ZUR ARITHMETIK IN ABELSCHEN ZAHLKÖRPERN

Zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften der Fakultät für Informatik der Universität Fridericiana zu Karlsruhe (TH)

genehmigte

DISSERTATION

von

BJÖRN GROHMANN

aus Böblingen

Tag der mündlichen Prüfung:	6. Dezember 2005
Erster Gutachter:	Prof. Dr. Jacques Calmet
Zweiter Gutachter:	Prof. Dr. Claus-G. Schmidt

I n d e r W ü s t e d e r W i s s e n s c h a f t – Dem wissenschaftlichen Menschen erscheinen auf seinen bescheidenen und mühsamen Wanderungen, die oft genug Wüstenreisen sein müssen, jene glänzenden Lufterscheinungen, die man „philosophische Systeme“ nennt: sie zeigen mit zauberischer Kraft der Täuschung die Lösung aller Räthsel und den frischesten Trunk wahren Lebenswassers in der Nähe; das Herz schwelgt und der Ermüdete berührt das Ziel aller wissenschaftlichen Ausdauer und Noth beinahe schon mit den Lippen, so dass er wie unwillkürlich vorwärts drängt. Freilich bleiben andere Naturen, von der schönen Täuschung wie betäubt, stehen: die Wüste verschlingt sie, für die Wissenschaft sind sie todt. Wieder andere Naturen, welche jene subjectiven Tröstungen schon öfter erfahren haben, werden wohl auf's Aeusserste missmuthig und verfluchen den Salzgeschmack, welchen jene Erscheinungen im Munde hinterlassen und aus dem ein rasender Durst entsteht – ohne dass man nur Einen Schritt damit irgend einer Quelle näher gekommen wäre.

Friedrich Nietzsche [64]

Mein herzlicher Dank geht an dieser Stelle an die Personen, welche zum Gelingen der vorliegenden Arbeit beigetragen haben. Im einzelnen sind das Herr Prof. Dr. Thomas Beth (1949-2005), welcher mein erster Informatiklehrer war und damit meine „informatische“ Sicht der Dinge entscheidend mitgeprägt hat und auf dessen Initiative hin diese Arbeit entstanden ist. Herr Prof. Dr. Jacques Calmet, der sich nach dem tragischen Tod von Prof. Beth bereiterklärt hat, das Referat zu übernehmen, und der mich von diesem Zeitpunkt an in freundlichster Weise unterstützt hat. Herr Prof. Dr. Claus-Günther Schmidt, durch dessen sympathische und zuverlässige Hilfe die letzten „Ungenauigkeiten“ in dieser Arbeit eliminiert werden konnten, sowie Herr Prof. Dr. Roland Vollmar, welcher nicht zuletzt durch seine freundschaftliche Art und seinen unermüdlichen Einsatz dazu beigetragen hat, daß diese Arbeit auch einen zeitlichen Abschluß fand. Desweiteren bedanke ich mich bei meinen ehemaligen Kollegen des Institus für Algorithmen und Kognitive Systeme (IAKS) für die vielen Jahre der Zusammenarbeit in partnerschaftlicher Atmosphäre.

Inhaltsverzeichnis

Kapitel 1

Überblick

Die vorliegende Arbeit beschäftig sich mit der Arithmetik von abelschen Zahlkörpern. Mit dem Begriff *Arithmetik* („Rechenkunst“) verbindetet man im allgemeinen die, einem mathematischen Objekt innewohnenden Gesetzmäßigkeiten. Die Untersuchung dieser Gesetzmäßigkeiten bildet die Grundlage für effiziente Verfahren. Die „Kunst“ besteht darin, durch möglichst geschickte Anwendung bestehender Relationen, eine effiziente Realisierung einer gegebenen Operation durchzuführen.

Ein einfaches Beispiel für so eine Operation wäre etwa die Multiplikation zweier Gaußscher Zahlen:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Diese läßt sich bekanntermaßen, aufgrund der Distributivgesetze, durch drei nicht-skalare Multiplikationen realisieren,

$$(ac - bd) + ((a + b)(c + d) - ac - bd)i,$$

was, im allgemeinen Fall, eine Verbesserung im Vergleich zu obiger Methode darstellt.

Die in dieser Arbeit vorgestellten Probleme sind überwiegend algebraischer Natur – die hergeleiteten Verfahren arbeiten, im Gegensatz zu numerischen Verfahren, exakt. Diese geforderte Genauigkeit hat ihren „Preis“, wie das folgende Beispiel verdeutlicht. So läßt sich etwa zeigen, daß für die Realisierung einer Multiplikation in der Algebra $\mathbb{C}[x]/(x^n)$ mindestens $2n - 1$ nicht-skalare Multiplikationen in $\mathbb{C}$ notwendig sind. Wenn man hingegen einen kleinen Fehler $\epsilon \neq 0$ akzeptiert, d. h. die Algebra $\mathbb{C}[x]/(x^n - \epsilon)$ zugrunde legt, so kann man schon mit n solcher Operationen auskommen.

Die Bausteine einer „schnellen Faltung“ in einer Algebra A bestehen in der Regel aus einem Isomorphismus

$$\varphi : A \longrightarrow B_1 \times \cdots \times B_k,$$

sowie effizienten Verfahren für die „kleineren Teile“ B_j. Im Falle der Algebra $\mathbb{C}[x]/(x^n-1)$ kann beispielsweise auf den, durch den Chinesische Restesatz gegebenen Einsetzungshomomorphismus

$$\mathbb{C}[x]/(x^n-1) \longrightarrow \mathbb{C}[x]/(x-1) \times \mathbb{C}[x]/(x-e^{2\pi i/n}) \times \cdots \times \mathbb{C}[x]/(x-e^{2\pi i(n-1)/n})$$

zurückgegriffen werden. Man spricht in diesem Zusammenhang auch von der *Diskreten Fourier Transformation* (DFT). Letztere läßt sich, genau wie ihre Inverse, mit einem Aufwand von $O(n \log n)$ Operationen in $\mathbb{C}$ realisieren – zzgl. der n nicht-skalaren Multiplikationen in den einzelnen Komponenten, ergibt sich also ein Gesamtaufwand von $O(n \log n)$ Operationen in $\mathbb{C}$.

Ein gewisser Nachteil besteht darin, daß sich Operation in $\mathbb{C}$ im allgemeinen nur approximativ behandeln lassen. Insbesondere stellt sich die Frage, wie man mit Algebren umgeht, deren Grundkörper nicht genügend „Wurzeln“ bereithalten. Zu diesem Zweck wird im zweiten Kapitel das Konzept der sog. Grundkörpertransformation, und im speziellen das, auf Beth et al. (vgl. [8]) zurückgehende Konzept der *Algebraischen Diskreten Fourier Transformation* (ADFT) untersucht.

Ein Beispiel für so eine ADFT ist etwa durch die Matrix

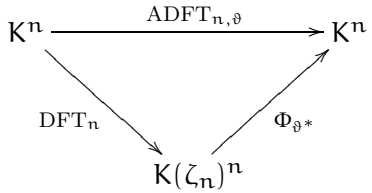
$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

gegeben. Diese realisiert den Isomorphismus

$$\mathbb{Q}[x]/(x^4-1) \longrightarrow \mathbb{Q}[x]/(x-1) \times \mathbb{Q}[x]/(x+1) \times \mathbb{Q}[x]/(x^2+1),$$

wobei das Bild der Abbildung in dem Körper $\mathbb{Q}[x]/(x^2+1) \simeq \mathbb{Q}(i)$ nun bzgl. der Normalbasis $\{(1+i)/2, (1-i)/2\}$ dargestellt ist. Es fällt auf, daß die Matrix, mit Ausnahme von Vorzeichenwechsel keine weiteren skalaren Faktoren enthält. Durch die Darstellung in Tensorschreibweise auf der rechten Seite wird zudem der Algorithmus für die Berechnung gleich „mitgeliefert“.

Für einen Körper $K \subseteq \mathbb{C}$, $n \in \mathbb{N}$ und $\zeta_n := e^{2\pi i/n}$ ist die $\mathrm{ADFT}_{n,\vartheta}$ als Kompositum einer DFT_n, sowie einer weiteren Abbildung durch folgendes Diagramm beschrieben:



Bei dem Element ϑ handelt es sich um einen Normalbasiserzeuger der Erweiterung $K(\zeta_n)/K$. Die Abbildung Φ_{ϑ^*} transformiert das Spektrum der DFT in eine Darstellung bzgl. dieser Normalbasis.

Ein wesentliches Ziel des folgenden Kapitels wird sein, Normalbasen zu konstruieren bzgl. derer die entsprechenden Matrizen eine möglichst einfache Gestalt besitzen, d. h. deren Einträge wenige oder sogar keine zusätzlichen Skalare beinhalten. Einer der entscheidenden Sätze wird sein, daß solche sog. *schlanken Basen*, zumindest im rationalen Fall immer existieren. Für die korrespondierenden Transformationen bedeutet das, daß sich diese unter ausschließlicher Verwendung der Addition realisieren lassen. Das ist insofern beachtlich, da die Beträge der Koeffizienten der Teilerpolynome (über $\mathbb{Q}$) von $x^n - 1$ unbeschränkt sind, also für wachsendes n beliebig groß werden können. Das Kapitel schließt mit einer schnellen Variante der ADFT für den Zweierpotenzfall.

Kapitel 3 beginnt mit einer Diskussion zur Normalbasenarithmetik von abelschen Zahlkörpern. Um auf das weiter oben angesprochene Beispiel zurückzukommen, so stellt sich hier zunächst die Frage nach einem effizienten Verfahren für eine Faltung in $\mathbb{Q}(i)$ bzgl. der Normalbasis $\{\vartheta, \bar{\vartheta}\}$, mit $\vartheta := (1+i)/2$:

$$(a_+\vartheta + a_-\bar{\vartheta})(b_+\vartheta + b_-\bar{\vartheta}) = c_+\vartheta + c_-\bar{\vartheta}.$$

Die Koeffizienten c_+, c_- ergeben sich dabei durch

$$c_\pm = (a_+, a_-) W_\vartheta^{(\pm)} (b_+, b_-)^T,$$

mit den Faltungsmatrizen $W_\vartheta^{(+)}, W_\vartheta^{(-)}$, welche in diesem Fall von der einfachen Form

$$W_\vartheta^{(+)} = \frac{1}{2}\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} + \begin{pmatrix} 1 & \\ & \end{pmatrix}, \text{ bzw. } W_\vartheta^{(-)} = \frac{1}{2}\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} + \begin{pmatrix} & \\ & 1 \end{pmatrix}$$

sind. Insgesamt erhält man also auch hier, via

$$c_\pm = (1/2)(a_- - a_+)(b_+ - b_-) + a_\pm b_\pm$$

einen Algorithmus, welcher mit lediglich drei nicht-skalaren Multiplikationen auskommt.

Das Studium der Struktur derlei Faltungsmatrizen im allgemeinen Fall ist das vorrangige Ziel dieses Kapitels. Dabei werden die, in Kapitel 2 hergeleiteten Methoden zum Einsatz kommen. Für einen abelschen Zahlkörper K mit Galoisgruppe G, sowie $\sigma, \varphi, \rho \in G$ sind diese Matrizen im allgemeinen von der Form

$$W_{\vartheta}^{(\rho)} = \frac{1}{|G|^2} \left(\sum_{\chi,\chi'} \kappa(\chi,\chi')_{\vartheta} \omega(\chi,\chi') \bar{\chi}(\sigma\rho^{-1}) \bar{\chi}'(\varphi\rho^{-1}) \right)_{\sigma,\varphi},$$

wobei, für Charaktere χ, χ' der Galoisgruppe, die Elemente $\kappa(\chi,\chi')_{\vartheta}$ von dem Normalbasiserzeuger ϑ abhängen, bzw.

$$\omega(\chi,\chi') := \frac{\tau(\chi)\tau(\chi')}{\tau(\chi\chi')}$$

die Elemente des Faktorensystems der korrespondierenden Gaußschen Summen darstellen. Die Gewichte

$$\alpha_K(\chi,\chi';\vartheta) := \kappa(\chi,\chi')_{\vartheta}\omega(\chi,\chi')$$

sind nun dafür verantwortlich, inwieweit sich obige Matrizen von der optimalen, aber eben „leider“ auch utopischen Faltung

$$\frac{1}{|G|^2} \left(\sum_{\chi,\chi'} \bar{\chi}(\sigma\rho^{-1}) \bar{\chi}'(\varphi\rho^{-1}) \right)_{\sigma,\varphi} = \left(\delta_{\sigma,\rho}\delta_{\varphi,\rho} \right)_{\sigma,\varphi}$$

entfernen[1]. Die „Güte“ eines Verfahrens hängt also einerseits von variablen Größen, auf der anderen Seite aber auch von den Invarianten $\omega(\chi,\chi')$ des entsprechenden Zahlkörpers ab.

Das Studium dieser Invarianten, in ausgewählten Fällen, wird den Rest des Kapitels in Anspruch nehmen. Dabei werden einige, z. T. unerwartete Querverbindungen zu anderen Disziplinen der Informatik, bzw. Mathematik zutage treten.

[1] Hierbei bezeichne δ das Kroneckerdelta.

Kapitel 2

Fourier

2.1 Die Diskrete Fourier Transformation

Grundlegend für die weiteren Betrachtungen ist die *Diskrete Fourier Transformation* (DFT). Dazu seien die wichtigsten Eigenschaften noch einmal zusammengestellt. Für $\mathbb{C}$, den Körper der komplexen Zahlen, $n \in \mathbb{N}$ und $\zeta_n := e^{2\pi i/n}$ eine *analytisch normierte* n*-te Einheitswurzel*, ist die DFT_n definiert als lineare Transformation

$$\mathrm{DFT}_n : \mathbb{C}^n \longrightarrow \mathbb{C}^n \tag{2.1}$$

des n-dimensionalen $\mathbb{C}$-Vektorraums $\mathbb{C}^n$ mit Transformationsmatrix

$$A_n := \left(\zeta_n^{kl}\right)_{k,l}, \tag{2.2}$$

$k, l \in \{0, 1, \ldots, n-1\}$. Faßt man dabei die Komponenten des Eingangsvektors $\mathbf{c} := (c_0, \ldots, c_{n-1})$ als Koeffizienten eines Polynoms $C(z) := c_{n-1}z^{n-1} + \ldots + c_1 z + c_0$ auf, so berechnet die DFT_n den Vektor $\hat{\mathbf{c}} := (\hat{c}_0, \ldots, \hat{c}_{n-1})$, mit $\hat{c}_k = C(\zeta_n^k)$. Anders ausgedrückt realisiert die DFT_n also den, durch den Chinesischen Restesatz gegebenen Isomorphismus

$$\mathbb{C}[z]/(z^n - 1) \longrightarrow \bigoplus_{k=0}^{n-1} \mathbb{C}[z]/(z - \zeta_n^k). \tag{2.3}$$

Die Umkehrfunktion, also die Transformationsmatrix der *Inversen Diskreten Fourier Transformation* (IDFT), ist gegeben durch

$$I_n := A_n^{-1} = \frac{1}{n}\left(\zeta_n^{-kl}\right)_{k,l}, \tag{2.4}$$

d. h., in anderen Worten, die Matrix $\frac{1}{\sqrt{n}}A_n$ ist unitär.

Zu den grundlegenden Eigenschaften der DFT_n resp. ihrer Matrix zählen:

Quasiinversion: Für $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{C}^n$ sei die Matrix S_n definiert via

$$(c_0, c_1, \ldots, c_{n-1})S_n = (c_0, c_{n-1}, c_{n-2}, \ldots, c_1). \tag{2.5}$$

Dann ist

$$A_n^2 = nS_n, \text{ und damit } \mathrm{DFT}_n^4 = n^2 \cdot \mathrm{id}_n. \tag{2.6}$$

Es genügt daher, eine im algorithmischen Sinne geeignete Realisierung der DFT zur Verfügung zu stellen, da es sich implizit stets auch um die Realisierung ihrer Inversen handelt.

Faltungseigenschaft: Der *zyklischen Faltung* im Definitionsbereich entspricht die (punktweise) Multiplikation im Bildbereich. Genauer gilt für Vektoren $\mathbf{c}, \mathbf{s}, \mathbf{t} \in \mathbb{C}^n$, mit $c_j = \sum_{k+l \equiv j(n)} s_k t_l$, die Beziehung $\hat{c}_j = \hat{s}_j \cdot \hat{t}_j$; in symbolischer Schreibweise:

$$\mathrm{DFT}_n(\mathbf{s} * \mathbf{t}) = \mathrm{DFT}_n(\mathbf{s}) \cdot \mathrm{DFT}_n(\mathbf{t}). \tag{2.7}$$

Vom algorithmischen Standpunkt zählt dies zu den wichtigsten Eigenschaften der DFT.

Phaseneigenschaft: Eine (zyklische) Verschiebung des Eingangsvektors um k Stellen (etwa nach rechts) korrespondiert im Wertebereich mit der Multiplikation eines sog. *Phasenfaktors*. Die Absolutbeträge der Komponenten des transformierten Vektors bleiben dabei unverändert. Ist R_n^k eine solche Schiebematrix, so gilt

$$R_n^k A_n = A_n \cdot \mathrm{diag}(1, \zeta_n^k, \ldots, \zeta_n^{k(n-1)}), \tag{2.8}$$

wobei letztere Matrix als Diagonalmatrix zu verstehen ist.

Parseval-Identität: Das Fourierspektrum ermöglicht Aussagen über die Korrelation der Eingangsdaten. Mit obigen Bezeichnungen hat man

$$\frac{1}{n} \sum_{j=0}^{n-1} \hat{c}_j \hat{\bar{d}}_j = \sum_{j=0}^{n-1} c_{n-1-j} d_j. \tag{2.9}$$

Plancherel-Identität: Eine weitere Eigenschaft, auf welche wir später noch Bezug nehmen, ist die folgende:

$$\sum_{j=0}^{n-1} |c_j|^2 = \frac{1}{n} \sum_{j=0}^{n-1} |\hat{c}_j|^2, \tag{2.10}$$

mit den inzwischen schon üblichen Bezeichnungen. Diese Beziehung legt eine Interpretation als eine Art Leistungserhaltungssatz nahe.

Unschärfeprinzip: Eng verknüpft mit letzterem ist die diskrete Variante eines bekannten Phänomens der kontinuierlichen Fourier Transformation. Bezeichne dazu für $\mathbf{c} \in \mathbb{C}^n$, $\operatorname{supp} \mathbf{c} := \{j \mid c_j \neq 0\}$ die Menge der Stellen der von Null verschieden Komponenten des Vektors $\mathbf{c}$, so gilt stets

$$|\operatorname{supp} \mathbf{c}|\,|\operatorname{supp} \hat{\mathbf{c}}| \geqslant n. \tag{2.11}$$

Insbesondere besitzt also ein sog. *peak* ($|\operatorname{supp} \mathbf{c}| = 1$) immer das volle Spektrum.

Produktzerlegung: Für Matrizen $A = (a_{kl}) \in \mathbb{C}^{n\times n}$ und $B = (b_{st}) \in \mathbb{C}^{m\times m}$ sei das *Kroneckerprodukt* wie üblich definiert durch $A \otimes B := (a_{kl}B) \in \mathbb{C}^{nm\times nm}$. Die Tatsache, daß A und B, im Falle von $n = m$, durch Zeilen- und/oder Spaltenpermutation auseinander hervorgehen, sei im weiteren durch $A \sim B$ bezeichnet. Für $n = \prod_p p^{e_p}$ ergibt sich nun als unmittelbare Folge des Chinesischen Restesatzes die Beziehung

$$A_n \sim \bigotimes_p A_{p^{e_p}}. \tag{2.12}$$

Die Realisierung einer DFT_n reduziert sich damit also im wesentlichen auf die Realisierung der Transformation für Primpotenzen p^{e_p}.

Vor diesem Hintergrund wollen wir uns nun dem Zweierpotenzfall etwas genauer widmen. Betrachten wir dazu als Beispiel zunächst den Fall $n = 4$. Für $i := \zeta_4$ geht die Matrix A_4 durch Vertauschung der mittleren beiden Spalten über in eine Matrix $\tilde{A}_4$ von der Form

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -i & i \end{pmatrix} = \begin{pmatrix} 1 & & 1 & \\ & 1 & & 1 \\ 1 & & -1 & \\ & 1 & & -1 \end{pmatrix} \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & i \end{pmatrix} \begin{pmatrix} 1 & 1 & & \\ 1 & -1 & & \\ & & 1 & 1 \\ & & 1 & -1 \end{pmatrix},$$

bzw. in Tensorschreibweise

$$\tilde{A}_4 = (A_2 \otimes E_2) \begin{pmatrix} E_2 & \\ & T_2 \end{pmatrix} (E_2 \otimes A_2),$$

wobei E die Einheitsmatrix entsprechender Größe bezeichne, sowie $T_2 := \operatorname{diag}(1, i)$. Diese Zerlegung liefert nun einen Algorithmus, welcher mit 9 arithmetischen Operationen die Komponenten des Vektors $\hat{\mathbf{c}}$ berechnet – wenn auch in permutierter Reihenfolge; im Vergleich dazu werden 16 Operationen bei der „naiven“ Berechnung via A_4 benötigt.

Allgemein ergibt sich für $n = 2^k$ und $\zeta := \zeta_n$ das folgende Schema. Durch eine geeignete Spaltenpermutation geht die Matrix A_n über in die Matrix

$$\tilde{A}_n = \left(A_2 \otimes E_{n/2}\right) \begin{pmatrix} E_{n/2} & \\ & T_{n/2} \end{pmatrix} \left(E_2 \otimes A_{n/2}\right). \tag{2.13}$$

Hierbei ist $T_{n/2} := \mathrm{diag}(1, \zeta, \zeta^2, \ldots, \zeta^{n/2-1})$ die sog. *Drehmatrix*; ihre von Null verschiedenen Einträge heißen *Drehfaktoren* (engl.: *twiddle factors*).

