Gruppenringe und ihre Anwendung auf die Gruppe der zyklotomischen Einheiten

(Diplomarbeit)

Angefertigt von
Marc Conrad
nach einem Thema von
Professor Dr. H. G. Zimmer
am Fachbereich Mathematik
der Universität des Saarlandes
Saarbrücken 1992

Eidesstattliche Erklärung

Hiermit erkläre ich an Eides Statt, daß ich die vorliegende Arbeit selbst angefertigt und nur die angegebenen Quellen und Hilfsmittel benutzt habe.

Saarbrücken, den

Mein besonderer Dank gilt Herrn Prof. Dr. Zimmer für die Vermittlung dieses interessanten Themas und für seine großzügige Unterstützung. Des weiteren möchte ich Herrn Prof. Dr. Hoechsmann danken für seine hilfreichen Anregungen und Gespräche, vor allem im Hinblick auf die Themensuche im Vorfeld dieser Arbeit, und Herrn Prof. Dr. Gekeler für seine nützlichen Kommentare zur Diplomarbeit selbst.

Außerdem Danke an Hans Crauel und an meine Schwester Anne Conrad für ihre guten Ratschläge und Hilfestellungen, was Diplomarbeiten im allgemeinen und im besonderen betrifft, sowie an die Mitglieder der SIMATH-Gruppe für deren Unterstützung im "technischen" Bereich, insbesondere die Verwendung von LaTeX, Unix und Apollo-Rechnern.

Marc Conrad

Contents

Einführung

Gruppenringe $\mathbb{Z}G$ mit abelscher Gruppe G und zyklotomische Einheiten, das heißt Einheiten der Form $1 - \epsilon_n$ mit einer n-ten Einheitswurzel ϵ_n, sind die beiden zentralen Themen dieser Arbeit. Die Untersuchung von Einheiten in diesen Gruppenringen führt in natürlicher Weise zu Fragestellungen, die zyklotomische Einheiten betreffen. Dies kommt in den Sätzen 1 und 3 zum Ausdruck. Andererseits wird es sich zeigen, daß es zum Rechnen innerhalb des Systems der zyklotomischen Einheiten nützlich ist, Gruppenringe zu benutzen. Diese Methodik, Gruppenringe für Beweise von Eigenschaften zyklotomischer Einheiten zu nutzen, schlägt sich besonders in den Beweisen zu Satz 2, dem Lemma von Bass und der Unabhängigkeit der Ramachandra-Einheiten (Satz 4) nieder.

Im ersten Kapitel werden zunächst Gruppenringe eingeführt. Die elementaren Eigenschaften dieser Struktur werden in der Literatur meist nur kurz oder als Übungsaufgabe abgehandelt. Daher werden diese Eigenschaften hier etwas ausführlicher herausgearbeitet. Der Abschnitt schließt mit Satz 1, der für die Gruppenalgebra $\mathbb{C}G$ (mit einer endlichen abelsche Gruppe G) die Einheiten und Nullteiler charakterisiert.

Des weiteren werden im ersten Kapitel zyklotomische Einheiten eingeführt. Es wird dabei als bekannt vorausgesetzt, daß die Automorphismengruppe des n-ten zyklotomischen Körpers isomorph zu $(\mathbb{Z}/n\mathbb{Z})^*$ ist. Darüber hinaus werden keine weitergehenden Eigenschaften dieser Körper benötigt. In Satz 2 wird dann, schon im Vorgriff auf das dritte Kapitel, ein explizites Erzeugendensystem der Gruppe der zyklotomischen Einheiten angegeben.

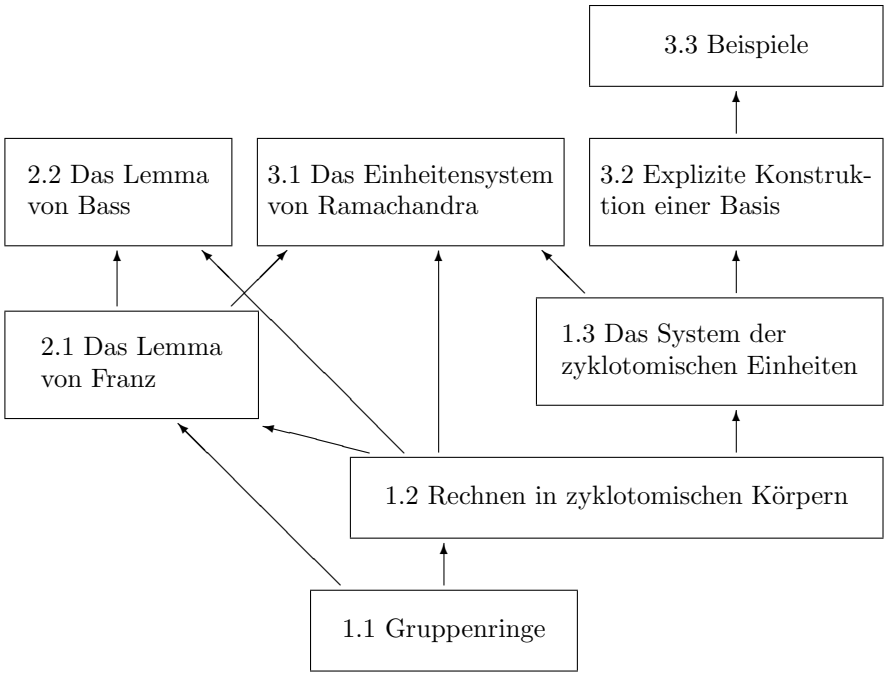
Kapitel 2 behandelt die Lemmata von Franz und Bass. Dabei ist es für den Beweis des Lemmas von Franz notwendig, Gaußsche Summen einzuführen und deren elementare Eigenschaften herzuleiten. Im Beweis selbst wird das Nichtverschwinden der Dirichletschen L-Funktion ausgenutzt. Diese in der analytischen Zahlentheorie fundamentale Tatsache wird im Anhang A bewiesen. Satz 3 macht eine Anwendung des Lemmas von Franz deutlich.

Das Lemma von Bass ist eine Verallgemeinerung des Lemmas von Franz. Es ist im Zusammenhang dieser Arbeit interessant, da für den Beweis – im Gegensatz zur Originalversion von Bass – Gruppenringe verwendet werden. Insbesondere wird der Gruppenring $\mathbb{Z}G_n$ zum Ring $\mathbb{Z}$ und zur Automorphismengruppe G_n des n-ten zyklotomischen Körpers betrachtet.

Im letzten Kapitel wird die Gruppe der zyklotomischen Einheiten weiter untersucht. Ramachandra definiert Einheiten in der Gruppe der zyklotomischen Einheiten, die eine Untergruppe von endlichem Index erzeugen. Die Unabhängigkeit dieser Einheiten ist Gegenstand von Satz 4. Der Beweis dieses Satzes wird wiederum mit Hilfe des Gruppenrings $\mathbb{Z}G_n$ geführt und unterscheidet sich dadurch wesentlich von Ramachandras Beweis.

Am Ende dieser Arbeit wird eine Basis der zyklotomischen Einheiten von $\mathbb{Z}[\epsilon_n]$ konstruiert, falls n von höchstens drei verschiedenen Primzahlen geteilt wird (Satz 5, 6 und 7). Mit Hilfe eines SIMATH-Programmes ist es möglich, eine Basis anzugeben und jedes Element der Form $1 - \epsilon_n^\nu$ als Produkt von Basiselementen darzustellen. Das 3. Kapitel enthält dazu einige Beispiele. Das Programm, mit dem diese Beispiele erstellt wurden, befindet sich im Anhang B.

Der logische Aufbau der einzelnen Abschnitte läßt sich wie folgt darstellen:



1 Grundlagen

Zunächst werden Gruppenringe eingeführt. Danach werden einige Relationen in $\mathbb{Z}[\epsilon_n]$ hergeleitet, die schließlich zur Definition der zyklotomischen Einheiten führen.

1.1 Gruppenringe

Der Gruppenring ist eine algebraische Struktur, die zunehmend an Bedeutung gewinnt. Wir werden uns hier auf endliche, später sogar auf abelsche Gruppen beschränken. Eine ähnliche Konstruktion ist auch für unendliche Gruppen möglich.

1.1.1 Definitionen und Bemerkung

Sei R ein beliebiger Ring und G eine endliche Gruppe. Die Verknüpfung in G sei multiplikativ geschrieben. RG bezeichne die Menge aller formalen Summen

$$\sum_{\sigma \in G} r_\sigma \sigma$$

mit Koeffizienten $r_\sigma \in R$. Dabei werden meistens die Summanden weggelassen, für die $r_\sigma = 0$ ist. Wenn klar ist, worüber summiert wird, wird auch der Summenindex weggelassen.

Auf RG werden eine Addition und eine Multiplikation gemäß

$$\sum_{\sigma \in G} r_\sigma \sigma + \sum_{\sigma \in G} s_\sigma \sigma := \sum_{\sigma \in G} (r_\sigma + s_\sigma)\sigma$$

und

$$(\sum_{\sigma \in G} r_\sigma \sigma)(\sum_{\tau \in G} s_\tau \tau) := \sum_{\rho \in G} \left(\sum_{\sigma\tau = \rho} r_\sigma s_\tau \right) \rho$$

definiert.

Lemma 1

RG bildet mit diesen Verknüpfungen einen Ring, sogar einen Ring mit Eins, falls R ein Ring mit Eins ist, und einen kommutativen Ring, falls R und G kommutativ sind.

Beweis

Die additive Gruppenstruktur ist sofort klar, da die Addition komponentenweise

erklärt ist. Die Assoziativität der Multiplikation folgt aus

$$\left((\sum_{\sigma\in G} r_\sigma\sigma)(\sum_{\tau\in G} s_\tau\tau)\right)(\sum_{\rho\in G} t_\rho\rho) \;=\; \left(\sum_{\mu\in G}\left(\sum_{\sigma\tau=\mu} r_\sigma s_\tau\right)\mu\right)(\sum_{\rho\in G} t_\rho\rho)$$
$$= \sum_{\nu\in G}\left(\sum_{\mu\rho=\nu}\sum_{\sigma\tau=\mu} r_\sigma s_\tau t_\rho\right)\nu \;=\; \sum_{\nu\in G}\left(\sum_{\sigma\tau\rho=\nu} r_\sigma s_\tau t_\rho\right)\nu$$

und

$$(\sum_{\sigma\in G} r_\sigma\sigma)\left((\sum_{\tau\in G} s_\tau\tau)(\sum_{\rho\in G} t_\rho\rho)\right) \;=\; (\sum_{\sigma\in G} t_\sigma\sigma)\left(\sum_{\mu\in G}\left(\sum_{\tau\rho=\mu} s_\tau\; t_\rho\right)\mu\right)$$
$$= \sum_{\nu\in G}\left(\sum_{\sigma\mu=\nu}\sum_{\tau\rho=\mu} r_\sigma s_\tau t_\rho\right)\nu \;=\; \sum_{\nu\in G}\left(\sum_{\sigma\tau\rho=\nu} r_\sigma s_\tau t_\rho\right)\nu.$$

Die Distributivität rechnet man ähnlich nach. Das Einselement ist, wenn 1 die Eins im Ring ist und σ_1 das neutrale Element der Gruppe, das Element $1\sigma_1$. Die Kommutativität ist aus der Definition der Multiplikation ersichtlich.

QED.

Diese Eigenschaften motivieren folgende Definition.

Definition

RG mit der oben eingeführten Addition und Multiplikation heißt Gruppenring zu R und G.
Ist $R = K$ Körper, so bezeichnet man KG auch als Gruppenalgebra.

In der Literatur findet sich auch die Bezeichnung $R[G]$.

Bemerkung

Die Schreibweise der Elemente als formale Summen und die Definition der Addition im Gruppenring ist gerade so, daß die formale Summe

$$\sum_{\sigma\in G} r_\sigma\sigma$$

auch als echte Summe der Gruppenringelemente $r_\sigma\sigma$ interpretiert werden kann.

1.1.2 Beispiel

Ist $G = C_n$ die von einem Element $x \in C_n$ erzeugte zyklische Gruppe der Ordnung n (das heißt $x^n = 1$) und $R = \mathbb{Z}$ der Ring der ganzen Zahlen, so ist

$$\mathbb{Z}C_n = \{\sum_{i=0}^{n-1} a_i x^i,\; a_i \in \mathbb{Z}\}.$$

Die Multiplikation ist in diesem Fall

$$\left(\sum_{i=0}^{n-1} a_i x^i\right)\left(\sum_{i=0}^{n-1} b_i x^i\right) = \sum_{k=0}^{n-1}\left(\sum_{i+j\equiv k \bmod n} a_i b_j\right) x^k$$

und entspricht gerade der Multiplikation im Polynomring $\mathbb{Z}[x]$ und anschließender Identifikation von x^k mit x^{n+k}. In der Tat läßt sich zeigen, daß

$$\mathbb{Z}C_n \cong \mathbb{Z}[x] \,/_{(x^n - 1)}$$

gilt.

1.1.3 Homomorphismen

Sowohl Homomorphismen von Ringen als auch Homomorphismen von Gruppen lassen sich übertragen zu Homomorphismen zwischen Gruppenringen. Davon handeln die nächsten beiden Lemmata.

Lemma 2

Seien G eine Gruppe, R und S zwei Ringe und $\varphi : R \to S$ ein Ringhomomorphismus. Dann ist

$$\begin{array}{rccc} \hat{\varphi}: & RG & \to & SG \\ & \sum\limits_{\sigma\in G} r_\sigma \sigma & \mapsto & \sum\limits_{\sigma\in G} \varphi(r_\sigma)\sigma \end{array}$$

ein Homomorphismus von Gruppenringen.

Ist φ injektiv bzw. surjektiv, so ist $\hat{\varphi}$ ebenfalls injektiv bzw. surjektiv.

Der Beweis ergibt sich direkt aus der Definition von Addition und Multiplikation im Gruppenring.

Lemma 3

Seien G und H zwei Gruppen und R ein Ring. Sei $\varphi : G \to H$ ein Homomorphismus von Gruppen. Dann ist

$$\begin{array}{rccc} \hat{\varphi}: & RG & \to & RH \\ & \sum\limits_{\sigma\in G} r_\sigma \sigma & \mapsto & \sum\limits_{\tau\in H}\left(\sum\limits_{\varphi(\sigma)=\tau} r_\sigma\right)\tau \end{array}$$

ein Homomorphismus von Gruppenringen.

Auch hier gilt, wenn φ injektiv bzw. surjektiv ist, daß auch $\hat{\varphi}$ injektiv bzw. surjektiv ist.

