mathfrak{V}]$ folgt $g_i \in F_{3n}([\mathfrak{U}, \mathfrak{V}])$. Da $i \in \{1, \ldots, r\}$ beliebig gewählt war, folgt auf diese Weise $g = g_1 + \ldots + g_r \in F_{3n}([\mathfrak{U}, \mathfrak{V}])$ nach Lemma 4.2.4. □

Satz 6.2.1.12 *Sei $q \neq 2$. Seien weiter $\mathfrak{U}, \mathfrak{V} \leq [U, U]$ gutartig mit $R_1 := R(\mathfrak{U})$ und $R_2 := R(\mathfrak{V})$. Dann gilt für alle ungeraden $n \in \mathbb{N}$ mit $n \geq R_1 + 2R_2$, daß $F_n([\mathfrak{U}, \mathfrak{V}]) = \mathbb{F}_{q^2}$ ist.*

Beweis: Falls $R_1 \neq R_2$ ist, folgt die Aussage aus Korollar 6.2.1.10(i). Falls $R_1 = R_2$ und $n > R_1 + 2R_2$ ist, folgt die Aussage aus Korollar 6.2.1.10(ii). Für den Fall $R_1 = R_2$ und $n = R_1 + 2R_2$ ergibt sich die Aussage aus Satz 6.2.1.11. □

Die Ergebnisse dieses Unterabschnittes lassen sich nun folgendermaßen zusammenfassen.

Hauptsatz 6.2.1.13 *Sei $q \neq 2$. Seien weiter $\mathfrak{U}, \mathfrak{V} \leq [U, U]$ gutartig mit $R_1 := R(\mathfrak{U})$, $S_1 := S(\mathfrak{U})$, $R_2 := R(\mathfrak{V})$ und $S_2 := S(\mathfrak{V})$. Man setze $\tilde{S} := \min\{2S_1 + 2R_2, 2S_2 + 2R_1, R_1 + R_2\}$ und $\tilde{R} := \min\{2S_1 + R_2, 2S_2 + R_1, 2R_1 + R_2, R_1 + 2R_2\}$. Dann ist $[\mathfrak{U}, \mathfrak{V}]$ gutartig mit $R([\mathfrak{U}, \mathfrak{V}]) = \tilde{R}$ und $S([\mathfrak{U}, \mathfrak{V}]) = \tilde{S}$.*

Beweis: Offensichtlich ist $\tilde{R}$ ungerade, $\tilde{S}$ gerade und $[\mathfrak{U}, \mathfrak{V}]$ eine Untergruppe von $[U, U]$. Außerdem gelten die folgenden Aussagen:

(i) Nach Korollar 6.2.1.3 gilt für alle $z \in [\mathfrak{U}, \mathfrak{V}]$, daß $R(z) \geq \tilde{R}$ und $S(z) \geq \tilde{S}$ ist.

(ii) Aus Lemma 6.2.1.8 und Satz 6.2.1.12 folgt, daß für alle ungeraden $n \in \mathbb{N}$ mit $n \geq \tilde{R}$ die Bedingung $F_n([\mathfrak{U}, \mathfrak{V}]) = \mathbb{F}_{q^2}$ gilt.

(iii) Aus Lemma 6.2.1.4 und Satz 6.2.1.7 folgt, daß für alle geraden $n \in \mathbb{N}$ mit $n \geq \tilde{S}$ die Bedingung $F_n([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$ gilt.

Insgesamt folgt daraus nach Lemma 6.1.8, daß $[\mathfrak{U}, \mathfrak{V}]$ gutartig ist mit $R([\mathfrak{U}, \mathfrak{V}]) = \tilde{R}$ und $S([\mathfrak{U}, \mathfrak{V}]) = \tilde{S}$. □

6.2.2 Der Kommutator zweier gutartiger Untergruppen von $[U, U]$ im Fall $q = 2$

Für $q = 2$ läßt sich die Abschätzung von Satz 6.2.1.2 noch verschärfen.

Satz 6.2.2.1 *Sei $q = 2$. Seien weiter $x, y \in [U, U]$ mit $R(x), R(y) \geq n$ und $T(x), T(y) \geq 2n$ für ein ungerades $n \in \mathbb{N}$. Dann gilt $R(xyx^{-1}y^{-1}) > 3n$.*

Beweis: Für x und y existieren die Zerlegungen $x = x_0 + x_1$ und $y = y_0 + y_1$ mit $x_0, y_0 \in Q_0$ und $x_1, y_1 \in Q_1$. Dabei sind nun x_0, x_1, y_0 und y_1 von der Form

$$x_0 = 1 + \sum_{i=n}^{\infty}{}'' a_i\tau^i,\ x_1 = \sum_{i=2}^{\infty}{}' a_i\tau^i,\ y_0 = 1 + \sum_{i=n}^{\infty}{}'' b_i\tau^i \text{ und } y_1 = \sum_{i=2}^{\infty}{}'' b_i\tau^i,$$

wobei nun die Koeffizienten $a_2, a_4, \ldots, a_{2n-2}$ sowie $b_2, b_4, \ldots, b_{2n-2}$ in $\mathbb{F}_q$ liegen müssen. Daraus folgt nun die Kongruenz

$$\begin{aligned} x_0 + \overline{x}_0 &\equiv \sum_{i=2}^{2n}{}'' (a_i^q + a_i)\tau^i \mod (\tau^{2n+1}) \\ &\equiv (a_{2n}^q + a_{2n})\tau^{2n} \mod (\tau^{2n+1}) \end{aligned}$$

und analog dazu

$$y_0 + \overline{y}_0 \equiv (a_{2n}^q + a_{2n})\tau^{2n} \mod (\tau^{2n+1}).$$

Wie im Beweis von Satz 6.2.1.2 erhält man für den Kommutator die Zerlegung $xyx^{-1}y^{-1} = z_0 + z_1$ mit $z_0 \in Q_0$ und

$$z_1 = \sum_{\substack{i,j,k,l \in \{0,1\} \\ i+j+k+l \ \text{ungerade}}} x_i y_j \overline{x}_k \overline{y}_l.$$

Für die einzelnen Summanden erhält man nun die Kongruenzen

$$\begin{aligned} x_0 y_1 \overline{x}_1 \overline{y}_1 &\equiv 1 \cdot b_n\tau^n \cdot a_n\tau^n \cdot b_n\tau^n \mod (\tau^{3n+1}) \equiv a_n^q b_n^{q+1}\tau^{3n} \mod (\tau^{3n+1}), \\ x_1 y_0 \overline{x}_1 \overline{y}_1 &\equiv a_n\tau^n \cdot 1 \cdot a_n\tau^n \cdot b_n\tau^n \mod (\tau^{3n+1}) \equiv a_n^{q+1} b_n^q \tau^{3n} \mod (\tau^{3n+1}), \\ x_1 y_1 \overline{x}_0 \overline{y}_1 &\equiv a_n\tau^n \cdot b_n\tau^n \cdot 1 \cdot b_n\tau^n \mod (\tau^{3n+1}) \equiv a_n b_n^{q+1}\tau^{3n} \mod (\tau^{3n+1}) \end{aligned}$$

und

$$x_1 y_1 \overline{x}_1 \overline{y}_0 \equiv a_n\tau^n \cdot b_n\tau^n \cdot a_n\tau^n \cdot 1 \mod (\tau^{3n+1}) \equiv a_n^2 b_n^q \tau^{3n} \mod (\tau^{3n+1})$$

sowie

$$\begin{aligned} x_0 y_0 \overline{x}_0 \overline{y}_1 + x_0 y_1 \overline{x}_0 \overline{y}_0 &= x_0 \overline{x}_0 y_0 y_1 + x_0 x_0 y_0 y_1 \\ &= x_0(\overline{x}_0 + x_0) y_0 y_1 \\ &\equiv 1 \cdot (a_{2n} + a_{2n}^q)\tau^{2n} \cdot 1 \cdot b_n\tau^n \mod (\tau^{3n+1}) \\ &\equiv b_n(a_{2n} + a_{2n}^q)\tau^{3n} \mod (\tau^{3n+1}) \end{aligned}$$

und

$$\begin{aligned} x_0 y_0 \overline{x}_1 \overline{y}_0 + x_1 y_0 \overline{x}_0 \overline{y}_0 &= x_1 \overline{x}_0 \overline{y}_0 \overline{x}_0 + x_1 \overline{x}_0 \overline{y}_0 y_0 \\ &= x_1 \overline{x}_0 \overline{y}_0 (\overline{y}_0 + y_0) \\ &\equiv a_n\tau^n \cdot 1 \cdot 1 \cdot (b_{2n}^q + b_{2n})\tau^{2n} \mod (\tau^{3n+1}) \\ &\equiv a_n(b_{2n} + b_{2n}^q)\tau^{3n} \mod (\tau^{3n+1}). \end{aligned}$$