In Abb. 2.1 ist das Flußdiagramm des resultierenden Algorithmus, die sogenannte *Fast Fourier Transform* (FFT), für den Fall $n = 8$ dargestellt. Das Diagramm (resp. obige Zerlegung) ist dabei wie folgt zu interpretieren. In der ersten Stufe wird die n-dimensionale Algebra $\mathbb{C}[z]/(z^n - 1)$ in zwei Teilalgebren halber Dimension zerlegt:

$$\mathbb{C}[z]/(z^n - 1) \longrightarrow \mathbb{C}[z]/(z^{n/2} - 1) \times \mathbb{C}[z]/(z^{n/2} + 1). \tag{2.14}$$

Die, der rechten Teilalgebra zugehörigen Komponenten werden dann via $T_{n/2}$ „gedreht“

$$T_{n/2} : \mathbb{C}[z]/(z^{n/2} + 1) \longrightarrow \mathbb{C}[z]/(z^{n/2} - 1), \tag{2.15}$$

woraufhin der Algorithmus auf jeder Teilalgebra mit der Berechnung einer DFT halber Dimension nach obigem Schema fortsetzt. Abschließend werden die Komponenten bzgl. der Binärdarstellung ihrer Indizes spiegelverkehrt ausgelesen, d. h. es wird ein sog. *bit-reversal* vorgenommen um die ursprüngliche Reihenfolge wieder herzustellen.

Für den Gesamtaufwand $\Upsilon(n)$, also die mit obigem Verfahren benötigte Anzahl arithmetischer Operationen zur Berechnung von $\hat{\mathbf{c}} = \mathrm{DFT}_n(\mathbf{c})$, gilt somit

$$\Upsilon(n) = 2 \cdot \Upsilon(n/2) + O(n) \in O(n \log n). \tag{2.16}$$

Eine ausführliche Diskussion des hier betrachteten Verfahrens und weiterer Methoden, sowie eine verallgemeinerte, auf der Darstellungstheorie endlicher Gruppen basierende Sichtweise, findet sich in [9].

2.2 Die Algebraische Diskrete Fourier Transformation

Bevor wir nun zum eigentlichen Studienobjekt dieses Kapitels, der *Algebraischen Diskreten Fourier Transformation* (ADFT) kommen, wollen wir uns einem bekannteren Spezialfall, der sog. *Diskreten Hartley Transformation* (DHT) zuwenden. Für $\mathbb{R}$, den Körper der reellen Zahlen und einer natürlichen Zahl n, ist die DHT_n definiert als lineare Transformation

$$\mathrm{DHT}_n : \mathbb{R}^n \longrightarrow \mathbb{R}^n, \tag{2.17}$$

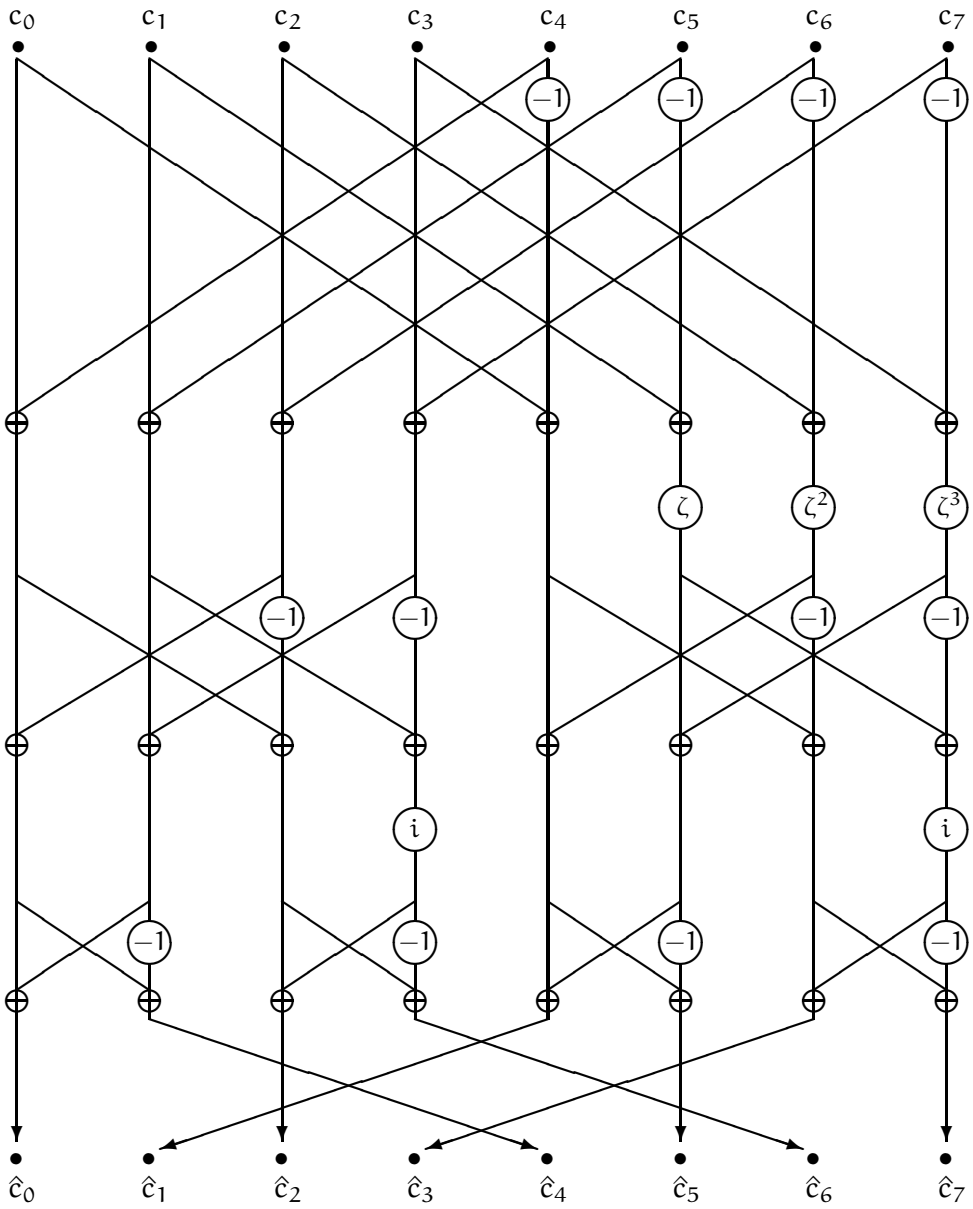


Abbildung 2.1: Flußdiagramm zur FFT_8

mit Transformationsmatrix

$$Y_n := (\cos(2\pi kl/n) + \sin(2\pi kl/n))_{k,l}\,, \tag{2.18}$$

$k, l \in \{0, 1, \ldots, n-1\}$. An der Definition von Y_n ist schon zu erkennen, daß es sich um eine Art „reelle DFT“ handelt, bei der gewissermaßen das „i“ vergessen wurde; im Falle von $n = 1, 2$ sind die Matrizen A_n und Y_n sogar identisch. Für $n \geqslant 3$ ist der genaue Zusammenhang mit der DFT_n der folgende. Zunächst beschränken wir den Definitionsbereich der DFT_n auf den Vektorraum $\mathbb{R}^n$. Für den Wertebereich bedeutet das, daß die Komponenten des Spektralvektors $\hat{\mathbf{c}} = \mathrm{DFT}_n(\mathbf{c})$, mit $\mathbf{c} \in \mathbb{R}^n$, nun in komplex-konjugierter Form vorliegen, d. h. es gilt

$$\overline{\hat{c}_k} = \hat{c}_{-k}, \tag{2.19}$$

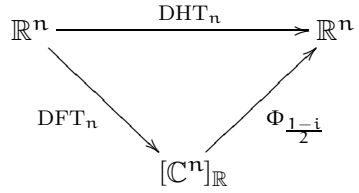
wobei die Indizes modulo n zu verstehen sind (dies ist leicht einzusehen, wenn man sich die Definition von $\hat{c}_k$ als Wert des Polynoms $C(z)$ an der Stelle ζ_n^k in Erinnerung ruft). Diesen Raum bezeichnen wir fortan mit $[\mathbb{C}^n]_{\mathbb{R}}$. Für $\alpha \in \mathbb{C}$ definieren wir nun eine Linearform

$$\phi_\alpha(c) := c\,\alpha + \overline{c\,\alpha} \tag{2.20}$$

auf (dem $\mathbb{R}$-Vektorraum) $\mathbb{C}$, welche wir in natürlicher Weise auf den Wertebereich fortsetzen:

$$\Phi_\alpha(\hat{\mathbf{c}}) := (\phi_\alpha(\hat{c}_0), \ldots, \phi_\alpha(\hat{c}_{n-1})) \in \mathbb{R}^n. \tag{2.21}$$

Aus der Konjugationseigenschaft des Spektrums folgt nun sofort, daß diese Abbildung genau dann invertierbar ist, wenn es sich bei $\{\alpha, \overline{\alpha}\}$ um eine Basis des $\mathbb{R}$-Vektorraums $\mathbb{C}$ handelt, bzw. anders ausgedrückt, wenn das Element α eine *Normalbasis* der Galoiserweiterung $\mathbb{C}/\mathbb{R}$ erzeugt. Für $\alpha = (1-i)/2$ ergibt sich das folgende kommutative Diagramm:



(2.22)

Wie wir in Kürze ganz allgemein feststellen werden, ist die (*Spur-*) *Dualbasis* der Normalbasis $\{(1-i)/2, (1+i)/2\}$, in diesem Falle die Basis $\{(1+i)/2, (1-i)/2\}$, wieder normal. Bei einer Darstellung der Komponenten $\hat{c}_k$ bzgl. letzterer gilt somit

$$\phi_{(1-i)/2}(\hat{c}_k) = \phi_{(1-i)/2}(c_{k,1}(1+i)/2 + c_{k,-1}(1-i)/2) = c_{k,1},$$

und da sich, mit Blick auf die Definition von $[\mathbb{C}^n]_{\mathbb{R}}$ und der Normalbaseneigenschaft, die Konjugation als Vertauschung darstellt,

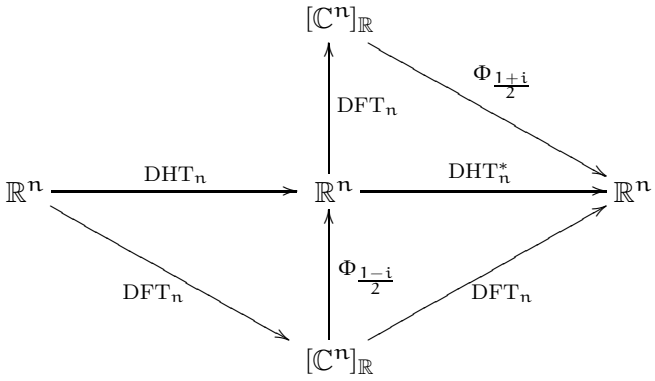
$$c_{-k,1} = c_{k,-1},$$

läßt sich zusammenfassend sagen, daß die DHT_n das Spektrum der DFT_n bzgl. der Normalbasis $\{(1+i)/2, (1-i)/2\}$ berechnet.

Aus dem Gesagten ergibt sich auch unmittelbar eine Beschreibung der Inversen. Dazu genügt es einzusehen, daß das folgende Diagramm kommutiert:

$$\begin{array}{ccc} [\mathbb{C}^n]_{\mathbb{R}} & \xrightarrow{\mathrm{DFT}_n} & \mathbb{R}^n \\ \Big\downarrow{\scriptstyle \Phi_{\frac{1-i}{2}}} & & \Big\uparrow{\scriptstyle \Phi_{\frac{1+i}{2}}} \\ \mathbb{R}^n & \xrightarrow[\mathrm{DFT}_n]{} & [\mathbb{C}^n]_{\mathbb{R}} \end{array} \tag{2.23}$$

Insgesamt ergibt sich



(2.24)

wobei DHT_n^*, wie aus dem Diagramm ersichtlich, die Projektion des Fourierspektrums auf die (duale) Basis $\{(1-i)/2, (1+i)/2\}$ darstellt; diese Vertauschung entspricht aber gerade der Operation der Spiegelmatrix S_n, sodaß letztendlich

$$\mathrm{DHT}_n^2 = n \cdot \mathrm{id}_n. \tag{2.25}$$

Wir wollen nun sehen, wie sich obiges Prinzip für beliebige Teilkörper $K \subseteq \mathbb{C}$ verallgemeinert. Vorab einige Bezeichnungen. Sei L/K eine endliche Galoiserweiterung mit Galoisgruppe $G := G(L/K)$. Ein Element $\vartheta \in L$ nennen wir G-*regulär*, wenn die Menge $\vartheta^G := \{\vartheta^\sigma; \sigma \in G\}$ eine Basis des K-Vektorraums L bildet. Wir sprechen in diesem Zusammenhang von einer *Normalbasis* ϑ^G der Körpererweiterung L/K; das Element ϑ heißt dabei der *Normalbasenerzeuger* (NBE). Ein solcher NBE existiert nach dem sog. *Normalbasen-Theorem* (vgl. [49], Th. VI 13.1) in jeder Galoiserweiterung. Da es sich bei L/K um eine separable Erweiterung handelt, ist die folgende Bilinearform

$$L \times L \longrightarrow K, \quad (\alpha, \beta) \longmapsto \mathrm{Sp}(\alpha\beta),$$

mit $\mathrm{Sp}(\alpha) := \mathrm{Sp}_{L/K}(\alpha) = \sum_{\sigma\in G} \alpha^\sigma$, nicht ausgeartet (vgl. [12], S. 4.7.7). Insbesondere existiert zu einem G-regulären $\vartheta \in L$ ein eindeutig bestimmtes $\vartheta^* \in L$, mit

$$\mathrm{Sp}(\vartheta^\sigma \vartheta^{*\rho}) = \delta_{\sigma,\rho}, \tag{2.26}$$

für alle $\sigma, \rho \in G$; dieses heißt das *Spurdual zu* ϑ und ist notwendigerweise selbst G-regulär. Für festes ϑ liefert also die resultierende Linearform

$$\phi_\vartheta(\alpha) := \mathrm{Sp}(\vartheta\alpha) \tag{2.27}$$

im Falle eines NBEs die Komponenten von $\alpha = \sum_\sigma a_\sigma \vartheta^{*\sigma} \in L$ bzgl. der Spurdualbasis ${\vartheta^*}^G$:

$$\phi_{\vartheta^\rho}(\alpha) = \sum_\sigma a_\sigma \phi_{\vartheta^\rho}(\vartheta^{*\sigma}) = a_\rho. \tag{2.28}$$

Für $n \in \mathbb{N}$ betrachten wir nun in Analogie zu $[\mathbb{C}^n]_{\mathbb{R}}$ den Vektorraum

$$[K(\zeta_n)^n]_K := \mathrm{DFT}_n(K^n). \tag{2.29}$$

Dieser n-dimensionale K-Vektorraum besteht gerade aus den Elementen $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in K(\zeta_n)^n$, mit der Eigenschaft

$$c_k^\sigma = c_{\sigma k}, \tag{2.30}$$

für $k = 0, 1, \ldots, n-1$ und alle $\sigma \in G := G(K(\zeta_n)/K)$, wobei wir σ auf der rechten Seite bzgl. der natürlichen Einbettung $G \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ mit einem Vertreter aus $\mathbb{Z}/n\mathbb{Z}$ identifizieren und der Index modulo n zu verstehen ist[1]. Bei einer Darstellung der $c_k = \sum_\sigma c_{k,\sigma}\vartheta^\sigma$ bzgl. der Normalbasis ϑ^G gilt also insbesondere für alle $\sigma, \rho \in G$

$$c_{k,\sigma\rho^{-1}} = c_{\rho k,\sigma} = c_{\rho k\sigma^{-1},1}. \tag{2.31}$$

Bezeichne abschließend noch

$$\Phi_\vartheta(\mathbf{c}) := (\phi_\vartheta(c_0), \ldots, \phi_\vartheta(c_{n-1})) \in K^n \tag{2.32}$$

die Fortsetzung von ϕ auf $[K(\zeta_n)^n]_K$, so gilt der

Satz 2.1 *Für ein* G*-reguläres* $\vartheta \in K(\zeta_n)$ *kommutiert das folgende Diagramm:*

$$\begin{array}{ccc} [K(\zeta_n)^n]_K & \xrightarrow{\mathrm{DFT}_n} & K^n \\ \Big\downarrow{\scriptstyle \Phi_\vartheta} & & \Big\uparrow{\scriptstyle \Phi_{\vartheta^*}} \\ K^n & \xrightarrow[\mathrm{DFT}_n]{} & [K(\zeta_n)^n]_K \end{array} \tag{2.33}$$

[1]Mit anderen Worten: jedes $\sigma \in G$ gibt wegen $\sigma(\zeta_n) = \zeta_n^{r_\sigma}$ Anlaß zu einem $r_\sigma \in \mathbb{Z}$ und dieses ist modulo n eindeutig bestimmt.

Beweis: Sei $(c_0, c_1, \ldots, c_{n-1}) \in [K(\zeta_n)^n]_K$. Wir zeigen, daß für alle l gilt

$$\sum_k c_k \zeta_n^{kl} = \sum_k \phi_\vartheta(c_k)\phi_{\vartheta^*}(\zeta_n^{kl}). \tag{2.34}$$

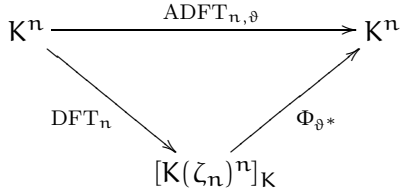
Denn mit $c_k = \sum_\sigma c_{k,\sigma}\vartheta^{*\sigma}$ und $\zeta_n^{kl} = \sum_\rho z_{kl,\rho}\vartheta^\rho$ ergibt sich

$$\begin{aligned} \mathrm{Sp}(\sum_k c_k \zeta_n^{kl}) &= \sum_{\sigma,\rho,k} c_{k,\sigma} z_{kl,\rho} \mathrm{Sp}(\vartheta^{*\sigma}\vartheta^\rho) \\ &= |G| \sum_k c_{k,1} z_{kl,1}, \end{aligned}$$

und das ist, mit Blick auf (2.28), gerade die Spur der rechten Seite von (2.34). □

Die Diagonale in obigem Diagramm gibt nun Anlaß zur Definition der Algebraischen Diskreten Fourier Transformation (ADFT):

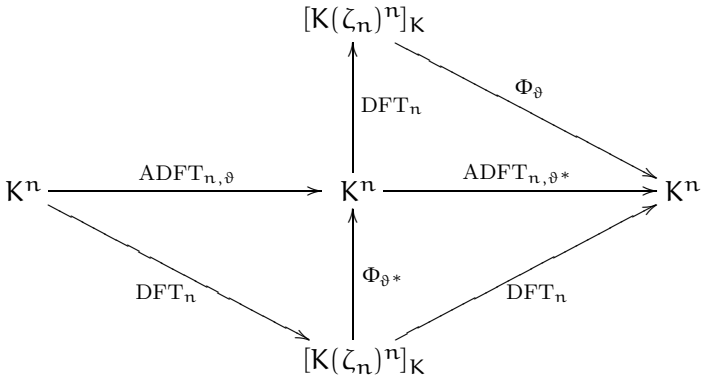
Definition 2.1 *Für einen Körper* $K \subseteq \mathbb{C}$, $n \in \mathbb{N}$ *und ein* $G(K(\zeta_n)/K)$*-reguläres Element* $\vartheta \in K(\zeta_n)$ *ist die* $\mathrm{ADFT}_{n,\vartheta}$ *definiert über das kommutative Diagramm:*



(2.35)

In Verbindung mit dem letzten Satz ergibt sich sofort das

Korollar 2.1 *In dem folgenden Diagramm kommutiert jedes Dreieck:*



(2.36)

Die Transformationsmatrix der $\mathrm{ADFT}_{n,\vartheta}$ bezeichnen wir im folgenden mit

$$A_{n,\vartheta} := \left(\phi_{\vartheta^*}(\zeta_n^{kl})\right)_{k,l} = \left(\mathrm{Sp}(\vartheta^*\zeta_n^{kl})\right)_{k,l}; \tag{2.37}$$

ihre Inverse ergibt sich unmittelbar aus (2.36):

$$I_{n,\vartheta} := A_{n,\vartheta}^{-1} = \frac{1}{n} A_{n,\vartheta^*} S_n = \frac{1}{n}\left(\mathrm{Sp}(\vartheta\zeta_n^{-kl})\right)_{k,l}. \tag{2.38}$$

In Worten bedeutet das, daß die Inverse der $\mathrm{ADFT}_{n,\vartheta}$ im wesentlichen, d. h. bis auf Vorfaktor und Permutation, durch die duale Transformation $\mathrm{ADFT}_{n,\vartheta^*}$ beschrieben ist. Insbesondere folgt, in Anlehnung an den DFT-Fall:

Satz 2.2 *Sei* K *ein Zahlkörper und* ϑ *ein* NBE *der Erweiterung* $K(\zeta_n)/K$. *Gilt dann für* $\alpha \in K(\zeta_n)$ *und* $\sigma \in G(K(\zeta_n)/K)$ *stets*

$$(\bar{\alpha})^\sigma = \overline{(\alpha^\sigma)}, \tag{2.39}$$

so ist die Matrix $\frac{1}{\sqrt{n}} A_{n,\vartheta}$ *genau dann unitär, wenn* $\vartheta^* = \bar{\vartheta}$.

Wir reden von *Quasiinversion*, falls die Mengen ϑ^G und ϑ^{*G}, wie etwa im Falle der DHT, identisch sind. Die Basis ϑ^G heißt in diesem Zusammenhang *quasiselbstdual*; gilt stärker $\vartheta = \vartheta^*$, so sprechen wir von einer *selbstdualen* Basis ϑ^G. Letztere existiert allerdings nur bei ungerader Gruppenordnung; vgl. [6].