Beweis

Man rechnet die Eigenschaften direkt nach. Für die Addition hat man

$$\hat{\varphi}(\sum_{\sigma\in G} r_\sigma\sigma) + \hat{\varphi}(\sum_{\sigma\in G} s_\sigma\sigma) = \sum_{\tau\in H}\left(\sum_{\varphi(\sigma)=\tau} r_\sigma\right)\tau + \sum_{\tau\in H}\left(\sum_{\varphi(\sigma)=\tau} s_\sigma\right)\tau$$
$$= \sum_{\tau\in H}\left(\sum_{\varphi(\sigma)=\tau} r_\sigma + s_\sigma\right)\tau \;=\; \hat{\varphi}(\sum_{\sigma\in G}(r_\sigma + s_\sigma)\sigma),$$

und für die Multiplikation rechnet man nach:

$$\hat{\varphi}(\sum_{\sigma\in G} r_\sigma\sigma)\hat{\varphi}(\sum_{\sigma'\in G} s_{\sigma'}\sigma') \;=\; \left(\sum_{\tau\in H}(\sum_{\varphi(\sigma)=\tau} r_\sigma)\tau\right)\left(\sum_{\tau'\in H}(\sum_{\varphi(\sigma')=\tau'} s_{\sigma'})\tau'\right)$$
$$= \sum_{\rho\in H}\left(\sum_{\tau\tau'=\rho}(\sum_{\varphi(\sigma)=\tau} r_\sigma)(\sum_{\varphi(\sigma')=\tau'} s_{\sigma'})\right)\rho = \sum_{\rho\in H}\left(\sum_{\tau\tau'=\rho}\sum_{\varphi(\sigma)=\tau}\sum_{\varphi(\sigma')=\tau'} r_\sigma s_{\sigma'}\right)\rho$$
$$= \sum_{\rho\in H}\left(\sum_{\varphi(\sigma)\varphi(\sigma')=\rho} r_\sigma s_{\sigma'}\right)\rho \;=\; \sum_{\rho\in H}\left(\sum_{\varphi(\sigma\sigma')=\rho} r_\sigma s_{\sigma'}\right)\rho$$
$$= \sum_{\rho\in H}\sum_{\varphi(\mu)=\rho}\left(\sum_{\sigma\sigma'=\mu} r_\sigma s_{\sigma'}\right)\rho \;=\; \varphi(\sum_{\mu\in G}\left(\sum_{\sigma\sigma'=\mu} r_\sigma s_{\sigma'}\right)\rho).$$

Falls φ injektiv ist, sieht man die Injektivität von $\hat{\varphi}$ wie folgt: Sei

$$\hat{\varphi}(\sum_{\sigma\in G} r_\sigma\sigma) = \sum_{\tau\in H}\left(\sum_{\varphi(\sigma)=\tau} r_\sigma\right)\tau = 0.$$

Die innere Summe im zweiten Term besteht wegen der Injektivität von φ aus höchstens einem Element. Dieses muß dann Null sein. Also ist jedes $r_\sigma = 0$.
Um die Surjektivität zu zeigen, wähle man sich zu jedem $\tau \in H$ genau ein $\sigma_\tau \in G$, für das $\varphi(\sigma_\tau) = \tau$ gilt. Ein Urbild zu $\sum s_\tau\,\tau \in RH$ ist $\sum s_\tau\sigma_\tau \in RG$. Damit ist Lemma 2 gezeigt.

QED.

In Gruppenringen können wir den Ring R und, falls R ein Ring mit Eins ist, die Gruppe G in RG wiederfinden. Und zwar mit der Einbettung

$$\begin{aligned} R &\hookrightarrow RG \\ r &\mapsto r\sigma_1 \end{aligned}$$

im ersten Fall und mit der Einbettung

$$\begin{aligned} G &\hookrightarrow RG \\ \sigma &\mapsto 1\sigma \end{aligned}$$

im zweiten Fall, wobei 1 die Eins in R und σ_1 das neutrale Element in G bezeichnen. Die Injektivität der Abbildungen ist offensichtlich. Die Einbettung von G ist dabei als Monomorphismus in die Einheitengruppe von RG zu interpretieren. Auf Grund dieser Einbettungen werden dann auch Elemente aus R und G als Elemente aus RG identifiziert. (Z.B. schreibt man 1 statt $1\sigma_1$ und $p - \sigma$ statt $p\sigma_1 - 1\sigma$, usw.)

Mit der Abbildung

$$\begin{array}{rcl} R \times RG & \rightarrow & RG \\ (r, \sum r_\sigma \sigma) & \mapsto & \sum r r_\sigma \sigma \end{array}$$

rechnet man sofort nach, daß RG die Eigenschaften eines R-Moduls hat. Jeder Gruppenring RG ist also als R-Modul interpretierbar.

Im weiteren Verlauf wird meistens $R = \mathbb{Z}$ der Ring der ganzen Zahlen sein. Zunächst betrachten wir allerdings $R = \mathbb{C}$, den Körper der komplexen Zahlen.

Lemma 4

Sei G eine Gruppe, $\mathbb{C}\,G$ die Gruppenalgebra zu $\mathbb{C}$ und G, und es sei χ ein abelscher Charakter von G, das heißt ein Homomorphismus von G in die multiplikative Gruppe von $\mathbb{C}$. Dann ist die Abbildung

$$\begin{array}{rccl} \hat{\chi}: & \mathbb{C}\,G & \rightarrow & \mathbb{C} \\ & \sum r_\sigma \sigma & \mapsto & \sum r_\sigma \chi(\sigma) \end{array}$$

ein Ringhomomorphismus. Zusätzlich ist $\hat{\chi}$ $\mathbb{C}$-linear, wenn $\mathbb{C}\,G$ als $\mathbb{C}$-Vektorraum aufgefaßt wird.

Es ist zu beachten, daß links eine formale Summe steht und im Unterschied dazu rechts eine Summe komplexer Zahlen. Normalerweise wird der von χ induzierte Homomorphismus ebenfalls mit χ (statt $\hat{\chi}$) bezeichnet, wenn die Gefahr der Verwechslung nicht besteht.
Die Einschränkung von $\hat{\chi}$ auf $\mathbb{Z}G$ bildet natürlich ebenfalls einen Homomorphismus.

Beweis

Die Additivität und $\mathbb{C}$-Linearität von $\hat{\chi}$ folgt sofort aus der Definition der Abbildung $\hat{\chi}$. Die Multiplikativität der Abbildung erhält man, wenn man die Relation

$$\begin{aligned} (\sum_{\sigma\in G} r_\sigma \chi(\sigma))(\sum_{\tau\in G} s_\tau \chi(\tau)) &= \sum_{\sigma\in G}\sum_{\tau\in G} r_\sigma \chi(\sigma) s_\tau \chi(\tau) \\ = \sum_{\sigma\in G}\sum_{\tau\in G} r_\sigma s_\tau \chi(\sigma\tau) &= \sum_{\rho\in G} \left(\sum_{\sigma\tau=\rho} r_\sigma s_\tau \right) \chi(\rho) \end{aligned}$$

benutzt, die nur eine Manipulation von Summen komplexer Zahlen unter Ausnutzung der Homomorphieeigenschaft von χ darstellt.

QED.

Lemma 4 erlaubt es, die Einheiten in $\mathbb{C}\,G$ zu charakterisieren, falls G eine abelsche Gruppe ist.

1.1.4 Einheiten in der Gruppenalgebra $\mathbb{C}\,G$

Ist $R = \mathbb{C}$ und G abelsch, so ist es möglich, die Einheiten in $\mathbb{C}\,G$ (das heißt die in $\mathbb{C}\,G$ invertierbaren Elemente) zu charakterisieren, nicht zuletzt weil der R-Modul dann sogar Vektorraum ist.

Satz 1 (Charakterisierung von Einheiten)
Sei G eine endliche abelsche Gruppe, $\mathbb{C}\,G$ die zugehörige Gruppenalgebra. Sei $g \in \mathbb{C}\,G$. Dann gelten folgende Aussagen:

a) *Wenn für jeden Charakter χ von G gilt, daß*

$$\chi(g) \neq 0$$

ist, so ist g invertierbar, also eine Einheit im Gruppenring $\mathbb{C}\,G$.

b) *Gilt für (mindestens) einen Charakter $\chi(g) = 0$, so ist g Nullteiler.*

c) *Gilt für alle Charaktere χ, daß $\chi(g) = 0$ ist, dann folgt $g = 0$.*

d) *Gilt für alle Charaktere χ, daß $\chi(g) = 1$ ist, dann folgt $g = 1$.*

Insbesondere folgt aus a und b, daß jede Nichteinheit in $\mathbb{C}\,G$ bereits Nullteiler ist.

Beweis

Aussage d ist eine direkte Folgerung aus c (es ist $0 = \chi(g) - 1 = \chi(g - 1)$ für jeden Charakter χ also $g - 1 = 0$).

Die Aussagen a-c werden zusammen bewiesen. Sei n die Dimension des Vektorraums $\mathbb{C}\,G$ als $\mathbb{C}$-Vektorraum. Da G, als Teilmenge von $\mathbb{C}\,G$ betrachtet, eine Basis des Vektorraums $\mathbb{C}\,G$ bildet, ist $n = \#G$, die Anzahl der Elemente der Gruppe G. Die Anzahl der Charaktere von G ist ebenfalls n, da die Charaktergruppe isomorph zur Gruppe ist (G ist nach Voraussetzung abelsch). Interpretiert man die Charaktere gemäß Lemma 4 als lineare Abbildungen des Vektorraum $\mathbb{C}\,G$, so hat man n lineare Abbildungen, die im Dualraum zu $\mathbb{C}\,G$ liegen. Zunächst wird gezeigt, daß diese eine Basis des Dualraums bilden. Dazu ist nur lineare Unabhängigkeit zu zeigen, da die Dimension des Dualraums gleich der Dimension des Vektorraums, also n, ist. Die lineare Unabhängigkeit zeigt man wie folgt (vgl. Lang, S. 209):

Ein Charakter ist offensichtlich linear unabhängig. Nimmt man an, die Charaktere wären linear abhängig, dann sei unter allen nichttrivialen Darstellungen

der Null die Darstellung

$$a_1\chi_1 + \cdots + a_\nu\chi_\nu = 0 \qquad (*)$$

mit paarweise verschiedenen Charakteren χ_i und $a_i \in \mathbb{C}$ eine mit minimalem ν. Es ist $\nu \geq 2$ und kein a_i ist gleich 0. Da $\chi_1 \neq \chi_2$ ist, gibt es ein $\tau \in G$, so daß $\chi_1(\tau) \neq \chi_2(\tau)$ ist. Für alle $\sigma \in G$ gilt so

$$a_1\chi_1(\sigma\tau) + \cdots + a_\nu\chi_\nu(\sigma\tau) = 0.$$

Da die χ_i Charaktere sind, erhält man

$$a_1\chi_1(\tau)\chi_1 + \cdots + a_\nu\chi_\nu(\tau)\chi_\nu = 0.$$

Dividiert man nun durch $\chi_1(\tau)$ und subtrahiert $(*)$, so hebt sich der Term $a_1\chi_1$ weg, und man erhält

$$\left(a_2\frac{\chi_2(\tau)}{\chi_1(\tau)} - a_2\right)\chi_2 + \cdots + \left(a_\nu\frac{\chi_\nu(\tau)}{\chi_1(\tau)} - a_\nu\right)\chi_\nu = 0.$$

Da $\chi_1(\tau) \neq \chi_2(\tau)$, ist der erste Koeffizient ungleich Null, und man hätte eine nichttriviale Darstellung der Null mit weniger als ν Charakteren. Das ist ein Widerspruch zur Minimalität von ν.

Um nun die Aussagen des Satzes zu zeigen, betrachte man zur Basis $\{\chi_1, \ldots, \chi_n\}$ die duale Basis in $\mathbb{C}G$, also eine Basis $\{g_1, \ldots, g_n\}$ mit der Eigenschaft

$$\chi_i(g_j) = \delta_{ij} := \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases} .$$

Jedes $g \in \mathbb{C}G$ hat zu dieser Basis die Darstellung

$$g = \sum_{i=1}^{n} \chi_i(g)g_i$$

(ist nämlich $g = \sum a_i g_i$, so erhält man

$$\begin{aligned} \sum_{i=1}^{n} \chi(g)g_i &= \sum_{i=1}^{n} \chi(\sum_{j=1}^{n} a_j g_j)g_i = \sum_{i=1}^{n}\sum_{j=1}^{n} a_j\chi_i(g_j)g_i \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_j\delta_{ij}g_i = \sum_{k=1}^{n} a_k g_k = g \ \ ). \end{aligned}$$

Aus dieser Darstellung folgt $g = 0$, wenn $\chi_i(g)$ für jeden Charakter χ_i verschwindet und somit Teil c des Satzes.

Für die Teile a und b berechnen wir zunächst die Darstellungsmatrix der linearen Abbildung

$$\begin{aligned} \Phi_g : \mathbb{C}G &\to \mathbb{C}G \\ h &\mapsto gh \end{aligned}$$

zur Basis $\{g_1, \ldots, g_n\}$, indem wir die Wirkung von Φ_g auf die g_j feststellen:

$$\Phi_g(g_j) \;=\; gg_j \;=\; \sum_{i=1}^{n} \chi_i(gg_j)g_i \;=\; \sum_{i=1}^{n} \chi_i(g)\chi_i(g_j)g_i \;=\; \chi_j(g)g_j.$$

Die Darstellungsmatrix von Φ_g hat also Diagonalgestalt mit den Elementen $\chi_1(g), \ldots, \chi_n(g)$ auf der Diagonalen. Die Determinante ist

$$\det\Phi_g = \prod_{i=1}^{n} \chi_i(u).$$

Ist jeder Faktor ungleich Null, so auch die Determinante, und Φ_g ist invertierbar, das heißt bijektiv. Insbesondere hat dann die 1 von $\mathbb{C}G$ (als Gruppenring) ein Urbild g_1. Mit diesem gilt

$$1 = \Phi_g(g_1) = gg_1,$$

g_1 ist also invers zu g, und Teil a folgt.

Ist mindestens ein $\chi(g) = 0$, so verschwindet auch die Determinante von Φ_g. Die Abbildung Φ_g hat also einen nichttrivialen Kern. Mit anderen Worten, es existiert ein $g_0 \neq 0$ mit $\Phi_g(g_0) = gg_0 = 0$. Damit folgt schließlich Teil b.

QED.

Korollar

Sei G eine endliche abelsche Gruppe, $g \in \mathbb{Z}G$. Es gelte $\chi(g) \neq 0$ für jeden Charakter χ von G. Ist

$$gh = 0,$$

so ist schon $h = 0$.

Beweis

Man betrachte die Einbettung von $\mathbb{Z}G$ in $\mathbb{C}G$ und multipliziere mit dem Inversen von g in $\mathbb{C}G$.

1.1.5 Die Augmentationsabbildung

In Abschnitt 1.1.3 wurde gezeigt, wie durch einen abelschen Charakter von G ein Homomorphismus des Gruppenringes in die komplexen Zahlen induziert wird.