Außerdem gilt nach Korollar 4.3.9 die Gleichung

$$\begin{aligned} a_{2n} + a_{2n}^q &= \sum_{i=1}^{2n-1} a_i a_{2n-i}^q \\ &= \sum_{i=1}^{n-1}{}' \underbrace{a_i}_{=0} a_{2n-i}^q + \sum_{i=1}^{n-1}{}'' a_i \underbrace{a_{2n-i}^q}_{\in \mathbb{F}_q} + a_n a_n^q + \sum_{i=n+1}^{2n-1}{}' a_i \underbrace{a_{2n-i}^q}_{=0} + \sum_{i=n+1}^{2n-1}{}'' a_i \underbrace{a_{2n-i}^q}_{\in \mathbb{F}_q} \\ &= a_n^{q+1} + \sum_{i=1}^{n-1}{}'' a_i a_{2n-i} + \sum_{i=n+1}^{2n-1}{}'' a_i a_{2n-i} \\ &= a_n^{q+1}. \end{aligned}$$

Ebenso zeigt man $b_{2n}^q + b_{2n} = b_n^{q+1}$. Insgesamt erhält man damit die Kongruenz

$$\begin{aligned} z_1 &\equiv (a_n^q b_n^2 + a_n^2 b_n^q + b_n(a_n^{q+1} + a_{2n}^q + a_{2n}) + a_n(b_n^{q+1} + b_{2n}^q + b_{2n}))\tau^{3n} \mod (\tau^{3n+1}) \\ &\equiv (a_n^q b_n^2 + a_n^2 b_n^q)\tau^{3n} \mod (\tau^{3n+1}) \\ &\equiv 0 \mod (\tau^{3n+1}). \end{aligned}$$

Das besagt nun nichts anderes, als daß $R(xyx^{-1}y^{-1}) > 3n$ ist. □

Korollar 6.2.2.2 *Sei $q = 2$. Seien weiter $\mathfrak{U}, \mathfrak{V} \le [U,U]$ gutartig mit $R_1 := R(\mathfrak{U})$, $R_2 := R(\mathfrak{V})$, $S_1 := S(\mathfrak{U})$ und $S_2 := S(\mathfrak{V})$. Man setze $\tilde{S} := \min\{2S_1 + 2R_2, 2S_2 + 2R_1, R_1 + R_2\}$ und $\tilde{R} := \min\{2S_1 + R_2, 2S_2 + R_1, 2R_1 + R_2, R_1 + 2R_2\}$. Dann gilt für alle $z \in [\mathfrak{U}, \mathfrak{V}]$, daß $R(z) \ge \tilde{R}$ und $S(z) \ge \tilde{S}$ ist. Falls zusätzlich $S_1 \ge R_1$, $S_2 \ge R_2$ und $R_1 = R_2$ ist, gilt sogar $R(z) \ge \tilde{R} + 2$.*

Beweis: Die Aussagen $R(z) \ge \tilde{R}$ und $S(z) \ge \tilde{S}$ gelten nach Korollar 6.2.1.3. Sei also $S_1 \ge R_1$, $S_2 \ge R_2$ und $R_1 = R_2$. Man setze $n := R_1 = R_2$. Dann gilt

$$\tilde{S} = \min\{2S_1 + 2n, 2S_2 + 2n, n\} = 2n \text{ und } \tilde{R} = \min\{2S_1 + n, 2S_2 + n, 3n\} = 3n.$$

Man definiere nun $W_1 := \{xyx^{-1}y^{-1} \mid x \in \mathfrak{U}, y \in \mathfrak{V}\}$ und $W_2 := \{yxy^{-1}x^{-1} \mid x \in \mathfrak{U}, y \in \mathfrak{V}\}$. Sei nun $w_1 = xyx^{-1}y^{-1} \in W_1$ beliebig mit $x \in \mathfrak{U}$ und $y \in \mathfrak{V}$. Wegen $R(x), R(y) \ge n$ und $T(x) \ge T(\mathfrak{U}) = \min\{2R(\mathfrak{U}), 2S(\mathfrak{U})\} = 2n$ sowie $T(y) \ge T(\mathfrak{V}) = \min\{2R(\mathfrak{V}), 2S(\mathfrak{V})\} = 2n$ gemäß Lemma 6.1.13 folgt nach Satz 6.2.2.1, daß $R(w_1) > 3n$ bzw. $R(w_1) \ge 3n + 2 = \tilde{R}$ ist. Ebenso zeigt man $R(w_2) \ge \tilde{R}$ für alle $w_2 \in W_2$, so daß man insgesamt $R(w) \ge \tilde{R}$ für alle $w \in W_1 \cup W_2$ erhält. Sei nun $z \in [\mathfrak{U}, \mathfrak{V}]$ beliebig. Dann läßt sich z als *endliches* Produkt $z = w^{(1)} \cdot \ldots \cdot w^{(n)}$ von Elementen $w^{(1)}, \ldots, w^{(n)} \in W_1 \cup W_2$ schreiben. Wegen $2(\tilde{R} + 2) = 6n + 4 \ge 2n = \tilde{S}$ folgt durch fortlaufende Anwendung von Lemma 6.1.10, daß $S(z) \ge \tilde{S}$ und $R(z) \ge \tilde{R}$ gilt. □

Hauptsatz 6.2.2.3 *Sei $q = 2$. Seien weiter $\mathfrak{U}, \mathfrak{V} \le [U,U]$ gutartig mit $R_1 := R(\mathfrak{U})$, $R_2 := R(\mathfrak{V})$, $S_1 := S(\mathfrak{U})$ und $S_2 := S(\mathfrak{V})$. Man setze $\tilde{S} := \min\{2S_1 + 2R_2, 2S_2 + 2R_1, R_1 + R_2\}$ und $\tilde{R} := \min\{2S_1 + R_2, 2S_2 + R_1, 2R_1 + R_2, R_1 + 2R_2\}$. Dann ist $[\mathfrak{U}, \mathfrak{V}]$ gutartig mit $S([\mathfrak{U}, \mathfrak{V}]) = \tilde{S}$. Falls zusätzlich $S_1 \ge R_1$, $S_2 \ge R_2$ und $R_1 = R_2$ gilt, ist $R([\mathfrak{U}, \mathfrak{V}]) = \tilde{R} + 2$. Ansonsten ist $R([\mathfrak{U}, \mathfrak{V}]) = \tilde{R}$.*

Beweis: Man setze $R := \tilde{R} + 2$, falls $S_1 \ge R_1$, $S_2 \ge R_2$ und $R_1 = R_2$ gilt, und $R := \tilde{R}$ in allen anderen Fällen. Offensichtlich ist nun R ungerade und $\tilde{S}$ gerade sowie $[\mathfrak{U}, \mathfrak{V}]$ eine Untergruppe von $[U,U]$. Außerdem gelten die folgenden Aussagen:

(i) Nach Korollar 6.2.2.2 gilt für alle $z \in [\mathfrak{U}, \mathfrak{V}]$, daß $R(z) \ge R$ und $S(z) \ge \tilde{S}$ ist.

(ii) Falls $R_1 \ne R_2$ ist, folgt aus Lemma 6.2.1.8 und Korollar 6.2.1.10(i), daß für alle ungeraden $n \in \mathbb{N}$ mit $n \ge \tilde{R}$ die Bedingung $F_n([\mathfrak{U}, \mathfrak{V}]) = \mathbb{F}_{q^2}$ gilt. Falls $R_1 = R_2$ und ($S_1 \le R_1$ oder $S_2 \le R_2$) ist, folgt dieser Sachverhalt wegen $R = \min\{2S_1 + R_2, 2S_2 + R_1\}$ allein aus Lemma 6.2.1.8. Falls dagegen $R_1 = R_2$, $S_2 \ge R_2$ und $R_1 = R_2$ ist, folgt dieser Sachverhalt wegen $R = R_1 + 2R_2 + 2$ allein aus Korollar 6.2.1.10(ii).

(iii) Aus Lemma 6.2.1.4 und Satz 6.2.1.7 folgt, daß für alle geraden $n \in \mathbb{N}$ mit $n \ge \tilde{S}$ die Bedingung $F_n([\mathfrak{U}, \mathfrak{V}]) \supset \mathbb{F}_q$ gilt.

Insgesamt folgt daraus nach Lemma 6.1.8, daß $[\mathfrak{U}, \mathfrak{V}]$ gutartig ist mit $R([\mathfrak{U}, \mathfrak{V}]) = R$ und $S([\mathfrak{U}, \mathfrak{V}]) = \tilde{S}$, was nach der Definition von R der Aussage des Haupsatzes entspricht. □

6.2.3 Der Kommutator von U_n mit einer gutartigen Untergruppe von $[U,U]$

Hier ist es zunächst erforderlich $R(U_n)$, $S(U_n)$ und $T(U_n)$ zu bestimmen.