Um das Bild der $\mathrm{ADFT}_{n,\vartheta}$ zu verstehen, genügt es zu bemerken, daß mit $\rho \in G(K(\zeta_n)/K)$ und den vereinbarten Konventionen gilt

$$\phi_{\vartheta^*}(\hat{c}_{k\rho^{-1}}) = \phi_{\vartheta^*\rho}(\hat{c}_k), \tag{2.40}$$

was mit Blick auf (2.31) den folgenden Satz rechtfertigt:

Satz 2.3 (Beth, [9]) *Die* $\mathrm{ADFT}_{n,\vartheta}$ *berechnet das Spektrum der* DFT_n *bzgl. der Normalbasis* $\vartheta^{G(K(\zeta_n)/K)}$.

Betrachten wir als Beispiel $K := \mathbb{Q}$ und $n := 6$. Die Elemente der Menge $\{\zeta_6, \zeta_6^5\}$ bilden dann eine Normalbasis des 6-ten Kreisteilungskörpers $\mathbb{Q}(\zeta_6)$ über $\mathbb{Q}$. Wegen $1 = -\zeta_6^3 = \zeta_6 + \zeta_6^5$,

sowie $\zeta_6 + \zeta_6^4 = \zeta_6^2 + \zeta_6^5 = 0$, besitzt die Transformationsmatrix der $\mathrm{ADFT}_{6,\zeta_6}$ die Gestalt

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & -1 & -1 & 0 \\ 1 & 0 & -1 & 1 & 0 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 0 & 1 & -1 & 0 \\ 1 & 0 & -1 & -1 & 0 & 1 \end{pmatrix}.$$

Dabei fällt zunächst einmal auf, daß sich diese Transformation unter ausschließlicher Verwendung der Addition realisieren läßt[2]. Normalbasen mit dieser Eigenschaft bezeichnen wir fortan als *schlanke Basen*. Die Frage nach Existenz und Aussehen solcher Basen rückt hier in natürlicher Weise in den Vordergrund. In diesem Kapitel zeigen wir u. a. den

Satz 2.4 *Im Falle des n-ten Kreisteilungskörpers $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ existiert eine schlanke Basis für alle n.*

Dieser hat als unmittelbare Folge das

Korollar 2.2 *Sei n eine natürliche Zahl und $K \subseteq \mathbb{C}$ ein Körper. Gilt dann*

$$G(K(\zeta_n)/K) \simeq (\mathbb{Z}/n\mathbb{Z})^\times, \tag{2.41}$$

so besitzt die Erweiterung $K(\zeta_n)/K$ eine schlanke Basis.

Für den Beweis bedarf es noch einiger Vorbereitung. Wir werden ihn im übernächsten Abschnitt führen; er wird konstruktiv sein, d. h. wir werden Basen angeben, welche die notwendigen Bedingungen erfüllen und, in Verbindung damit, eine explizite Konstruktionsmethode für die resultierenden Transformationen erhalten.

Zunächst aber zurück zu unserem Beispiel. Bei genauer Betrachtung der Matrix

[2] Einen Vorzeichenwechsel betrachten wir hier, wie allg. üblich, im Hinblick auf eine mögliche Realisierung nicht als skalare Multiplikation.

A_{6,ζ_6} stellt sich heraus, daß diese sich via Zeilen- und Spaltenpermutation in folgende Matrix überführen läßt:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 0 & 0 & -1 & -1 \\ 1 & -1 & 0 & 0 & -1 & 1 \\ 1 & 1 & -1 & -1 & 0 & 0 \\ 1 & -1 & -1 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = A_{3,-\zeta_3^2} \otimes A_{2,1}.$$

In der vorliegenden Situation überträgt sich also – in gewisser Weise – die Produktzerlegungseigenschaft der DFT. Wir behandeln den allgemeinen Fall von zwei Seiten. Bezeichne dazu, für natürliche Zahlen n_1, n_2 und $j = 1, 2$, ϑ_j einen NBE der Erweiterung $K(\zeta_{n_j})/K$.

Satz 2.5 *Gilt* $(n_1, n_2) = 1$ *und* $K(\zeta_{n_1}) \cap K(\zeta_{n_2}) = K$*, so ist*

$$A_{n_1,\vartheta_1} \otimes A_{n_2,\vartheta_2} \sim A_{n_1 n_2,\vartheta_1\vartheta_2}. \tag{2.42}$$

Bevor wir den Beweis führen wollen wir noch die Frage stellen, ob für einen NBE ϑ des Kompositums $K(\zeta_{n_1}, \zeta_{n_2})/K$ auch stets eine Zerlegung in obigem Sinne existiert. Schreiben wir abkürzend $\mathrm{Sp}_j(\cdot) := \mathrm{Sp}_{K(\zeta_{n_1},\zeta_{n_2})/K(\zeta_{n_j})}(\cdot)$ für die Spurabbildung auf die entsprechenden Zwischenkörper, so liefert der folgende Satz das Kriterium:

Satz 2.6 *Unter der Voraussetzung* $K(\zeta_{n_1}) \cap K(\zeta_{n_2}) = K$ *gilt: ein* NBE ϑ *der Erweiterung* $K(\zeta_{n_1}, \zeta_{n_2})/K$ *besitzt genau dann eine Zerlegung der Form*

$$\vartheta = \vartheta_1\vartheta_2, \tag{2.43}$$

mit $\vartheta_j \in K(\zeta_{n_j})$*, wenn gilt*

$$\mathrm{Sp}(\vartheta)\vartheta = \mathrm{Sp}_1(\vartheta)\mathrm{Sp}_2(\vartheta). \tag{2.44}$$

Im Falle von $\mathrm{Sp}(\vartheta) = 1 = (n_1, n_2)$ *ist dann also insbesondere*

$$A_{n_1 n_2,\vartheta} \sim A_{n_1,\mathrm{Sp}_1(\vartheta)} \otimes A_{n_2,\mathrm{Sp}_2(\vartheta)}. \tag{2.45}$$

Beweis: Die Bedingung $K(\zeta_{n_1}) \cap K(\zeta_{n_2}) = K$ liefert uns, nach der Galoistheorie, eine Zerlegung der Galoisgruppe $G(K(\zeta_{n_1}, \zeta_{n_2})/K)$ in der Form

$$G(K(\zeta_{n_1}, \zeta_{n_2})/K) \simeq G(K(\zeta_{n_1})/K) \times G(K(\zeta_{n_2})/K);$$

insbesondere ist also $\vartheta_1\vartheta_2$ ein NBE der Erweiterung $K(\zeta_{n_1}, \zeta_{n_2})/K$ und darüber hinaus gilt

$$(\vartheta_1\vartheta_2)^* = \vartheta_1^*\vartheta_2^* \tag{2.46}$$

aufgrund der Eindeutigkeit des Spurduals. Die Teilerfremdheit der Zahlen n_1, n_2 garantiert uns neben $K(\zeta_{n_1}, \zeta_{n_2}) = K(\zeta_{n_1 n_2})$ noch $s_1, s_2 \in \mathbb{Z}$ mit $s_1 n_1 + s_2 n_2 = 1$, sodaß insgesamt gilt

$$\begin{aligned} \mathrm{Sp}((\vartheta_1\vartheta_2)^*\zeta_{n_1 n_2}) &= \mathrm{Sp}_2(\vartheta_1^*\zeta_{n_1}^{s_2})\mathrm{Sp}_1(\vartheta_2^*\zeta_{n_2}^{s_1}) \\ &= \mathrm{Sp}_{K(\zeta_{n_1})/K}(\vartheta_1^*\zeta_{n_1}^{s_2})\mathrm{Sp}_{K(\zeta_{n_2})/K}(\vartheta_2^*\zeta_{n_2}^{s_1}). \end{aligned}$$

Der Rest steht in Analogie zum DFT-Fall. Was die Aussage des zweiten Satzes angeht, so ist zunächst einmal klar, daß das Element $\mathrm{Sp}_j(\vartheta)$ einen NBE der Erweiterung $K(\zeta_{n_j})$ darstellt. Gilt umgekehrt $\vartheta = \vartheta_1\vartheta_2$, so ist $\mathrm{Sp}_1(\vartheta) = \vartheta_1\mathrm{Sp}_1(\vartheta_2)$, und wegen $K(\zeta_{n_1}) \cap K(\zeta_{n_2}) = K$ gilt $\mathrm{Sp}_1(\vartheta_2) \in K$; insbesondere ist also $\mathrm{Sp}(\vartheta) = \mathrm{Sp}_2(\mathrm{Sp}_1(\vartheta)) = \mathrm{Sp}_1(\vartheta_2)\mathrm{Sp}_2(\vartheta_1)$. Insgesamt ergibt sich

$$\mathrm{Sp}_1(\vartheta)\mathrm{Sp}_2(\vartheta) = \vartheta_1\vartheta_2\mathrm{Sp}_1(\vartheta_2)\mathrm{Sp}_2(\vartheta_1) = \vartheta\mathrm{Sp}(\vartheta),$$

und damit der Satz. □

Ferner entnehmen wir dem Beweis, daß unter den gegebenen Voraussetzungen bereits alle möglichen Zerlegungen durch

$$\vartheta = ((a/\mathrm{Sp}(\vartheta))\mathrm{Sp}_1(\vartheta))((1/a)\mathrm{Sp}_2(\vartheta)), \tag{2.47}$$

mit $a \in K^\times$, charakterisiert sind. Die Existenz einer solchen Zerlegung ist allerdings nicht immer gewährleistet: so erzeugt z. B. das Element $\zeta_3\zeta_5 + 1$ eine Normalbasis der Erweiterung $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$ – es besitzt aber, wegen $9(\zeta_3\zeta_5 + 1) \neq (4 - \zeta_3)(2 - \zeta_5)$, keine Darstellung der gewünschten Form.

Mit Hilfe der letzten beiden Sätze erhalten wir unmittelbar die „zahme“ Variante von Satz 2.4. Bezeichne dazu μ die *Möbiusfunktion*, so gilt der

Satz 2.7 *Sei n eine natürliche und quadratfreie Zahl, dann erzeugt das Element*

$$\vartheta := \mu(n)\zeta_n \tag{2.48}$$

eine schlanke Basis der Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.

Beweis: Wegen Satz 2.6 und der schwachen Multiplikativität der Möbiusfunktion dürfen wir uns auf den Primzahlfall beschränken. Das Element $\vartheta := -\zeta_p$, p prim, ist dann offensichtlich ein NBE der Erweiterung $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ und der Eintrag der Matrix $A_{p,-\zeta_p}$ an der Position (k,l) entspricht 1 bzw. -1, je nachdem ob $kl \equiv 0 \bmod p$ oder $kl \equiv 1 \bmod p$; in allen anderen Fällen ist er 0. □

Das Vorzeichen $\mu(n)$ ist für obige Existenzaussage nicht von Bedeutung; es ist so gewählt, daß sich die Anzahl der benötigten Vorzeichenwechsel bei einer Realisierung der $\mathrm{ADFT}_{n,\vartheta}$ auf ein Minimum reduziert. Nach dem Gesagten gilt für die Anzahl der notwendigen arithmetischen Operationen $\Upsilon_\vartheta(n)$ mit obigen Parametern die Abschätzung:

Satz 2.8 *Im Falle von* $\mu(n) \neq 0$ *gilt*

$$\Upsilon_\vartheta(n) \leqslant 2n \sum_{p|n} \left(1 - \frac{1}{p}\right), \tag{2.49}$$

wobei das p *in der Summe die Primteiler von* n *durchläuft.*

Notabene: Das in Satz 2.7 definierte Element $\vartheta := \mu(n)\zeta_n$ erzeugt auch eine Basis der Hauptordnung $\mathbb{Z}[\zeta_n]$ von $\mathbb{Q}(\zeta_n)$; eine sog. *Ganzheitsnormalbasis*. Eine notwendige Bedingung für die Existenz einer solchen Basis einer endlichen (Galois-) Erweiterung $K/\mathbb{Q}$ ist, daß die Erweiterung an jeder (endlichen) Stelle höchstens *zahm verzweigt*. Im Falle des Kreisteilungskörpers $\mathbb{Q}(\zeta_n)$ ist das gleichbedeutend mit $\mu(n) \neq 0$. Ohne näher auf die Begrifflichkeiten einzugehen (vgl. [62]), skizzieren wir hier kurz das Argument: für einen Erzeuger θ einer Ganzheitsnormalbasis von $K/\mathbb{Q}$ mit Galoisgruppe $G := G(K/\mathbb{Q})$ gilt zunächst einmal notwendigerweise $\mathrm{Sp}(\theta) = \pm 1$, und damit insbesondere für jede (endliche) Stelle $\mathfrak{p}$ von K, mit $\mathfrak{p}^e | p$,

$$\sum_{\sigma \in G} \theta^\sigma \equiv \pm 1 \bmod \mathfrak{p}.$$

Bezeichne $I_\mathfrak{p}$ die Trägheitsgruppe von $\mathfrak{p}$ über K, dann folgt daraus

$$|I_\mathfrak{p}| \sum_{\sigma' \in G/I_\mathfrak{p}} \theta^{\sigma'} \equiv \pm 1 \bmod \mathfrak{p},$$

und damit $(p, |I_\mathfrak{p}|) = (p, e) = 1$.

2.3 Normalbasen und Gaußsche Summen

Um auch im allgemeinen Fall schlanke Basen zu konstruieren, werden wir uns nun einer speziellen Darstellung algebraischer Zahlen bedienen, welche auf H.-W. Leopoldt (vgl. [52]) zurückgeht. Vorab vereinbaren wir die folgenden Bezeichnungen.

Wir beginnen mit einer endlichen abelschen (multiplikativen) Gruppe G. Als *Charaktere* von G bezeichnen wir die (Gruppen-) Homomorphismen

$$\chi : G \longrightarrow \mathbb{C}^\times \tag{2.50}$$

von G in die Einheitengruppe des Körpers der komplexen Zahlen. Diese bilden bzgl. der Multiplikation $\chi\psi(a) := \chi(a)\psi(a)$ selbst wieder eine, zu G isomorphe Gruppe, die *Charaktergruppe* $G^\wedge$ von G. Das neutrale Element χ_0 dieser Gruppe heißt der *Hauptcharakter*. Für ihn gilt also $\chi_0(a) = 1$, für alle $a \in G$. Da G endlich ist, gilt zudem für alle $\chi \in G^\wedge$:

$$\chi^{|G|} = \chi_0; \tag{2.51}$$

das Bild eines Charakters liegt also in der Menge der $|G|$-ten Einheitswurzeln. Für χ^{-1} schreiben wir aus diesem Grund auch $\bar{\chi}$. Die Charaktere von G erfüllen u. a. die folgenden Relationen:

$$\sum_a \chi(a) = \begin{cases} |G|, & \chi = \chi_0 \\ 0, & \chi \neq \chi_0 \end{cases} \tag{2.52}$$

$$\sum_a \chi(a)\bar{\psi}(a) = \begin{cases} |G|, & \chi = \psi \\ 0, & \chi \neq \psi \end{cases} \tag{2.53}$$

und, wenn wir $(G^\wedge)^\wedge$ wieder mit G identifizieren, entsprechend

$$\sum_\chi \chi(a) = \begin{cases} |G|, & a = 1 \\ 0, & a \neq 1 \end{cases} \tag{2.54}$$

$$\sum_\chi \chi(a)\bar{\chi}(b) = \begin{cases} |G|, & a = b \\ 0, & a \neq b \end{cases} \tag{2.55}$$

Den *Wertekörper* eines Charakters χ bezeichnen wir kurz mit $\mathbb{Q}(\chi) := \mathbb{Q}(\chi(a), a \in G)$. Für ihn gilt, wie schon erwähnt, $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\zeta_{|G|})$. Entsprechend definieren wir für $\rho \in G(\mathbb{Q}(\chi)/\mathbb{Q})$: $\chi^\rho(a) := (\chi(a))^\rho$ für alle $a \in G$.

Wir betrachten nun einen abelschen Zahlkörper $K/\mathbb{Q}$. Als *Charaktere von* K bezeichnen wir die Charaktere der Galoisgruppe $G(K/\mathbb{Q})$. Nach dem *Satz von Kronecker-Weber* (vgl. [82] Th. 14.1) existiert in Abhängigkeit von K eine natürliche Zahl $n := n(K)$, sodaß gilt: $K \subseteq \mathbb{Q}(\zeta_n)$. Die Charaktere

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times \tag{2.56}$$

der Galoisgruppe der Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ haben einen speziellen Namen: sie heißen *Restklassen-* oder auch *Dirichletcharaktere*. Die Zahl n nennt man einen *Erklärungsmodul* des Charakters χ. Er (der Charakter) heißt *eigentlich* oder *primitiv*, wenn er nicht schon als Kompositum $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ mit einem echten Teiler m von n entsteht. Den Erklärungsmodul, bzgl. dessen der Charakter χ primitiv ist (resp. der größte gemeinsame Teiler aller Erklärungsmoduln) bezeichnen wir im folgenden mit f_χ und nennen ihn den *Führer* von χ. Der Hauptcharakter χ_0 (und nur dieser) hat den Führer $f_{\chi_0} = 1$ (Beachte: einen Charakter mit Führer 2 kann es nach Definition nicht geben).

Aus Notationsgründen denken wir uns die Dirichletcharaktere als Funktionen auf den ganzen Zahlen, indem wir für $a \in \mathbb{Z}$ festsetzen:

$$\chi(a) := \chi(a \bmod f_\chi), \tag{2.57}$$

falls $(a, f_\chi) = 1$ und $\chi(a) = 0$, sonst. Ein Charakter χ heißt in diesem Zusammenhang *gerade* (resp. *ungerade*), falls $\chi(-1) = 1$ (resp. $\chi(-1) = -1$). Die ganze Zahl

$$d_K := \prod_\chi \chi(-1) f_\chi, \tag{2.58}$$

wobei χ die Charaktere von K durchläuft, heißt die *Diskriminante* des (abelschen) Zahlkörpers K.

Nach dem Chinesischen Restesatz korrespondiert zu einer Zerlegung $m = m_1 \cdots m_r$ eines Erklärungsmoduls m von χ in paarweise teilerfremde Faktoren, eine (eindeutige) Zerlegung

$$\chi = \chi_{m_1} \cdots \chi_{m_r}, \tag{2.59}$$

wobei $\chi_{m_i}(a) := \chi(a_i)$, mit $a_i \equiv a \bmod m_i$ und $a_i \equiv 1 \bmod \frac{m}{m_i}$. Entsprechend gilt für den Führer

$$f_\chi = f_{\chi_{m_1}} \cdots f_{\chi_{m_r}}. \tag{2.60}$$

Die zum Restklassencharakter χ mit Erklärungsmodul m gehörigen *Gaußschen Summen* sind nun definiert durch

$$\tau(\chi|\zeta_m^a) := \sum_{x \cap m} \chi(x) \zeta_m^{ax}, \tag{2.61}$$

$a \in \mathbb{Z}$, wobei „$x \cap m$“ bedeute, daß x ein primes Restesystem modulo m durchläuft.

$$\tau(\chi) := \tau(\chi|\zeta_{f_\chi}) \tag{2.62}$$

heißt die zu χ gehörige *normierte eigentliche Gaußsche Summe*. Für sie gilt u. a.

$$\tau(\chi)\tau(\bar{\chi}) = \chi(-1)f_\chi, \tag{2.63}$$

insbesondere also $\tau(\chi) \neq 0$. Für den allgemeinen Fall setzen wir $\zeta_m^a = \zeta_{m_0}^{a_0}$ mit $(a_0, m_0) = 1$, und erhalten $\tau(\chi|\zeta_m^a) = 0$, falls $f_\chi \not| m_0$. Gilt $f_\chi | m_0$, so haben wir (vgl. [33])

$$\tau(\chi|\zeta_m^a) = \frac{\varphi(m)}{\varphi(m_0)}\mu(\frac{m_0}{f_\chi})\chi(\frac{m_0}{f_\chi})\bar{\chi}(a_0)\tau(\chi), \tag{2.64}$$

wobei φ die Eulerfunktion und μ wieder die Möbiusfunktion bezeichne; $\tau(\chi|\zeta_m^a)$ verschwindet also nur dann nicht, wenn $f_\chi | m_0$, $\frac{m_0}{f_\chi}$ quadratfrei und zu f_χ teilerfremd ist.

Zur Zerlegung des Erklärungsmoduls $m = m_1 \cdots m_r$ in paarweise teilerfremde Faktoren korrespondiert eine Zerlegung der entsprechenden Summen:

$$\tau(\chi|\zeta_m^a) = \prod_{i=1}^{r} \chi_{m_i}(\frac{m}{m_i})\tau(\chi_{m_i}|\zeta_{m_i}^a). \tag{2.65}$$

Die Werte der eigentlichen Summen $\tau(\chi)$ und insbesondere die der Elemente

$$\omega(\chi, \chi') := \frac{\tau(\chi)\tau(\chi')}{\tau(\chi\chi')} \tag{2.66}$$

des *Faktorensystems der Gaußschen Summen* werden wir im nächsten Kapitel noch genauer betrachten.

Wir kommen nun zu der oben angesprochenen Darstellung:

Satz 2.9 (Leopoldt, [52]) *Sei* K *ein abelscher Zahlkörper mit Galoisgruppe* G. *Dann besitzt jedes* $\vartheta \in K$ *eine eindeutige Darstellung*

$$\vartheta = \frac{1}{|G|}\sum_{\chi} y_K(\chi|\vartheta)\tau(\chi), \tag{2.67}$$

wobei χ *die Charaktere von* K *durchläuft.*

Die Koordinaten $y_K(\chi|\vartheta)$ *sind Elemente des Wertekörpers von* χ, *also*

$$y_K(\chi|\vartheta) \in \mathbb{Q}(\chi) \tag{2.68}$$

und zu konjugierten Charakteren gehören konjugierte Koordinaten, d.h. für $\rho \in G(\mathbb{Q}(\chi)/\mathbb{Q})$ *ist*

$$y_K(\chi^\rho|\vartheta) = y_K(\chi|\vartheta)^\rho. \tag{2.69}$$

Umgekehrt definiert jedes die Bedingungen (2.68),(2.69) erfüllende System $y(\chi)$ *in eindeutiger Weise ein Element aus* K*.*

Aufgrund der zentralen Bedeutung für dieses Kapitel soll der Beweis des Satzes an dieser Stelle noch einmal skizziert werden. Wir orientieren uns dabei überwiegend an der neueren Arbeit [54].