Der triviale Charakter induziert dabei die Abbildung

$$\begin{array}{rccc} \text{aug}: & \mathbb{C}G & \to & \mathbb{C} \\ & \sum r_\sigma \sigma & \mapsto & \sum r_\sigma. \end{array}$$

Wie man sofort nachrechnen kann, ist diese Abbildung auch dann ein Homomorphismus, wenn man statt $\mathbb{C}$ einen beliebigen Ring nimmt.

Definition

Sei R ein Ring, G eine Gruppe, RG der Gruppenring zu R und G. Dann heißt der Homomorphismus

$$\begin{array}{rccc} \text{aug}: & RG & \to & R \\ & \sum r_\sigma \sigma & \mapsto & \sum r_\sigma \end{array}$$

Augmentationsabbildung.

Der Kern dieser Abbildung, das heißt die Menge der Elemente g aus RG mit $\text{aug}(g) = 0$, heißt das Augmentationsideal von RG. Es wird mit ΔRG bezeichnet.

Das Augmentationsideal läßt sich mit Hilfe des nachfolgenden Lemmas auch anders charakterisieren.

Lemma 5

Sei RG der Gruppenring zu R und G, und sei σ_1 das neutrale Element von G, dann gilt:

$$\Delta RG = \{g \in RG \mid g = \sum_{\sigma \in G \setminus \{\sigma_1\}} r_\sigma(\sigma - 1),\ r_\sigma \in R\}.$$

Beweis

" $\subseteq$ ": Ist $g = \sum r_\sigma \sigma$ und $\text{aug}(g) = 0$, so ist $\sum r_\sigma = 0$. Durch Subtraktion erhält man

$$r_{\sigma_1} = -\sum_{\sigma \in G \setminus \{\sigma_1\}} r_\sigma$$

und somit die eindeutige Darstellung

$$g = \sum_{\sigma \in G \setminus \{\sigma_1\}} r_\sigma \sigma - \sum_{\sigma \in G \setminus \{\sigma_1\}} r_\sigma = \sum_{\sigma \in G \setminus \{\sigma_1\}} r_\sigma(\sigma - 1).$$

" $\supseteq$ ": Wegen $\text{aug}(\sigma - 1) = 1 - 1 = 0$ für jedes $\sigma \in G$ gilt

$$\text{aug}(\sum_{\sigma \in G \setminus \{\sigma_1\}} r_\sigma(\sigma - 1)) = \sum_{\sigma \in G \setminus \{\sigma_1\}} r_\sigma \text{aug}(\sigma - 1) = 0.$$

QED.

1.1.6 Einige Bemerkungen über Einheiten im Gruppenring $\mathbb{Z}G$

Es sei G im folgenden immer abelsch. Die explizite Konstruktion von Einheiten in Gruppenringen $\mathbb{Z}G$ ist im allgemeinen schwierig. Man betrachte den durch einen Gruppencharakter χ induzierten Homomorphismus

$$\begin{array}{rccc} \chi: & \mathbb{Z}G & \to & \mathbb{C} \\ & \sum r_\sigma \sigma & \mapsto & \sum r_\sigma \chi(\sigma). \end{array}$$

Diese Abbildung schöpft $\mathbb{C}$ als Bildbereich bei weitem nicht aus. Ist nämlich $n = \#G$ die Anzahl der Elemente von G, so ist der Bildbereich höchstens $\mathbb{Z}[\epsilon_n]$, der Ganzheitsring des n-ten zyklotomischen Zahlkörpers (für jedes Gruppenelement σ gilt nach dem kleinen Fermatschen Satz $\sigma^n = \sigma_1$, somit $\chi(\sigma)^n = 1$). Je nach Struktur von G und χ ist der Bildbereich sogar nur ein Teilring von $\mathbb{Z}[\epsilon_n]$ (ist beispielsweise χ der triviale Charakter, so ist der Bildbereich $\mathbb{Z}$). Da χ Homomorphismus ist, wird jede Einheit aus $\mathbb{Z}G$ in eine Einheit aus $\chi(\mathbb{Z}G)$ abgebildet. Dies ist die Motivation gewesen, im Rahmen dieser Arbeit Einheiten in $\mathbb{Z}[\epsilon_n]$ zu untersuchen.

1.2 Rechnen in zyklotomischen Körpern

1.2.1 Automorphismen in zyklotomischen Zahlkörpern

Es sei n im folgenden eine beliebige, aber feste natürliche Zahl. Der zyklotomische Zahlkörper $\mathbb{Q}[\epsilon_n]$ ist der Zahlkörper, der entsteht, wenn man zu $\mathbb{Q}$ alle n-ten Einheitswurzeln adjungiert. Die Automorphismen von $\mathbb{Q}[\epsilon_n]$ sind gerade die Abbildungen, die primitive n-te Einheitswurzeln auf primitive n-te Einheitswurzeln abbilden. Bezeichnet ϵ_n eine feste primitive n-te Einheitswurzel, so sind dementsprechend die Automorphismen die Abbildungen

$$\begin{array}{rccc} \sigma_\nu: & \mathbb{Q}[\epsilon_n] & \to & \mathbb{Q}[\epsilon_n] \\ & \epsilon_n & \mapsto & \epsilon_n^\nu \\ & \sigma_\nu|_{\mathbb{Q}} & = & \mathrm{id}_{\mathbb{Q}}, \end{array}$$

wobei ν zu n teilerfremd ist.
Gilt $\nu \equiv \mu \bmod n$, so ist wegen

$$\epsilon_n^{\nu+rn} = \epsilon_n^\nu (\epsilon_n^n)^r = \epsilon_n^\nu$$

$\sigma_\nu = \sigma_\mu$. Zudem ist für zwei Automorphismen σ_ν und σ_μ

$$\sigma_\nu(\sigma_\mu(\epsilon_n)) = \sigma_{\nu\mu}(\epsilon_n).$$

Genauer gilt, daß die Automorphismengruppe des zyklotomischen Zahlkörpers $\mathbb{Q}[\epsilon_n]$ isomorph zu $(\mathbb{Z}/n\mathbb{Z})^*$ ist. Ein Beweis dieser fundamentalen Eigenschaft

der Kreisteilungskörper findet sich beispielsweise bei Washington, S. 11, Theorem 2.5. Die Automorphismengruppe wird von nun an mit G_n bezeichnet und mit $(\mathbb{Z}/n\mathbb{Z})^*$ identifiziert. Die Elemente aus G_n werden wie oben mit σ_ν bezeichnet.

1.2.2 Der Gruppenring der Automorphismen

Wir betrachten nun den Gruppenring $\mathbb{Z}G_n$ zum Ring der ganzen Zahlen und zur Automorphismengruppe G_n. Ein Element g dieses Gruppenrings hat die Darstellung

$$g = \sum_{\sigma_\nu \in G_n} a_{\sigma_\nu} \sigma_\nu.$$

Dies wird in der Regel geschrieben als

$$g = \sum_{\nu \in G_n} a_\nu \sigma_\nu,$$

um doppelte Indizes zu vermeiden (es wird also an manchen Stellen, an denen keine Verwechselungen auftreten können, ν statt σ_ν geschrieben).

Im folgenden sei $\mathbb{Q}[\epsilon_n]^* := \mathbb{Q}[\epsilon_n] \setminus \{0\}$.

Definition

Sei u aus $\mathbb{Q}[\epsilon_n]^*$ und $g = \sum a_\nu \sigma_\nu$ ein Element des Gruppenrings $\mathbb{Z}G_n$. Dann wird $u^g \in \mathbb{Q}[\epsilon_n]^*$ definiert durch

$$u^g = u^{\sum a_\nu \sigma_\nu} := \prod_\nu \sigma_\nu(u)^{a_\nu}.$$

Mit dieser Definition gelten die üblichen "Potenzgesetze", die in den nächsten beiden Lemmata bewiesen werden.

Lemma 1

Sei $g \in \mathbb{Z}G_n$. Die durch g induzierte Abbildung

$$\begin{array}{ccc} \mathbb{Q}[\epsilon_n]^* & \to & \mathbb{Q}[\epsilon_n]^* \\ u & \mapsto & u^g \end{array}$$

ist ein Endomorphismus der multiplikativen Gruppe von $\mathbb{Q}[\epsilon_n]$. Mit anderen Worten, zu $u, v \in \mathbb{Q}[\epsilon_n]^*$ gilt

$$(uv)^g = u^g v^g.$$

Beweis
Ist $g = \sum a_\nu \sigma_\nu$, so erhält man (unter Ausnutzung der Homomorphieeigenschaft der σ_ν)

$$(uv)^g = \prod_\nu \sigma_\nu(uv)^{a_\nu} = \prod_\nu (\sigma_\nu(u)^{a_\nu}\sigma_\nu(v)^{a_\nu}) = \prod_\nu \sigma_\nu(u)^{a_\nu} \prod_\nu \sigma_\nu(v)^{a_\nu} = u^g v^g.$$

QED. *Lemma 2*

Die Addition zweier Elemente des Gruppenrings entspricht der (punktweisen) Multiplikation zweier Endomorphismen, die Multiplikation entspricht der Hintereinanderausführung zweier Endomorphismen. In Formeln bedeutet das:

$$\begin{aligned} u^{g+h} &= u^g u^h \\ u^{gh} &= (u^g)^h \end{aligned}$$

für $u \in \mathbb{Q}[\epsilon_n]^*$ *und* $g, h \in \mathbb{Z}G_n$.
Beweis
Die Formeln ergeben sich wieder durch Einsetzen der Definition und Umsortieren von Faktoren. Setzt man $g = \sum a_\nu \sigma_\nu$ und $h = \sum b_\nu \sigma_\nu$, so folgt

$$u^{(g+h)} = u^{\sum (a_\nu + b_\nu)\sigma_\nu} = \prod \sigma_\nu(u)^{a_\nu + b_\nu} = \prod \sigma_\nu(u)^{a_\nu} \prod \sigma_\nu(u)^{b_\nu} = u^g u^h.$$

Weiter ist

$$(u^g)^h = \left(\prod_\nu \sigma_\nu(u)^{a_\nu}\right)^h = \prod_\mu \sigma_\mu \left(\prod_\nu \sigma_\nu(u)^{a_\nu}\right)^{b_\mu} = \prod_\mu \prod_\nu \sigma_\mu(\sigma_\nu(u))^{a_\nu b_\mu}.$$

Wegen $\sigma_\mu(\sigma_\nu(u)) = \sigma_{\mu\nu}(u)$ folgt schließlich

$$\begin{aligned} &\prod_\mu \prod_\nu \sigma_\mu(\sigma_\nu(u))^{a_\nu b_\mu} = \prod_\mu \prod_\nu \sigma_{\mu\nu} u^{a_\nu b_\mu} = \prod_\tau \left(\prod_{\mu\nu=\tau} \sigma_\tau(u^{a_\nu b_\mu})\right) \\ &= \prod_\tau \sigma_\tau(u)^{\sum_{\mu\nu=\tau} a_\nu b_\mu} = u^{\sum_\tau (\sum_{\mu\nu=\tau} a_\nu b_\mu)\sigma_\tau} = u^{hg} = u^{gh}, \end{aligned}$$

wobei zuletzt noch die Kommutativität von $\mathbb{Z}G_n$ ausgenutzt wurde.

QED.

Die folgende Definition und das dazugehörige Lemma zeigen, daß die Definition von u^g ebenfalls mit der Einbettung eines zyklotomischen Körpers in einen anderen verträglich ist.

Definition
Es sei d ein Teiler von n und $g = \sum a_\nu \sigma_\nu \in \mathbb{Z}G_n$. Dann werde $g(d) \in \mathbb{Z}G_d$ definiert durch

$$g(d) := \sum_{\mu \in G_d} (\sum_{\substack{\nu \in G_n, \\ \nu \equiv \mu \bmod d}} a_\nu) \sigma_\mu .$$

Man kann sich $g(d)$ als das Element in $\mathbb{Z}G_d$ vorstellen, das entsteht, indem in $g = \sum a_\nu \sigma_\nu$ alle σ_ν modulo d reduziert werden.
Mit dieser Definition gilt das folgende Lemma:

Lemma 3
Es sei d ein Teiler von n und u aus $\mathbb{Q}[\epsilon_d]^*$, so daß also $u \in \mathbb{Q}[\epsilon_d]^* \subseteq \mathbb{Q}[\epsilon_n]^*$ ist. Sei g aus $\mathbb{Z}G_n$. Dann gilt

$$u^g = u^{g(d)}.$$

Dabei wird u links als Element aus $\mathbb{Q}[\epsilon_n]^*$ und rechts als Element von $\mathbb{Q}[\epsilon_d]^*$ aufgefaßt.

Der Beweis ergibt sich direkt aus der Definition von $g(d)$.

Bemerkung
Mit obigen Bezeichnungen ist $g(1)$ gerade die Augmentationsabbildung. Nach Lemma 3 gilt also für $z \in \mathbb{Z}, z \neq 0$:

$$z^g = z^{\mathrm{aug}(g)}.$$

1.2.3 Die P-Teiler einer natürlichen Zahl

Nachfolgend spielen gewisse Teiler von n eine besondere Rolle. Diese Teiler werden als P-Teiler von n bezeichnet. Sie sind wie folgt definiert.

Definition
Sei $n \in \mathbb{N}$ durch

$$n = \prod_p p^{\alpha_p}$$

eindeutig in paarweise teilerfremde Primzahlpotenzen zerlegt. Ist $d \neq 1$ ein Teiler von n, dann heißt

$$t = \prod_{p|d} p^{\alpha_p}$$

der zu d gehörige P-Teiler von n.

Ist t zusätzlich Potenz einer Primzahl, so heißt t primer P-Teiler.

Der P-Teiler t enthält also als Faktoren genau diejenigen Primzahlen, die auch d als Faktoren hat. Jede Primzahl kommt allerdings in t mit der vollen Potenz vor, das heißt in der Potenz, mit der sie auch in n vorkommt.

Bemerkung

Jede natürliche Zahl n besitzt eine eindeutige Zerlegung

$$n = \prod_{i=1}^{k} q_i$$

in prime, paarweise teilerfremde P-Teiler q_i. Es gilt nach dem chinesischen Restsatz

$$G_n \cong \prod_{i=1}^{k} G_{q_i}.$$

Beispiel

Falls $n = 360 = 2^3 \cdot 3^2 \cdot 5$ ist, so sind die P-Teiler gerade 5, $8 = 2^3$, $9 = 3^2$, $40 = 2^3 \cdot 5$, $45 = 3^2 \cdot 5$, $72 = 2^3 \cdot 3^2$ und 360. Die *primen* P-Teiler sind 5, 8 und 9. Der beispielsweise zum Teiler 10 gehörige P-Teiler ist 40.