Lemma 6.2.3.1 *Sei $n \in \mathbb{N}$. Dann gilt:*

(i) $R(U_n) = \begin{cases} n & \text{falls } n \text{ ungerade} \\ n+1 & \text{falls } n \text{ gerade,} \end{cases}$

(ii) $S(U_n) = \begin{cases} n+1 & \text{falls } n \text{ ungerade} \\ n & \text{falls } n \text{ gerade,} \end{cases}$

(iii) $T(U_n) = \begin{cases} n+1 & \text{falls } n \text{ ungerade} \\ n & \text{falls } n \text{ gerade.} \end{cases}$

Beweis: Sei $\tilde{g}(n)$ die kleinste gerade Zahl größer oder gleich n und $\tilde{u}(n)$ die kleinste ungerade Zahl größer oder gleich n. Dann gilt offensichtlich

$$\tilde{g}(n) = \left\{ \begin{array}{ll} n & \text{falls } n \text{ ungerade} \\ n+1 & \text{falls } n \text{ gerade} \end{array} \right\} \text{ und } \tilde{u}(n) = \left\{ \begin{array}{ll} n+1 & \text{falls } n \text{ ungerade} \\ n & \text{falls } n \text{ gerade} \end{array} \right\}.$$

Damit bleibt $R(U_n) = \tilde{u}(n)$ und $S(U_n) = T(U_n) = \tilde{g}(n)$ zu zeigen. Sei dazu $x \in U_n$ beliebig. Dann ist x von der Form $x = \sum_{i=n}^{\infty} a_i \tau^i$. Da $R(x)$ immer ungerade ist und und $S(x)$ bzw. $T(x)$ immer gerade sind, folgt sofort $R(x) \geq \tilde{u}(n)$ und $S(x), T(x) \geq \tilde{g}(n)$. Damit erhält man $R(U_n) \geq \tilde{u}(n)$ und $S(U_n), T(U_n) \geq \tilde{g}(n)$. Wählt man $x := 1 + \tau^{\tilde{u}(n)}$, so gilt $R(x) = \tilde{u}(n)$ und damit $R(U_n) = \tilde{u}(n)$. Wählt man dagegen $x := 1 + \alpha\tau^{\tilde{g}(n)}$, so gilt $S(x), T(x) = \tilde{g}(n)$, womit man $S(U_n) = T(U_n) = \tilde{g}(n)$ erhält. □

Satz 6.2.3.2 *Sei $n \in \mathbb{N}$ und $\mathfrak{U} \leq [U,U]$ gutartig. Seien weiter $S_1 := S(U_n)$, $S_2 := S(\mathfrak{U})$, $R_1 := R(U_n)$ und $R_2 := R(\mathfrak{U})$. Man setze $\tilde{S} := \min\{2S_2 + 2R_1, R_1 + R_2\}$ und $\tilde{R} := \min\{2S_1 + R_2, 2S_2 + R_1, R_1 + 2R_2\}$. Dann gilt für alle $x \in [U_n, \mathfrak{U}]$, daß $R(z) \geq \tilde{R}$ und $S(z) \geq \tilde{S}$ ist.*

Beweis: Man setze $T_1 := T(U_n)$ und $T_2 := T(\mathfrak{U})$. Aus Lemma 6.2.3.1 folgt $T_1 + 1 \geq R_1$ und damit $T_1 + 2R_2 \geq R_1 + R_2$. Wegen $T_2 = \min\{2S_2, 2R_2\}$ nach Lemma 6.1.13 erhält man

$$\tilde{S} = \min\{T_1 + 2R_2, T_2 + 2R_1, R_1 + R_2\}.$$

Da nach Lemma 6.2.3.1 außerdem $R_1 + 1 \geq T_1$ und damit $2R_1 + R_2 \geq T_1 + R_2$ sowie $T_1 = S_1$ gilt, erhält man zusätzlich

$$\tilde{R} = \min\{T_1 + R_2, T_2 + R_1, 2R_1 + R_2, R_1 + 2R_2\}.$$

Man definiere nun $W_1 := \{xyx^{-1}y^{-1} \mid x \in U_n, y \in \mathfrak{U}\}$ und $W_2 := \{yxy^{-1}x^{-1} \mid x \in U_n, y \in \mathfrak{U}\}$. Sei nun $w_1 = xyx^{-1}y^{-1} \in W_1$ beliebig mit $x \in U_n$ und $y \in \mathfrak{U}$. Wegen $R(x) \geq R_1$ und $R(y) \geq R_2$ sowie $T(x) \geq T_1$ und $T(y) \geq T_2$ folgt nun aus Satz 6.2.1.2, daß $R(w_1) \geq \tilde{R}$ und $S(w_1) \geq \tilde{S}$ gilt. Ebenso zeigt man $R(w_2) \geq \tilde{R}$ und $S(w_2) \geq \tilde{S}$ für alle $w_2 \in W_2$, so daß man insgesamt $R(w) \geq \tilde{R}$ und $S(w) \geq \tilde{S}$ für alle $w \in W_1 \cup W_2$ erhält. Sei nun $z \in [\mathfrak{U}, U_n]$ beliebig. Dann läßt sich z als *endliches* Produkt $z = w^{(1)} \cdot \ldots \cdot w^{(n)}$ von Elementen $w^{(1)}, \ldots, w^{(n)} \in W_1 \cup W_2$ schreiben. Wegen

$$2\tilde{R} = \min\{2T_1 + 2R_2, 2T_2 + 2R_1, 4R_1 + 2R_2, 2R_1 + 4R_2\} \geq \tilde{S}$$

folgt durch fortlaufende Anwendung von Lemma 6.1.10, daß $S(z) \geq \tilde{S}$ und $R(z) \geq \tilde{R}$ gilt. □

Lemma 6.2.3.3 *Sei $n \in \mathbb{N}$ und $\mathfrak{U} \leq [U,U]$ gutartig. Man setze $R_1 := R(U_n)$ und $S_2 := S(\mathfrak{U})$. Dann gilt für alle geraden $m \in \mathbb{N}$ mit $m \geq 2R_1 + 2S_2$, daß $F_m([U_n, \mathfrak{U}]) \supset \mathbb{F}_q$ ist.*

Beweis: Es gilt $[U_n, \mathfrak{U}] \geq [E_n, \mathfrak{U}]$, wobei E_n gutartig ist mit $R(E_n) = R(U_n)$ (vgl. Beispiel 6.1.9 und Lemma 6.2.3.1). Aus Satz 6.2.1.7 folgt $F_m([U_n, \mathfrak{U}]) \supset F_m([E_n, \mathfrak{U}]) \supset \mathbb{F}_q$. □

Lemma 6.2.3.4 *Sei $n \in \mathbb{N}$ und $\mathfrak{U} \leq [U,U]$ gutartig. Man setze $R_1 := R(U_n)$ und $R_2 := R(\mathfrak{U})$. Dann gilt für alle geraden $m \in \mathbb{N}$ mit $m \geq R_1 + R_2$, daß $F_m([U_n, \mathfrak{U}]) \supset \mathbb{F}_q$ ist.*

Beweis: Es gilt $[U_n, \mathfrak{U}] \geq [E_n, \mathfrak{U}]$, wobei E_n gutartig ist mit $R(E_n) = R(U_n)$. Aus Lemma 6.2.1.4 folgt $F_m([U_n, \mathfrak{U}]) \supset F_m([E_n, \mathfrak{U}]) \supset \mathbb{F}_q$. □

Lemma 6.2.3.5 *Sei $n \in \mathbb{N}$ und $\mathfrak{U} \le [U,U]$ gutartig. Man setze $R_1 := R(U_n)$ und $R_2 := R(\mathfrak{U})$. Dann gilt für alle ungeraden $m \in \mathbb{N}$ mit $m \ge R_1 + 2R_2$, daß $F_m([U_n,\mathfrak{U}]) = \mathbb{F}_{q^2}$ ist.*

Beweis: Man setze $j := R_2$ und $i := m - 2j$. Dann gilt $m = i + 2j$, wobei i und j ungerade sind mit $i \ge R(U_n)$ und $j = R(\mathfrak{U})$.

Sei nun $g \in \mathbb{F}_{q^2}$ beliebig. Nach Lemma 1.1.6 gibt es nun Elemente $a, b \in \mathbb{F}_{q^2}$ mit $ab^q + ba^q = 0$ und $g = ab^{q+1}$. Wegen $b^{q+1} \in \mathbb{F}_q$ folgt nach Satz 1.1.3, daß es ein $c \in \mathbb{F}_{q^2}$ gibt mit $c^q + c = b^{q+1}$. Für $\tilde{y} := 1 + b\tau^j + c\tau^{2j}$ gilt nun die Kongruenz

$$\begin{aligned} \mathrm{N}(\tilde{y}) &= (1 + b\tau^j + c\tau^{2j})(1 + b\tau^j + c^q\tau^{2j}) \\ &\equiv 1 + (c + b^{q+1} + c^q)\tau^{2j} \mod U_{2j+1} \\ &\equiv 1 \mod U_{2j+1}. \end{aligned}$$

Außerdem sind die Bedingungen $R(\tilde{y}) \ge j \ge R(\mathfrak{V})$ und $S(\tilde{y}) \ge 2j = 2R(\mathfrak{V}) \ge S(\mathfrak{V})$ nach Lemma 6.1.12 erfüllt. Damit folgt nach Satz 6.1.22, daß es ein $y^* \in (\tau^{2j+2}) \cap Q_0$ und ein $y \in \mathfrak{V}$ gibt mit $y \equiv \tilde{y} + y^* \mod U_{n+1}$. Man setze nun $x := 1 + a\tau^i \in U_n$.