Die Darstellung (2.67) ergibt sich durch Anwendung des zu χ gehörigen primitiven Idempotents

$$1_\chi := \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma)\sigma \tag{2.70}$$

des (zerfallenden) Gruppenrings von G auf das Element ϑ via

$$1_\chi\vartheta = \frac{1}{|G|}\sum_{\sigma}\chi(\sigma)\vartheta^\sigma = \frac{1}{|G|}y_K(\chi|\vartheta)\tau(\chi) \tag{2.71}$$

(das in der Originalarbeit [52] angegebene Idempotent projiziert hingegen auf die konjugierte Summe $\tau(\bar{\chi})$).

Entsprechend unterscheidet sich der folgende Satz von [52]:

Satz 2.10 *Die oben definierten* χ*-Koordinaten sind auf folgende Weise quasiinvariant unter* G*:*

$$y_K(\chi|\vartheta^\sigma) = \bar{\chi}(\sigma)y_K(\chi|\vartheta), \tag{2.72}$$

für alle $\sigma \in G$*.*

Die Eindeutigkeit der Darstellung (2.67) ergibt sich nun wie folgt. Sei

$$0 = \frac{1}{|G|}\sum_{\chi} y(\chi)\tau(\chi)$$

eine Darstellung der Null, wobei die $y(\chi)$ den Bedingungen (2.68) und (2.69) genügen. Desweiteren sei $m \in \mathbb{N}$ ein Vielfaches von $|G|$ und d_K, der Diskriminante von K. Für

$(z, m) = 1$ bezeichne $\sigma_z \in G(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ den Automorphismus, welcher durch $\zeta_m^{\sigma_z} := \zeta_m^z$ gegeben ist. Nach der *Automorphieregel für Gaußsche Summen* gilt dann

$$\tau(\chi)^{\sigma_z} = \bar{\chi}^z(z)\tau(\chi^z), \tag{2.73}$$

vgl. (2.64). Für einen Ausdruck $A := \frac{1}{|G|}\sum_\chi y(\chi)\tau(\chi)$, wie oben, folgt demnach

$$A^{\sigma_z} = \frac{1}{|G|}\sum_\chi \bar{\chi}(z)y(\chi)\tau(\chi) \tag{2.74}$$

und somit $0 = 1_\chi 0 = \frac{1}{|G|}y(\chi)\tau(\chi)$, also $y(\chi) = 0$.

Falls $z \in \bigcap_\chi \operatorname{Kern}\chi$ folgt außerdem $A^{\sigma_z} = A$, d. h. der Ausdruck ist tatsächlich ein Element von K.

Wir wählen nun einen festen Charakter χ von K und definieren K_χ als denjenigen Teilkörper von K, welcher invariant unter dem Kern von χ bleibt, also $K_\chi := K^{\operatorname{Kern}\chi}$. Für

$$y_K(\chi|\vartheta) = \frac{1}{f_\chi}\sum_\sigma \chi(\sigma)\vartheta^\sigma\,\overline{\tau(\chi)} \tag{2.75}$$

folgt dann wegen

$$\overline{\tau(\chi)} = \sum_{x \cap f_\chi} \bar{\chi}(x)\zeta_{f_\chi}^{-x} = \sum_{z \bmod \operatorname{Kern}\chi} \bar{\chi}(z)\operatorname{Sp}_{\mathbb{Q}(\zeta_{f_\chi})/K_\chi}(\zeta_{f_\chi}^{-1})^{\sigma_z},$$

sowie

$$\sum_\sigma \chi(\sigma)\vartheta^\sigma = \sum_{z \bmod \operatorname{Kern}\chi} \bar{\chi}(z)\operatorname{Sp}_{K/K_\chi}(\vartheta)^{\sigma_z},$$

mit Hilfe elementarer Umformung:

Satz 2.11 (Leopoldt, [52]) *Für die χ-Koordinaten gilt mit obigen Bezeichnungen:*

$$y_K(\chi|\vartheta) = \frac{1}{f_\chi}\sum_{z \bmod \operatorname{Kern}\chi} \chi(z)\operatorname{Sp}_{K_\chi/\mathbb{Q}}\left\{\operatorname{Sp}_{K/K_\chi}(\vartheta)^{\sigma_z}\operatorname{Sp}_{\mathbb{Q}(\zeta_{f_\chi})/K_\chi}(\zeta_{f_\chi}^{-1})\right\}. \tag{2.76}$$

Zum einen folgen also die Aussagen (2.68) und (2.69), zum anderen ist zu erkennen, daß $y_K(\chi|\vartheta)$ nur von $\operatorname{Sp}_{K/K_\chi}(\vartheta)$ abhängt.

Im allgemeinen hat man die folgende Reduktionsregel:

Satz 2.12 (Leopoldt, [52]) *Ist* L *ein beliebiger Teilkörper von* K *und* χ *bereits ein Charakter von* L*, so gilt*

$$y_K(\chi|\vartheta) = y_L(\chi|\operatorname{Sp}_{K/L}(\vartheta)). \tag{2.77}$$

Soweit zum Beweis von Satz 2.9.

Das Element $\vartheta \in K$ ist bekanntlich genau dann ein NBE, wenn die zugehörige Diskriminante von Null verschieden ist:

$$d(\vartheta^\sigma, \sigma \in G) := \det((\vartheta^{\sigma\rho}))^2 = \det(\operatorname{Sp}(\vartheta^\sigma\vartheta^\rho)) \neq 0. \tag{2.78}$$

Der folgende Satz liefert den Zusammenhang mit den χ-Koordinaten:

Satz 2.13 (Leopoldt, [52]) *Sei* d_K *die Diskriminante von* K*, dann gilt*

$$d(\vartheta^\sigma, \sigma \in G) = \left(\prod_\chi y_K(\chi|\vartheta)\right)^2 d_K. \tag{2.79}$$

Insbesondere ist das Element ϑ *also genau dann* G*-regulär, wenn die* $y_K(\chi|\vartheta)$ *sämtlich von Null verschieden sind.*

Dieses Kriterium gibt uns nun die Möglichkeit der expliziten Konstruktion von Normalbasen. Desweiteren haben wir für das Spurdual den folgenden

Satz 2.14 *Sei* $\vartheta = \frac{1}{|G|}\sum_\chi y_K(\chi|\vartheta)\tau(\chi) \in K$ *ein* NBE *von* $K/\mathbb{Q}$*, dann gilt für die* χ*-Koordinaten des Spurduals* ϑ^**:*

$$y_K(\chi|\vartheta^*) = \frac{\chi(-1)}{f_\chi y_K(\bar\chi|\vartheta)}. \tag{2.80}$$

Beweis: Zunächst einmal stellen wir fest, daß die Elemente $\chi(-1)/f_\chi y_K(\bar\chi|\vartheta)$ die Bedingungen (2.68) und (2.69) erfüllen, da konjugierte Charaktere den gleichen Führer haben. Der Satz ergibt sich nun durch einsetzen von ϑ, ϑ^* in die folgende Gleichung:

$$\operatorname{Sp}(\alpha^\sigma\beta^\rho) = \frac{1}{|G|}\sum_\chi y_K(\chi|\alpha)y_K(\bar\chi|\beta)\bar\chi(\sigma)\chi(\rho)\chi(-1)f_\chi, \tag{2.81}$$

mit $\alpha, \beta \in K$ und $\sigma, \rho \in G$. Letztere gilt wegen

$$\alpha^{\sigma}\beta^{\rho} = \frac{1}{|G|^2} \sum_{\chi,\psi} \bar{\chi}(\sigma)\bar{\psi}(\rho) y_K(\chi|\alpha) y_K(\psi|\beta) \tau(\chi)\tau(\psi)$$

und damit, nach Spurbildung und Umgruppierung der Terme,

$$\mathrm{Sp}(\alpha^{\sigma}\beta^{\rho}) = \frac{1}{|G|} \sum_{\chi,\psi} \bar{\chi}(\sigma)\bar{\psi}(\rho) y_K(\chi|\alpha) y_K(\psi|\beta) \tau(\chi)\tau(\psi) \frac{1}{|G|} \sum_{\pi} \bar{\chi}(\pi)\bar{\psi}(\pi).$$

Daraus folgt (2.81) durch Anwendung von (2.53), sowie Gleichung (2.63). □

Korollar 2.3 *Ein Normalbasiserzeuger ϑ eines abelschen Zahlkörpers K ist genau dann selbstdual, wenn für alle Charaktere χ von K gilt*

$$|y_K(\chi|\vartheta)|^2 = \frac{\chi(-1)}{f_\chi}. \tag{2.82}$$

Hingegen ist für alle Charaktere χ von K

$$|y_K(\chi|\vartheta)|^2 = \frac{1}{f_\chi} \tag{2.83}$$

genau dann, wenn $\vartheta^* = \bar{\vartheta}$.

An Gleichung (2.82) läßt sich u. a. ablesen, daß unter den abelschen Zahlkörpern höchstens die reellen Zahlkörper selbduale Normalbasen besitzen. Eine hinreichende Bedingung für die Existenz dieser Basen ist, wie schon erwähnt, daß der Körpergrad zudem ungerade ist; vgl. [6].

2.4 Schlanke Basen für die rationale ADFT

Mit den Hilfsmitteln des letzten Abschnitts sind wir in der Lage den Beweis von Satz 2.4 zu führen. Zunächst bringen wir die Transformationsmatrix $A_{n,\vartheta}$ der rationalen ADFT in eine, für unsere Zwecke geeignete Darstellung:

Satz 2.15 *Für die Transformationsmatrix der rationalen* ADFT *gilt mit den vereinbarten Bezeichnungen:*

$$A_{n,\vartheta} = \frac{1}{\varphi(n)} \left(\sum_{\chi} \frac{y(\chi|\zeta_n^{kl})}{y(\chi|\vartheta)} \right)_{k,l}. \tag{2.84}$$

Beweis: Die Darstellung (2.84) ergibt sich wegen $A_{n,\vartheta} = \left(\mathrm{Sp}(\vartheta^* \zeta_n^{kl})\right)_{k,l}$ nach Einsetzen von ϑ^* bzw. ζ_n^{kl} in (2.81), sowie durch Anwendung von (2.80). □

Als nächstes bestimmen wir die Werte der χ-Koordinaten der Einheitswurzeln. Wir setzen $\zeta_n^{kl} = \zeta_{n_0}^{a_0}$, wobei $(n_0, a_0) = 1$ und erhalten nach (2.75) bzw. (2.64)

$$y(\chi|\zeta_n^{kl}) = y(\chi|\zeta_{n_0}^{a_0}) = \begin{cases} \frac{\varphi(n)}{\varphi(n_0)} \mu(\frac{n_0}{f_\chi}) \chi(\frac{n_0}{f_\chi}) \bar{\chi}(a_0), & f_\chi | n_0 \\ 0, & \text{sonst} \end{cases} . \tag{2.85}$$

Nach dem Gesagten dürfen wir $n_0 = p^e$, p prim, annehmen. Bezeichne abkürzend $c = c_{a_0,n_0} = c_{k,l} := \frac{1}{\varphi(n)} \sum_\chi \frac{y(\chi|\zeta_n^{kl})}{y(\chi|\vartheta)}$, so erhalten wir nacheinander die Fälle:

$\underline{n_0 = 1}$: Also $c = \frac{1}{y(\chi_0|\vartheta)}$. Wir setzen

$$y(\chi_0|\vartheta) = 1 \tag{2.86}$$

und damit $c = 1$.

$\underline{n_0 = 2}$: Nach dem letzten Fall gilt $c = \frac{-1}{y(\chi_0|\vartheta)} = -1$.

$\underline{n_0 = p \neq 2}$: Es folgt $c = \frac{1}{\varphi(p)} \left(-1 + \sum_{\chi, f_\chi = p} \frac{\bar{\chi}(a_0)}{y(\chi|\vartheta)}\right)$. Für die Charaktere χ, mit $f_\chi = p$, wählen wir

$$y(\chi|\vartheta) = -1 \tag{2.87}$$

und damit $c = \frac{-1}{p-1} \sum_\chi \chi(a_0)$, also $c = -1$, falls $a_0 \equiv 1 \bmod p$, ansonsten $c = 0$.

$\underline{n_0 = 2^s, s > 1}$: In diesem Fall folgt $c = \frac{1}{\varphi(2^s)} \sum_{\chi, f_\chi = 2^s} \frac{\bar{\chi}(a_0)}{y(\chi|\vartheta)}$. Nach Wahl von

$$y(\chi|\vartheta) = \frac{1}{2}, \tag{2.88}$$

für die Charaktere vom Führer $2^s \geqslant 4$, erhalten wir wegen $\sum_{\chi, f_\chi = 2^s} \bar{\chi}(a_0) = \sum_\chi \bar{\chi}(a_0) - \sum_{\chi, f_\chi < 2^s} \bar{\chi}(a_0)$ nacheinander $c = 1$, falls $a_0 \equiv 1 \bmod 2^s$, $c = -1$, falls $a_0 \equiv 1 + 2^{s-1} \bmod 2^s$, und $c = 0$ sonst.

$\underline{n_0 = p^s, s > 1, p \neq 2}$: Für die Charaktere χ mit $f_\chi = p^s$ machen wir den Ansatz

$$y(\chi|\vartheta) = \frac{1}{p} \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \bar{\chi}(1 + ip^{s-1}), \tag{2.89}$$

$\left(\frac{i}{p}\right)$ das Legendresymbol, und da $\bar{\chi}(1+ip^{s-1})$ wegen $f_\chi = p^s$ stets eine primitive p-te Einheitswurzel und $\left(\frac{i}{p}\right)$ ein quadratischer Charakter ist, folgt $y(\chi|\vartheta)\overline{y(\chi|\vartheta)} = \frac{1}{p}$; und damit

$$\begin{aligned} c &= \frac{1}{\varphi(p^s)} \sum_{\chi, f_\chi = p^s} \frac{\bar{\chi}(a_0)}{y(\chi|\vartheta)} \\ &= \frac{1}{\varphi(p^s)} \sum_{\chi, f_\chi = p^s} \bar{\chi}(a_0) \sum_i \left(\frac{i}{p}\right) \chi(1+ip^{s-1}), \end{aligned}$$

bzw. nach Umordnung der Terme

$$c = \frac{1}{\varphi(p^s)} \sum_i \left(\frac{i}{p}\right) \sum_{\chi, f_\chi = p^s} \bar{\chi}(a_0)\chi(1+ip^{s-1}).$$

Da $\sum_{\chi, f_\chi = p^s} \bar{\chi}(a_0)\chi(1+ip^{s-1})$ nur dann von Null verschieden ist, falls $a_0 \equiv 1 + jp^{s-1} \bmod p^s$, $(j,p) = 1$, folgt wegen $\sum_i \left(\frac{i}{p}\right) = 0$: $c = \left(\frac{j}{p}\right)$, in diesem Fall, und $c = 0$ sonst.

Schließlich überzeugt man sich noch davon, daß die so definierten $y(\chi|\vartheta)$ die Bedingungen (2.68) und (2.69) erfüllen. Damit ist Satz 2.4 bewiesen. □

2.5 Die Schnelle Algebraische Fourier Transformation

Nachdem die Existenz schlanker Basen gezeigt ist, wollen wir uns nun der Struktur der Transformationsmatrizen $A_{n,\vartheta}$ im Zweierpotenzfall widmen und ein Analogon zur FFT, die *Schnelle Algebraische Fourier Transformation* (SADFT) entwickeln.

Sei also $n := 2^k > 1$. Bezeichne

$$\vartheta_n := \frac{1}{\varphi(n)} \left(1 + \frac{1}{2} \sum_{\chi \neq \chi_0} \tau(\chi)\right) \tag{2.90}$$

die, im letzten Abschnitt definierte (schlanke) Normalbasis der Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, sowie $N_{n,\vartheta_n} := \left(\mathrm{Sp}(\vartheta_n^{*\sigma}\zeta_n^l)\right)_{l,\sigma}$, mit $l = 0, \ldots, n/2-1$ und $\sigma \in G(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, die zugehörige *Basiswechselmatrix*. Schreiben wir noch abkürzend $A_n := A_{n,\vartheta_n}$, bzw. $N_n := N_{n,\vartheta_n}$ so gilt der

Satz 2.16 *Durch geeignete Spaltenpermutation geht die Matrix A_n über in die Matrix*

$$\tilde{A}_n = (A_2 \otimes E_{n/2}) \begin{pmatrix} A_{n/2} & \\ & N_n \end{pmatrix}. \tag{2.91}$$

Beweis: Die Zerlegung ergibt sich durch Anordnung der Spalten wie folgt: zunächst die geraden $0, 2, \ldots, n-2$ und dann die Inversen der ungeraden Spaltennummern $(\mathrm{mod}\, n)$ $1, 3^{-1}, \ldots, (n-1)^{-1}$. Für $n \geqslant 4$ und einen zunächst beliebigen NBE $\theta \in \mathbb{Q}(\zeta_n)$, gelangt man dadurch zu einer Zerlegung der Form

$$\tilde{A}_{n,\theta} = \begin{pmatrix} A_{n/2,\theta'} & N_{n,\theta} \\ A_{n/2,\theta'} & -N_{n,\theta} \end{pmatrix} = (A_2 \otimes E_{n/2}) \begin{pmatrix} A_{n/2,\theta'} & \\ & N_{n,\theta} \end{pmatrix}.$$

Desweiteren ist zu beachten, daß der Eintrag an der Stelle (l, s), wegen $\zeta_n^{ls} = \zeta_{n_0}^{a_0}$, nur von dem Tupel (n_0, a_0) abhängt; vgl. den letzten Abschnitt. Der neue Erzeuger $\theta' \in \mathbb{Q}(\zeta_{n/2})$ entsteht also aus θ durch Weglassen der höchsten χ-Koordinaten, d. h. durch $y(\chi|\theta') := y(\chi|\theta)$ für $f_\chi \leqslant n/2$. Die Wahl $\theta := \vartheta_n$ liefert schließlich (2.91) □

Der Gesamtaufwand zur Realisierung der Transformation ergibt sich also als Summe aus einer Transformation halber Länge, einem Basiswechsel und einem Rest; in Zeichen:

$$\Upsilon_A(n) = \Upsilon_A(n/2) + \Upsilon_N(n) + n. \tag{2.92}$$

Für die Basiswechselmatrix N_n haben wir den folgenden

Satz 2.17 *Für $n \geqslant 4$ und ϑ_n wie oben, geht die Matrix N_n durch geeignete Zeilenpermutation über in die Matrix*

$$\tilde{N}_n = \begin{pmatrix} N_{n/2} & \\ & E_{n/4} \end{pmatrix} (A_2 \otimes E_{n/4}). \tag{2.93}$$

Beweis: Die Zeilenpermutation ordnet erst die geraden und dann die ungeraden Zeilennummern. Damit hat man, zunächst wieder für einen beliebigen NBE $\theta \in \mathbb{Q}(\zeta_n)$, unter Beachtung von $(2^{k-1}+s)^{-1} \equiv 2^{k-1} + s^{-1} \bmod 2^k$, für $k \geqslant 2$ und ungerade s, eine Zerlegung der Form

$$\tilde{N}_{n,\theta} = \begin{pmatrix} N_{n/2,\theta'} & N_{n/2,\theta'} \\ R_{n,\theta} & -R_{n,\theta} \end{pmatrix} = \begin{pmatrix} N_{n/2,\theta'} & \\ & R_{n,\theta} \end{pmatrix} (A_2 \otimes E_{n/4}),$$

mit einer Matrix

$$R_{n,\theta} := \left(\mathrm{Sp}(\theta^* \zeta_n^{ls^{-1}})\right)_{l,s}, \tag{2.94}$$

$l, s = 1, \ldots, n/2 - 1$; l, s ungerade. Der Erzeuger $\theta' \in \mathbb{Q}(\zeta_{n/2})$ ergibt sich auf die gleiche Weise wie oben. Dem letzten Abschnitt zufolge gilt nun nach Wahl von $\theta := \vartheta_n$ zunächst

$$R_{n,\vartheta_n} = E_{n/4} \tag{2.95}$$

und damit der Satz. □

Als Folgerung aus dem letzten Satz ergibt sich also damit, wegen der Abschätzung

$$\Upsilon_N(n) = \Upsilon_N(n/2) + n/2 \leqslant n - 2, \tag{2.96}$$

für die Transformation von Polynomial- in Normalbasis das

Korollar 2.4 *Der Aufwand für die Realisierung des Basiswechsels* $(\zeta_n^i)_j \to (\vartheta_n^\sigma)_\sigma$ *ist mit obiger Methode linear.*

Eingesetzt in (2.92) erhalten wir als Aufwand für die SADFT im Zweierpotenzfall:

Satz 2.18 *Für* $n := 2^k$ *und* ϑ_n *wie in (2.90), erlaubt das dargestellte Verfahren eine Realisierung der* $\mathrm{ADFT}_{n,\vartheta_n}$ *mit Hilfe von* $O(n)$ *Additionen.*

In Abb. 2.2 ist das Flußdiagramm des resultierenden Algorithmus für den Fall $n = 8$ dargestellt.