1.2.4 Rechnen mit Einheitswurzeln

Lemma 4

Sei ϵ_n eine feste primitive n-te Einheitswurzel. Es sei zu jedem Teiler d von n die primitive d-te Einheitswurzel ϵ_d definiert durch $\epsilon_d := \epsilon_n^{n/d}$. Es gilt:

a) *Ist dt ein Teiler von n, so ist*

$$\epsilon_{dt}^{t} = \epsilon_d.$$

b) *Sind zusätzlich t und d zueinander teilerfremd, so ist*

$$\epsilon_{dt} = \epsilon_d^{\sigma_t^{-1}} \; \epsilon_t^{\sigma_d^{-1}}.$$

Beweis

Teil a folgt direkt aus

$$\epsilon_{dt}^{t} = \epsilon_n^{\frac{nt}{dt}} = \epsilon_n^{n/d} = \epsilon_d.$$

Sind d und t teilerfremd, so existieren a und b aus $\mathbb{Z}$ mit

$$1 = bt + ad.$$

Dabei ist zusätzlich a zu d invers modulo t und umgekehrt b modulo d invers zu t. Es gilt

$$\epsilon_{dt} = \epsilon_{dt}^{bt+ad} = \epsilon_{dt}^{bt}\epsilon_{dt}^{ad} = \epsilon_d^b \epsilon_t^a = \epsilon_d^{\sigma_b}\epsilon_t^{\sigma_a},$$

und Teil b folgt.

QED.

Bemerkung

Aus Teil b des vorangehenden Lemmas folgt, daß, wenn d und t zueinander teilerfremd sind, sich jede primitive dt-te Einheitswurzel ϵ_{dt} als Produkt einer primitiven d-ten und einer primitiven t-ten Einheitswurzel ϵ_d beziehungsweise ϵ_t darstellen läßt. Bei geeigneter Wahl von ϵ_d und ϵ_t gilt also

$$\epsilon_{dt} = \epsilon_d \epsilon_t.$$

1.2.5 Elementare Relationen im Ring $\mathbb{Z}[\epsilon_n]$

Das System der zyklotomischen Einheiten wird im wesentlichen von Elementen der Form $1-\epsilon_d$ erzeugt werden. Wir wollen zunächst einige Relationen in $\mathbb{Z}[\epsilon_n]$ zur Verfügung stellen, um mit Ausdrücken dieser Art zu rechnen. Zunächst ein Lemma, das die Grundlage für die weiteren liefert:

Lemma 5

Es sei $q = p^\alpha$, p prim, $\hat{q} := p^{\alpha-1}$ und ϵ_q eine primitive q-te Einheitswurzel, η sei eine beliebige komplexe Zahl.
Dann gilt:

a)
$$\prod_{a\in G_q}(1-\eta\epsilon_q^a) = \frac{1-\eta^q}{1-\eta^{\hat{q}}} = \sum_{i=0}^{p-1}\eta^{\hat{q}i}$$

(ist im mittleren Term der Nenner gleich Null, so ist die Gleichung als Grenzwert für $1-\eta^{\hat{q}} \to 0$ aufzufassen).

b)
$$\prod_{a\in G_q}(1-\epsilon_q^a) = p.$$

c) *Ist ϵ_p eine primitive p-te Einheitswurzel, so gilt*

$$\prod_{a=0}^{p-1}(1-\eta\epsilon_p^a) = 1-\eta^p.$$

Beweis

Es durchläuft ϵ_q^a alle q-ten Einheitswurzeln, wenn a alle Werte zwischen 0 und $q-1$ durchläuft. Es gilt also die Polynomgleichheit

$$\prod_{a=0}^{q-1}(1-x\epsilon_q^a) = 1-x^q$$

(die Polynome haben die gleichen Nullstellen, und bei beiden ist der niedrigste Koeffizent 1). Für $q=p$ und Einsetzen von $x=\eta$ folgt Aussage c. Um ein Polynom zu erhalten, das als Nullstellen gerade die *primitiven* q-ten Einheitswurzeln hat, dividiert man durch ein Polynom, das als Nullstellen gerade die $\hat{q}$-ten Einheitswurzeln hat, also durch $1-x^{\hat{q}}$. So erhält man

$$\prod_{a\in G_q}(1-x\epsilon_q^a) = \frac{1-x^q}{1-x^{\hat{q}}} = \sum_{i=1}^{p-1} x^{\hat{q}i}.$$

Teil b folgt nun, indem man $x=1$ einsetzt (und den mittleren Term ignoriert). Teil a folgt durch Einsetzen von $x=\eta$.

QED.

Definition

Sei $n=td$, dann wird das Element $N_t \in \mathbb{Z}G_n$ definiert durch

$$N_t := \sum_{a\equiv 1 \bmod d} \sigma_a.$$

Lemma 6

Es sei $q=p^\alpha$ ein primer P-Teiler von n und $t\neq 1$ eine zu q teilerfremde natürliche Zahl, so daß qt ein Teiler von n ist. Dann gilt:

a) $(1-\epsilon_t\epsilon_q)^{N_q} = (1-\epsilon_t)^{\sigma_q(1-\sigma_p^{-1})}$.

b) $(1-\epsilon_q)^{N_q} = p$.

c) $(1-\epsilon_t)^{N_q} = (1-\epsilon_t)^{\phi(q)}$.

Dabei ist ϕ die Eulersche ϕ-Funktion, es ist also $\phi(q)=\#G_q$.

Beweis

Wir schreiben $n=qd$. Nach Definition des Elementes N_q ist

$$(1-\epsilon_t\epsilon_q)^{N_q} = \prod_{a\equiv 1 \bmod d}(1-\epsilon_t^a\epsilon_q^a).$$

Da $a\equiv 1 \bmod d$ und t ein Teiler von d ist, gilt $a\equiv 1 \bmod t$, und es ist $\epsilon_t^a=\epsilon_t$. Andererseits muß a wegen des Chinesischen Restsatzes jeden Wert modulo q

durchlaufen. Die Anwendung von Lemma 5, a ergibt

$$\prod_{a \in G_q} (1 - \epsilon_t \epsilon_q^a) \quad = \quad \frac{1 - \epsilon_t^q}{1 - \epsilon_t^{\hat{q}}},$$

und es folgt Teil a.

Teil b der Aussage folgt analog mit Hilfe von Lemma 5, b.

Teil c wird bewiesen durch Betrachtung von $N_q(d)$, also dem Element, das man erhält, wenn alle σ_ν modulo d reduziert werden. Es ist

$$N_q(d) = \sum_{a \equiv 1 \bmod d} 1 = \phi(q).$$

Es gilt schließlich mit Lemma 3

$$(1 - \epsilon_t)^{N_q} = (1 - \epsilon_t)^{N_q(d)} = (1 - \epsilon_t)^{\phi(q)}.$$

QED.

Lemma 7

Es sei $q = p^\alpha$ ein primer P-Teiler von n mit $\alpha \geq 2$. Sei t ein zu p teilerfremder Teiler von n und ϵ_{tp^β} eine primitive tp^β-te Einheitswurzel. Dann gilt:

$$(1 - \epsilon_{tp^\beta})^{N_p} = \begin{cases} 1 - \epsilon_{tp^\alpha}^p & \text{falls} \quad \beta = \alpha \\ (1 - \epsilon_{tp^\beta})^p & \text{falls} \quad \beta < \alpha \end{cases}.$$

Beweis

Wir schreiben $n = pd$. Dann sind $1 + 0d$, $1 + 1d$, $\ldots$, $1 + (p-1)d$ gerade die p Zahlen modulo n, die kongruent 1 modulo d sind. $\epsilon_{tp^\alpha}^d$ ist eine primitive p-te Einheitswurzel. Es folgt im Fall $\beta = \alpha$ nach Lemma 5, c

$$(1 - \epsilon_{tp^\alpha})^{N_p} = \prod_{a=0}^{p-1} (1 - \epsilon_{tp^\alpha}^{1+da}) \quad = \quad \prod_{a=0}^{p-1} (1 - \epsilon_{tp^\alpha} \epsilon_{tp^\alpha}^{da}) = 1 - \epsilon_{tp^\alpha}^p.$$

Im Fall $\beta < \alpha$ ist $\epsilon_{tp^\beta}^d = 1$, und man erhält

$$(1 - \epsilon_{tp^\beta})^{N_p} \quad = \quad \prod_{a=0}^{p-1} (1 - \epsilon_{tp^\beta}) = (1 - \epsilon_{tp^\beta})^p.$$

QED.

Lemma 8

Es seien d und t zwei Teiler von n, so daß $d|t$ gilt und zusätzlich jede Primzahl, die t teilt, auch d teilt (dies ist beispielsweise der Fall, wenn t der zu d gehörige P-Teiler ist). Seien ϵ_t und ϵ_d beliebige primitive t-te beziehungsweise d-te Einheitswurzeln. Dann existiert ein Element $M_{t,d}$ im Gruppenring $\mathbb{Z}G_n$, so daß

$$(1-\epsilon_t)^{M_{t,d}} = 1-\epsilon_d$$

gilt.

Beweis

Wir betrachten zunächst den Fall, daß $t/d = p$ Primzahl ist, ϵ_t^p ist dann eine primitive d-te Einheitswurzel. Sei σ_s ein Automorphismus von $\mathbb{Q}[\epsilon_t]$, der ϵ_t^p auf ϵ_d abbildet. Wir betrachten N_p als Element von $\mathbb{Z}G_t$ definiert. Sei $M'_{t,d} := \sigma_s N_p$. Es gilt mit Lemma 7:

$$(1-\epsilon_t)^{M'_{t,d}} = ((1-\epsilon_t)^{N_p})^{\sigma_s} = (1-\epsilon_t^p)^{\sigma_s} = 1-\epsilon_d.$$

Wir wählen nun $M_{t,d} \in \mathbb{Z}G_n$, so daß $M_{t,d}(t) = M'_{t,d}$ gilt.

Der allgemeine Fall ergibt sich nun durch wiederholte Betrachtung des obigen Falles. Man schreibt $t = p_1 \cdots p_k d$ mit Primzahlen p_ν und konstruiert sich sukzessive Elemente $M_1, \ldots, M_k \in \mathbb{Z}G_n$, für die jeweils

$$(1-\epsilon_{p_\nu \cdots p_k d})^{M_\nu} = (1-\epsilon_{p_{\nu+1}\cdots p_k d})$$

gilt. Mit $M_{t,d} := M_1 \cdots M_k$ folgt die Behauptung.

QED.

1.3 Das System der zyklotomischen Einheiten

Es bezeichne n im folgenden immer eine beliebige, aber feste natürliche Zahl.

Definition (vgl. Washington, S. 143)

Es bezeichne $U\mathbb{Z}[\epsilon_n]$ die Einheitengruppe von $\mathbb{Z}[\epsilon_n]$. Sei ϵ_n eine primitive n-te Einheitswurzel. Dann heißt

$$C^{(n)} := < \{\pm\epsilon_n, 1-\epsilon_n^a \mid a \in \mathbb{Z}\} > \cap\ U\mathbb{Z}[\epsilon_n]$$

die Gruppe der zyklotomischen Einheiten.

Ziel dieses Abschnittes ist es, ein Erzeugendensystem dieser Gruppe explizit anzugeben.

Lemma 1

Es sei d ein Teiler von n und ϵ_d eine primitive d-te Einheitswurzel. Dann gilt für ein $\nu \in \mathbb{Z}$, das zu n teilerfremd ist,

$$\frac{1-\epsilon_d^\nu}{1-\epsilon_d} \in C^{(n)}.$$

Beweis

Es ist $\epsilon_d = \epsilon_n^a$ für ein geeignetes $a \in \mathbb{Z}$. Wegen

$$\frac{1-\epsilon_d^\nu}{1-\epsilon_d} = \sum_{i=0}^{\nu-1} \epsilon_d^i \in \mathbb{Z}[\epsilon_n]$$

liegt dieses Element tatsächlich in $\mathbb{Z}[\epsilon_n]$. Sei nun $\mu \in \mathbb{Z}$, so daß μ invers zu ν modulo d ist, also $\mu\nu \equiv 1 \bmod d$ gilt. Da

$$\left(\frac{1-\epsilon_d^\nu}{1-\epsilon_d}\right)^{-1} = \frac{1-\epsilon_d}{1-\epsilon_d^\nu} = \frac{1-\epsilon_d^{\mu\nu}}{1-\epsilon_d^\nu} = \sum_{i=0}^{\mu-1} \epsilon_d^{\nu i} \in \mathbb{Z}[\epsilon_n]$$

ist, folgt die Behauptung.

QED.

Lemma 2

Sei d ein Teiler von n, aber keine Primzahlpotenz, und sei ϵ_d eine primitive d-te Einheitswurzel. Dann ist

$$1-\epsilon_d \in C^{(n)}.$$

Beweis

Es ist zu zeigen, daß $1-\epsilon_d$ in $\mathbb{Z}[\epsilon_n]$ invertierbar ist. Dazu schreibt man $d = qt$, wobei $q = p^\alpha$ ein primer P-Teiler von d ist und $\epsilon_d = \epsilon_q\epsilon_t$. Es folgt mit Hilfe von N_q (Lemma 6, a aus Abschnitt 1.2.5)

$$\prod_{\nu \in G_q} (1-\epsilon_t\epsilon_q^\nu) = (1-\epsilon_t\epsilon_q)^{N_q} = (1-\epsilon_t)^{\sigma_q(1-\sigma_p^{-1})} = \left(\frac{1-\epsilon_t^{\sigma_p^{-1}}}{1-\epsilon_t}\right)^{-\sigma_q},$$

also

$$\left(\frac{1-\epsilon_t^{\sigma_p^{-1}}}{1-\epsilon_t}\right)^{\sigma_q} (1-\epsilon_t\epsilon_q) \prod_{\nu \in G_q \setminus \{\sigma_1\}} (1-\epsilon_t\epsilon_q^\nu) = 1,$$

so daß das Inverse zu $1-\epsilon_d = 1-\epsilon_t\epsilon_q$ gerade

$$\left(\frac{1-\epsilon_t^{\sigma_p^{-1}}}{1-\epsilon_t}\right)^{\sigma_q} \prod_{\nu\in G_q\setminus\{\sigma_1\}} (1-\epsilon_t\epsilon_q^{\nu}) \in \mathbb{Z}[\epsilon_n]$$

ist.

Lemma 3

Ist $q=p^\alpha$ Primzahlpotenz und ϵ_q primitive q-te Einheitswurzel, so ist $1-\epsilon_q$ nie eine Einheit in $\mathbb{Z}[\epsilon_n]$.

Beweis

Wäre $1-\epsilon_q$ Einheit, so auch $(1-\epsilon_q)^{\sigma_\nu}$ für $\sigma_\nu \in G_q$ und schließlich auch

$$\prod_{\nu\in G_q} (1-\epsilon_q)^{\sigma_\nu} = (1-\epsilon_q)^{N_q}.$$

Nach Lemma 6, b des vorangegangenen Abschnitts ist $(1-\epsilon_q)^{N_q} = p$, und p ist sicher nicht in $\mathbb{Z}[\epsilon_n]$ invertierbar.

QED.