Wegen $m = i + 2j$ erhält man nun die Kongruenzen

$$\begin{aligned} yx &\equiv (1 + b\tau^j + c\tau^{2j} + y^*)(1 + a\tau^i) \mod U_{m+1} \\ &\equiv 1 + b\tau^j + c\tau^{2j} + a\tau^i + ab^q\tau^{i+j} + y^* + ac\tau^m \mod U_{m+1} \end{aligned}$$

sowie

$$\begin{aligned} xy &\equiv (1 + a\tau^i)(1 + b\tau^j + c\tau^{2j} + y^*) \mod U_{m+1} \\ &\equiv 1 + b\tau^j + c\tau^{2j} + a\tau^i + ba^q\tau^{i+j} + x^* + y^* + ac^q\tau^m \mod U_{m+1}. \end{aligned}$$

Wegen $ab^q = ba^q$ folgt daraus die Kongruenz

$$xy \equiv (1 + a(c^q + c)\tau^m)yx \mod U_{m+1}.$$

Hieraus ergibt sich

$$\begin{aligned} xyx^{-1}y^{-1} &\equiv 1 + ab^{q+1}\tau^m \mod U_{m+1} \\ &\equiv 1 + g\tau^m \mod U_{m+1}. \end{aligned}$$

Wegen $xyx^{-1}y^{-1} \in [\mathfrak{U}, U_n]$ folgt nun $g \in F_n([U_n,\mathfrak{U}])$. Da $g \in \mathbb{F}_{q^2}$ beliebig gewählt war, ist damit $F_n([U_n,\mathfrak{U}]) = \mathbb{F}_{q^2}$ gezeigt. □

Lemma 6.2.3.6 *Sei $n \in \mathbb{N}$ und $\mathfrak{U} \le [U,U]$ gutartig. Man setze $R_1 := R(U_n)$ und $S_2 := S(\mathfrak{U})$. Dann gilt für alle ungeraden $m \in \mathbb{N}$ mit $m \ge 2S_2 + R_1$, daß $F_m([U_n,\mathfrak{U}]) = \mathbb{F}_{q^2}$ ist.*

Beweis: Es gilt $[U_n,\mathfrak{U}] \ge [E_n,\mathfrak{U}]$, wobei E_n gutartig ist mit $R(E_n) = R(U_n)$. Aus Lemma 6.2.1.8 folgt $F_m([U_n,\mathfrak{U}]) = F_m([E_n,\mathfrak{U}]) = \mathbb{F}_{q^2}$. □

Lemma 6.2.3.7 *Sei $n \in \mathbb{N}$ und $\mathfrak{U} \le [U,U]$ gutartig. Man setze $S_1 := S(U_n)$ und $R_2 := R(\mathfrak{U})$. Dann gilt für alle ungeraden $m \in \mathbb{N}$ mit $m \ge S_1 + R_2$, daß $F_m([U_n,\mathfrak{U}]) = \mathbb{F}_{q^2}$ ist.*

Beweis: Man setze $i := S_1$ und $j := m - i$. Dann gilt $m = i + j$, wobei i gerade und j ungerade sowie $j \ge R(\mathfrak{U})$ und $i \ge n$ ist.

Sei nun $g \in \mathbb{F}_{q^2}$ beliebig. Man wähle $a \in \mathbb{F}_{q^2} - \mathbb{F}_q$ und setze $b := \frac{g}{a+a^q}$. Außerdem wähle man $y \in \mathfrak{U}$ mit $y \equiv 1 + b\tau^j \mod U_{j+1}$. Für $x := 1 + a\tau^i \in U_n$ erhält man nun nach Lemma 4.1.1 die Kongruenz

$$\begin{aligned} xy &\equiv (1 + (ab^{q^i} + ba^{q^j})\tau^m)yx \mod U_{m+1} \\ &\equiv (1 + b(a^q + a)\tau^m)yx \mod U_{m+1}. \end{aligned}$$

Daraus folgt

$$xyx^{-1}y^{-1} \equiv 1 + g\tau^m \mod U_{m+1}.$$

Wegen $xyx^{-1}y^{-1} \in [U_n, \mathfrak{U}]$ folgt $g \in F_m([U_n, \mathfrak{U}])$. Da $g \in \mathbb{F}_{q^2}$ beliebig gewählt war, ist damit $F_m([U_n, \mathfrak{U}]) = \mathbb{F}_{q^2}$ gezeigt. □

Auch die Ergebnisse dieses Unterabschnittes lassesn sich in einem Satz zusammenfassen.

Hauptsatz 6.2.3.8 *Sei $n \in \mathbb{N}$ und $\mathfrak{U} \leq [U, U]$ gutartig mit $S_1 := S(U_n)$, $S_2 := S(\mathfrak{U})$, $R_1 := R(U_n)$ und $R_2 := R(\mathfrak{U})$. Man setze weiter $\tilde{S} := \min\{2S_2 + 2R_1, R_1 + R_2\}$ und $\tilde{R} := \min\{S_1 + R_2, 2S_2 + R_1, R_1 + 2R_2\}$. Dann ist $[U_n, \mathfrak{U}]$ gutartig mit $R([U_n, \mathfrak{U}]) = \tilde{R}$ und $S([U_n, \mathfrak{U}]) = \tilde{S}$.*

Beweis: Offensichtlich ist $\tilde{R}$ ungerade und $\tilde{S}$ gerade und $[\mathfrak{U}, U_n]$ eine Untergruppe von $[U, U]$. Außerdem gelten die folgenden Aussagen:

(i) Nach Satz 6.2.3.2 gilt für alle $z \in [U_n, \mathfrak{U}]$, daß $R(z) \geq \tilde{R}$ und $S(z) \geq \tilde{S}$ ist.

(ii) Aus den Lemmata 6.2.3.5, 6.2.3.6 und 6.2.3.7 folgt, daß für alle ungeraden $n \in \mathbb{N}$ mit $m \geq \tilde{R}$ die Bedingung $F_m([U_n, \mathfrak{U}]) = \mathbb{F}_{q^2}$ gilt.

(iii) Aus den Lemmata 6.2.3.3 und 6.2.3.4 folgt, daß für alle geraden $n \in \mathbb{N}$ mit $m \geq \tilde{S}$ die Bedingung $F_m([U_n, \mathfrak{U}]) \supset \mathbb{F}_q$ gilt.

Insgesamt folgt daraus nach Lemma 6.1.8, daß $[U_n, \mathfrak{U}]$ gutartig ist mit $R([U_n, \mathfrak{U}]) = \tilde{R}$ und $S([U_n, \mathfrak{U}]) = \tilde{S}$. □

6.3 Folgerungen aus den Hauptsätzen

6.3.1 Die absteigende Zentralreihe von U_n

Satz 6.3.1.1 *Sei $k \in \mathbb{N}$ und $n \in \mathbb{N}_0$. Dann ist $Z^k(U_n)$ gutartig. Für die Charakterisierungsindizes erhält man:*

(i) Falls n gerade ist, gilt $R(Z^k(U_n)) = (k+1)n + 1$ und $S(Z^k(U_n)) = (k+1)n + 2$.

(ii) Falls n ungerade ist, gilt $R(Z^k(U_n)) = k(n+1) + n$ und $S(Z^k(U_n)) = k(n+1) + n - 1$.

Beweis: Sei zunächst $n = 0$. Wegen $[U_0, U_0] = E_1$ nach Korollar 4.3.5 und $[E_1, U_0] = E_1$ nach Korollar 4.4.3 folgt $Z^k(U_0) = E_1$ für alle $n \in \mathbb{N}$. Nach Beispiel 6.1.9 ist E_1 gutartig mit $R(E_1) = 1$ und $S(E_1) = 2$. Damit ist die Aussage des Satzes für den Fall $n = 0$ gezeigt. Für alle übrigen $n \in \mathbb{N}_0$ erfolgt der Beweis durch Induktion über k.

1. Fall n gerade: Für $k = 1$ gilt $Z^1(U_n) = [U_n, U_n] = E_{2n+1}$ nach Korollar 4.3.5. Nach Beispiel 6.1.9 ist $Z^1(U_n)$ gutartig mit $R(Z^1(U_n)) = 2n+1$ und $S(Z^1(U_n)) = 2n+2$. Sei nun $k \in \mathbb{N}$ beliebig. Nach Induktionsannahme ist $Z^k(U_n)$ eine gutartige Untergruppe von $[U, U]$ mit $R(Z^k(U_n)) = (k+1)n + 1$ und $S(Z^k(U_n)) = (k+1)n + 2$. Wegen $R(U_n) = n + 1$ und $S(U_n) = n$ folgt nach Hauptsatz 6.2.3.8, daß $Z^{k+1}(U_n)$ gutartig ist mit

$$\begin{aligned} R(Z^{k+1}(U_n)) &= \min\{n + (k+1)n + 1, 2((k+1)n + 2) + n + 1, n + 1 + 2((k+1)n + 1)\} \\ &= (k+2)n + 1 \end{aligned}$$

und

$$\begin{aligned} S(Z^{k+1}(U_n)) &= \min\{2((k+1)n + 2) + 2(n+1), n + 1 + (k+1)n + 1\} \\ &= (k+2)n + 2. \end{aligned}$$

2. Fall n ungerade: Für $k = 1$ gilt $Z^1(U_n) = [U_n, U_n] = E_{2n}$ nach Korollar 4.3.5. Nach Beispiel 6.1.9 ist $Z^1(U_n)$ gutartig mit $R(Z^1(U_n)) = 2n + 1$ und $S(Z^1(U_n)) = 2n$. Sei nun $k \in \mathbb{N}$ beliebig.