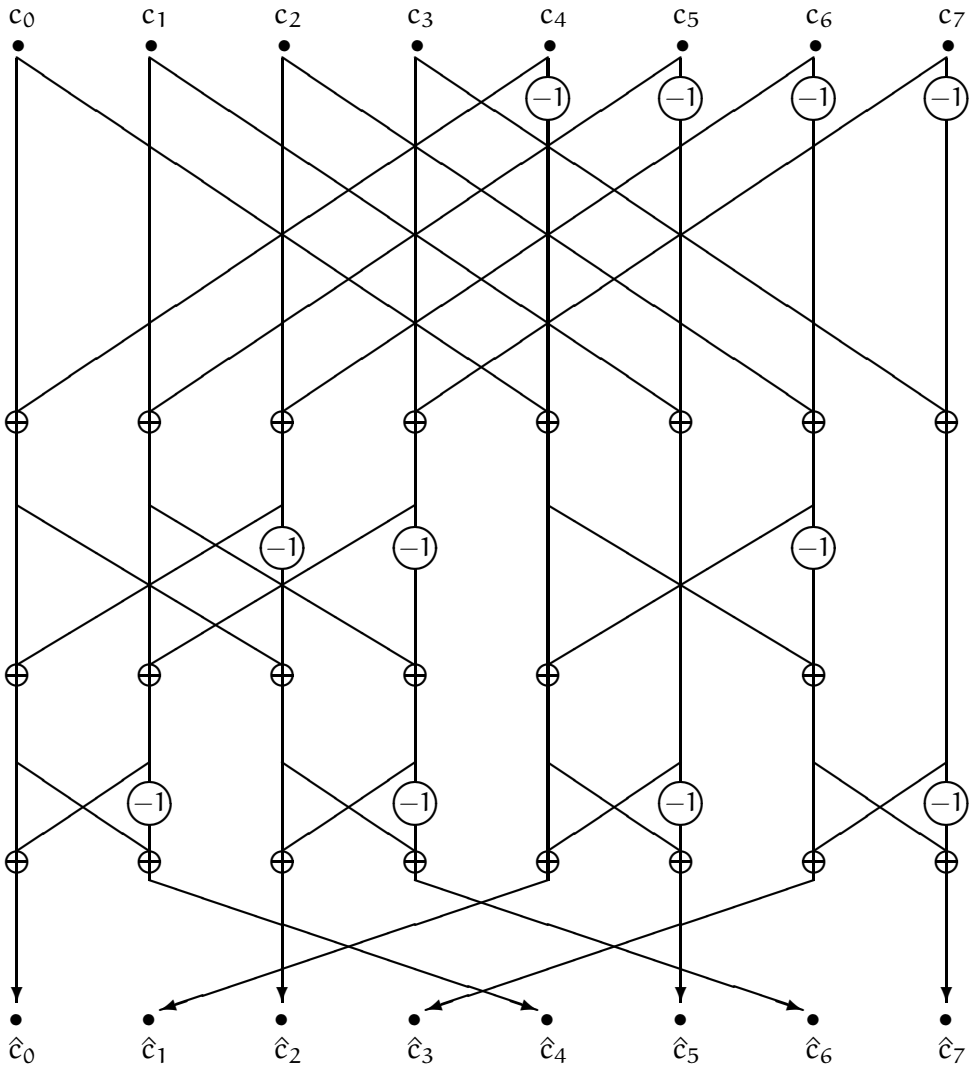


Abbildung 2.2: Flußdiagramm zur SADFT_8

Kapitel 3

Fermat

3.1 Normalbasenarithmetik

Nachdem wir im letzten Kapitel gesehen haben, wie sich im abelschen Fall Normalbasen konstruieren, bzw. manipulieren lassen, wollen wir nun einen genaueren Blick auf die, diese Basen betreffende Arithmetik werfen.

Sei dazu im Folgenden K ein abelscher Zahlkörper, G die zugehörige Galoisgruppe, sowie ϑ^G eine Normalbasis der Erweiterung $K/\mathbb{Q}$. Für Elemente $\alpha, \beta \in K$, mit $\alpha = \sum_\sigma a_\sigma \vartheta^\sigma$, $\beta = \sum_\varphi b_\varphi \vartheta^\varphi$, $a_\sigma, b_\varphi \in \mathbb{Q}$, besitzt dann das Produkt die Darstellung

$$\alpha\beta = \sum_\rho \{\alpha, \beta\}_{\vartheta,\rho} \vartheta^\rho, \tag{3.1}$$

wobei es sich bei der Abbildung

$$\{\cdot,\cdot\}_{\vartheta,\rho} : K \times K \longrightarrow \mathbb{Q} \tag{3.2}$$

um eine nichtausgeartete, symmetrische Bilinearform des $|G|$-dimensionalen $\mathbb{Q}$-Vektorraums K handelt. Entsprechend sind die zugehörigen Matrizen $W_\vartheta^{(\rho)} \in \mathbb{Q}^{|G|\times|G|}$ definiert via

$$\{\alpha, \beta\}_{\vartheta,\rho} = (a_\sigma)_\sigma W_\vartheta^{(\rho)} (b_\varphi)_\varphi^T. \tag{3.3}$$

Genauer:

Definition 3.1 *Sei K ein abelscher Zahlkörper mit Galoisgruppe G und ϑ ein Erzeuger einer Normalbasis der Erweiterung $K/\mathbb{Q}$. Dann heißt die Matrix*

$$W_\vartheta^{(\rho)} = \left(\mathrm{Sp}_{K/\mathbb{Q}}(\vartheta^\sigma \vartheta^\varphi \vartheta^{*\rho})\right)_{\sigma,\varphi} \tag{3.4}$$

die Faltungsmatrix *von* K *zu* $\rho \in G$.

Ein Ziel dieses Kapitels soll sein, die Struktur dieser Matrizen genauer zu betrachten. Insbesondere soll der Frage nachgegangen werden, inwieweit diese Struktur durch die gegebene Normalbasis auf der einen, und auf der anderen Seite durch die, allein von dem Zahlkörper abhängigen Invarianten bestimmt ist.

Zunächst fällt auf, daß sich die Faltungsmatrizen $W_\vartheta^{(\rho)}$, wegen

$$\mathrm{Sp}_{K/\mathbb{Q}}(\vartheta^\sigma \vartheta^\varphi \vartheta^{*\rho}) = \mathrm{Sp}_{K/\mathbb{Q}}(\vartheta^{\sigma\rho^{-1}} \vartheta^{\varphi\rho^{-1}} \vartheta^*), \tag{3.5}$$

durch Zeilen- bzw. Spaltenvertauschungen ineinander überführen lassen. Das ist insofern verständlich, da sich eine Konjugation bzgl. einer Normalbasis als eine Permutation der Koeffizienten darstellt.

Mit den Bezeichnungen des vorherigen Kapitels erhalten wir desweiteren den

Satz 3.1 *Die Matrix* $W_\vartheta^{(\rho)}$ *besitzt bzgl. der* χ*-Koordinaten die Darstellung:*

$$W_\vartheta^{(\rho)} = \frac{1}{|G|} \left(\sum_\chi \frac{y(\chi|\vartheta^\sigma \vartheta^\varphi)}{y(\chi|\vartheta^\rho)} \right)_{\sigma,\varphi}. \tag{3.6}$$

Beweis: Die Gleichung (3.6) erhält man aus (3.4) mit Hilfe von (2.81), sowie unter Ausnutzung von (2.80). □

Aus obiger Darstellung ergibt sich beispielsweise für den Fall $K := \mathbb{Q}(\zeta_p)$, $p > 2$ prim, mit $\vartheta := -\zeta_p$ und unter Beachtung des Isomorphismus $G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$:

$$W_{-\zeta_p}^{(\rho)} = \Big([\sigma + \varphi \equiv 0 \bmod p] - [\sigma + \varphi \equiv \rho \bmod p] \Big)_{\sigma,\varphi}, \tag{3.7}$$

wobei die Konvention $[\texttt{TRUE}] = 1$, bzw. $[\texttt{FALSE}] = 0$ gelten soll. In diesem Fall handelt es sich also bei den Einträgen der Matrix $W_{-\zeta_p}^{(\rho)}$ um Einträge der Matrix $A_{p,-\zeta_p}$ aus dem letzten Kapitel.

Genau wie die Transformationsmatrizen der ADFT besitzen die Faltungsmatrizen, unter gewissen Voraussetzungen eine Produktzerlegungseigenschaft. Seien dazu K_1, K_2 abelsche Zahlkörper mit Normalbasen $\vartheta_1^{G_1}, \vartheta_2^{G_2}$ und Diskriminanten d_1, d_2. Gilt dann

$(d_1, d_2) = 1$, so ist offensichtlich $\vartheta := \vartheta_1\vartheta_2$ ein NBE der Erweiterung $K/\mathbb{Q}$, mit $K := K_1K_2$. Für $\rho \in G := G(K/\mathbb{Q}) \simeq G_1 \times G_2$ schreiben wir ρ_j für die Projektion auf G_j, $j = 1, 2$.

Satz 3.2 *In obiger Situation, d.h. im Falle teilerfremder Diskriminanten gilt*

$$W_\vartheta^{(\rho)} \sim W_{\vartheta_1}^{(\rho_1)} \otimes W_{\vartheta_2}^{(\rho_2)}. \tag{3.8}$$

Beweis: Für einen Charakter χ von K gilt mit Blick auf (2.71) zunächst einmal

$$y(\chi|\vartheta) = \frac{1}{f_\chi} \sum_\sigma \chi(\sigma)\vartheta^\sigma \overline{\tau(\chi)}. \tag{3.9}$$

Nach Voraussetzung ist χ von der Form $\chi = \chi_1\chi_2$, mit Charakteren χ_j von K_j. Damit ergibt sich nach (2.65)

$$\begin{aligned} y(\chi|\vartheta) &= \frac{1}{f_{\chi_1} f_{\chi_2}} \sum_{\sigma_1,\sigma_2} \chi_1(\sigma_1)\chi_2(\sigma_2)\vartheta_1^{\sigma_1}\vartheta_2^{\sigma_2}\bar\chi_1(f_{\chi_2})\bar\chi_2(f_{\chi_1})\overline{\tau(\chi_1)\tau(\chi_2)} \\ &= \bar\chi_1(f_{\chi_2})\bar\chi_2(f_{\chi_1})y(\chi_1|\vartheta_1)y(\chi_2|\vartheta_2). \end{aligned}$$

Entsprechend zeigt man

$$\begin{aligned} y(\chi|\vartheta^\sigma\vartheta^\varphi) &= \frac{1}{f_{\chi_1} f_{\chi_2}} \sum_{\rho_1,\rho_2} \chi_1(\rho_1)\chi_2(\rho_2)\vartheta_1^{\sigma_1\rho_1}\vartheta_2^{\sigma_2\rho_2}\vartheta_1^{\varphi_1\rho_1}\vartheta_2^{\varphi_2\rho_2}\bar\chi_1(f_{\chi_2})\bar\chi_2(f_{\chi_1})\overline{\tau(\chi_1)\tau(\chi_2)} \\ &= \bar\chi_1(f_{\chi_2})\bar\chi_2(f_{\chi_1})y(\chi_1|\vartheta_1^{\sigma_1}\vartheta_1^{\varphi_1})y(\chi_2|\vartheta_2^{\sigma_2}\vartheta_2^{\varphi_2}). \end{aligned}$$

Durch Einsetzen in (3.6) ergibt sich schließlich der Satz. □

Ganz analog zu Satz 2.6 beweist man auch die andere Richtung:

Satz 3.3 *Der abelsche Zahlkörper $K = K_1K_2$ mit* NBE *ϑ sei das Kompositum zweier abelscher Zahlkörper K_j mit teilerfremden Diskriminaten d_j. Genau dann ist ϑ von der Form*

$$\vartheta = \vartheta_1\vartheta_2, \tag{3.10}$$

mit ϑ_j ein NBE *der Erweiterung $K_j/\mathbb{Q}$, wenn gilt*

$$\mathrm{Sp}_{K/\mathbb{Q}}(\vartheta)\vartheta = \mathrm{Sp}_{K/K_1}(\vartheta)\mathrm{Sp}_{K/K_2}(\vartheta). \tag{3.11}$$

Bis auf rationale Konstanten sind dadurch alle Zerlegungen von ϑ gegeben.

Beweis: Es genügt sich zu vergewissern, daß unter den gegebenen Voraussetzungen bereits $K_1 \cap K_2 = \mathbb{Q}$ gilt. Die weitere Argumentation verläuft nun entsprechend der des Beweises von Satz 2.6. □

Wir wollen noch einen Schritt weitergehen und den Zusammenhang der Matrix $W_\vartheta^{(\rho)}$ mit den χ-Koordinaten $y(\chi|\vartheta)$ genauer untersuchen. Betrachten wir dazu zunächst beliebige $\alpha, \beta \in K$, mit Darstellungen $\alpha = \frac{1}{|G|}\sum_\chi y(\chi|\alpha)\tau(\chi)$ und $\beta = \frac{1}{|G|}\sum_\chi y(\chi|\beta)\tau(\chi)$. Das Produkt

$$\alpha\beta = \frac{1}{|G|^2}\sum_{\chi,\chi'} y(\chi|\alpha)y(\chi'|\beta)\tau(\chi)\tau(\chi')$$

läßt sich dann in folgender Form schreiben:

$$\alpha\beta = \frac{1}{|G|}\sum_\psi \left\{ \frac{1}{|G|}\sum_{\chi\chi'=\psi} y(\chi|\alpha)y(\chi'|\beta)\omega(\chi,\chi') \right\} \tau(\psi), \tag{3.12}$$

wobei $\omega(\chi,\chi')$, wie schon erwähnt, durch

$$\omega(\chi,\chi') := \frac{\tau(\chi)\tau(\chi')}{\tau(\chi\chi')} \tag{3.13}$$

gegeben ist. Der Ausdruck in geschweiften Klammern erfüllt dabei die Bedingungen (2.68) und (2.69), denn nach der Automorphieregel für Gaußsche Summen (2.73) folgt einerseits

$$\omega(\chi,\chi') \in \mathbb{Q}(\chi,\chi'), \quad \text{sowie} \quad \omega(\chi,\chi')^\sigma = \omega(\chi^\sigma,\chi'^\sigma), \tag{3.14}$$

für $\sigma \in G(\mathbb{Q}(\chi,\chi')/\mathbb{Q})$. Auf der anderen Seite bleibt er invariant unter Morphismen $\varphi \in G(\mathbb{Q}(\chi,\chi')/\mathbb{Q}(\chi\chi'))$ und ist damit Element des Wertekörpers $\mathbb{Q}(\chi\chi')$. Damit ist der folgende Satz bewiesen:

Satz 3.4 *Für $\alpha, \beta \in K$ ergeben sich die χ-Koordinaten des Produkts zu*

$$y(\psi|\alpha\beta) = \frac{1}{|G|}\sum_{\chi\chi'=\psi} y(\chi|\alpha)y(\chi'|\beta)\omega(\chi,\chi'), \tag{3.15}$$

für alle Charaktere ψ von K.

Man sieht deutlich, daß es sich hierbei um eine „gewichtete“ Faltung handelt. Schreiben wir noch abkürzend

$$\kappa(\chi,\chi')_\vartheta := \frac{y(\chi|\vartheta)y(\chi'|\vartheta)}{y(\chi\chi'|\vartheta)}, \tag{3.16}$$

so ergibt sich mit dieser Vorbemerkung die folgende Darstellung:

Satz 3.5 *Die Faltungsmatrix* $W_\vartheta^{(\rho)}$ *ist von der Form*

$$W_\vartheta^{(\rho)} = \frac{1}{|G|^2}\left(\sum_{\chi,\chi'} \kappa(\chi,\chi')_\vartheta \omega(\chi,\chi')\bar{\chi}(\sigma\rho^{-1})\bar{\chi}'(\varphi\rho^{-1})\right)_{\sigma,\varphi}. \tag{3.17}$$

Diese Darstellung beschreibt nun, wie das Produkt der Faktorensysteme

$$\alpha_K(\chi,\chi';\vartheta) := \kappa(\chi,\chi')_\vartheta \omega(\chi,\chi') \tag{3.18}$$

der χ-Koordinaten bzw. der Gaußschen Summen des Zahlkörpers die „Entfernung“ von der, ohne Zweifel wünschenswerten komponentenweisen Multiplikation

$$\frac{1}{|G|^2}\left(\sum_{\chi,\chi'} \bar{\chi}(\sigma\rho^{-1})\bar{\chi}'(\varphi\rho^{-1})\right)_{\sigma,\varphi} = \left(\delta_{\sigma,\rho}\delta_{\varphi,\rho}\right)_{\sigma,\varphi} \tag{3.19}$$

bestimmt. Während bei der „Wahl“ der Elemente $\kappa(\chi,\chi')_\vartheta$ noch gewisse Freiheitsgrade existieren, so wird sich spätestens im nächsten Abschnitt herausstellen, daß es sich bei der expliziten Bestimmung der $\omega(\chi,\chi')$, schon in vermeintlich „einfachen Fällen“ um einen komplexen Vorgang handelt. So wird allein schon die Frage, in welchen Fällen diese trivial sind, d. h.

$$\omega(\chi,\chi') \in \mathbb{Z}, \tag{3.20}$$

weitreichende Konsequenzen haben.

Betrachten wir zunächst aber zur Veranschaulichung einen quadratischen Zahlkörper K, sowie einen NBE $\vartheta = (1/2)(y(\chi_0|\vartheta) + y(\chi|\vartheta)\tau(\chi))$ der Erweiterung $K/\mathbb{Q}$. Nach Definition gilt dann $\omega(\chi_0,\chi) = 1$, bzw. $\omega(\chi,\chi) = \chi(-1)f_\chi$, und damit

$$W_\vartheta^{(\rho)} = \frac{y(\chi_0|\vartheta)}{4}\left\{\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + 2\chi(\rho)\begin{pmatrix} 1 & \\ & -1 \end{pmatrix} + \lambda_\vartheta \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\right\},$$

mit $\lambda_\vartheta := (y(\chi|\vartheta)/y(\chi_0|\vartheta))^2\chi(-1)f_\chi$. Unter Beachtung von $y(\chi_0|\vartheta) = \mathrm{Sp}(\vartheta)$ und einer weiteren Umformung ergibt sich schließlich

$$W_\vartheta^{(+)} = \mathrm{Sp}(\vartheta)\left\{\frac{1-\lambda_\vartheta}{4}\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} + \begin{pmatrix} 1 & \\ & \end{pmatrix}\right\}, \tag{3.21}$$

bzw.

$$W_\vartheta^{(-)} = \mathrm{Sp}(\vartheta)\left\{\frac{1-\lambda_\vartheta}{4}\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} + \begin{pmatrix} & \\ & 1 \end{pmatrix}\right\}, \tag{3.22}$$

wobei wir die Elemente der Galoisgruppe $G(K/\mathbb{Q})$ nun symbolisch mit $\{+,-\}$ bezeichnet haben. Wegen

$$(a_+, a_-)W_\vartheta^{(\pm)}(b_+, b_-)^T = \mathrm{Sp}(\vartheta)\{((1-\lambda_\vartheta)/4)(a_- - a_+)(b_+ - b_-) + a_\pm b_\pm\}$$

benötigt das resultierende Verfahren dabei drei *nicht-skalare* Multiplikationen, und ist damit in diesem Sinne optimal.

Als letztes Beispiel wollen wir uns noch den Fall eines Zwischenkörpers von $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ anschauen. Sei dazu H eine Untergruppe von $G(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, sowie K der zugehörige Fixkörper. Der Einfachheit halber wählen wir als NBE der Erweiterung $K/\mathbb{Q}$ das Element

$$\vartheta := \mathrm{Sp}_{\mathbb{Q}(\zeta_p)/K}(-\zeta_p) = \frac{1}{(K:\mathbb{Q})}\left(1 - \sum_{\chi\neq\chi_0}\tau(\chi)\right), \tag{3.23}$$

wobei die letzte Gleichheit aus (2.77) folgt.

Im Gegensatz zum letzten Beispiel, ergibt sich an dieser Stelle die Frage der $\omega(\chi,\chi')$ im nichttrivialen Fall. Einer bekannten Tatsache zufolge (vgl. [7]), stellen sich diese hier als *Jacobisummen* dar:

Satz 3.6 *Im Falle von* $f_\chi = f_{\chi'} = p$ *und* $\chi\chi' \neq \chi_0$ *gilt*

$$\omega(\chi,\chi') = \sum_{a=2}^{p-1}\chi(a)\chi'(1-a). \tag{3.24}$$

Durch Einsetzen in Gleichung (3.17) folgt dann

$$W_\vartheta^{(\rho)} = \frac{1}{|G|^2}\left(W_1 - W_2\right),$$

wobei die Matrizen W_i durch

$$W_1 = \Big(|G|[\sigma=\rho] + |G|[\varphi=\rho] + p|G|[\sigma\equiv-\varphi \bmod H] - (p-1) - 2\Big)_{\sigma,\varphi},$$

bzw. durch

$$W_2 = \left(\sum_{a=2}^{p-1} \sum_{(\chi,\chi') \in T} \chi(a)\chi'(1-a)\bar{\chi}(\sigma\rho^{-1})\bar{\chi}'(\varphi\rho^{-1}) \right)_{\sigma,\varphi}$$

gegeben sind. Die Menge T besteht dabei aus den, im Sinne von Satz 3.6, nichttrivalen Tupeln, also $T := \{(\chi,\chi') | \chi, \chi', \chi\chi' \neq \chi_0\}$. Indem wir die fehlenden Glieder hinzufügen, kommen wir zu der Darstellung $W_2 = W_3 - W_4$, wobei die Matrix

$$W_4 = -\Big(|G|[\sigma = \rho] + |G|[\varphi = \rho] + |G|[\sigma \equiv -\varphi \bmod H] - p - 1 \Big)_{\sigma,\varphi}$$

die trivialen Terme sammelt, und W_3 durch

$$W_3 = \left(\sum_{a=2}^{p-1} \left(\sum_{\chi} \chi(a)\bar{\chi}(\sigma\rho^{-1}) \right) \left(\sum_{\chi'} \chi'(1-a)\bar{\chi}'(\varphi\rho^{-1}) \right) \right)_{\sigma,\varphi}$$

beschrieben ist. Nach einer weiteren Umformung und Zusammenfassung der einzelnen Komponenten ergibt sich schließlich der

Satz 3.7 *Sei* H *eine Untergruppe von* $G(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, K *der zugehörige Fixkörper und* ϑ *wie in* (3.23) *ein* NBE *der Erweiterung* $K/\mathbb{Q}$. *Dann beschreibt*

$$W_\vartheta^{(\rho)} = \left(|H|[\sigma \equiv -\varphi \bmod H] - \sum_{h,h' \in H} [\sigma h + \varphi h' \equiv \rho \bmod p] \right)_{\sigma,\varphi} \tag{3.25}$$

die Faltungsmatrix von K.