Lemma 4

Es sei $q=p^\alpha$ ein primer P-Teiler von n und ϵ_q eine primitive q-te Einheitswurzel. Ist

$$u = \prod_{\nu\in G_q} (1-\epsilon_q^{\nu})^{a_\nu} \in U\mathbb{Z}[\epsilon_n],$$

also invertierbar, dann hat u die Darstellung

$$u = \prod_{\nu\in G_q} \left(\frac{1-\epsilon_q^{\nu}}{1-\epsilon_q}\right)^{a_\nu}.$$

Beweis

Man schreibt

$$u = (1-\epsilon_q)^{\sum a_\nu} \prod_{\nu\in G_q} \left(\frac{1-\epsilon_q^{\nu}}{1-\epsilon_q}\right)^{a_\nu}.$$

Da $u \in U\mathbb{Z}[\epsilon_n]$ ist, und $\dfrac{1-\epsilon_q^{\nu}}{1-\epsilon_q} \in U\mathbb{Z}[\epsilon_n]$, muß auch $(1-\epsilon_q)^{\sum a_\nu} \in U\mathbb{Z}[\epsilon_n]$ sein. Nach dem vorangegangenem Lemma 3 ist $(1-\epsilon_q)^{\sum a_\nu}$ nur invertierbar, wenn $\sum a_\nu$ verschwindet, und die Behauptung folgt.

QED.

Da jedes Element aus $C^{(n)}$ ein Produkt von Elementen $1-\epsilon_d^\nu,\ \sigma_\nu \in G_d$, und $\pm\epsilon_n$ ist, kann man also ein Erzeugendensystem von $C^{(n)}$ explizit angeben.

Proposition

Die Gruppe $C^{(n)}$ der zyklotomischem Einheiten wird von den Elementen

$$\frac{1-\epsilon_q^\nu}{1-\epsilon_q} \quad \text{mit } q|n \text{ und } q \text{ ist Primzahlpotenz, } \sigma_\nu \in G_q,$$

$$1-\epsilon_d^\nu \quad \text{mit } 1<d|n \text{ und } d \text{ ist keine Primzahlpotenz, } \sigma_\nu \in G_d,$$

und $\pm\epsilon_n$ erzeugt.

Es wird nun zum Abschluß dieses Abschnittes gezeigt, daß man sich sogar nur auf die Betrachtung von P-Teilern beschränken kann.

Satz 2 (Erzeugendensystem von $C^{(n)}$)

Es sei T_n die Menge aller P-Teiler von n und $P_n \subset T_n$ die Menge aller primen P-Teiler. Das System der zyklotomischen Einheiten wird erzeugt durch die Menge

$$\begin{aligned} E^{(n)} := \quad & \{(1-\epsilon_t)^{\sigma_\nu} \mid t \in T_n \setminus P_n,\ \sigma_\nu \in G_t\} \\ \cup \quad & \{(1-\epsilon_q)^{\sigma_\nu - 1} \mid q \in P_n,\ \sigma_\nu \in G_q\} \\ \cup \quad & \{\pm\epsilon_n\}. \end{aligned}$$

Beweis

Es wird gezeigt, daß sich jedes Element aus der vorangegangenen Proposition durch Elemente aus $E^{(n)}$ darstellen läßt.

Sei $d \neq 1$ ein beliebiger Teiler von n und t der zu d gehörige P-Teiler von n. Es sei $\sigma_\nu \in G_t$ beliebig. Falls d keine Primzahlpotenz ist, so ist zu zeigen, daß

$$1-\epsilon_d^\nu$$

durch Elemente $1-\epsilon_t^\mu$, die aus $E^{(n)}$ sind, darstellbar ist.

Für jedes $g = \sum a_\mu \sigma_\mu \in \mathbb{Z}G_t$ wird das Element

$$(1-\epsilon_t)^g = \prod_{\mu \in G_t} (1-\epsilon_t^\mu)^{a_\mu}$$

durch $E^{(n)}$ erzeugt. Mit Lemma 8 aus dem Abschnitt über elementare Relationen (1.1.2) folgt, daß ein Element $M_{t,d} \in \mathbb{Z}G_t$ existiert, für das $(1-\epsilon_t)^{M_{t,d}} = 1-\epsilon_d$ ist. Es folgt schließlich

$$1-\epsilon_d^\nu = (1-\epsilon_t)^{\sigma_\nu M_{d,t}} \in < E^{(n)} > .$$

Ist d Primzahlpotenz, so ist zu zeigen, daß jedes Element der Form

$$\frac{1-\epsilon_d^\nu}{1-\epsilon_d}$$

durch $E^{(n)}$ erzeugt wird. Es gilt ähnlich dem obigen Fall für jedes $g \in \Delta\mathbb{Z}G_t$, daß $(1-\epsilon_t)^g$ im Erzeugnis von $E^{(n)}$ liegt. Denn jedes $g \in \Delta\mathbb{Z}G_t$ hat die Darstellung $g = \sum a_\mu(\sigma_\mu - 1)$ (Abschnitt 1.1.5, Lemma 5), so daß

$$(1-\epsilon_t)^g = \left(\prod_{\mu\neq 1}(1-\epsilon_t)^{\sigma_\mu - 1}\right)^{a_\mu}$$

ist. Mit $g = (\sigma_\nu - 1)M_{t,d} \in \Delta\mathbb{Z}G_t$ folgt

$$\frac{1-\epsilon_d^\nu}{1-\epsilon_d} = (1-\epsilon_d)^{\sigma_\nu - 1} = (1-\epsilon_t)^{(\sigma_\nu - 1)M_{t,d}} \in < E^{(n)} > .$$

QED.

2 Die Lemmata von Franz und Bass

2.1 Das Lemma von Franz

Das Lemma von Franz ist sowohl für das Lemma von Bass als auch für die Konstruktion des Einheitensystems von Ramachandra grundlegend. Der Beweis dieses Lemmas wird hier zunächst zurückgeführt auf das Nichtverschwinden der Dirichletschen L-Funktion. Für diese Tatsache finden sich in der Literatur verschiedene Beweise. Ein weiterer Beweis, der mit wenig Funktionentheorie auskommt und statt dessen Eigenschaften zyklotomischer Körper ausnutzt, befindet sich im Anhang A dieser Arbeit.

2.1.1 Der Führer eines Charakters modulo n

Zum Beweis des Lemmas von Franz werden Gaußsche Summen benutzt. Für diese ist der Begriff des Führers eines Charakters, wie er im folgenden definiert wird, grundlegend.

Sei χ ein Charakter modulo n, das heißt ein Homomorphismus von G_n in die multiplikative Gruppe des Körpers der komplexen Zahlen.

Es sei $\chi(a)$ für $a \in \mathbb{Z}, (a,n) = 1$ in üblicher Weise definiert als $\chi(\sigma_a)$.

Definition

Sei f die kleinste natürliche Zahl, die n teilt, so daß für alle zu n teilerfremden $b \in \mathbb{Z}$ gilt

$$b \equiv 1 \bmod f \Rightarrow \chi(b) = 1. \qquad (*)$$

Dann heißt f der Führer von χ mod n.

Da die Bedingung zumindest für $f = n$ gilt, ist die Existenz von f gesichert.

Lemma 1

Es gilt für $a, b \in \mathbb{Z}$, a und b teilerfremd zu n:

$$a \equiv b \bmod f \Rightarrow \chi(a) = \chi(b).$$

Beweis

Sei c das zu a Inverse modulo n, also $ca \equiv 1 \bmod n$. Es gilt wegen $f|n$, daß auch $ca \equiv 1 \bmod f$ ist. Man erhält so $cb \equiv ca \equiv 1 \bmod f$, und nach $(*)$ folgt $\chi(cb) = \chi(c)\chi(b) = 1$, also $\chi(b) = \chi(c)^{-1} = \chi(a)$, da a zu c modulo n invers ist.

QED.

Ziel ist es nun, χ als Charakter modulo dem Führer f zu betrachten. Insbesondere muß χ also auch auf jenen Zahlen definiert werden, die zwar teilerfremd zu f sind, aber einen gemeinsamen Teiler mit n haben.

Lemma 2

Sei $a \in \mathbb{Z}$, a teilerfremd zum Führer f. Man wähle ein $x \in \mathbb{Z}$, das zu n teilerfremd ist und für das

$$x \equiv a \bmod f$$

gilt. Definiert man χ auf a durch $\chi(a) := \chi(x)$, so ist χ Charakter mod f.

Beweis

Sind x und y zwei Zahlen mit $x \equiv a \bmod f$ und $y \equiv a \bmod f$, so ist $x \equiv y \bmod f$. Nach Lemma 1 gilt $\chi(x) = \chi(y)$. Auf dem erweiterten Definitionsbereich ist χ somit eine wohldefinierte Funktion. Daß χ auf dem erweiterten Definitionsbereich Homomorphismus ist, also Charakter modulo f, ist aus der Konstruktion offensichtlich.

QED.

Definition

Die Erweiterung des Definitionsbereiches eines Charakters gemäß Lemma 2 nennt man "χ als eigentlichen Charakter seines Führers betrachten".

Das folgende Lemma wird später beim Rechnen mit Gaußschen Summen benötigt werden.

Lemma 3

Sei χ ein Charakter modulo n mit Führer f. Sei d ein echter Teiler von f. Dann existiert ein zu f teilerfremdes $b \in \mathbb{Z}$ mit

$$b \equiv 1 \bmod d \qquad \textit{und} \qquad \chi(b) \neq 1.$$

Beweis

Sei d ein Teiler von f, für den kein solches b existiert. Mit diesem d folgt für alle zu f teilerfremden Zahlen b mit $b \equiv 1 \bmod d$, daß $\chi(b) = 1$ ist. Da f als Führer von χ minimal mit dieser Eigenschaft ist, gilt $f \leq d$, so daß d kein echter Teiler von f sein kann.

QED.

2.1.2 Gaußsche Summen

Das Bild eines Charakters modulo f ist immer eine $\phi(f)$-te Einheitswurzel, da $G_f = (\mathbb{Z}/f\mathbb{Z})^*$ eine Gruppe mit $\phi(f)$ Elementen ist. Andererseits ist G_f gerade die Galoisgruppe von $\mathbb{Q}[\epsilon_f]$, des kleinsten Körpers, der gerade die f-ten Einheitswurzeln enthält. Gaußsche Summen sind ein Hilfsmittel, um f-te und $\phi(f)$-te Einheitswurzeln miteinander zu verbinden.

Sei χ ein Charakter modulo n. Es werde χ als eigentlicher Charakter modulo seinem Führer f betrachtet. Weiter sei ϵ_f eine beliebige, aber feste primitive f-te Einheitswurzel.

Definition
Sei $a \in \mathbb{Z}$.

$$g_a(\chi) := \sum_{l \in G_f} \chi(l)\epsilon_f^{al}$$

heißt Gaußsche Summe.

Das nächste Lemma unterscheidet nun die Fälle, ob a teilerfremd zu f ist oder nicht.

Lemma 4
Es gilt:

a) $g_a(\chi) = 0$, *falls a und f einen gemeinsamen Teiler haben.*

b) $g_a(\chi) = \chi(a)^{-1} g_1(\chi)$, *falls* $(a, f) = 1$.

Beweis
Zu a: Da a und f einen gemeinsamen Teiler haben, existiert ein echter Teiler d von f, so daß $\epsilon_f^{ad} = 1$ ist. Nach Lemma 3 gibt es ein zu f teilerfremdes b mit $b \equiv 1 \bmod d$ und $\chi(b) \neq 1$. Schreibt man $b = 1 + md$ mit $m \in \mathbb{Z}$, so ist $\epsilon_f^{ab} = \epsilon_f^a(\epsilon_f^{ad})^m = \epsilon_f^a$. Nun substituiert man in der Summe

$$g_a(\chi) = \sum_{l \in G_f} \chi(l)\epsilon_f^{al} = \sum_{l \in G_f} \chi(l)\epsilon_f^{abl}$$

$k := bl$ (die Abbildung $x \mapsto bx$ ist ein Isomorphismus auf G_f) und erhält

$$g_a(\chi) = \sum_{k \in G_f} \chi(kb^{-1})\epsilon_f^{ak} = \chi^{-1}(b) \sum_{k \in G_f} \chi(k)\epsilon_f^{ak} = \chi^{-1}(b) g_a(\chi).$$

Wegen $\chi(b) \neq 1$ ist auch $\chi^{-1}(b) \neq 1$, also folgt $g_a(\chi) = 0$.
Zu b: Analog zum Beweis von a substituiert man jetzt $k := al$ und erhält

$$g_a(\chi) = \sum_{k \in G_f} \chi(ka^{-1})\epsilon_f^{k} = \chi^{-1}(a) g_1(\chi).$$

QED.

Lemma 5
Sei χ Charakter modulo seinem Führer f. Es gilt $|g_1(\chi)|^2 = f$. Insbesondere ist also $g_1(\chi) \neq 0$.

Beweis

Da $|\chi(a)| = 1$, gilt $\bar{\chi}(a) = \chi(a)^{-1}$ (der Querstrich bedeutet hier die komplexe Konjugation). Außerdem hat man $\overline{\epsilon_f^k} = \epsilon_f^{-k}$. Nach Lemma 4 ist $|g_1(\chi)|^2 = |g_a(\chi)|^2 = g_a(\chi)\bar{g_a}(\chi)$, falls a und f teilerfremd sind. Summiert man über alle möglichen $a \in \mathbb{Z}/f\mathbb{Z}$ auf und benutzt, daß $g_a(\chi) = 0$ für alle nicht zu f teilerfremden a ist, folgt

$$\begin{aligned}\phi(f)|g_1(\chi)|^2 &= \sum_{a=0}^{f-1} g_a(\chi)\bar{g_a}(\chi) \\ &= \sum_{a=0}^{f-1}(\sum_l \chi(l)\epsilon_f^{al} \sum_k \bar{\chi}(k)\epsilon_f^{-ak}) \\ &= \sum_{a=0}^{f-1}\sum_{l,k} \chi(l)\bar{\chi}(k)\epsilon_f^{al}\epsilon_f^{-ak} \\ &= \sum_{l,k} \chi(l)\bar{\chi}(k) \sum_{a=0}^{f-1} \epsilon_f^{a(l-k)}.\end{aligned}$$

Ist in der letzten Summe $l = k$, so ist die innere Summe gerade f. Ist andererseits $l \neq k$, so verschwindet die innere Summe (es gilt

$$\sum_{a=0}^{f-1} \epsilon_f^{a(l-k)} = \frac{\epsilon_f^{(l-k)f} - 1}{\epsilon_f^{l-k} - 1} = 0$$

wegen $\epsilon_f^{l-k} - 1 \neq 0$). Insgesamt wird also $\phi(f)$-mal f aufsummiert, da der Fall $l = k$ gerade $\phi(f)$-mal auftritt und die anderen Terme keinen Beitrag zur Summe liefern. Man hat schließlich

$$\phi(f)|g_1(\chi)|^2 = \phi(f)f,$$

und die Behauptung folgt.

QED.