Nach Induktionsannahme ist $Z^k(U_n)$ eine gutartige Untergruppe von $[U,U]$ mit $R(Z^k(U_n)) = k(n+1)+n$ und $S(Z^k(U_n)) = k(n+1)+n-1$. Wegen $R(U_n) = n$ und $S(U_n) = n+1$ folgt nach Hauptsatz 6.2.3.8, daß $Z^{k+1}(U_n)$ gutartig ist mit

$$\begin{aligned} R(Z^{k+1}(U_n)) &= \min\{n+1+k(n+1)+n, 2(k(n+1)+n-1)+2n, n+2(k(n+1)+n)\} \\ &= (k+1)(n+1)+n \end{aligned}$$

und

$$\begin{aligned} S(Z^{k+1}(U_n)) &= \min\{2(k(n+1)+n-1)+2n, n+k(n+1)+n\} \\ &= (k+1)(n+1)+n-1. \end{aligned}$$

□

Korollar 6.3.1.2 *Sei $n \in \mathbb{N}$. Dann gilt:*

(i) G_n ist genau dann nilpotent, wenn $n = 1$ ist. Dabei gilt $l_{nil}(G_1) = 1$.

(ii) Die Faktorgruppe $\hat{G}_n$ ist nilpotent mit der Länge

$$l_{nil}(\hat{G}_n) = \begin{cases} 0 & \text{falls } n = 1 \\ \frac{1}{2}g(n+2) & \text{falls } n \neq 1. \end{cases}$$

Beweis: (i)Für $n = 1$ ist $G_1 \cong \mathbb{F}_{q^2}$ abelsch und damit nilpotent der Länge 1. Sei nun $n \neq 1$. Dann gilt $R(Z^k(U)) = 2$ nach Satz 6.3.1.1 für alle $k \in \mathbb{N}$. Daraus folgt $Z^k(U) \not\subset U_2 \subset U_n$. Das bedeutet $Z^k(G_n) = Z^k(U) \cdot U_n/U_n \neq \{1 \cdot U_n\}$ für alle $k \in \mathbb{N}$. Somit ist G_n nicht nilpotent.

(ii) Offensichtlich besteht $\hat{G}_1$ nur aus dem neutralen Element und ist folglich nilpotent der Länge 0. Weiter gilt $\hat{G}_2 \neq \{1 \cdot U_2\}$ sowie $Z^1(\hat{G}_2) = Z^1(U_1) \cdot U_1/U_2 = E_2 \cdot U_1/U_2 = \{1 \cdot U_2\}$ nach Korollar 4.3.5. Folglich ist $\hat{G}_2$ nilpotent der Länge 1. Damit ist die Aussage des Korollares für den Fall $n \leq 2$ gezeigt. Sei nun $n > 2$. Man setze $k := \frac{1}{2}g(n+2)$.

Falls n ungerade ist, gilt $k = \frac{1}{2}(n+1) \geq 2$. Nach Satz 6.3.1.1 sind $Z^k(U_1)$ und $Z^{k-1}(U_1)$ gutartig, wobei $R(Z^k(U_1)) = n+2$ und $S(Z^k(U_1)) = n+1$ sowie $S(Z^{k-1}(U_1)) = n-1$ ist. Daraus folgt nach Lemma 6.1.5, daß $Z^k(U_1) \subset U_n$ und $Z^{k-1}(U_1) \not\subset U_n$ gilt. Damit erhält man $Z^k(\hat{G}_n) = \{1 \cdot U_n\}$ und $Z^{k-1}(\hat{G}_n) \neq \{1 \cdot U_n\}$. Also ist $\hat{G}_n$ nilpotent der Länge k.

Falls n gerade ist, gilt $k = \frac{1}{2}n \geq 2$. Nach Satz 6.3.1.1 sind $Z^k(U_1)$ und $Z^{k-1}(U)$ gutartig, wobei $R(Z^k(U_1)) = n+1$ und $S(Z^k(U_1)) = n$ sowie $R(Z^{k-1}(U_1)) = n-1$ ist. Daraus folgt nach Lemma 6.1.5, daß $Z^k(U_1) \subset U_n$ und $Z^{k-1}(U_1) \not\subset U_n$ gilt. Damit erhält man $Z^k(\hat{G}_n) = \{1 \cdot U_n\}$ und $Z^{k-1}(\hat{G}_n) \neq \{1 \cdot U_n\}$. Also ist $\hat{G}_n$ nilpotent der Länge k. □

6.3.2 Die abgeleitete Reihe von U_n

Alle nachfolgenden Aussagen über die abgeleitete Reihe von U_n ergeben sich aus dem folgenden Satz.

Satz 6.3.2.1 *Sei $\mathfrak{U} \leq [U,U]$ gutartig mit $R := R(\mathfrak{U})$ und $S := S(\mathfrak{U})$. Dann ist $[\mathfrak{U},\mathfrak{U}]$ gutartig mit $S([\mathfrak{U},\mathfrak{U}]) = 2R$. Für den ungeraden Charakterisierungsindex gilt*

$$R([\mathfrak{U},\mathfrak{U}]) = \begin{cases} 2S+R & \text{falls } S < R \\ 3R & \text{falls } S > R \text{ und } q \neq 2 \\ 3R+2 & \text{falls } S > R \text{ und } q = 2. \end{cases}$$

Beweis: Nach Hauptsatz 6.2.1.13 (im Fall $q \neq 2$) bzw. nach Hauptsatz 6.2.2.3 (im Fall $q = 2$) folgt die Gutartigkeit von $[\mathfrak{U}, \mathfrak{U}]$ mit $S([\mathfrak{U}, \mathfrak{U}]) = \min\{2S + 2R, R + R\} = 2R$. Für den Fall $S < R$ erhält man mit diesen beiden Sätzen $R([\mathfrak{U}, \mathfrak{U}]) = \min\{2S + R, 3R\} = 2S + R$ für den ungeraden Charakterisierungsindex. Falls $S > R$ und $q \neq 2$ ist, erhält man $R([\mathfrak{U}, \mathfrak{U}]) = \min\{2S+R, 3R\} = 3R$ mit Hauptsatz 6.2.1.13. Falls $S > R$ und $q = 2$ ist, erhält man $R([\mathfrak{U}, \mathfrak{U}]) = \min\{2S + R, 3R\} + 2 = 3R + 2$ mit Hauptsatz 6.2.2.3. □

Es ist sofort klar, daß aus Satz 6.3.2.1 die Gutartigkeit aller Glieder der abgeleiteten Reihe einer beliebigen gutartigen Untergruppe von $[U, U]$ folgt. Um hier die Charakterisierungsindizes effizient berechnen zu können, definiert man die folgende Funktion.

Definition 6.3.2.2 *Die Funktion $\tilde{f} : \mathbb{N}_0 \longrightarrow \mathbb{R}$ sei gegeben durch*

$$\tilde{f}(k) := \frac{1}{\sqrt{17}} \left(\left(\frac{1 + \sqrt{17}}{2} \right)^k - \left(\frac{1 - \sqrt{17}}{2} \right)^k \right)$$

für alle $k \in \mathbb{N}$.

Um die Funktionswerte von $\tilde{f}$ rekursiv zu berechnen, benötigt man das folgende Lemma.

Lemma 6.3.2.3 *Für $\tilde{f}$ gelten die folgenden Rechenregeln:*

(i) $\tilde{f}(0) = 0,\ \tilde{f}(1) = 1.$

(ii) Für alle $k \in \mathbb{N}$ gilt die Rekursionsformel $\tilde{f}(k + 1) = \tilde{f}(k) + 4\tilde{f}(k - 1)$.

Beweis: (i) Die Aussage ist elementar.