Bei den, von ρ abhängenden Summanden der Einträge von $W_\vartheta^{(\rho)}$, handelt es sich um sog. *Kreisteilungszahlen*. Allgemein ist für eine Primzahl $p = kf + 1$ mit Primitivwurzel g und ganze Zahlen s und t die Kreisteilungszahl

$$(s,t)_k \tag{3.26}$$

der Ordnung k definiert als die Anzahl der Zahlen $n \pmod p$, für welche die Werte n/g^s und $(n+1)/g^t$ von Null verschiedene k-te Potenzreste darstellen.

Entsprechend (vgl. [7]) ist die Anzahl der Lösungen $0 \leqslant u_1, u_2 < f$ der Kongruenz

$$1 + g^{ku_1+s} + g^{ku_2+t} \equiv 0 \bmod p \tag{3.27}$$

durch die Zahl

$$(s,t+(1/2)kf)_k = \begin{cases} (s,t)_k, & f \equiv 0 \bmod 2 \\ (s,t+(1/2)k)_k, & f \not\equiv 0 \bmod 2 \end{cases} \tag{3.28}$$

gegeben. Mit dieser Vorbemerkung und aufgrund der leicht einzusehenden Tatsache $(s,t)_k = (-s,t-s)_k$ erhalten wir das

Korollar 3.1 *In der gegebenen Situation sind die* $k := |G(K/\mathbb{Q})|$ *Faltungsmatrizen von* K*, im Falle von* $|H| \equiv 0 \bmod 2$ *zu den Matrizen*

$$|H|E_k - \Big((s-r,t-r)_k\Big)_{s,t}, \tag{3.29}$$

sowie im Falle von $|H| \not\equiv 0 \bmod 2$*, zu den Matrizen*

$$|H|E_k - \Big((t-s,s-r)_k\Big)_{s,t}, \tag{3.30}$$

mit $r,s,t = 0,\ldots,k-1$*, äquivalent.*

Das Studium der Faltungsmatrizen „reduziert“ sich damit in diesem Beispiel auf die Untersuchung der sog. *Kreisteilungsmatrizen* $((s,t)_k)_{s,t}$. Für kleine Ordnungen finden sich diese etwa in [7].

3.2 Mirimanoffpolynome

Das letzte Beispiel gibt schon einen Hinweis auf den Zusammenhang zwischen der Arithmetik einer abelschen Erweiterung $K/\mathbb{Q}$ auf der einen, und dem Faktorensystem Gaußscher Summen auf der anderen Seite. Um eine Vorstellung von den $\omega(\chi,\chi')$ im allgemeinen Fall zu erhalten, verschaffen wir uns zunächst einen Überblick über die Werte der Gaußschen Summen.

Die Summen mit höheren Führern sind, im Gegensatz zu dem Fall $f_\chi = p$ (vgl. [7] Th. 1.6.1), immer von der Form „$\sqrt{f_\chi}$ mal Einheitswurzel“. Genauer gilt (vgl. [7] Th. 1.6.2):

Satz 3.8 *Sei* p *eine ungerade Primzahl,* $2 \leqslant r \in \mathbb{N}$ *und* $k := p^r$. *Desweiteren sei* χ *ein primitiver Charakter (mod* k*), mit* $\chi(1+p) = \zeta_{k/p}^{-1}$. *Dann gilt für die korrespondierende Gaußsche Summe*

$$\tau(\chi) = \begin{cases} \sqrt{k}\zeta_k, & \text{falls } r = 2 \\ \sqrt{k}\zeta_k i^{(1-p)/2}\zeta_p^{(p^2-1)/8}, & \text{falls } r = 3 \\ \sqrt{k}\zeta_k^{\lambda}, & \text{für gerade } r > 3 \\ \sqrt{k}\zeta_k^{\lambda} i^{(1-p)/2}, & \text{für ungerade } r > 3 \end{cases}, \tag{3.31}$$

mit einer ganzen p*-adischen Zahl*

$$\lambda := \frac{p}{\log(1+p)}\left(1 - \log\left(\frac{p}{\log(1+p)}\right)\right), \tag{3.32}$$

wobei es sich bei der Funktion log *um den* p*-adischen Logarithmus handelt.*

Auf eine Darstellung der p-adischen Analysis können wir an dieser Stelle verzichten; wir werden sie im Folgenden nicht brauchen. Desweitern sei bemerkt, daß ein äquivalenter Satz auch für Zweierpotenzen existiert, vgl. dazu [7], Th. 1.6.3.

Nach (2.73) und der Produktformel (2.65) sind durch diesen Satz alle Werte $\omega(\chi, \chi')$, zumindest für Charaktere mit ungeradem Führer vollständig beschrieben. Wir betrachten nun den Fall der reellen Erweiterung $K/\mathbb{Q}$ vom Grad $p > 2$, deren Diskriminante ausschließlich durch p teilbar ist[1]. Diese ergibt sich beispielsweise als Teilerweiterung von $\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}$, durch $K := \mathbb{Q}(\Gamma)$, mit

$$\Gamma := \mathrm{Sp}_{\mathbb{Q}(\zeta_{p^2})/K}(\zeta_{p^2}). \tag{3.33}$$

Die nichttrivialen Charaktere von K haben demnach alle den Führer p^2 und sind zudem gerade. Wir wählen einen festen Erzeuger χ der Charaktergruppe von K, welcher wie in Satz 3.8, durch $\chi(1-p) = \zeta_p$ normiert sein soll. Für $k, l \in \mathbb{Z}$, mit $k, l, k+l \not\equiv 0 \bmod p$, folgt dann

$$\omega(\chi^k, \chi^l) = p\frac{\chi^k(k)\chi^l(l)}{\chi^{k+l}(k+l)}. \tag{3.34}$$

Um für eine ganze Zahl $k \not\equiv 0 \bmod p$ den Wert von $\chi(k)$ zu bestimmen, definieren wir den *Fermatquotient* $q_p(k)$ als die kleinste positive ganze Zahl, welche der Gleichung

$$k^{p-1} \equiv 1 + q_p(k)p \bmod p^2 \tag{3.35}$$

[1] In dieser Erweiterung ist also p die einzige endliche (rein-)verzweigte Stelle.

genügt. Aufgrund der Normierung von χ ergibt sich damit

$$\chi(k) = \zeta_p^{q_p(k)}. \tag{3.36}$$

Desweiteren läßt sich an dieser Gleichung ablesen, daß sich die Funktion $q_p(\cdot)$ modulo p wie eine Logarithmusfunktion verhält:

$$q_p(ab) \equiv q_p(a) + q_p(b) \bmod p. \tag{3.37}$$

Um auf Gleichung (3.34) zurückzukommen, so ergibt sich, nach Auswertung des Charakters χ gemäß (3.36), nunmehr der

Satz 3.9 *Mit den vereinbarten Bezeichnungen gilt, für* $k, l, k+l \not\equiv 0 \bmod p$*,*

$$\omega(\chi^k, \chi^l) = p\zeta_p^{-(k+l)\gamma_p(\frac{k}{k+l})}, \tag{3.38}$$

wobei es sich bei dem Polynom

$$\gamma_p(t) := \sum_{j=1}^{p-1} \frac{1}{j} t^j \in \mathbb{F}_p[t] \tag{3.39}$$

um das $(p-1)$-ste Mirimanoffpolynom *handelt.*

Beweis: Unter Beachtung der Kongruenz

$$\frac{1}{p}\binom{p}{s} \equiv \frac{(-1)^{s+1}}{s} \bmod p, \tag{3.40}$$

für $s = 1, \ldots, p-1$, folgt zunächst

$$\gamma_p(t) \equiv \frac{1 - t^p - (1-t)^p}{p} \equiv (t-1)q_p(t-1) - tq_p(t) \bmod p \tag{3.41}$$

und damit, unter Zuhilfenahme von (3.37), der Satz. □

Die Aussage des letzten Satzes macht ein Studium der Werte, und insbesondere der Nullstellen besagter Polynome, resp. der Fermatquotienten unumgänglich. Vom Standpunkt der Zahlentheorie aus handelt es sich jedoch um „alte Bekannte“, mit z. T. kurios anmutenden arithmetischen Eigenschaften. So existiert beispielsweise eine Beziehung zu der, kürzlich von P. Mihăilescu bewiesenen *Catalanschen Vermutung*, Abhängigkeiten zur Teilbarkeit der Klassenzahl bestimmter Zahlkörper, Beziehungen

zu den *Bernoullizahlen*, und damit zur *Riemannschen Zetafunktion* – um nur einige zu nennen.

Der Fermatquotient hat im Jahr 1909 durch das sog. *Wieferichkriterium* eine gewisse Berühmtheit erlangt; es besagt, daß für eine ungerade Primzahl p und ganze Zahlen x, y, z, mit $p \nmid xyz$, welche die Gleichung

$$x^p + y^p + z^p = 0 \tag{3.42}$$

erfüllen, stets gilt

$$2^{p-1} \equiv 1 \bmod p^2. \tag{3.43}$$

Anders ausgedrückt, in diesem Fall ist also $q_p(2) = 0$.

Bis zum heutigen Tag sind nur zwei Primzahlen bekannt, welche der Bedingung (3.43) genügen: die Zahl 1093, gefunden von W. Meissner im Jahr 1913, sowie 3511, endeckt im Jahr 1921/22 durch N. Beeger (vgl. [69]).

Ein Jahr nach Wieferich konnte Mirimanoff bereits zeigen, daß, im Falle der Gültigkeit von Gleichung (3.42), auch

$$3^{p-1} \equiv 1 \bmod p^2 \tag{3.44}$$

gelten muß. Es folgte eine Reihe von Arbeiten (vgl. [69]), deren gemeinsames Ergebnis das folgende Kriterium beinhaltet: falls die oben definierten Zahlen p, x, y, z die Bedingungen $p \nmid xyz$ und (3.42) erfüllen, so gilt für alle natürliche $l \leqslant 113$ auch $q_p(l) = 0$.

Obwohl *Fermats Letzter Satz*, wie er oft genannt wird, inzwischen als bewiesen gilt, ist bis zum jetzigen Zeitpunkt nicht bekannt, ob eine ungerade Primzahl p existiert, welche der Bedingung

$$q_p(2) = q_p(3) = 0 \tag{3.45}$$

genügt. Allgemeiner formuliert stellt sich hier also die Frage nach einer oberen Schranke für die Zahl

$$\kappa_p := \min\{q \in \mathbb{N} \mid q_p(q) \neq 0\}. \tag{3.46}$$

Aufgrund von (3.37) folgt, daß es sich bei κ_p um eine Primzahl handelt, welche trivialerweise durch $\kappa_p < p$ beschränkt ist.

Art und Anzahl der Werte des Polynoms $\gamma_p(t)$, und insbesondere die Nullstellen werden schon seit längerer Zeit, nicht zuletzt wegen des offensichtlichen Zusammenhangs mit Fermats Letztem Satz, genauer untersucht; um nur ein Beispiel aus diesem Bereich

zu nennen: Mirimanoff konnte zeigen, daß im Falle der Gültigkeit der Gleichung (3.42), wie immer unter der Nebenbedingung $p \nmid xyz$, für $s := y/(x+y) \equiv -y/z \bmod p$ auch

$$\gamma_p(s) \equiv 0 \bmod p \tag{3.47}$$

gelten muß (vgl. [69]). Ebenso läßt sich, wie leicht an (3.41) abzulesen ist, die oben definierte Zahl κ_p wie folgt charakterisieren:

$$\kappa_p = \min\{q \in \mathbb{N} \,|\, \gamma_p(q) \not\equiv 0 \bmod p\}. \tag{3.48}$$

Da nun jede Nullstelle z, $z \not\equiv 0, 1 \bmod p$, von $\gamma_p(t)$ auch Nullstelle der Ableitung $\gamma'_p(t) = 1 + t + \ldots + t^{p-2}$ ist, also stets eine doppelte Nullstelle darstellt, ergibt sich, aufgrund der Charakterisierung (3.48), bereits die Abschätzung

$$\kappa_p \leqslant \frac{p+1}{2}. \tag{3.49}$$

Die Anwendungen derlei Untersuchungen sind jedoch keineswegs auf rein zahlentheoretische Fragestellungen beschränkt. So basiert beispielsweise der erste deterministische polynomiale Algorithmus zur Primzahlerkennung (vgl. [3]) auf einer Variante des Kriteriums: n ist prim, gdw.

$$1 - t^n \equiv (1-t)^n \bmod n; \tag{3.50}$$

das ist aber gerade, mit Blick auf (3.41) die, das Mirimanoffpolynom definierende Gleichung.

Diese letzte Gleichung besagt außerdem, daß sich der Wert des Polynoms $\gamma_p(t)$ an jeder beliebigen Stelle *effizient* berechnen läßt, oder in Zeichen der Komplexitätstheorie ausgdrückt, daß für die Menge $W_\gamma := \{(p, \gamma_p(a_p)) \,|\, p > 2, p \text{ prim}, a_p \in \mathbb{F}_p\}$ gilt

$$W_\gamma \in \mathrm{NP}. \tag{3.51}$$

Die Menge des Wertebereichs ist also nichtdeterministisch-polynomial entscheidbar. Die Frage nach der Umkehrung dieser Aussage ist zum jetzigen Zeitpunkt noch völlig offen:

$$W_\gamma \in \mathrm{co-NP}\ ? \tag{3.52}$$

Tatsächlich liegt die Vermutung „nahe“, daß es sich bei dem Polynom $\gamma_p(t)$ um eine Art „Einwegfunktion“ handeln könnte.

Als letztes Beispiel für eine mögliche Anwendung in der Kryptographie betrachten

wir den Zusammenhang des Mirimanoffpolynoms mit dem *Diskreten Logarithmus Problem* in der Einheitengruppe des endlichen Körpers $\mathbb{F}_p$. Für einen Erzeuger ω von $\mathbb{F}_p^\times$ und ein beliebiges Element α dieser Gruppe schreiben wir

$$\mathrm{dLog}_\omega(\alpha) := \min\{k \in \mathbb{N}_0 \,|\, \omega^k = \alpha\} \tag{3.53}$$

für den diskreten Logarithmus von α zur Basis ω. Dann läßt sich zeigen, daß gilt

$$\sum_{k=1}^{p-2} \gamma_p(\omega^k)\alpha^k \equiv (\mathrm{dLog}_\omega(\alpha)+1)^{-1} \bmod p. \tag{3.54}$$

Wir beginnen nun mit der Untersuchung der Nullstellen des Polynoms $\gamma_p(t)$. Dazu notieren wir zunächst die zwei folgenden elementaren Eigenschaften, welche sich leicht an der Darstellung (3.41) ablesen lassen:

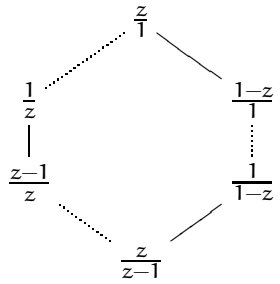
$$\gamma_p(a) \equiv \gamma_p(1-a) \bmod p, \tag{3.55}$$

sowie, für $a \not\equiv 0 \bmod p$,

$$\gamma_p(a) \equiv -a\gamma_p(\frac{1}{a}) \bmod p. \tag{3.56}$$

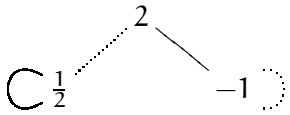
Für die nichttrivialen Nullstellen z von $\gamma_p(t)$, also $z \not\equiv 0, 1 \bmod p$, bedeutet das, ihre Existenz vorausgesetzt, daß diese, abgesehen von zwei Ausnahmefällen stets in „Sechsergruppen“ auftreten:

(3.57)

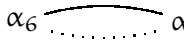


Die Ausnahmen bestehen, im Falle von $\gamma_p(2) \equiv 0 \bmod p$, aus der „Dreiergruppe“

(3.58)



sowie, im Falle von $p \equiv 1 \bmod 3$, aus den Nullstellen α_6, α_6^5, des Polynoms $t^2-t+1 \in \mathbb{F}_p[t]$:



(3.59)

Desweiteren läßt sich leicht nachprüfen, daß ein „Vierer“ unter den gegebenen Voraussetzungen nicht existeren kann.

An der Eigenschaft (3.55) kann man, in Verbindung mit der bisherigen Abschätzung (3.49) zudem ablesen, daß höchstens die Hälfte der Nullstellen von $\gamma_p(t)$ zu einer oberen Schranke von κ_p beitragen. Wir können diese damit noch einmal verbessern:

$$\kappa_p \leqslant \left\lfloor \frac{p+5}{4} \right\rfloor . \tag{3.60}$$

3.3 Relationen für γ_p

Das Polynom $\gamma_p(t)$ erfüllt eine Reihe bemerkenswerter Relationen. Um nur ein Beispiel zu nennen: Aus

$$\gamma_p(a) \equiv \gamma_p(a+1) \equiv 0 \bmod p \tag{3.61}$$

folgt stets auch

$$\gamma_p(a^2) \equiv 0 \bmod p. \tag{3.62}$$

Derlei Relationen resultieren meist aus dem direkten Zusammenhang mit dem Faktorensytem der Gaußschen Summen und damit aus dem folgenden Satz:

Satz 3.10 *Für* $a, b \not\equiv 0, 1 \bmod p$*, sowie* $ab \not\equiv 1 \bmod p$*, gilt*

$$(1-ab)\gamma_p(\frac{1-b}{1-ab}) + (1-b)\gamma_p(a) \equiv (1-ab)\gamma_p(\frac{1-a}{1-ab}) + (1-a)\gamma_p(b). \tag{3.63}$$

Beweis: Zunächst stellen wir fest, daß mit obigen Bezeichnungen, für beliebige Charaktere χ, χ', χ'' stets

$$\omega(\chi, \chi'\chi'')\omega(\chi', \chi'') = \omega(\chi\chi', \chi'')\omega(\chi, \chi') \tag{3.64}$$

gilt. Dies läßt sich direkt an der Definition der $\omega(\chi, \chi')$ ablesen. Nach Anwendung von Satz 3.9 ergibt sich damit, für k, l, j, mit $k, l, j, k+l, l+j, k+l+j \not\equiv 0 \bmod p$,

$$(k+l+j)\gamma_p(\frac{k}{k+l+j}) + (l+j)\gamma_p(\frac{l}{l+j}) \equiv (k+l+j)\gamma_p(\frac{k+l}{k+l+j}) + (k+l)\gamma_p(\frac{k}{k+l}).$$

Nach Durchführung der Substitutionen $1-a := l/(l+j)$ und $b := k/(k+l)$, sowie elementarer Umformungen folgt, unter Beachtung der obigen Nebenbedingung, schließlich die Aussage. □

Der letzte Satz gestattet also durch Vorgabe bestimmter Nullstellen des Polynoms, neue zu „produzieren“. Die Aussage des anfangs betrachteten Beispiels ergibt sich etwa durch Einsetzen von a und $b := 1/(a+1)$ in Gleichung (3.63).

Ein für unsere Fragestellung ganz wesentlicher Satz ist nun der folgende.

Satz 3.11 *Für* $1 \leqslant u, v < \kappa_p$ *gilt*

$$\gamma_p(\frac{u}{v}) \equiv 0 \bmod p. \tag{3.65}$$

Beweis: Nach Division von (3.63) durch $(1-a)(1-b)$ und anschließender Substitution $e := 1/(1-a)$, sowie $d := 1/(1-b)$, ergibt sich zunächst, für $e, d \not\equiv 0, 1 \bmod p$ und $e + d \not\equiv 1 \bmod p$, die Relation

$$(e+d-1)\left(\gamma_p(\frac{d-1}{e+d-1}) - \gamma_p(\frac{d}{e+d-1})\right) \equiv \gamma_p(e) - \gamma_p(d). \tag{3.66}$$

Die Aussage des Satzes folgt nun induktiv, unter Beachtung von (3.55), (3.56), sowie der bisherigen Abschätzung (3.60). □

Wir erhalten unmittelbar eine signifikante Verbesserung der bisherigen oberen Schranke von κ_p. Bezeichne dazu, für $0 \leqslant a < p$,

$$\eta_{a,p} := |\{c \mid 0 \leqslant c < p, \gamma_p(c) \equiv a \bmod p\}| \tag{3.67}$$

die entsprechende Anzahlfunktion des Polynoms $\gamma_p(t)$, so gilt der

Satz 3.12 *Mit obigen Bezeichnungen ist*

$$\kappa_p \in O(\sqrt{\eta_{0,p}}) \tag{3.68}$$

Beweis: Die Schranke folgt mit Hilfe von Satz 3.11, sowie der Tatsache, daß für natürliches q und

$$s_q := |\{(u,v) \mid 1 \leqslant u, v \leqslant q, \mathrm{ggT}(u,v) = 1\}|$$

stets gilt

$$s_q \geqslant \sum_{k=1}^{q} q - q\left(\sum_{l \mid k} \frac{1}{l}\right) \geqslant q^2\left(1 - \sum_{l \leqslant q} \frac{1}{l^2}\right) \geqslant q^2\left(2 - \frac{\pi^2}{6}\right).$$

Wir behaupten nun, daß für genügend großes p gilt:

$$\kappa_p \leqslant \lfloor\sqrt{p}\rfloor.$$

Angenommen das wäre falsch, so hätten wir zunächst mehr als

$$(\lfloor\sqrt{p}\rfloor)^2\left(2-\frac{\pi^2}{6}\right) > \frac{p}{3}$$

Nullstellen von der Form a/b, mit $(a,b)=1$ und $1 \leqslant a,b \leqslant \lfloor\sqrt{p}\rfloor$. Nun ist mit a/b aber auch $1-a/b$ eine Nullstellen von γ_p. Das folgende Lemma zeigt, daß noch einmal knapp die Hälfte dieser Nullstellen dazukommt:

Lemma 1 *Für p prim und Zahlen a,b, mit $1 \leqslant a,b \leqslant \lfloor\sqrt{p}\rfloor$ und $a > b$, existieren <u>keine</u> Zahlen c,d, mit $1 \leqslant c,d \leqslant \lfloor\sqrt{p}\rfloor$, sodaß gilt:*

$$1-\frac{a}{b} \equiv \frac{c}{d} \bmod p.$$

Mit Hilfe dieses Lemmas haben wir also für genügend großes p und unter der Annahme $\kappa_p > \lfloor\sqrt{p}\rfloor$ mindestens

$$\left\lceil\frac{p}{3}\right\rceil + \left\lceil\frac{1}{2}\left(\left\lceil\frac{p}{3}\right\rceil - 1\right)\right\rceil = \frac{p+1}{2}$$

Nullstellen von γ_p produziert, was aber, da wir die 0 nicht mitzählen und jede Nullstelle (außer der 1) doppelt vorkommt, nicht sein kann. Daher gilt also $\kappa_p \leqslant \lfloor\sqrt{p}\rfloor$ und somit existieren $\Omega(\kappa_p^2)$ viele Nullstellen von γ_p.