Lemma 6

Sei χ jetzt auf ganz $\mathbb{Z}$ definiert durch die übliche Festsetzung $\chi(a) = 0$, falls a und f nicht teilerfremd sind. Für ein beliebiges $a \in \mathbb{Z}$ gilt dann

$$\bar{\chi}(a)g_1(\chi) = g_a(\chi),$$

mit anderen Worten

$$\bar{\chi}(a) = \frac{g_a(\chi)}{g_1(\chi)}.$$

Beweis
Nach Lemma 5 ist $g_1(\chi) \neq 0$. Für teilerfremdes a und f gilt so die Behauptung mit Lemma 4, b (es ist $\bar{\chi} = \chi^{-1}$). Sonst folgt sie, da beide Seiten gleich 0 sind.

QED.

2.1.3 Eine Darstellung der Dirichletschen L-Funktion im Punkte 1

Sei χ ein Charakter modulo n, als eigentlicher Charakter seines Führers f betrachtet. Wir definieren χ wie im vorhergehenden Abschnitt als Funktion über $\mathbb{Z}$ durch die Festlegung $\chi(a) := \chi(\sigma_a)$, falls a und f teilerfremd sind, und $\chi(a) = 0$ sonst.

Die Dirichletsche L-Funktion ist im Punkte 1 definiert durch die unendliche Reihe

$$\mathrm{L}(1, \chi) = \sum_{a=1}^{\infty} \frac{\chi(a)}{a}.$$

Daß diese Reihe tatsächlich konvergiert, wird im Anhang A, Lemma 1 gezeigt. Die folgende Darstellung dieser Reihe, die wir zum Beweis des Lemmas von Franz benötigen, findet sich bei Franz, S. 254 und geht ursprünglich auf E. Hecke zurück. *Lemma 7*

Sei χ ein gerader Charakter (das heißt, es gilt $\chi(\sigma_{-1}) = 1$), aber nicht der Hauptcharakter. Es werde χ als eigentlicher Charakter seines Führers f betrachtet. Es sei ϵ_f eine primitive f-te Einheitswurzel. Dann gilt für die Dirichletsche L*-Funktion*

$$\mathrm{L}(1, \bar{\chi}) \quad = \quad \frac{-1}{g_1(\chi)} \sum_{k \in G_f} \chi(k) \log |1 - \epsilon_f^k|.$$

Beweis
Wir betrachten zunächst den Logarithmus auf der rechten Seite. Allgemein hat man für den Hauptzweig des komplexen Logarithmus die Reihenentwicklung

$$\log(1 - x) = -\sum_{a=1}^{\infty} \frac{x^a}{a},$$

falls x im Inneren des Einheitskreises liegt. Liegt x auf dem *Rand* des Einheitskreises, wie es der Fall ist, wenn $x = \epsilon_f$ Einheitswurzel ist, so gilt die Entwicklung nach dem Abelschen Grenzwertsatz (vgl. Endl/Luh, S. 179) immer noch, wenn $x \neq 1$ ist (das heißt, die Reihe konvergiert auch in diesem Fall). Die Additionstheoreme sind jedoch für komplexes Argument nicht mehr so gültig, wie man es vom reellen her gewohnt ist. Es gilt nur noch $\log(x) + \log(y) =$

$\log(xy) + 2\pi im$ für ein geeignetes, von x und y abhängiges $m \in \mathbb{Z}$. Man erhält, da $(1-\epsilon_f^k)(1-\epsilon_f^{-k}) = |1-\epsilon_f^k|^2$ ist,

$$\begin{aligned} 2\log|1-\epsilon_f^k| &= \log|1-\epsilon_f^k|^2 = \log\Big((1-\epsilon_f^k)(1-\epsilon_f^{-k})\Big) \\ &= 2\pi im + \log(1-\epsilon_f^k) + \log(1-\epsilon_f^{-k}) = 2\pi im - \sum_{a=1}^{\infty}\frac{\epsilon_f^{ak}}{a} - \sum_{a=1}^{\infty}\frac{\epsilon_f^{-ak}}{a} \end{aligned}$$

mit irgendeiner ganzen Zahl m. Es sind ϵ_f^{-k} und ϵ_f^k zueinander komplex konjugiert. Also ist

$$\sum_{a=1}^{\infty}\frac{\epsilon_f^{ak}}{a} + \sum_{a=1}^{\infty}\frac{\epsilon_f^{-ak}}{a} \quad = \quad \sum_{a=1}^{\infty}\frac{\epsilon_f^{ak}+\epsilon_f^{-ak}}{a}$$

reell, da $\epsilon_f^{ak} + \epsilon_f^{-ak}$ reell ist. Es folgt

$$2\pi im = \sum_{a=1}^{\infty}\frac{\epsilon_f^{ak}+\epsilon_f^{-ak}}{a} + 2\log|1-\epsilon_f^k| \in \mathbb{R},$$

also $m = 0$, und man erhält

$$-2\log|1-\epsilon_f^k| = \sum_{a=1}^{\infty}\frac{\epsilon_f^{ak}}{a} + \sum_{a=1}^{\infty}\frac{\epsilon_f^{-ak}}{a}. \qquad (*)$$

Sei nun $M \in \mathbb{N}$ beliebig. Mit $\mathrm{L}^M(1,\chi)$ sei die endliche Summe

$$\mathrm{L}^M(1,\chi) \quad = \quad \sum_{a=1}^{M}\frac{\chi(a)}{a}$$

bezeichnet.

Setzt man gemäß Lemma 6 aus Abschnitt 2.1.2 über Gaußsche Summen

$$\bar{\chi}(a) = \frac{g_a(\chi)}{g_1(\chi)},$$

wobei $g_a(\chi) = \sum\limits_{k\in G_f}\chi(k)\epsilon_f^{ak}$ war, erhält man

$$\begin{aligned} \mathrm{L}^M(1,\bar{\chi}) &= \frac{1}{g_1(\chi)}\sum_{a=1}^{M}\frac{g_a(\chi)}{a} = \frac{1}{g_1(\chi)}\sum_{a=1}^{M}\sum_{k\in G_f}\frac{\chi(k)\epsilon_f^{ak}}{a} \\ &= \frac{1}{g_1(\chi)}\sum_{k\in G_f}\chi(k)\sum_{a=1}^{M}\frac{\epsilon_f^{ak}}{a}. \end{aligned}$$

Da wir für den Charakter $\chi(\sigma_{-1}) = 1$ (und damit $\chi(k) = \chi(-k)$) vorausgesetzt haben, gilt, wenn man $-k$ statt k einsetzt,

$$\mathrm{L}^M(1, \bar{\chi}) = \frac{1}{g_1(\chi)} \sum_{k \in G_f} \chi(k) \sum_{a=1}^{M} \frac{\epsilon_f^{-ak}}{a}.$$

Faßt man dies zusammen, ergibt sich

$$2\mathrm{L}^M(1, \bar{\chi}) \quad = \quad \frac{1}{g_1(\chi)} \sum_{k \in G_f} \chi(k) \left(\sum_{a=1}^{M} \frac{\epsilon_f^{ak}}{a} + \sum_{a=1}^{M} \frac{\epsilon_f^{-ak}}{a} \right).$$

Mit $M \to \infty$ und $(*)$ folgt die Behauptung.

QED.

2.1.4 Formulierung und Beweis des Lemmas von Franz

Das folgende Lemma ist etwas allgemeiner als das Lemma in der Originalfassung (vgl. Franz, S. 253).

Lemma von Franz

Mit ϵ_d seien beliebige, aber feste primitive d-te Einheitswurzeln bezeichnet. Gelten für ein $g = \sum a_\nu \sigma_\nu \in \mathbb{Z}G_n$ die Voraussetzungen

$$\begin{aligned} a_\nu &= a_{-\nu} && \text{für alle } \sigma_\nu \in G_n, \\ (1 - \epsilon_d)^g &= 1 && \text{für alle P-Teiler } d \text{ von } n, \end{aligned}$$

dann folgt $g = 0$, das heißt $a_\nu = 0$ für alle σ_ν.

Franz fordert zusätzlich $\sum a_\nu = 0$ und $(1 - \epsilon_d)^g = 1$ für *alle* Teiler d von n. Diese Bedingungen sind, wie wir unten sehen werden, redundant. Ansonsten folgt der Beweis im wesentlichen dem Beweis des Lemmas im Original.

Beweis

Zunächst wird hier die Behauptung des Lemmas auf das Nichtverschwinden der Dirichletschen L-Funktion im Punkte 1 zurückgeführt. Ein Beweis dieser in der Zahlentheorie öfter verwendeten Tatsache befindet sich im Anhang A.

Nach Teil c des Satzes über die Charakterisierung von Einheiten in Gruppenringen (Satz 1) genügt es zu zeigen, daß $\chi(g) = 0$ für jeden Character χ von G_n gilt.

Zunächst wird dies für den Hauptcharakter gezeigt. Das heißt, es ist zu zeigen, daß $\mathrm{aug}(g) = \sum a_\nu = 0$ gilt. Sei dazu $q = p^\alpha$ ein primer P-Teiler von n. Dann

gilt nach Voraussetzung $(1-\epsilon_q)^g = 1$. Darauf wenden wir das Element N_q an, und es gilt mit Lemma 6, b aus dem Abschnitt 1.2.5 über elementare Relationen

$$1 = (1-\epsilon_q)^{gN_q} = ((1-\epsilon_q)^{N_q})^g = p^g = p^{\mathrm{aug}(g)},$$

also $p^{\mathrm{aug}(g)} = 1$ und somit $\mathrm{aug}(g) = 0$.

Falls für einen Charakter $\chi(\sigma_{-1}) = -1$ gilt, so ist $\chi(\sigma_\nu) = -\chi(\sigma_{-\nu})$. Für einen solchen Charakter ist $\sum a_\nu \chi(\sigma_\nu) = 0$ auf Grund der Voraussetzung $a_\nu = a_{-\nu}$.

Sei also $\chi(\sigma_{-1}) = 1$ und χ nicht der Hauptcharakter. Wir betrachten χ als eigentlichen Charakter seines Führers f. Sei $g(f) = \sum b_\mu \sigma_\mu$, so daß also $b_\mu = \sum\limits_{\nu \equiv \mu \bmod f} a_\nu$ ist. Dann gilt

$$\chi(g) = \sum_{\nu \in G_n} a_\nu \chi(\sigma_\nu) = \sum_{\mu \in G_f} \sum_{\nu \equiv \mu \bmod f} a_\nu \chi(\sigma_\mu) = \sum_{\mu \in G_f} b_\mu \chi(\sigma_\mu) = \chi(g(f)).$$

Es ist $\chi(g(f)) = 0$ zu zeigen. Dazu beweisen wir zunächst

$$\prod_{\mu \in G_f} (1-\epsilon_f^{l\mu})^{b_\mu} = 1 \qquad (*)$$

für alle $\sigma_l \in G_f$:

Es sei d der zu f gehörige P-Teiler von n. Mit dem in Abschnitt 1.2.5, Lemma 8 konstruierten Element $M_{d,f}$, für das $(1-\epsilon_d)^{M_{d,f}} = 1-\epsilon_f$ gilt, ist

$$1 = (1-\epsilon_d)^{gM_{d,f}\sigma_l} = (1-\epsilon_f^l)^g = (1-\epsilon_f^l)^{g(f)} = \prod_{\mu \in G_f} (1-\epsilon_f^{l\mu})^{b_\mu},$$

und $(*)$ folgt.

Bildet man Beträge und logarithmiert die Gleichung $(*)$, so erhält man

$$\sum_{\mu \in G_f} b_\mu \log|1-\epsilon_f^{\mu l}| = 0$$

und somit auch

$$\sum_{l \in G_f} \bar{\chi}(\sigma_l) \sum_{\mu \in G_f} b_\mu \log|1-\epsilon_f^{\mu l}| = \sum_{\mu \in G_f} b_\mu \sum_{l \in G_f} \bar{\chi}(\sigma_l) \log|1-\epsilon_f^{\mu l}| = 0.$$

Mit der Substitution $k := \mu l$, also $\sigma_l = \sigma_\mu^{-1}\sigma_k$, folgt

$$\sum_{\mu \in G_f} b_\mu \sum_{k \in G_f} \bar{\chi}(\sigma_\mu^{-1}\sigma_k) \log|1-\epsilon_f^k|$$

$$= \left(\sum_{\mu \in G_f} b_\mu \bar{\chi}(\sigma_\mu^{-1})\right) \left(\sum_{k \in G_f} \bar{\chi}(\sigma_k) \log|1-\epsilon_f^k|\right) \quad = \quad 0,$$

und wegen $\bar{\chi}(\sigma_\mu^{-1}) = \chi(\sigma_\mu)$ ergibt sich

$$\chi(g(f)) \left(\sum_{k \in G_f} \bar{\chi}(\sigma_k) \log |1 - \epsilon_f^k| \right) \quad = \quad 0.$$

Nach Lemma 7 gilt für den zweiten Faktor die Darstellung

$$\sum_{k \in G_f} \bar{\chi}(\sigma_k) \log |1 - \epsilon_f^k| \quad = \quad -g_1(\bar{\chi}) \mathrm{L}(1, \chi) \; \neq \; 0$$

mit der Gaußschen Summe $g_1(\bar{\chi})$ und der Dirichletschen L-Funktion $\mathrm{L}(1, \chi)$, die beide ungleich Null sind (Lemma 5 in Abschnitt 2.1.1 und Satz 8 in Anhang A). Es folgt, daß der erste Faktor verschwindet, also $\chi(g(f)) = 0$.

QED.

2.1.5 Das Ideal $\mathbb{Z}G_n^+$

Definition
Sei $\mathbb{Z}G_n$ der Gruppenring zu $\mathbb{Z}$ und G_n. Dann heißt

$$\mathbb{Z}G_n^+ := (1 + \sigma_{-1})\mathbb{Z}G_n$$

das symmetrische Ideal von $\mathbb{Z}G_n$.

Lemma 8
Im Fall $n > 2$, also im Fall, daß 1 und σ_{-1} verschieden sind, gilt für ein $g = \sum a_\nu \sigma_\nu \in \mathbb{Z}G_n$:

$$g \in \mathbb{Z}G_n^+ \quad \Leftrightarrow \quad a_\nu = a_{-\nu}.$$

Beweis
Es gilt für $h = \sum b_\nu \sigma_\nu \in \mathbb{Z}G_n$ beliebig

$$(1 + \sigma_{-1})h = \sum (b_\nu + b_{-\nu})\sigma_\nu.$$

Da $b_\nu + b_{-\nu} = b_{-\nu} + b_\nu$ ist, folgt "$\Rightarrow$". Hat man umgekehrt $g = \sum a_\nu \sigma_\nu \in \mathbb{Z}G_n$ mit $a_\nu = a_{-\nu}$, so schreibt man

$$g = (1 + \sigma_{-1}) \sum_{\substack{0 < \nu < n/2 \\ (\nu, n) = 1}} a_\nu \sigma_\nu,$$

und es folgt "$\Leftarrow$".