(ii) Die Aussage ergibt sich aus der folgenden Rechnung:

$$\begin{aligned}
\tilde{f}(k+1) &= \tfrac{1}{\sqrt{17}} \left(\left(\tfrac{1+\sqrt{17}}{2}\right)^{k+1} - \left(\tfrac{1-\sqrt{17}}{2}\right)^{k+1} \right) \\
&= \tfrac{1}{\sqrt{17}} \left(\left(\tfrac{1+\sqrt{17}}{2}\right)^{k-1} \left(\tfrac{1+\sqrt{17}}{2} + 4\right) - \left(\tfrac{1-\sqrt{17}}{2}\right)^{k-1} \left(\tfrac{1-\sqrt{17}}{2} + 4\right) \right) \\
&= \tfrac{1}{\sqrt{17}} \left(\left(\tfrac{1+\sqrt{17}}{2}\right)^{k} - \left(\tfrac{1-\sqrt{17}}{2}\right)^{k} \right) + \tfrac{4}{\sqrt{17}} \left(\left(\tfrac{1+\sqrt{17}}{2}\right)^{k-1} - \left(\tfrac{1-\sqrt{17}}{2}\right)^{k-1} \right) \\
&\tilde{f}(k) + 4\tilde{f}(k-1).
\end{aligned}$$

□

Satz 6.3.2.4 *Sei $\mathfrak{U} \leq [U, U]$ gutartig mit $R := R(\mathfrak{U})$ und $S := S(\mathfrak{U})$, so daß $2S > R > S$ gilt. Dann ist $D^k(\mathfrak{U})$ für alle $k \in \mathbb{N}$ gutartig und es gilt $R(D^k(\mathfrak{U})) = 2S\tilde{f}(k) + R\tilde{f}(k + 1)$ sowie $S(D^k(\mathfrak{U})) = 4S\tilde{f}(k - 1) + 2R\tilde{f}(k)$.*

Beweis: Der Beweis erfolgt durch Induktion über k.

Induktionsanfang $k = 1$: Nach Satz 6.3.2.1 ist $D^1(\mathfrak{U}) = [\mathfrak{U}, \mathfrak{U}]$ gutartig mit $S(D^1(\mathfrak{U})) = 2R = 4S\tilde{f}(0) + 2R\tilde{f}(1)$. Wegen $S < R$ gilt weiter $R(D^1(\mathfrak{U})) = 2S + R = 2S\tilde{f}(1) + R\tilde{f}(2)$.

Induktionsschritt $k \longrightarrow k + 1$: Nach Induktionsannahme ist $D^k(\mathfrak{U})$ gutartig mit $R(D^k(\mathfrak{U})) = 2S\tilde{f}(k) + R\tilde{f}(k + 1)$ und $S(D^k(\mathfrak{U})) = 4S\tilde{f}(k - 1) + 2R\tilde{f}(k)$. Nach Satz 6.3.2.1 ist $D^{k+1}(\mathfrak{U}) = [D^k(\mathfrak{U}), D^k(\mathfrak{U})]$ gutartig mit $S(D^{k+1}(\mathfrak{U})) = 2R(D^k(\mathfrak{U})) = 4S\tilde{f}(k) + 2R\tilde{f}(k + 1)$. Wegen

$$\begin{aligned}
R(D^k(\mathfrak{U})) &= 2S\tilde{f}(k) + R\tilde{f}(k + 1) \\
&= 2S\tilde{f}(k) + R(\tilde{f}(k) + 4\tilde{f}(k - 1)) \\
&= 4R\tilde{f}(k - 1) + (2S + R)\tilde{f}(k) \\
&> 4S\tilde{f}(k - 1) + 2R\tilde{f}(k) \\
&= S(D^k(\mathfrak{U}))
\end{aligned}$$

folgt weiter

$$\begin{aligned}
R(D^{k+1}(\mathfrak{U})) &= 2S(D^k(\mathfrak{U})) + R(D^k(\mathfrak{U})) \\
&= 2(4S\tilde{f}(k-1) + 2R\tilde{f}(k)) + 2S\tilde{f}(k) + R\tilde{f}(k+1) \\
&= 2S(\tilde{f}(k) + 4\tilde{f}(k-1)) + R(\tilde{f}(k+1) + 4\tilde{f}(k)) \\
&= 2S\tilde{f}(k+1) + R\tilde{f}(k+2).
\end{aligned}$$

□

Korollar 6.3.2.5 *Sei $n \in \mathbb{N}_0$ ungerade. Dann ist $D^k(U_n)$ gutartig für alle $k \in \mathbb{N}$. Dabei gilt $R(D^1(U_n)) = 2n+1$ und $S(D^1(U_n)) = 2n$. Falls $k > 1$ ist, gilt $R(D^k(U_n)) = 4n\tilde{f}(k-1) + (2n+1)\tilde{f}(k)$ und $S(D^k(U_n)) = 8n\tilde{f}(k-2) + (4n+2)\tilde{f}(k-1)$.*

Beweis: Nach Korollar 4.3.5 gilt $D^1(U_n) = [U_n, U_n] = E_{2n}$. Gemäß Beispiel 6.1.9 ist E_{2n} gutartig mit $R(E_{2n}) = 2n+1$ und $S(E_{2n}) = 2n$. Damit ist die Aussage des Korollares im Fall $k = 1$ gezeigt. Sei nun $k > 1$. Wegen $2(2n) > 2n+1 > 2n$ folgt nach Satz 6.3.2.4, daß $D^k(U_n) = D^{k-1}(D^1(U_n))$ gutartig ist mit $R(D^k(U_n)) = 4n\tilde{f}(k-1) + (2n+1)\tilde{f}(k)$ und $S(D^k(U_n)) = 8n\tilde{f}(k-2) + (4n+2)\tilde{f}(k-1)$. □

Korollar 6.3.2.6 *Sei $q \neq 2$ und $n \in \mathbb{N}_0$ gerade. Dann ist $D^k(U_n)$ gutartig für alle $k \in \mathbb{N}$. Für die Charakterisierungsindizes erhält man:*

	$k=1$	$k=2$	$k>2$
$R(D^k(U_n)) =$	$2n+1$	$6n+3$	$(8n+4)\tilde{f}(k-2) + (6n+3)\tilde{f}(k-1))$
$S(D^k(U_n)) =$	$2n+2$	$4n+2$	$(16n+8)\tilde{f}(k-3) + (12n+6)\tilde{f}(k-2))$.

Beweis: Nach Korollar 4.3.5 gilt $D^1(U_n) = [U_n, U_n] = E_{2n+1}$. Gemäß Beispiel 6.1.9 ist E_{2n} gutartig mit $R(E_{2n+1}) = 2n+1$ und $S(E_{2n+1}) = 2n+2$. Nach Satz 6.3.2.1 folgt, daß $D^2(U_n) = [D^1(U_n), D^1(U_n)]$ gutartig ist mit $S(D^2(U_n)) = 4n+2$. Wegen $2n+1 < 2n+2$ folgt weiter $R(D^2(U_n)) = 6n+3$. Damit ist die Aussage des Korollares im Fall $k \leq 2$ gezeigt. Sei nun $k > 2$. Wegen $2(4n+2) > 6n+3 > 4n+2$ folgt nach Satz 6.3.2.4, daß $D^k(U_n) = D^{k-2}(D^2(U_n))$ gutartig ist mit $R(D^k(U_n)) = (8n+4)\tilde{f}(k-2) + (6n+3)\tilde{f}(k-1)$ und $S(D^k(U_n)) = (16n+8)\tilde{f}(k-3) + (12n+6)\tilde{f}(k-2)$. □

Korollar 6.3.2.7 *Sei $q = 2$ und $n \in \mathbb{N}$ gerade. Dann ist $D^k(U_n)$ gutartig für alle $k \in \mathbb{N}$. Für die Charakterisierungsindizes erhält man:*

	$k=1$	$k=2$	$k>2$
$R(D^k(U_n)) =$	$2n+1$	$6n+5$	$(8n+4)\tilde{f}(k-2) + (6n+5)\tilde{f}(k-1))$
$S(D^k(U_n)) =$	$2n+2$	$4n+2$	$(16n+8)\tilde{f}(k-3) + (12n+10)\tilde{f}(k-2))$.

Beweis: Nach Korollar 4.3.5 gilt $D^1(U_n) = [U_n, U_n] = E_{2n+1}$. Gemäß Beispiel 6.1.9 ist E_{2n} gutartig mit $R(E_{2n+1}) = 2n+1$ und $S(E_{2n+1}) = 2n+2$. Nach Satz 6.3.2.1 folgt, daß $D^2(U_n) = [D^1(U_n), D^1(U_n)]$ gutartig ist mit $S(D^2(U_n)) = 4n+2$. Wegen $2n+1 < 2n+2$ folgt weiter $R(D^2(U_n)) = 6n+5$. Damit ist die Aussage des Korollares im Fall $k \leq 2$ gezeigt. Sei nun $k > 2$. Wegen $2(4n+2) > 6n+5 > 4n+2$ folgt nach Satz 6.3.2.4, daß $D^k(U_n) = D^{k-2}(D^2(U_n))$ gutartig ist mit $R(D^k(U_n)) = (8n+4)\tilde{f}(k-2) + (6n+5)\tilde{f}(k-1)$ und $S(D^k(U_n)) = (16n+8)\tilde{f}(k-3) + (12n+10)\tilde{f}(k-2)$. □

Korollar 6.3.2.8 *Sei $q = 2$. Dann ist $D^k(U)$ gutartig für alle $k \in \mathbb{N}$. Für die Charakterisierungsindizes erhält man:*

	$k=1$	$k=2$	$k=3$	$k=4$	$k>4$
$R(D^k(U)) =$	1	5	9	29	$39\tilde{f}(k-4) + 29\tilde{f}(k-3)$
$S(D^k(U)) =$	2	2	10	18	$72\tilde{f}(k-5) + 58\tilde{f}(k-4))$.