Beweis des Lemmas: Aus der Gleichung

$$bd - ad \equiv bc \bmod p$$

folgt zunächt, wegen $a > b$ die Existenz eines $k > 0$, sodaß gilt

$$bd - ad + kp = bc.$$

Desweiteren teilt b die Zahl $kp - ad$, also etwa $kp - ad = sb$ mit $s > 0$ und damit insbesondere $d + s = c$, d. h. es gilt $c > d$, sowie

$$1 \leqslant s \leqslant \lfloor\sqrt{p}\rfloor.$$

Aus der letzten Ungleichung folgt unter den Voraussetzungen des Lemmas:

$$kp = sb + ad < 2p,$$

also $k = 1$, und damit $bd - ad + p = bc$, bzw. $d = (p-bc)/(a-b)$. Wegen $c > d$ ergibt sich daraus aber $ac > p$, was im Widerspruch zu den Voraussetzungen steht. □

3.4 Explizite Formeln

Bei Satz 3.12 handelt es sich wohl um die derzeit stärkste obere Schranke von κ_p. Ein genaueres Bild verspricht die weitere Untersuchung der Anzahlfunktion $\eta_{a,p}$ des letzten Abschnitts. Zu diesem Zweck kehren wir zu den anfangs definierten Matrizen $W_\vartheta^{(\rho)}$ zurück und betrachten diese für den Körper $K := \mathbb{Q}(\Gamma)$, wobei Γ wie in (3.33) definiert ist.

Als Normalbasis der Erweiterung $K/\mathbb{Q}$ wählen wir das Element

$$\vartheta := \frac{1-\Gamma}{p} = \frac{1}{p}\left(1 - \frac{1}{p}\sum_{\chi\neq\chi_0}\tau(\chi)\right). \tag{3.69}$$

Die letzte Gleichung folgt aus (2.77); desweiteren erkennt man an (2.80), daß es sich bei der so definierten Basis $\vartheta^{G(K/\mathbb{Q})}$ um eine selbstduale Basis handelt.

Zur Berechnung von $W_\vartheta^{(\rho)}$ teilen wir diese wieder in zwei Teile:

$$W_\vartheta^{(\rho)} = \frac{1}{p^2}\left(W_1 + W_2\right),$$

wobei die Matrix W_1 durch

$$W_1 = \left(p[\sigma=\rho] + p[\varphi=\rho] + p[\sigma=\varphi] - 2\right)_{\sigma,\varphi} \tag{3.70}$$

beschrieben ist, sowie

$$W_2 = \left(\sum_{(\chi,\chi')\in T}\kappa(\chi,\chi')_\vartheta\omega(\chi,\chi')\bar{\chi}(\sigma\rho^{-1})\bar{\chi}'(\varphi\rho^{-1})\right)_{\sigma,\varphi},$$

mit $T := \{(\chi,\chi')|\chi,\chi',\chi\chi' \neq \chi_0\}$. Wir wählen einen festen Erzeuger χ der Charaktergruppe von K, welcher wieder durch $\chi(1-p) = \zeta_p$ normiert sein soll. Für $\sigma \in G(K/\mathbb{Q})$ definieren wir die ganze Zahl σ' via $\chi(\sigma) = \chi(1-\sigma'p) = \zeta_p^{\sigma'}$. Mit Hilfe von Satz 3.9, sowie einer einmaligen Anwendung von (3.56), ergibt sich dann

$$W_2 = -\sum_{j=1}^{p-2}\left(\sum_{k=1}^{p-1}\zeta_p^{k(\gamma_p(1+j)-(\sigma'-\rho')-j(\varphi'-\rho'))}\right)_{\sigma,\varphi}.$$

Da es sich bei der inneren Summe um eine Spur handelt, folgt schließlich

$$W_2 = \left(p - 2 - p\sum_{j=1}^{p-2}[\gamma_p(1+j) \equiv (\sigma'-\rho') + j(\varphi'-\rho') \bmod p]\right)_{\sigma,\varphi}. \tag{3.71}$$

Bedingt durch diese Vorbemerkung, ergibt sich nun die folgende explizite Formel für die Anzahl der Nullstellen von $\gamma_p(t)$:

Satz 3.13 *Es gilt*

$$\eta_{0,p} = 2 + \frac{1}{p}\left(\frac{\mathrm{Sp}_{K/\mathbb{Q}}(\Gamma^3)}{p} + p - 2\right). \tag{3.72}$$

Beweis: Wie an (3.71) zu erkennen ist „zählt“ der Eintrag der Matrix $W_\vartheta^{(\mathrm{id})}$, bis auf Konstanten, an der Stelle $(\sigma = \mathrm{id}, \varphi = \mathrm{id})$ die nichttrivialen Nullstellen des Polynoms $\gamma_p(t)$. Diesen Eintrag erhält man aber, wegen $\vartheta^* = \vartheta$, durch den Ausdruck $\mathrm{Sp}(\vartheta^3)$, vgl. (3.4). Wegen $\mathrm{Sp}(\Gamma) = 0$, sowie

$$\mathrm{Sp}_{K/\mathbb{Q}}(\Gamma^2) = p(p-1), \tag{3.73}$$

wie leicht an (2.81) zu erkennen ist, folgt schließlich der Satz. □

Mit der gleichen Technik zeigt man auch die folgenden Gleichung:

Satz 3.14 *Für* $\sigma \neq \mathrm{id}$ *ist*

$$\eta_{\sigma',p} = \frac{1}{p}\left(\frac{\mathrm{Sp}_{K/\mathbb{Q}}(\Gamma^\sigma\Gamma^2)}{p} + p - 2\right). \tag{3.74}$$

Beweis: Hier zählt der Eintrag der Matrix $W_\vartheta^{(\mathrm{id})}$ an der Stelle (σ, id), bis auf Konstanten, die Anzahl der a, mit $\gamma_p(a) \equiv \sigma' \bmod p$. Dieser Eintrag ist aber, mit der gleichen Argumentation wie oben, durch den Ausdruck $\mathrm{Sp}(\vartheta^\sigma\vartheta^2)$ beschrieben. Unter zusätzlicher Beachtung von

$$\mathrm{Sp}(\Gamma^\sigma\Gamma) = -p, \tag{3.75}$$

für $\sigma \neq \mathrm{id}$, ergibt sich damit die Aussage des Satzes. □

Auch das „4. Moment“ $\mathrm{Sp}(\Gamma^4)$ birgt Informationen über $\gamma_p(t)$. Sei dazu

$$\nu_p := |\{(a,b) \mid 1 < a, b < p,\ \gamma_p(a) \equiv \gamma_p(b) \bmod p\}|, \tag{3.76}$$

so gilt für diesen Wert der

Satz 3.15 *Die oben definierte Anzahl* ν_p *erfüllt*

$$\nu_p = \frac{1}{p}\left(\frac{\mathrm{Sp}_{K/\mathbb{Q}}(\Gamma^4)}{p} - 2p + 3\right). \tag{3.77}$$

Beweis: Zunächst gilt für $\psi \neq \chi_0$, wegen (3.15) und Satz 3.9

$$y_K(\psi|\Gamma^2) = \sum_{j=2}^{p-1} \zeta_p^{-\psi'\gamma_p(j)}, \tag{3.78}$$

wobei die Zahl ψ' via $\psi(1-p) = \zeta_p^{\psi'}$ definiert ist, und damit, vgl. (2.81),

$$\begin{aligned}\mathrm{Sp}_{K/\mathbb{Q}}(\Gamma^4) &= \frac{1}{p}\sum_{\chi} y_K(\chi|\Gamma^2)y_K(\bar{\chi}|\Gamma^2)\chi(-1)f_\chi \\ &= p((p-1)^2 - (p-2)^2) + p^2\nu_p,\end{aligned}$$

wegen $y(\chi_0|\Gamma^2) = \mathrm{Sp}(\Gamma^2) = p(p-1)$. □

Dieses „Spiel“ läßt sich natürlich fortsetzen. Wir betrachten ein letztes Beispiel zu diesem Thema. Sei dazu

$$\nu'_p := |\{(a,b,c) \mid 1 < a,b,c < p,\ \gamma_p(a) + a\gamma_p(b) \equiv \gamma_p(c) \bmod p\}|. \tag{3.79}$$

Wie oben folgt dann zunächst, für $\psi \neq \chi_0$,

$$y_K(\psi|\Gamma^3) = p - 1 + \sum_{r,s=2}^{p-1} \zeta_p^{-\psi'(r\gamma_p(s)+\gamma_p(r))} \tag{3.80}$$

und damit

$$\mathrm{Sp}_{K/\mathbb{Q}}(\Gamma^5) = -p^4 + 2\eta_{0,p}p^3 + (\nu'_p - 2(\eta_{0,p}+1))p^2 + 4p. \tag{3.81}$$

Aus dieserart Relationen ergeben sich nützliche Kongruenzen, wie beispielsweise, wegen $\mathrm{Sp}(\Gamma^5) \equiv \mathrm{Sp}(\Gamma) \equiv 0 \bmod 5$,

$$-p^4 + 2\eta_{0,p}p^3 + (\nu'_p - 2(\eta_{0,p}+1))p^2 + 4p \equiv 0 \bmod 5, \tag{3.82}$$

und daraus, im Falle von $p \equiv 1 \bmod 5$, das kuriose

$$\nu'_p + 1 \equiv 0 \bmod 5. \tag{3.83}$$

3.5 Mirimanoffpolynome und Quantenalgorithmen

Bei näherer Betrachtung der zuletzt beschriebenen Relationen, fällt der Zusammenhang zwischen der Anzahl der Nullstellen $\eta_{0,p}$, des Polynoms $\gamma_p(t)$, und des Maximums

$$\Gamma_{max,p} := \max_{\sigma}\{|\Gamma^{\sigma}|\}, \tag{3.84}$$

der Konjugierten von Γ ins Auge. So gilt etwa wegen

$$\eta_{0,p}^2 \ll \nu_p \ll \frac{\Gamma_{max,p}^4}{p} \ll \Gamma_{max,p}^3, \tag{3.85}$$

was leicht an der Definition von ν_p und dem anschließenden Satz 3.15 abzulesen ist, schon die Abschätzung

$$\eta_{0,p} \in O(\Gamma_{max,p}^{3/2}). \tag{3.86}$$

Entsprechend ergibt sich, wegen $\Gamma_{max,p} \gg \sqrt{p}$, aus der Definition der Zahl ν'_p sowie der darauffolgenden Spurgleichung (3.81):

$$\eta_{0,p}^3 \ll \nu'_p \ll \frac{\Gamma_{max,p}^5}{p} \ll \Gamma_{max,p}^4, \tag{3.87}$$

und damit bereits

$$\eta_{0,p} \in O(\Gamma_{max,p}^{4/3}). \tag{3.88}$$

Durch die konsequente Fortführung dieser Argumentationskette gelangt man schließlich zu der Abschätzung

$$\eta_{0,p} \in \Gamma_{max,p}^{1+o(1)}. \tag{3.89}$$

Tatsächlich gilt stärker:

Satz 3.16 *Für die Anzahl der Nullstellen des Polynoms $\gamma_p(t)$ gilt die obere Schranke:*

$$\eta_{0,p} \in O(\Gamma_{max,p}). \tag{3.90}$$

Beweis: Der Satz ist eine direkte Folgerung aus Satz 3.13 in Verbindung mit Theorem 15 aus [48]. Der Autor bestimmt dort das Maximum der Funktion

$$f(x_1, \ldots, x_k) := \sum_{i=1}^{k} x_i^3,$$

unter gewissen Nebenbedingungen, und erhält daraus

$$\frac{1}{p^2}\mathrm{Sp}_{K/\mathbb{Q}}(\Gamma^3) < \Gamma_{\max,p}.$$

Mit Blick auf Satz 3.13 folgt damit die Abschätzung für $\eta_{0,p}$. □

Für das Maximum der Konjugierten von Γ haben wir nun:

$$\sqrt{p-1} < \Gamma_{\max,p} < p-1. \tag{3.91}$$

Beide Schranken folgen aus den Gleichungen $\mathrm{Sp}(\Gamma^2) = p(p-1)$, bzw. $\mathrm{Sp}(\Gamma) = 0$. Jede Bewegung in Richtung der unteren Schranke würde, wegen $\kappa_p^2 \ll \eta_{0,p} \ll \Gamma_{\max,p}$, eine unmittelbare Verbesserung der Abschätzung von κ_p bedeuten.

Obwohl numerische Experimente darauf hindeuten, konnte bisher *kein* Satz der Form:

$$\Gamma_{\max,p} \notin \Omega(p) \tag{3.92}$$

gezeigt werden. Wir werden nun ein Argument betrachten, welches „wahrscheinlich“ für die Gültigkeit von (3.92) spricht.

Da im Folgenden das „p“ variieren wird, schreiben wir von nun an Γ_p statt Γ. Desweiteren bezeichne, wie weiter oben schon geschehen, die Zahl σ' die kleinste, nichtnegative ganze Zahl, welche für $\sigma \in G(\mathbb{Q}(\Gamma_p)/\mathbb{Q}))$ und den via $\chi(1-p) = \zeta_p$ normierten Charakter χ durch $\chi(\sigma) = \chi(1-\sigma' p) = \zeta_p^{\sigma'}$ gegeben ist.

Im weiteren Verlauf sollen nun die Auswirkungen der folgenden Annahme untersucht werden:

Annahme 3.1 *Es existieren* $s, p_0 \in \mathbb{N}$*, sodaß für alle primen* $p > p_0$ *gilt:*

$$\Gamma_{\max,p} > \frac{p}{(\log p)^s}. \tag{3.93}$$

Wenn diese nicht zutrifft, liegt schon in unendlich vielen Fällen eine Verbesserung der bestehenden oberen Schranke von κ_p vor:

Satz 3.17 *Für den Fall, daß die Annahme 3.1 falsch ist, existieren für alle* $\epsilon > 0$ *unendlich viele Primzahlen* p*, mit* $\kappa_p < \epsilon\sqrt{p}$*.*

Wir betrachten nun, für $t \in \mathbb{N}$, die Menge

$$\mathrm{MAX}\Gamma_{p,t} := \{\sigma' \mid 0 \leqslant \sigma' < p,\ |\Gamma_p^{\sigma}/\Gamma_{\max,p}| > 1 - 1/(\log p)^t\}, \tag{3.94}$$

und stellen zunächst einmal fest, daß unter der Annahme 3.1, für festes p, wegen $\mathrm{Sp}(\Gamma_p^2) = p(p-1)$, nur eine polynomiale (d. h. polynomial in $\log p$) Anzahl von Elementen in $\mathrm{MAX}\Gamma_{p,t}$ enthalten ist.

Die Frage lautet nun: existiert ein Algorithmus, welcher nach Eingabe einer Primzahl p, mit polynomialem Aufwand eine Zahl a berechnet, mit $a \in \mathrm{MAX}\Gamma_{p,t}$?

Die Beantwortung dieser Frage scheint nicht einfach. Zwar läßt sich, mit Hilfe einer polynomialen Anzahl von Schritten die Eingabe, d. h. die Primzahlfrage klären, vgl. [3], doch schon bei der, die Menge definierenden Bedingung ist nicht klar, wie diese in „polynomialer Zeit“ überprüft werden soll. Davon abgesehen geht es im wesentlichen darum, unter $2^{\log p}$ Kandidaten, in $(\log p)^c$ Schritten einen zu finden, welcher „in der Nähe“ von $\Gamma_{\max,p}$ liegt. Das scheint zudem, wie oben gesehen, um so schwieriger, je größer das Betragsmaximum der Konjugierten von Γ_p wird.

Erstaunlicherweise gilt der folgende

Satz 3.18 *Unter der Annahme 3.1 gilt: für alle $t \in \mathbb{N}$ existiert eine Konstante c_t und ein Quantenalgorithmus, welcher nach Eingabe einer Primzahl p, in $(\log p)^{c_t}$ Schritten, und mit einer Wahrscheinlichkeit nahe bei 1, ein Element der Menge $\mathrm{MAX}\Gamma_{p,t}$ berechnet.*

Beweis: Sei p eine genügend große Primzahl. Für $0 \leqslant x < p^2$ definieren wir die Funktion f durch $f(x) := p$, falls $x \equiv 0 \bmod p$, sowie, im Falle von $x \not\equiv 0 \bmod p$, durch $f(x) := s_x$, wobei s_x die kleinste, nichtnegative ganze Zahl bedeute, mit

$$s_x \equiv q_p(x) + q_p(x^p) \bmod p. \tag{3.95}$$

Nach Definition des Fermatquotienten q_p, ist die Funktion f dann mit Hilfe einer polynomialen Anzahl von Schritten realisierbar.

Der Algorithmus läuft wie folgt. Zunächst „präparieren“ wir den Zustand

$$\frac{1}{p}\sum_{x=0}^{p^2-1} |x\rangle|f(x)\rangle. \tag{3.96}$$

Nach Anwendung einer Quantenfouriertransformation auf das erste Register ergibt sich

$$\frac{1}{p^2}\sum_{a,x=0}^{p^2-1}\zeta_{p^2}^{ax}|a\rangle|f(x)\rangle, \tag{3.97}$$

was im Anschluß einer „Messung“ den Zustand $|a\rangle|s\rangle$, mit einer Wahrscheinlichkeit von

$$\frac{1}{p^4}\left|\sum_{f(x)=s}\zeta_{p^2}^{ax}\right|^2 \tag{3.98}$$

hervorbringt. Als Ergebnis der Berechnung notieren wir die kleinste, nichtnegative ganze Zahl σ', welche der Gleichung

$$\sigma' \equiv q_p(a) + s \bmod p \tag{3.99}$$

genügt.

Wir zeigen als nächstes, daß unter Beachtung der oben vereinbarten Konvention, die Wahrscheinlichkeit dafür, daß $|\Gamma^\sigma| = \Gamma_{\max,p}$ gilt,

$$\Pr(\text{„}|\Gamma^\sigma| = \Gamma_{\max,p}\text{“}) = \left(1-\frac{1}{p}\right)\left(\frac{\Gamma_{\max,p}}{p}\right)^2 \tag{3.100}$$

erfüllt, was unter der Annahme 3.1 zu

$$\Pr(\text{„}|\Gamma^\sigma| = \Gamma_{\max,p}\text{“}) > \left(1-\frac{1}{p}\right)\frac{1}{(\log p)^{2s}} \tag{3.101}$$

führt.

Um das einzusehen bemerken wir, daß, für $\varphi \in G(\mathbb{Q}(\Gamma_p)/\mathbb{Q})$, nach Definition von Γ_p, sowie nach Satz 2.12, gilt

$$\Gamma_p^\varphi = \frac{1}{p}\sum_{\chi\neq\chi_0}\bar{\chi}(1-\varphi' p)\tau(\chi), \tag{3.102}$$

und damit, nach Anwendung von Satz 3.8

$$\Gamma_p^\varphi = \frac{1}{p}\sum_{k=1}^{p-1}\bar{\chi}^k(1-\varphi' p)p\chi^k(k)\zeta_{p^2}^k = \sum_{k=1}^{p-1}\zeta_{p^2}^{k(1+p(q_p(k)-\varphi'))}. \tag{3.103}$$

Da die Charaktere die Ordnung p haben, kann das „k“ im Exponent durch „$k+jp$“ ersetzt werden; d. h. es gilt

$$(k+jp)(1+p(q_p((k+jp))-\varphi')) \equiv k(1+p(q_p(k)-\varphi')) \bmod p^2, \tag{3.104}$$

was zur Folge hat, daß

$$f(k(1+p(q_p(k)-\varphi'))) = \varphi'. \tag{3.105}$$

Desweiteren besitzt, für jedes $a \not\equiv 0 \bmod p$, die Restklasse a mod p^2 einen Vertreter der Form

$$a \equiv \omega_a(1-q_p(a)p) \bmod p^2, \tag{3.106}$$

mit $\omega_a^{p-1} \equiv 1 \bmod p^2$, und nach Definition von Γ_p folgt damit in diesem Fall

$$\sum_{f(x)=\varphi'} \zeta_{p^2}^{ax} = \sum_{f(x)=\varphi'} \zeta_{p^2}^{\omega_a(1-q_p(a)p)x} = \sum_{f(x)=\varphi'} \zeta_{p^2}^{(1-q_p(a)p)x} = \Gamma_p^{\sigma}, \tag{3.107}$$

mit $\sigma' \equiv q_p(a)+\varphi' \bmod p$. Die Tatsache, daß nun $|\Gamma^{\sigma}| = \Gamma_{\max,p}$ gilt, ergibt sich also in $p(p-1)$ Fällen und damit auch die Gleichung (3.100).