QED.

Mit dieser Definition und Lemma 8 liest sich das Lemma von Franz wie folgt:
Lemma von Franz (alternative Formulierung)
Es sei $g \in \mathbb{Z}G_n^+$, und es gelte für alle P-Teiler d von n

$$(1 - \epsilon_d)^g = 1,$$

so ist $g = 0$.
Korollar
Sei $g = \sum a_\nu \sigma_\nu \in \mathbb{Z}G_n$ beliebig, und es gelte für alle P-Teiler d von n

$$(1 - \epsilon_d)^g = 1,$$

so ist $(1 + \sigma_{-1})g = 0$, das heißt, für alle $\sigma_\nu \in G_n$ gilt $a_\nu = -a_{-\nu}$.
Beweis
Mit $(1 - \epsilon_d)^g = 1$ ist auch $(1 - \epsilon_d)^{(1+\sigma_{-1})g} = 1$. Da

$$(1 + \sigma_{-1})g = (1 + \sigma_{-1}) \sum a_\nu \sigma_\nu = \sum (a_\nu + a_{-\nu})\sigma_\nu$$

ist, folgt nach dem Lemma von Franz $a_\nu + a_{-\nu} = 0$, also $a_\nu = -a_{-\nu}$.

QED.

2.1.6 Skizze einer Anwendung des Lemmas von Franz auf Gruppenringe mit zyklischer Gruppe

Es sei $C_n =< x >$ die von x erzeugte zyklische Gruppe der Ordnung n und $\mathbb{Z}C_n$ der Gruppenring zu $\mathbb{Z}$ und C_n. Die Gruppe der Einheiten von $\mathbb{Z}C_n$ sei mit $U\mathbb{Z}C_n$ bezeichnet. Man definiert ganz analog, wie wir es für den Ring $\mathbb{Z}[\epsilon_n]$ getan haben (vgl. Abschnitt 1.2.2), zur Einheit $u = \sum r_\mu x^\mu \in U\mathbb{Z}C_n$ und zu $g = \sum a_\nu \sigma_\nu \in \mathbb{Z}G_n$ die Bezeichnungsweise

$$u^g := \prod_{\nu \in G_n} \left(\sum_{\mu=0}^{n-1} r_\mu x^{\mu\nu} \right) \in U\mathbb{Z}C_n.$$

Man rechnet nach, daß mit dieser Definition die gleichen "Potenzgesetze" gelten, wie sie im Ring $\mathbb{Z}[\epsilon_n]$ hergeleitet wurden.
Ist w eine Einheit in $\mathbb{Z}C_n$, so ist die Abbildung

$$\begin{array}{rccc} \kappa_w : & \Delta\mathbb{Z}G_n^+ & \to & U\mathbb{Z}C_n \\ & g & \mapsto & w^g \end{array}$$

ein Homomorphismus von der additiven Gruppe $\Delta\mathbb{Z}G_n^+$ in die Einheitengruppe $U\mathbb{Z}C_n$ (dabei bezeichnet $\Delta\mathbb{Z}G_n^+$ alle Elemente aus $\mathbb{Z}G_n^+$ mit Augmentation

0). Für einen Teiler d von n bezeichne χ_d den Charakter von C_n, der x auf ϵ_d abbildet. Gilt für w zusätzlich

$$\chi_d(w) = (1 - \epsilon_d)^h$$

(dabei darf h nicht von d abhängen), so kann man Aussagen über die Injektivität von κ_w machen. Ist nämlich $\kappa_w(g) = 1$ für ein $g \in \Delta\mathbb{Z}G_n^+$, so ist

$$(1 - \epsilon_d)^{hg} = 1$$

für jeden Teiler d von n, und mit dem Lemma von Franz folgt $hg = 0$. Ist h in $\Delta\mathbb{Z}G_n^+$ kein Nullteiler, so folgt $g = 0$, und die Abbildung κ_w ist in diesem Fall injektiv.

Zum Schluß dieses Abschnitts wird nach einer Methode von Klaus Hoechsmann explizit ein solches $w \in \mathbb{Z}C_n$ konstruiert. Es werden anschließend Bedingungen für das zugehörige h herausgearbeitet, unter denen h kein Nullteiler in $\Delta\mathbb{Z}G_n^+$ ist.

Wir können uns das Rechnen im Gruppenring $\mathbb{Z}C_n$ so vorstellen, als ob wir im Polynomring $\mathbb{Z}[x]$ rechnen mit der zusätzlichen Relation $x^n = 1$.

Es sei $f_b(x)$ für $b \in \mathbb{N}$ definiert durch

$$f_b(x) = \sum_{i=0}^{b-1} x^i.$$

Für jedes $b, c \in \mathbb{N}$ und $g \in \mathbb{Z}C_n$ gilt

$$\begin{aligned} f_b(x) f_c(x^b) &= f_{bc}(x), \\ g f_n(x) &= \mathrm{aug}(g) f_n(x). \end{aligned}$$

Seien nun b und c so gewählt, daß c invers zu b modulo n ist, so daß also ein $k \in \mathbb{Z}$ existiert mit $cb = 1 + kn$. Es folgt

$$f_b(x) f_c(x^b) = f_{bc}(x) = 1 + \sum_{i=1}^{kn} x^i = 1 + k f_n(x).$$

Die Einheit w_b wird definiert durch

$$w_b := f_c(x) f_b(x) - k f_n(x). \qquad (*)$$

Das Inverse zu w_b ist

$$w_b^{-1} = f_c(x^b) f_b(x^c) - k f_n(x),$$

wie man folgendermaßen nachrechnet:

$$\begin{aligned} w_b w_b^{-1} &= (f_c(x)f_b(x) - kf_n(x))(f_c(x^b)f_b(x^c) - kf_n(x)) \\ &= f_c(x)f_b(x^c)f_b(x)f_c(x^b) - f_c(x)f_b(x)kf_n(x) \\ &\quad -f_c(x^b)f_b(x^c)kf_n(x) + k^2 f_n(x)f_n(x) \\ &= (1+kf_n(x))(1+kf_n(x)) - cbkf_n(x) - cbkf_n(x) + k^2 nf_n(x) \\ &= (1+kf_n(x))(1+kf_n(x)) - 2(1+kn)kf_n(x) + k^2 nf_n(x) \\ &= 1 + 2kf_n(x) + nk^2 f_n(x) - 2kf_n(x) - 2k^2 nf_n(x) + k^2 nf_n(x) = 1. \end{aligned}$$

Das zu diesem w_b gehörige h wird wie folgt hergeleitet. Sei $d \neq 1$ ein Teiler von n. Der Charakter χ_d ordnet x gerade eine primitive d-te Einheitswurzel zu. Für ein $a \in \mathbb{N}$ ist

$$\chi_d(f_a(x)) = \sum_{i=0}^{a-1} \epsilon_d^i = \frac{1-\epsilon_d^a}{1-\epsilon_d},$$

so daß

$$\chi_d(f_b(x)) = (1-\epsilon_d)^{(\sigma_b - 1)}$$

und

$$\chi_d(f_n(x)) = 0$$

gilt. Es folgt

$$\chi_d(w_b) = \chi_d(f_b(x))\chi_d(f_c(x)) - k\chi_d(f_n(x)) = (1-\epsilon_d)^{(\sigma_b-1)(\sigma_c-1)}.$$

Somit ist $h = (\sigma_b - 1)(\sigma_c - 1)$.

Es ist jetzt zu klären, wie b gewählt werden muß, damit $g = 0$ folgt, falls $g \in \Delta\mathbb{Z}G_n^+$ und $gh = 0$ ist (also κ_w injektiv ist). Wir werden dazu Teil c des Satzes über die Charakterisierung von Einheiten (Abschnitt 1.1.4) anwenden, der besagt, daß genau dann $g = 0$ ist, wenn $\chi(g)$ für jeden Charakter χ von G_n verschwindet. (Man muß hier Charaktere χ von G_n unterscheiden von Charakteren χ_d von C_n!) Sei also χ ein beliebiger Charakter auf der Gruppe G_n. Da b und c modulo n invers sind, ist $\chi(\sigma_b) = 1$ genau dann, wenn $\chi(\sigma_c) = 1$ ist. Im Falle $\chi(\sigma_b) \neq 1$ folgt dementsprechend

$$\chi(h) = (\chi(\sigma_b) - 1)(\chi(\sigma_c) - 1) \neq 0.$$

Und es gilt für einen solchen Charakter

$$\chi(gh) = 0 \Rightarrow \chi(g)\chi(h) = 0 \Rightarrow \chi(g) = 0.$$

Ist χ der Hauptcharakter oder gilt $\chi(\sigma_{-1}) = -1$, so ist $\chi(g) = 0$, da $g \in \Delta\mathbb{Z}G_n^+$ ist. Wir wollen dies in einem Satz zusammenfassen.

Satz 3 (Injektivität von κ_w)
Seien $n \in \mathbb{N}$ und $\sigma_b \in G_n$. Es gelte für jeden Charakter χ von G_n eine der drei folgenden Bedingungen a,b oder c:

a) $\chi \equiv 1$, *das heißt χ ist Hauptcharakter,*

b) $\chi(\sigma_{-1}) = -1$,

c) $\chi(\sigma_b) \neq 1$.

Sei nun zu diesem b eine Einheit $w := w_b \in U\mathbb{Z}C_n$ gemäß $(*)$ konstruiert. Dann ist die Abbildung

$$\begin{array}{rccc} \kappa_w : & \Delta\mathbb{Z}G_n^+ & \to & U\mathbb{Z}C_n \\ & g & \mapsto & w^g \end{array}$$

injektiv.
Umgekehrt ist κ nicht injektiv, falls es einen Charakter χ von G_n gibt, der keine der Bedingungen a-c erfüllt.

Beweis
Es bleibt nach dem oben Gesagten die Umkehrung des Satzes zu zeigen. Sei $\hat{\chi}$ ein Charakter für den keine der Bedingungen a-c gilt. Das heißt, es ist für ein geeignetes $\sigma_a \in G_n$

a) $\hat{\chi}(\sigma_a) \neq 1$, da $\hat{\chi}$ nicht der Hauptcharakter ist,

b) $\hat{\chi}(\sigma_{-1}) = 1$,

c) $\hat{\chi}(\sigma_b) = 1$.

Sei nun $m \in \mathbb{N}$, so daß $\sigma_b^m = 1$ gilt (zum Beispiel $m = \phi(n)$). Dann wird g definiert durch

$$g := (1 + \sigma_{-1})(\sigma_a - \sigma_b) \sum_{i=0}^{m-1} \sigma_b^i \ \in \ \Delta\mathbb{Z}G_n^+.$$

Es ist $g \neq 0$, da

$$\begin{array}{rccccc} \hat{\chi}(g) = & \hat{\chi}(1 + \sigma_{-1}) & \hat{\chi}(\sigma_a - \sigma_b) & \hat{\chi}(\sum_{i=0}^{m-1} \sigma_b^i) & \\ = & 2 & (\hat{\chi}(\sigma_a) - 1) & m & \neq 0. \end{array}$$

Andererseits ist $gh = 0$, da

$$(\sigma_b - 1) \sum_{i=0}^{m-1} \sigma_b^i = \sum_{i=0}^{m-1} (\sigma_b^{i+1} - \sigma_b^i) = \sigma_b^m - 1 = 0$$

ist. Für jeden Charakter χ_d von C_n gilt daher

$$\chi_d(w^g) = (1-\epsilon_d)^{hg} = (1-\epsilon_d)^0 = 1,$$

und nach dem Satz über die Charakterisierung von Einheiten in Gruppenringen, Teil d, folgt $w^g = 1$, also $\kappa(g) = w^g = 1$. Da g ungleich Null ist, kann κ nicht injektiv sein.

QED.

Es stellt sich schließlich die Frage, ob überhaupt $\sigma_b \in G_n$ existieren, so daß κ_w injektiv ist. Ist $n = p^\alpha$ oder $n = 2p^\alpha$ mit einer Primzahl p, so kann σ_b so gewählt werden, daß σ_b eine Primitivwurzel (also ein Erzeuger) von G_n ist. Mit dieser Wahl folgt aus $\chi(\sigma_b) = 1$, daß χ der Hauptcharakter ist. Es ist also für jeden Charakter eine der Bedingungen a oder c erfüllt.

Im allgemeinen Fall ist es hinreichend, daß G_n von den Elementen σ_b und σ_{-1} erzeugt wird (die einzige Möglichkeit, zu verhindern, daß χ mit $\chi(\sigma_b) = 1$ nicht der Hauptcharakter ist, besteht darin, $\chi(\sigma_{-1}) = -1$ zu definieren). Das ist beispielsweise für $n = 15$ und $b = 2$ der Fall.

2.2 Das Lemma von Bass

Das Lemma von Bass ist eine Verallgemeinerung des Lemmas von Franz in dem Sinne, daß nicht nur das Produkt über Ausdrücke $1-\epsilon_n^a$ für ein zu n teilerfremdes a gebildet wird, sondern alle a zwischen 0 und $n-1$ auftauchen. Im Rahmen dieser Arbeit ist es interessant, da der hier geführte Beweis im Unterschied zur Originalversion (vgl. Bass, S. 401, Th. 3) mit dem Gruppenring $\mathbb{Z}G_n$ arbeitet.

2.2.1 Formulierung und Beweis des Lemmas von Bass

Lemma von Bass

Sei ϵ_n eine beliebige, aber feste primitive n-te Einheitswurzel. Für jeden Teiler von n sei $\epsilon_d := \epsilon_n^{n/d}$ und g_d aus $\mathbb{Z}G_d^+$. Gilt für jedes $a|n$ die Relation

$$\prod_{d|n}{}' (1-\epsilon_d^a)^{g_d} = 1, \qquad (*)$$

so folgt

$$g_d = 0$$

für alle $d > 1$.

Der Strich am Produktzeichen bedeute dabei, daß das Produkt nur über die Faktoren gebildet wird, die ungleich 0 sind, für die also $\epsilon_d^a \neq 1$ ist.

Beweis

Zunächst zeigen wir, daß die Voraussetzung "$(*)$ gilt für $a|n$" äquivalent zur Voraussetzung "$(*)$ gilt für $a \in \mathbb{Z}$" ist. Sei also $a \in \mathbb{Z}$. Wir schreiben $a \equiv sb \bmod n$, so daß b ein Teiler von n ist und s zu n teilerfremd (dies ist möglich, wenn man $b = (a, n)$ setzt und s so wählt, daß $\frac{a}{b} \equiv s \bmod \frac{n}{b}$ und $(s, n) = 1$ ist). Es gilt dann

$$\prod_{d|n}{}' (1 - \epsilon_d^a)^{g_d} = \prod_{d|n}{}' (1 - \epsilon_d^b)^{\sigma_s g_d} = 1^{\sigma_s} = 1.$$

Der Beweis des Lemmas von Bass läuft nun so ab, daß mit Induktion $g_d = 0$ für $1 < d < n$ gezeigt wird. Damit folgt die Behauptung aus dem Lemma von Franz. Es werden auf zwei verschiedene Arten die Voraussetzungen geschaffen, um das Lemma von Bass für einen Teiler von n anzuwenden.