Beweis: Nach Korollar 4.3.5 gilt $D^1(U) = [U,U] = E_1$. Gemäß Beispiel 6.1.9 ist E_1 gutartig mit $R(E_1) = 1$ und $S(E_1) = 2$. Nach Satz 6.3.2.1 folgt, daß $D^2(U) = [D^1(U), D^1(U)]$ gutartig ist mit $S(D^2(U)) = 2$. Wegen $1 < 2$ erhält man $R(D^2(U)) = 5$. Weiter folgt, daß $D^3(U) = [D^2(U), D^2(U)]$ gutartig ist mit $S(D^3(U)) = 10$. Wegen $2 < 5$ erhält man $R(D^3(U)) = 9$. Weiter folgt, daß $D^4(U) = [D^3(U), D^3(U)]$ gutartig ist mit $S(D^4(U)) = 18$. Wegen $9 < 10$ erhält man $R(D^4(U)) = 29$. Damit ist die Aussage des Korollares im Fall $k \leq 4$ gezeigt. Sei nun $k > 4$. Wegen $2 \cdot 18 > 29 > 18$ folgt nach Satz 6.3.2.4, daß $D^k(U) = D^{k-4}(D^4(U))$ gutartig ist mit $R(D^k(U)) = 36\tilde{f}(k-4) + 29\tilde{f}(k-3)$ und $S(D^k(U)) = 72\tilde{f}(k-5) + 58\tilde{f}(k-4)$. □

Mit den Korollaren 6.3.2.6 und 6.3.2.8 kann man nun die auflösbare Länge der Faktorgruppen G_n bestimmen. Zur Vereinfachung wählt man ähnlich wie in Kapitel 4 folgende Abkürzung.

Bezeichnung 6.3.2.9 *Für alle $k \in \mathbb{N}_0$ setze man*

$$f_q(k) := \begin{cases} 0 & \textit{falls } k = 0 \\ \min\{S(D^k(U)), R(D^k(U))\} & \textit{falls } k > 0. \end{cases}$$

Die Bedeutung von $f_q(k)$ erkennt man, wenn man Lemma 6.1.5 zu Hilfe zieht. Es gilt nämlich $f_q(k) = \max\{i \in \mathbb{N}_0 \mid D^k(U) \subset U_i\}$.

Satz 6.3.2.10 *Sei $k \in \mathbb{N}$.*

(i) Falls $q \neq 2$ ist, gilt:

	$k=1$	$k=2$	$k>2$
$f_q(k) =$	1	2	$8\tilde{f}(k-3) + 6\tilde{f}(k-2)$.

(ii) Falls $q = 2$ ist, gilt:

	$k=1$	$k=2$	$k=3$	$k=4$	$k>4$
$f_q(k) =$	1	2	9	18	$72\tilde{f}(k-5) + 58\tilde{f}(k-4)$.

Beweis: (i) Falls $q \neq 2$ ist, folgt nach Korollar 6.3.2.6, daß $f_q(1) = \min\{1,2\} = 1$ und $f_q(2) = \min\{2,5\} = 2$ ist. Für $k > 2$ erhält man

$$\begin{aligned} f_q(k) &= \min\{4\tilde{f}(k-2) + 3\tilde{f}(k-1), 8\tilde{f}(k-3) + 6\tilde{f}(k-2)\} \\ &= \min\{4\tilde{f}(k-2) + 3(\tilde{f}(k-2) + 4\tilde{f}(k-3)), 8\tilde{f}(k-3) + 6\tilde{f}(k-2)\} \\ &= 8\tilde{f}(k-3) + 6\tilde{f}(k-2). \end{aligned}$$

(ii) Falls $q = 2$ ist, folgt nach Korollar 6.3.2.8, daß $f_q(1) = \min\{1,2\} = 1$, $f_q(2) = \min\{2,5\} = 2$, $f_q(3) = \min\{9,10\} = 9$ und $f_q(4) = \min\{29,18\} = 18$ ist. Für $k > 4$ erhält man

$$\begin{aligned} f_q(k) &= \min\{36\tilde{f}(k-2) + 29\tilde{f}(k-1), 72\tilde{f}(k-3) + 58\tilde{f}(k-2)\} \\ &= \min\{36\tilde{f}(k-2) + 29(\tilde{f}(k-2) + 4\tilde{f}(k-3)), 72\tilde{f}(k-3) + 58\tilde{f}(k-2)\} \\ &= 72\tilde{f}(k-3) + 58\tilde{f}(k-2). \end{aligned}$$

□

Korollar 6.3.2.11 *Die Folge* $\{f_q(k)\}_{k\in\mathbb{N}_0}$ *ist* streng *monoton wachsend.*

Beweis: 1. Fall $q \neq 2$: Nach Satz 6.3.2.10 gilt

$$f_q(0) = 0 < f_q(1) = 1 < f_q(2) = 2 < f_q(3) = 6.$$

Sei nun $k \in \mathbb{N}$ mit $k \geq 3$. Dann gilt ebenfalls nach Satz 6.3.2.10, daß

$$\begin{aligned} f_q(k+1) + f_q(k) &= 8\tilde{f}(k-2) + 6\tilde{f}(k-1) - (8\tilde{f}(k-3) + 6\tilde{f}(k-2)) \\ &= 8\tilde{f}(k-2) + 6(\tilde{f}(k-2) + 4\tilde{f}(k-3)) - 8\tilde{f}(k-3) - 6\tilde{f}(k-2)) \\ &= 8\tilde{f}(k-2) + 16\tilde{f}(k-3) \\ &> 0 \end{aligned}$$

ist, und damit $f_q(k+1) > f_q(k)$ gilt. Somit ist $\{f_q(k)\}_{k\in\mathbb{N}_0}$ streng monoton wachsend.

2. Fall $q = 2$: Nach Satz 6.3.2.10 gilt

$$f_q(0) = 0 < f_q(1) = 1 < f_q(2) = 2 < f_q(3) = 9 < f_q(4) = 18 < f_q(5) = 58.$$

Sei nun $k \in \mathbb{N}$ mit $k \geq 5$. Dann gilt ebenfalls nach Satz 6.3.2.10, daß

$$\begin{aligned} f_q(k+1) + f_q(k) &= 72\tilde{f}(k-2) + 58\tilde{f}(k-1) - (72\tilde{f}(k-3) + 58\tilde{f}(k-2)) \\ &= 72\tilde{f}(k-2) + 58(\tilde{f}(k-2) + 4\tilde{f}) - 72\tilde{f}(k-3) - 58\tilde{f}(k-2)) \\ &= 72\tilde{f}(k-2) + 160\tilde{f}(k-3) \\ &> 0 \end{aligned}$$

ist, und damit $f_q(k+1) > f_q(k)$ gilt. Somit ist $\{f_q(k)\}_{k\in\mathbb{N}_0}$ streng monoton wachsend. □

Satz 6.3.2.12 *Sei* $n \in \mathbb{N}$. *Dann ist* G_n *auflösbar. Die auflösbare Länge* l *von* G_n *ist dabei durch die Bedingung*

$$l \in \mathbb{N} \textit{ und } f_q(l-1) < n \leq f_q(l)$$

eindeutig bestimmt.

Beweis: Da $\{f_q(k)\}_{k\in\mathbb{N}_0}$ streng monoton wachsend ist und $f_q(0) = 0$ gilt, gibt es genau ein $l \in \mathbb{N}$, das die Bedingung $f_q(l-1) < n \leq f_q(l)$ erfüllt. Für ein solches l gilt nun $D^l(G_n) = (D^l(U)\cdot U_n)/U_n$ mit $D^l(U) \subset U_{f_q(l)} \subset U_n$ sowie $D^{l-1}(G_n) = D^{l-1}(U)\cdot U_n/U_n$ mit $D^l(U) \not\subset U_n$. Daraus folgt $D^l(G_n) = \{1\cdot U_n\}$ und $D^{l-1} \neq \{1\cdot U_n\}$. Somit ist G_n auflösbar der Länge l. □

Mit Satz 6.3.2.12 ist nun die auflösbare Länge von G_n für alle $n \in \mathbb{N}$ vollständig bestimmt. Der abschließende Unterabschnitt befaßt sich nun mit dem Zusammenhang zwischen n und $l = l(n)$ für große n.

6.3.3 Asymptotisches Verhalten der auflösbaren Länge von G_n

Um das asymptotische Verhalten der auflösbaren Länge l von G_n zu beschreiben, ist es zunächst notwendig, das asymptotische Verhalten von $\tilde{f}(k)$ für $k \to \infty$ zu untersuchen. Man setze dazu

$$\hat{f}(k) := \tilde{f}(k)\cdot\left(\frac{2}{1+\sqrt{17}}\right)^k$$

für alle $k \in \mathbb{N}$. Damit gilt dann

$$\lim_{k\to\infty}\hat{f}(k) = \lim_{k\to\infty}\frac{1}{\sqrt{17}}\left(1-\left(\frac{1-\sqrt{17}}{1+\sqrt{17}}\right)^k\right) = \frac{1}{\sqrt{17}}.$$

Nach Satz 6.3.2.12 gilt für die auflösbare Länge l von G_l die Bedingung

$$f_q(l-1) < n \leq f_q(l).$$

Da $\{f_q(k)\}_{k\in\mathbb{N}_0}$ streng monoton wachsend ist, muß nun für $n \to \infty$ auch l gegen ∞ gehen. Für große n und damit für große l sind nach Satz 6.3.2.10 die Fälle $q \neq 2$ und $q = 2$ zu unterscheiden.