Für $\varphi \in G(\mathbb{Q}(\Gamma_p)/\mathbb{Q})$ definieren wir nun die Zahl α_φ via $|\Gamma^{\varphi}| = \alpha_\varphi \Gamma_{\max,p}$; außerdem bezeichne $\sigma_{\max}$ das Element der Galoisgruppe, für welches $|\Gamma^{\sigma_{\max}}| = \Gamma_{\max,p}$ gelte. Nach $(\log p)^k$ Durchläufen des Algorithmus betrachten wir die Differenz der Erwartungswerte von $\sigma'_{\max}$ und φ' und fordern, daß diese oberhalb einer bestimmten Schranke liegt:

$$(\log p)^k\left(1-\frac{1}{p}\right)\left(\frac{\Gamma_{\max,p}}{p}\right)^2 - (\log p)^k\left(1-\frac{1}{p}\right)\alpha_\varphi^2\left(\frac{\Gamma_{\max,p}}{p}\right)^2 > (\log p)^{5+k/2}. \tag{3.108}$$

Aufgelöst nach α_φ folgt, unter der Annahme 3.1 und für $k > 12+4s$,

$$\alpha_\varphi < 1 - \frac{1}{(\log p)^{k-10}}. \tag{3.109}$$

Zusammengefaßt folgt, daß, für $t \in \mathbb{N}$, $k-10 > t$ und $k > 12+4s$, der Algorithmus, sofern er nach $(\log p)^k$ Durchläufen den am häufigsten gezogenen Kandidaten ausgibt, mit hoher Wahrscheinlichkeit ein Element der Menge $\mathrm{MAX}\Gamma_{p,t}$ gefunden hat. Daß diese Wahrscheinlichkeit nahe bei 1 liegt, ergibt sich, da es sich um eine Binomialverteilung handelt, mit Hilfe der Standardmethoden der Wahrscheinlichkeitsrechnung. □

Als eine Zusammenfassung der Ergebnisse formulieren wir den, von der getroffenen Annahme unabhängigen Satz:

Satz 3.19 *Mindestens eine der beiden folgenden Aussagen ist wahr:*

1. *Für alle* $t \in \mathbb{N}$ *existiert eine Konstante* c_t *und ein Quantenalgorithmus, welcher nach Eingabe einer Primzahl* p*, in* $(\log p)^{c_t}$ *Schritten, und mit einer Wahrscheinlichkeit nahe bei* 1*, ein Element der Menge* $\mathrm{MAX}\Gamma_{p,t}$ *berechnet.*

2. *Für alle* $\epsilon > 0$ *existieren unendliche viele Primzahlen* p*, mit* $\kappa_p < \epsilon\sqrt{p}$*.*

Kapitel 4

Ausblick

Wir wollen an dieser Stelle noch einige Bemerkungen zu Fragestellungen anfügen, welche in dieser Arbeit nicht behandelt werden konnten, deren weitere Erforschung sich aber als durchaus fruchtbar erweisen könnte.

Zunächst wurde zu Beginn des zweiten Kapitels die ADFT sowie ihre Inverse bzgl. eines Teilkörpers des Körpers der komplexen Zahlen definiert. Es sei bemerkt, daß weder die archimedischen Eigenschaften, noch die Charakteristik von $\mathbb{C}$ notwendige Voraussetzungen bilden; die Definitionen können für beliebige Körper K, sofern die Existenz von Einheitswurzeln ζ_n gesichert ist (d. h. char K teilt nicht n) verallgemeinert werden. Auch die Aussage von Satz 2.1 bleibt erhalten. Am einfachsten sieht man das, indem man die Gleichung

$$\mathrm{ADFT}_{n,\vartheta} \cdot \mathrm{ADFT}_{n,\vartheta^*} = \mathrm{DFT}_n^2$$

mit den gegebenen Definitionen elementar nachrechnet. Gleiches gilt für die Aussagen über das Spektrum der ADFT.

Den Beweis von Satz 2.4 über die Existenz schlanker Basen hatten wir geführt, indem wir für alle Dimensionen explizit einen Vertreter jener Basen angegeben haben. Es sei an dieser Stelle darauf hingewiesen, daß diese weder eindeutig bestimmt, noch in irgendeiner Weise kanonisch wären. Tatsächlich steht eine exakte Klassifikation aller schlanken Basen noch aus. Allgemein stellt sich hierbei die Frage nach einem bezeichnenden Charakteristikum all jener $y(\chi|\vartheta)$, welche die Eigenschaften von Satz 2.9 erfüllen und für welche der Ausdruck

$$\frac{1}{\varphi(p^s)} \sum_{\chi, f_\chi = p^s} \frac{\bar{\chi}(a_0)}{y(\chi|\vartheta)}$$

die Werte $0, \pm 1$ annimmt.

Eventuell kann es sinnvoll sein, diesen Wertebereich zu erweitern, in dem Sinne, daß man auch Werte wie $\pm\sqrt{2}, \pm 1/2$, etc. zuläßt. Solche „quasi-schlanken Basen“ sind etwa dann notwendig, wenn die Transformation zusätzlichen Bedingungen genügen soll. So kann es beispielsweise für manche Anwedungen wünschenswert (oder sogar notwendig) sein, daß die entsprechende Matrix unitär ist.

Eine der folgenden Aufgaben, welche sich aus den Betrachtungen des dritten Kapitels über die Normalbasenarithmetik ergeben, verlangt nach einer Beschreibung all jener (Normal-)Basen, bzgl. derer sich die, durch die Matrizen

$$W_{\vartheta}^{(\rho)} = \frac{1}{|G|^2} \left(\sum_{\chi,\chi'} \kappa(\chi,\chi')_{\vartheta} \omega(\chi,\chi') \bar{\chi}(\sigma\rho^{-1}) \bar{\chi}'(\varphi\rho^{-1}) \right)_{\sigma,\varphi}$$

gegebenen Bilinearformen simultan und effizient realisieren lassen. Hierbei steht nun, wie gesagt, nicht die Struktur der einzelnen Matrizen im Vordergrund, sondern die Realisierung der Matrizenfamilie als Ganzes. Als hilfreich könnte sich in diesem Zusammenhang, wie etwa in Korollar 3.1 angedeutet, das Studium der Kreisteilungsmatrizen unter algorithmischen Aspekten erweisen. Zudem sei an dieser Stelle noch auf die Arbeiten von H. de Groote ([25], [26], [27]) verwiesen, welche sich intensiv mit den theoretischen Grenzen der Realisierung von Bilinearformen auseinandersetzen.

Desweiteren besteht ein direkter Zusammenhang zwischen den hier dargestellten Faktorensystemen der Gaußschen Summen und den aus der lokalen Klassenkörpertheorie bekannten Hilbertsymbolen (vgl. [32], [62]). Tatsächlich erfüllen die Elemente $\omega(\chi,\chi')$, unter Vorlage einer entsprechenden Kohomologie, die Bedingungen eines 2-Kozykels, und die Frage, wann diese trivial sind ist gleichbedeutend mit der Frage, wann diese bereits 2-Koränder bilden. Eine mögliche Antwort könnte, wie so häufig, in der Struktur der entsprechenden Brauergruppe liegen.

Eine weitere interessante Problemstellung ergibt sich aus der Beziehung des $(p-1)$-sten Mirimanoffpolynoms und des diskreten Logarithmus eines Elements α der Einheitengruppe eines endlichen Körpers,

$$\sum_{k=1}^{p-2} \gamma_p(\omega^k)\alpha^k \equiv (\mathrm{dLog}_{\omega}(\alpha)+1)^{-1} \bmod p,$$

sowie der Tatsache, daß sich das Polynom γ_p effizient realisieren läßt. Allgemein stellt sich hier die Frage, ob eine Beziehung zwischen der „algorithmischen Güte“ einer Funktion f

und der ihrer transformierten Variante

$$F(t) = \sum_k f(\omega^k) t^k$$

besteht, und in welcher Art sich eine derartige Beziehung formulieren läßt. Umgekehrt wäre es interessant zu wissen, welche arithmetischen Konsequenzen sich für die Mirimanoffpolynome, und damit eventuell auch für die Faltung an sich, unter der Annahme ergeben, daß das Problem des diskreten Logarithmus in dieser Gruppe nicht in polynomialer Zeit lösbar ist.

Am Ende dieser Liste sei noch eine Bemerkung zu dem im letzten Abschnitt des vorangegangenen Kapitels vorgestellten Algorithmus gestattet. Dieser gehört zu den wenigen derzeit bekannten Quantenalgorithmen, welche *keine* Instanz des sog. „Hidden Subgroup Problems“ (HSP) lösen. Stattdessen trägt der Ansatz der Tatsache Rechnung, daß dieser überhaupt nur dann funktioniert, falls entsprechend wenige (d. h. nur polynomial viele) Lösungen existieren. Selbst wenn das hier betrachtete Problem, bzw. das daraus resultierende Entscheidungsproblem vermutlich noch nicht einmal in NP liegt, so liefert das Verfahren doch ein weiteres (kleines) Indiz für eine Idee, welche sich in einigen Jahren vielleicht schon als echte Vermutung präsentieren könnte. Diese Idee, welche schon von mehreren Autoren aufgegriffen wurde, beschreibt einen Zusammenhang zwischen den Komplexitätsklassen FewP und BQP in der Form:

$$\text{FewP} \subset \text{BQP}.$$

Bis eine derartige Vermutung allerdings ernsthaft formuliert werden kann, muß die Datenbasis noch vergrößert werden.

Literaturverzeichnis

[1] M. Aaltonen, K. Inkeri, *Catalan's Equation* $x^p - y^q = 1$ *and related Congruences*, Math. Comp., Vol. 56, No. 193, 359–370, 1991

[2] T. Agoh, *Fermat Quotiens for Composite Moduli*, J. Number Theory 66, 29–50, 1997

[3] M. Agrawal, N. Kayal, N. Saxena, PRIMES *is in* P, erhtl. unter: www.cse.iitk.ac.in/news/primality.html, 2002

[4] N. Aoki, *Abelian Fields Generated by a Jacobi Sum*, Comm. Math. Uni. St. Pauli, Vol 45, No.1, 1996

[5] M. Bauer, *Über die außerwesentlichen Diskriminatenteiler einer Gattung*, Math. Ann. 64, 572–576, 1907

[6] E. Bayer-Fluckiger, H. W. Lenstra, *Forms in odd degree extensions and self-dual normal bases*, Am. J. Math. 112, 359–373, 1990

[7] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Can. Math. Soc. Ser. Mono. Adv. Texts, Vol 21, Wiley-Inters. Publ., 1998

[8] Th. Beth, W. Fumy, R. Mühlfeld, *Zur Algebraischen Diskreten Fourier-Transformation*, Arch. Math. 40, 238–244, 1983

[9] Th. Beth, *Verfahren der schnellen Fourier-Transformation*, B. G. Teubner Stuttgart, 1984

[10] Th. Beth, *Generating Fast Hartley Transforms*, Proc. URSI-ISSSE 89, Erlangen, Deutschland, 688–692, 1989

[11] D. Bini, P. Favati, *On a Matrix Algebra related to the Discrete Hartley Transform*, Siam J. Math Anal. Appl., Vol. 12, No. 2, 500–507, 1993

[12] S. Bosch, *Algebra*, Springer, 1993

[13] D. M. Bressoud, *On the Value of Gaussian Sums*, J. Number Theory 13, 88–94, 1981

[14] R. Bungers, *Über Zahlkörper mit gemeinsamen außerwesentlichen Diskriminatenteilern*, Jber. Deutsche Math.-Verein. 46, 93–96, 1936

[15] D. J. Britten, F. W. Lemire, *A Structure Theorem for Rings Supporting a Discrete Fourier Transform*, Siam J. Appl. Math., Vol. 41, No. 2, 222–226, 1981

[16] L. Carlitz, *A note on common index divisors*, Proc. Amer. Math. Soc. 3, 688–692, 1952

[17] H. Davenport, H. Hasse, *Die Nullstellen der Kongruenzzetafunktion in gewissen zyklischen Fällen*, J. reine u. angew. Math. 172, 151–182, 1934

[18] H. T. Engstrom, *On the common index divisors of an algebraic field*, Trans. Amer. Math. Soc. 32, 223–237, 1930

[19] T. Funakura, *A Genaralization of the Chowla-Mordell Theorem on Gaussian Sums*, Bull. Londin Math Soc. 24, 424–430, 1991

[20] K. Girstmair, *Character Coordinates and Annihilators of Cyclotomic Numbers*, Mathematica, 375–389, 1987

[21] K. Girstmair, *Dirichlet Convolution of Cotangent Numbers and Relative Class Number Formulas*, Mh. Math. 110, 231–256, 1990

[22] A. Granville, *Powerfull Numbers and Fermat's Last Theorem*, C. R. Math. Rep. Acad. Canada, Vol. VIII, No. 3, 215–218, 1986

[23] B. Grohmann, *Über die rationale Algebraische Diskrete Fourier-Transformation*, Manuskript, 1996

[24] B. Grohmann, M. Rötteler, *Von* N^2 *nach* $\log^2 \mathsf{N}$*; Zur algebraischen Berechnungskomplexität allgemeiner Fouriertransformationen*, Informatik 99, Reihe Informatik aktuell, Springer, 247–252, 1999

[25] H. de Groote, *On Varieties of Optimal Algorithms for the Computation of Bilinear Mappings; I. The Isotropy Group of a Bilinear Mapping*, Theor. Comp. Science 7, 1–24, 1978

[26] H. de Groote, *II. Optimal Algorithms for* 2×2*-Matrix Multiplication*, Theor. Comp. Science 7, 127–148, 1978

[27] H. de Groote, *III. Optimal Algorithms for the Computation of* xy *and* yx *where* $\mathsf{x}, \mathsf{y} \in \mathsf{M}_2(\mathsf{K})$, Theor. Comp. Science 7, 239–249, 1978

[28] H. de Groote, *Characterization of Division Algebras of Minimal Rank and the Structure of their Algorithm Varieties*, Siam J. Comp., Vol 12, No. 1, 1983

[29] H. de Groote, *Lectures on the Complexity of Bilinear Problems*, LNCS 245, Springer Berlin Heidelberg, 1987

[30] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil I: Klassenkörpertheorie.*, Jahresb. D. M.-V. 35, 1–55, 1926

[31] H. Hasse, *Teil Ia: Beweise zu Teil I*, Jahresb. D. M.-V. 36, 233–311, 1927

[32] H. Hasse, *Teil II: Reziprozitätsgesetzte*, Jahresb. D. M.-V., Ergänzungsb. VI, 1930

[33] H. Hasse, *Vorlesung über Zahlentheorie*, Die Grundl. der Math. Wissensch. in Einzeld., Band LIX, Springer Berlin Göttingen Heidelberg, 1950

[34] H. Hasse, *Zum expliziten Reziprozitätsgesetz*, Arch. Math., Vol. XIII, 479–485, 1962

[35] C. Helou, *Norm residue symbol and cyclotomic units*, Acta Arith. LXXIII.2, 147–188, 1995

[36] K. Hensel, *Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung*, J. reine u. angew. Math. 113, 128–160, 1894

[37] J. Hong, M. Vetterli, *Hartley Transforms Over Finite Fields*, IEEE Trans. on Inform. Theory, Vol 39, No. 5, 1628–1638, 1993

[38] J. Hong, M. Vetterli, P. Duhamel, *Basefield Transforms with the Convolution Property*, Proc. of the IEEE, Vol. 82, No. 3, 400–412, 1994

[39] K. Inkeri, *On Catalans Problem*, Acta Arith. IX, 285–290, 1964

[40] K. Inkeri, *On Catalan's Conjecture*, J. Number Theory 34, 142–152, 1990

[41] K. Iwasawa, *On explicit formulas for the norm residue symbol*, J. Math. Soc. Japan, Vol. 20, Nos. 1–2, 151–165, 1968

[42] S. Jacubec, *On Divisibility of Class Number of Real Abelian Fields of Prime Conductor*, Abh. Math. Sem. Hamburg 63, 67–86, 1993

[43] S. Jacubec, *The Congruence for Gauss Period*, J. Number Theory 48, 36–45, 1994

[44] S. Jakubec, *Connection between the Wieferich congruence and divisibilitiy of* $\mathfrak{h}^+$, Acta Arith. LXXI.1, 55–64, 1995

[45] W. Johnson, *On the nonvanishing of Fermat quotients* $(mod\, p)$, J. reine u. angew. Math., 292, 196–200, 1977

[46] W. Johnson, *On the* p*-Divisibility of the Fermat Quotients*, Math. Comp., Vol 32, No. 141, 297–301, 1978

[47] J. M. Kim, *Coates-Wiles Series and Mirimanoff's Polynomial*, J. Number Theory 54, 173–179, 1995

[48] W. Klösgen, *Untersuchungen über Fermatsche Kongruenzen*, Ges. f. Math. u. Datenv., Bonn, Nr. 36, 1970

[49] S. Lang, *Algebra*, 3rd ed, Addison-Wesley, 1994

[50] D. H. Lehmer, *Incomplete Gauss Sums*, Mathematika 23, 125–135, 1976

[51] F. Lemmermeyer, *Reciprocity Laws; From Euler to Eisenstein*, SMM, Springer Berlin Heidelberg, 2000

[52] H.-W. Leopoldt, *Über die Hauptoprdnung der ganzen Elemente eines abelschen Zahlkörpers*, J. reine u. angew. Math. 201, 119–149, 1959

[53] M. Lerch, *Zur Theorie des Fermatschen Quotienten*, Math. Annalen, 60, 471–490, 1905

[54] G. Lettl, *The ring of integers of an abelian number field*, J. reine u. angew. Math. 404, S. 162 – 170, 1990

[55] J. H. Loxton, *Products related to Gauss sums*, J. reine u. angew. Math. 268/269, 53–67, 1974

[56] J. H. Loxton, *Some conjectures concerning Gauss sums*, J. reine u. angew. Math. 297, 153–158, 1978

[57] J. H. Loxton, *The Graphs of Exponential Sums*, Mathematika 30, 153–163, 1983

[58] D. S. Lubinsky, Z. Ziegler, *Coefficient Bounds in the Lorentz Representation of a Polynomial*, Cannad. Math. Bull., Vol 33 (2), 197–206, 1990

[59] P. L. Montgomery, *New Solutions of* $a^{p-1} \equiv 1 \pmod{p^2}$, Math. Comp., Vol 61, No. 203, 361–363, 1993

[60] T. Morishima, *Über den Fermatschen Quotienten*, Jpn. J. Math., 8, 159–173, 1931

[61] M. B. Nathanson, *Elementary Methods in Number Theory*, GTM 195, Springer New York, 2000

[62] J. Neukirch, *Algebraische Zahlentheorie*, Springer Berlin Heidelberg, 1992

[63] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, Grundlehren d. math. Wissensch., Vol. 323, Springer Berlin Heidelberg, 2000

[64] F. Nietzsche, *Menschliches, Allzumenschliches. Ein Buch für freie Geister*, zweiter Band 1886, DTV / W. de Gruyter Berlin New York, 1988

[65] R. Odoni, *On Gauss Sums* $(\mathrm{mod}\,\mathfrak{p}^{\mathfrak{n}})$, $\mathfrak{n} \geqslant 2$, Bull. London Math. Soc. 5, 325–327, 1973

[66] A. N. Parshin, I. R. Shafarevich (Eds.), *Number Theory I*, Encycl. of Math. Science, Vol 49, Springer Berlin Heidelberg, 1991

[67] A. N. Parshin, I. R. Shafarevich (Eds.), *Number Theory II*, Encycl. of Math. Science, Vol 62, Springer Berlin Heidelberg, 1992

[68] P. A. B. Pleasants *The number of generators of the integers of a number field*, Mathematika 21, 160–167, 1974

[69] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer New York, 1979

[70] A. M. Robert, *A Course in* $\mathfrak{p}$*-adic Analysis*, GTM 198, Springer New York, 2000

[71] H. Rothgiesser, *Zum Reziprozitätsgesetz für* $\mathfrak{l}^{\mathfrak{n}}$, Abh. Math. Sem. Hamburg 11, 1934

[72] C.-G. Schmidt, *Über die Führer von Gaußschen Summen als Größencharaktere*, J. Number Theory 12, 283–310, 1980

[73] K. Shiratani, *Note on the Kummer-Hilbert reciprocity law*, J. Math. Soc. Japan, Vol. 12, No. 4, 412–421, 1960

[74] J. Sliwa, *On the nonessential discriminant divisor of an algebraic number field*, Acta Arith. XLII, 57–72, 1982

[75] G. Steidl, *Generalization of the Algebraic Discrete Fourier Transform with Application to Fast Convolution*, Linear Alg. Appl. 139, 181–206, 1990

[76] A. A. Sukallo, *On determination of the index of a field of algebraic numbers*, Rosto. Gos. Univ. Uč. Zap. Fiz.-Mat. Fak., No. 4, 37–42, 1955

[77] G. Terjanian, *Sur la loi réciprocité des puissances* $\mathfrak{l}$*-èmes*, Acta Arith. LIV, 87–125, 1989

[78] R. Tijdeman, *On the equation of Catalan*, Acta Arith. XXIX, 197–209, 1976

[79] T. Uehara, *On a congruence relation between Jacobi sums and cyclotomic units*, J. reine u. angew. Math. 382, 199–214, 1987

[80] S. V. Vostokov, *Explicit Form of the Law of Reciprocity*, Math. USSR Izvestija, Vol. 13, No. 3, 557–588, 1979

[81] J. Wang, *On the Jacobi Sums Modulo* $\mathfrak{P}^{\mathfrak{n}}$, J. Number Theory 39, 50–64, 1991

[82] L. C. Washington, *Introduction to Cyclotomic Fields*, GTM 83, 2nd Ed., Springer New York, 1997

[83] A. L. Wells, Jr, *A Polynomial Form for Logarithms Modulo a Prime*, IEEE Trans. on Inform. Theory, Vol. 30, No. 6, 845–846, 1984

[84] S. Winograd, *On Multiplication in Algebraic Extension Fields*, Theor. Comp. Science 8, 359–377, 1979

[85] E. Zylinsky, *Zur Theorie der außerwesentlichen Diskriminantenteiler algebraischer Körper*, Math. Ann. 73, 273–274, 1913