1.Fall $q \neq 2$:
Für $l \geq 3$ gilt $f_q(l) = 8\tilde{f}(l-3) + 6\tilde{f}(l-2)$. Damit erhält man

$$8\tilde{f}(l-4) + 6\tilde{f}(l-3) < n \leq 8\tilde{f}(l-3) + 6\tilde{f}(l-2).$$

Das ist äquivalent zu

$$\frac{16}{1+\sqrt{17}}\hat{f}(l-4) + 6\hat{f}(l-3) < n\left(\frac{2}{1+\sqrt{17}}\right)^{l-3} \leq 8\hat{f}(l-3) + 3(1+\sqrt{17})\hat{f}(l-2).$$

Wegen $\lim\limits_{k\to\infty} \hat{f}(k) = \frac{1}{\sqrt{17}}$ erhält man als Grenzwert für die rechte Seite

$$\lim_{l\to\infty}\left(8\hat{f}(l-3) + 3(1+\sqrt{17})\hat{f}(l-2)\right) = \frac{1}{\sqrt{17}}\left(8 + 3(1+\sqrt{17})\right) = 3 + \frac{11}{\sqrt{17}}$$

und für die linke Seite

$$\lim_{l\to\infty}\left(\frac{16}{1+\sqrt{17}}\hat{f}(l-4) + 6\hat{f}(l-3)\right) = \frac{1}{\sqrt{17}}\left(\frac{16}{1+\sqrt{17}} + 6\right) = \frac{2}{1+\sqrt{17}}\left(3 + \frac{11}{\sqrt{17}}\right).$$

Damit läßt sich nun für große n bzw. große l der Zusammenhang näherungsweise beschreiben durch

$$\frac{2}{1+\sqrt{17}}\left(3 + \frac{11}{\sqrt{17}}\right) < n\left(\frac{2}{1+\sqrt{17}}\right)^{l-3} \leq 3 + \frac{11}{\sqrt{17}}.$$

Daraus folgt

$$\ln\left(\frac{2}{1+\sqrt{17}}\right) + \ln\left(3 + \frac{11}{\sqrt{17}}\right) < \ln(n) + (l-3)\ln\left(\frac{2}{1+\sqrt{17}}\right) \leq \ln\left(3 + \frac{11}{\sqrt{17}}\right).$$

Das ist wegen $\ln(\frac{2}{1+\sqrt{17}}) < 0$ äquivalent zu

$$\frac{\ln(3 + \frac{11}{\sqrt{17}}) - \ln(n)}{\ln(\frac{2}{1+\sqrt{17}})} + 1 > l - 3 \geq \frac{\ln(3 + \frac{11}{\sqrt{17}}) - \ln(n)}{\ln(\frac{2}{1+\sqrt{17}})}$$

und damit zu

$$\frac{\ln(3 + \frac{11}{\sqrt{17}}) - \ln(n)}{\ln(\frac{2}{1+\sqrt{17}})} + 4 > l \geq \frac{\ln(1 + \frac{11}{\sqrt{17}}) - \ln(n)}{\ln(\frac{2}{1+\sqrt{17}})} + 3.$$

Damit gilt näherungsweise

$$l = \left\lceil \frac{\ln(3 + \frac{11}{\sqrt{17}}) - \ln(n)}{\ln(\frac{2}{1+\sqrt{17}})} + 4 \right\rceil.$$

2.Fall $q = 2$:
Für $l \geq 5$ gilt $f_q(l) = 72\tilde{f}(l-5) + 58\tilde{f}(l-4)$. Damit erhält man

$$72\tilde{f}(l-6) + 58\tilde{f}(l-5) < n \leq 72\tilde{f}(l-5) + 58\tilde{f}(l-4).$$

Das ist äquivalent zu

$$\frac{144}{1+\sqrt{17}}\hat{f}(l-6)+58\hat{f}(l-5) < n\left(\frac{2}{1+\sqrt{17}}\right)^{l-5} \leq 72\hat{f}(l-5)+29(1+\sqrt{17})\hat{f}(l-4).$$

Wegen $\lim\limits_{k\to\infty}\hat{f}(k)=\frac{1}{\sqrt{17}}$ erhält man als Grenzwert für die rechte Seite

$$\lim_{l\to\infty}\left(72\hat{f}(l-5)+29(1+\sqrt{17})\hat{f}(l-4)\right)=\frac{1}{\sqrt{17}}\left(72+29(1+\sqrt{17})\right)=29+\frac{101}{\sqrt{17}}$$

und für die linke Seite

$$\lim_{l\to\infty}\left(\frac{144}{1+\sqrt{17}}\hat{f}(l-6)+58\hat{f}(l-5)\right)=\frac{1}{\sqrt{17}}\left(\frac{144}{1+\sqrt{17}}+58\right)=\frac{2}{1+\sqrt{17}}\left(29+\frac{101}{\sqrt{17}}\right).$$

Damit läßt sich nun für große n bzw große l der Zusammenhang näherungsweise beschreiben durch

$$\frac{2}{1+\sqrt{17}}\left(29+\frac{101}{\sqrt{17}}\right) < n\left(\frac{2}{1+\sqrt{17}}\right)^{l-5} \leq 29+\frac{101}{\sqrt{17}}.$$

Daraus folgt

$$\ln(\frac{2}{1+\sqrt{17}})+\ln(29+\frac{101}{\sqrt{17}}) < \ln(n)+(l-5)\ln(\frac{2}{1+\sqrt{17}}) \leq \ln(29+\frac{101}{\sqrt{17}}).$$

Das ist wegen $\ln(\frac{2}{1+\sqrt{17}})<0$ äquivalent zu

$$\frac{\ln(29+\frac{101}{\sqrt{17}})-\ln(n)}{\ln(\frac{2}{1+\sqrt{17}})}+1 > l-5 \geq \frac{\ln(29+\frac{101}{\sqrt{17}})-\ln(n)}{\ln(\frac{2}{1+\sqrt{17}})}$$

und damit zu

$$\frac{\ln(29+\frac{101}{\sqrt{17}})-\ln(n)}{\ln(\frac{2}{1+\sqrt{17}})}+6 > l \geq \frac{\ln(29+\frac{101}{\sqrt{17}})-\ln(n)}{\ln(\frac{2}{1+\sqrt{17}})}+5.$$

Damit gilt näherungsweise

$$l=\left\lceil\frac{\ln(29+\frac{101}{\sqrt{17}})-\ln(n)}{\ln(\frac{2}{1+\sqrt{17}})}+6\right\rceil.$$

Stichwortverzeichnis

Symbolverzeichnis

Literaturverzeichnis

[1] H. Carayol, Représentations cuspidales du group linéaire Ann. Sci. École Norm. Sup. (4) **17**, 191-225 (1984).

[2] L. Corwin, Representations of division algebras over local fields, Adv. in Math. **13**, 259-267 (1974).

[3] L. Corwin, Representations of division algebras over local fields: II, Pacific J. Math. **101** No. 1, 49-70 (1982).

[4] L. Corwin, Approximation of prime elements in division algebras over local fields and unitary representations of the multiplicative group, Pacific J. Math. **130** No. 2, 223-251 (1987).

[5] L. Corwin, The unitary dual for the multiplicative group of arbitrary division algebras over local fields, J. Amer. Math. Soc. **2** No. 3, 565-598 (1989).

[6] R Howe, Representation Theory for division algebras over local fields (tamely ramified case), Bull. Amer. Math. Soc. **77**, 1063-1066 (1971).

[7] Neal Koblitz, p-adic numbers, p-adic analysis, and zeta-functions, Springer-Verlag, 1977.

[8] H. Koch, Eisensteinsche Polynomfolgen und Arithmetik in Divisionsalgebren über lokalen Körpern, Math. Nachr. **104**, 229-251 (1981).

[9] H. Koch, Zur Arithmetik in Divisionsalgebren über lokalen Körpern, Math. Nachr. **100**, 9-19 (1981).

[10] H. Koch und E.-W. Zink, Zur Korrespondenz von Darstellungen der Galoisgruppen und der zentralen Divisionsalgebren über lokalen Körpern, Math. Nachr. **98**, 83-119 (1981).

[11] S. Lang, Algebra, 3rd edition, Addison-Wesley, 1993.

[12] M.-F. Vignéras, Arithmétique des algebrès des quaternions. Springer Lecture Notes, Vol. 800 (1980).

[13] J. B. Tunnel, On the local Langlands conjecture for $GL(2)$, Invent. Math. **46**, 179-200 (1978).

[14] Guan Chi-Wen, On the multiplicative groups of division algebras over discretely valued complete fields, Sci. China Ser. A **12** No. 9, 1251-1268 (1963).