Für $n = p$ Primzahl ist das Lemma von Bass identisch mit dem Lemma von Franz. Die Induktion ist somit für jede Primzahl verankert.

Wir schreiben nun $n = qt$. Dabei ist $q = p^\alpha$ ein primer P-Teiler von n. Mit $(*)$ für $a := pb$ und $b \in \mathbb{Z}$ beliebig gilt

$$\begin{aligned} 1 &= \prod_{d|n}{}' (1 - \epsilon_d^{pb})^{g_d} \\ &= \prod_{d|t}{}' \left((1 - \epsilon_d^{pb})^{g_d} (1 - \epsilon_{dp}^{pb})^{g_{dp}} (1 - \epsilon_{dp^2}^{pb})^{g_{dp^2}} \cdots (1 - \epsilon_{dp^\alpha}^{pb})^{g_{dp^\alpha}} \right). \end{aligned}$$

Wegen $\epsilon_{dp^\beta}^p = \epsilon_{dp^{\beta-1}}$ ist also

$$\begin{aligned} 1 = \prod_{d|t}{}' \Big(&(1 - \epsilon_d^b)^{\sigma_p g_d} (1 - \epsilon_d^b)^{g_{dp}(d)} (1 - \epsilon_{dp}^b)^{g_{dp^2}(dp)} \cdots \\ &\cdots (1 - \epsilon_{dp^{\alpha-1}}^b)^{g_{dp^\alpha}(dp^{\alpha-1})} \Big) \quad = \prod_{d|(n/p)}{}' (1 - \epsilon_d^b)^{h_d}, \end{aligned}$$

wobei

$$h_d = \begin{cases} \sigma_p g_d + g_{dp}(d) & \text{falls } p \nmid d \\ g_{dp}(d) & \text{falls } p|d \end{cases}$$

ist.

Mit dem Lemma von Bass für n/p folgt $h_d = 0$ für $1 < d \leq n/p$. Für $g_{dp}(d)$ bedeutet das

$$\begin{aligned} & g_{dp}(d) = -\sigma_p g_d \quad \text{falls} \quad p \nmid d \\ \text{und} \quad & g_{dp}(d) = 0 \quad \text{falls} \quad p|d. \end{aligned} \tag{$**$}$$

Sei jetzt $n = pt$. Wir benutzen das Element N_p, das im Abschnitt über elementare Relationen definiert wurde und unterscheiden die Fälle $p|t$ und $p \nmid t$.

$p \nmid t$: Für das Element N_p gilt nach Abschnitt 1.2.5, Lemma 6 (unter Verwendung von $\epsilon_{dp} = \epsilon_d^{\sigma_p^{-1}} \epsilon_p^{\sigma_d^{-1}}$):

$$\begin{aligned}(1-\epsilon_{dp})^{N_p} &= (1-\epsilon_d)^{(1-\sigma_p^{-1})} \\ (1-\epsilon_d)^{N_p} &= (1-\epsilon_d)^{\phi(p)} \\ (1-\epsilon_p)^{N_p} &= p.\end{aligned}$$

Sei nun b ein beliebiger Teiler von t. Man erhält

$$\begin{aligned}1 &= \prod_{d|n}{}'((1-\epsilon_d^b)^{g_d})^{N_p} \\ &= (1-\epsilon_p^b)^{N_p g_p} \prod_{1<d|t}{}' \left((1-\epsilon_d^b)^{N_p g_d}(1-\epsilon_{dp}^b)^{N_p g_{dp}}\right) \\ &= p^{g_p} \prod_{1<d|t}{}' \left((1-\epsilon_d^b)^{\phi(p) g_d}(1-\epsilon_d^b)^{(1-\sigma_p^{-1}) g_{dp}}\right) \\ &= p^{\mathrm{aug}(g_p)} \prod_{d|t}{}'(1-\epsilon_d^b)^{k_d}.\end{aligned}$$

Dabei ist

$$k_d = \phi(p) g_d + (1-\sigma_p^{-1}) g_{dp}(d) \in \mathbb{Z}G_t.$$

Es ist $\mathrm{aug}(g_p) = 0$: Dazu schreiben wir $t = q_1 \cdots q_m$ mit primen P-Teilern $q_i = p_i^{\alpha_i}$ und wenden auf den Term

$$p^{\mathrm{aug}(g_p)} \prod_{d|t}{}'(1-\epsilon_d^b)^{k_d}$$

sukzessive die Elemente N_{q_1} bis N_{q_m} an. So ergibt sich

$$1 = p^{\phi(q_1)\cdots\phi(q_m)\mathrm{aug}(g_p)} p_1^{s_1} \cdots p_m^{s_m}$$

mit irgendwelchen ganzen Zahlen $s_1, \ldots s_m$. Da die p_i alle ungleich p sind, muß $\phi(q_1)\cdots\phi(q_m)\mathrm{aug}(g_p)$ verschwinden, also ist $\mathrm{aug}(g_p) = 0$.

Man erhält so

$$\prod_{d|t}{}'(1-\epsilon_d^b)^{k_d} = 1$$

und nach der Induktionsvoraussetzung $k_d = 0$ für $1 < d \leq t$. Wegen $(**)$ ist $g_{dp}(d) = -\sigma_p g_d$, und es gilt

$$\begin{aligned}0 = k_d &= \phi(p) g_d + (1-\sigma_p^{-1}) g_{dp}(d) \\ &= (p-1) g_d + (1-\sigma_p^{-1})(-\sigma_p g_d) \\ &= (p-\sigma_p) g_d.\end{aligned}$$

Nach dem Satz über die Charakterisierung von Einheiten in Gruppenringen ist $p - \sigma_p$ in $\mathbb{Q}G_d$ kein Nullteiler (es gilt für jeden Charakter χ von G_d, daß $|p - \chi(\sigma_p)| \geq p - |\chi(\sigma_p)| = p - 1 > 0$ ist), und es folgt $g_d = 0$ für $1 < d \leq t$.

$p|t$: Mit dem Element N_p gilt in diesem Fall (Abschnitt 1.2.5, Lemma 7)

$$(1 - \epsilon_{dp^\beta})^{N_p} = \begin{cases} 1 - \epsilon_{dp^{\alpha-1}} & \text{falls} \quad \beta = \alpha \\ (1 - \epsilon_{dp^\beta})^p & \text{falls} \quad \beta < \alpha \end{cases}$$

für jedes zu p teilerfremde d. Dabei ist α der maximale p-Anteil von n, das heißt, $q = p^\alpha$ ist primer P-Teiler von n. Wir schreiben $n = p^\alpha s$. Sei b ein Teiler von t. Für $p \not| b$ gilt

$$\begin{aligned} 1 = \prod_{d|n}{}' (1 - \epsilon_d^b)^{g_d N_p} &= \prod_{d|t}{}' (1 - \epsilon_d^b)^{g_d N_p} \prod_{d|s}{}' (1 - \epsilon_{dp^\alpha}^b)^{g_{dp^\alpha} N_p} \\ &= \prod_{d|t}{}' (1 - \epsilon_d^b)^{pg_d} \prod_{d|s}{}' (1 - \epsilon_{dp^{\alpha-1}}^b)^{g_{dp^\alpha}(dp^{\alpha-1})} \end{aligned}$$

und für $p|b$

$$\begin{aligned} 1 = \prod_{d|n}{}' (1 - \epsilon_d^b)^{g_d N_p} &= \prod_{d|t}{}' (1 - \epsilon_d^b)^{g_d N_p} \prod_{d|s}{}' (1 - \epsilon_{dp^\alpha}^b)^{g_{dp^\alpha} N_p} \\ &= \prod_{d|t}{}' (1 - \epsilon_d^b)^{pg_d} \prod_{d|s}{}' (1 - \epsilon_{dp^{\alpha-1}}^{b/p})^{g_{dp^\alpha}(dp^{\alpha-1})N_p}. \end{aligned}$$

Wegen $(**)$ ist $g_{dp^\alpha}(dp^{\alpha-1}) = 0$. Das heißt, in beiden Fällen verschwindet das zweite Produkt. Es folgt

$$1 = \prod_{d|t}{}' (1 - \epsilon_d^b)^{pg_d},$$

und mit Induktion folgt $pg_d = 0$ für $1 < d \leq t$, mithin $g_d = 0$.

Zusammenfassend gilt somit: Hat man einen beliebigen echten Teiler d von n, so gibt es ein t mit $d|t$ und $pt = n$. Es folgt nach einem der beiden oben ausgeführten Fälle $g_d = 0$, und $(*)$ wird zu

$$(1 - \epsilon_n^a)^{g_n} = 1$$

für alle Teiler $a \neq 1$ von n. Mit Franz folgt $g_n = 0$, was schließlich noch zu zeigen war.

QED.

2.2.2 Weitere Bemerkungen zum Lemma von Bass

Ähnlich wie das Lemma von Franz kann man auch das Lemma von Bass auf Einheiten im Gruppenring $\mathbb{Z}C_n$ anwenden. Hat man zu jedem Teiler d von n eine Enheit $w_d \in \mathbb{Z}C_d$ konstruiert, so daß für jeden Charakter χ von C_n für alle $d|n$ entweder

$$\chi(w_d) = 1$$

oder

$$\chi(w_d) = (1 - \epsilon_d^a)^{h_d}$$

mit einem geeigneten $h_d \in \mathbb{Z}G_d$ und einem nur von χ abhängigen Teiler a von n, so folgt für ein $g_d \in \mathbb{Z}G_d^+$ aus der Relation

$$\prod_{d|n} w_d^{g_d} = 1,$$

daß $h_d g_d = 0$ ist.

Dies sollte nur als Anhaltspunkt dienen für weitere Überlegungen, die über den Rahmen dieser Arbeit hinausführen.

Eine Anwendung des Lemmas von Bass zur Konstruktion unabhängiger Einheiten im Gruppenring $\mathbb{Z}C_n$ findet sich bei Karpilovsky, S. 156ff. Die dort beschriebene Konstruktion geht auf H. Bass zurück.

3 Konstruktion von Basen in der Gruppe der zyklotomischen Einheiten

Sei $n \in \mathbb{N}$. Es wird nun die Gruppe der zyklotomischen Einheiten weiter untersucht. Diese war definiert durch (vgl. Abschnitt 1.1.3)

$$C^{(n)} = \quad < \{\pm\epsilon_n, 1-\epsilon_n^a \mid a \in \mathbb{Z}\} > \cap U\mathbb{Z}[\epsilon_n]$$

und wird nach Satz 2, Abschnitt 1.1.3 erzeugt durch

$$\begin{aligned} E^{(n)} = \quad & \{(1-\epsilon_t)^{\sigma_\nu} \mid t \in T_n \setminus P_n, \sigma_\nu \in G_t\} \\ \cup \quad & \{(1-\epsilon_q)^{(\sigma_\nu - 1)} \mid q \in P_n, \sigma_\nu \in G_q\} \\ \cup \quad & \{\pm\epsilon_n\}. \end{aligned}$$

Dabei war T_n die Menge aller P-Teiler und P_n die Menge aller primen P-Teiler von n.

Allgemein gilt für eine endlich erzeugte abelsche Gruppe die Zerlegung

$$G \cong G_{tor} \times \mathbb{Z}^r,$$

wobei G_{tor} den Torsionsanteil und r den Rang bezeichnet (siehe z.B. Lang, S. 49, Th. 8). Mit dem Wort "Basis" ist im folgenden immer eine Basis des torsionsfreien Anteils der Gruppe der zyklotomischen Einheiten gemeint, also r Elemente, die zusammen mit der Torsionsgruppe die Gruppe erzeugen.

Definition

Seien $u, v \in C^{(n)}$, dann sagt man "u ist gleich v modulo Torsion", wenn es eine Einheitswurzel $\epsilon \in C^{(n)}$ gibt, für die

$$u = \epsilon v$$

gilt. Man schreibt in diesem Fall $u \overset{\text{tor}}{=} v$.

Lemma 1

Es sei ϵ_d eine d-te Einheitswurzel, d ein Teiler von n, dann gilt

$$1 - \epsilon_d \overset{\text{tor}}{=} 1 - \epsilon_d^{-1}.$$

Beweis

Der Beweis folgt direkt aus

$$1 - \epsilon_d = -\epsilon_d(1 - \epsilon_d^{-1}).$$

QED.

Wegen dieser "trivialen" Abhängigkeit zwischen zyklotomischen Einheiten ist es sinnvoll, nur mit einem "halben" Restsystem von G_n zu arbeiten, das heißt mit einem Vertretersystem von $G_n/\{\pm 1\}$. Dazu wird folgende suggestive Bezeichnungsweise definiert.

Definition
Sei $n > 2$. Dann werden für $\sigma_\nu \in G_n$ folgende Bezeichnungen definiert:

$$\begin{aligned}
\sigma_\nu > 0 &:\Leftrightarrow \sigma_\nu \in \{\sigma_a \in G_n \mid 0 < a < +\frac{n}{2}\},\\
\sigma_\nu < 0 &:\Leftrightarrow \sigma_\nu \in \{\sigma_a \in G_n \mid -\frac{n}{2} < a < 0\},\\
\sigma_\nu > 1 &:\Leftrightarrow \sigma_\nu > 0 \text{ und } \sigma_\nu \neq \sigma_1,\\
\sigma_\nu < -1 &:\Leftrightarrow \sigma_\nu < 0 \text{ und } \sigma_\nu \neq \sigma_{-1},\\
\sigma_\nu = 1 &:\Leftrightarrow \sigma_\nu = \sigma_1,\\
\sigma_\nu = -1 &:\Leftrightarrow \sigma_\nu = \sigma_{-1}.
\end{aligned}$$

Es handelt sich hier ausdrücklich nur um eine Schreibweise. Mit "<" bzw. ">" wird also keine Ordnungsrelation oder ähnliches definiert. In G_n gibt es in diesem Sinne keine "positiven" oder "negativen" Zahlen. Trotzdem gilt mit dieser Bezeichnungsweise

$$\sigma_\nu > 0 \Leftrightarrow \sigma_{-\nu} < 0.$$

3.1 Das Einheitensystem von Ramachandra

Es gelte im folgenden $n > 2$. Das Einheitensystem von Ramachandra erzeugt eine Untergruppe der zyklotomischen Einheiten von endlichem Index in $U\mathbb{Z}[\epsilon_n]$. Es folgt also aus der Konstruktion dieses Einheitensystems, daß auch die Gruppe aller zyklotomischen Einheiten endlichen Index in $U\mathbb{Z}[\epsilon_n]$ hat. Nach dem Dirichletschen Einheitensatz ist der Rang der Einheitengruppe in $\mathbb{Z}[\epsilon_n]$, das heißt die maximale Anzahl unabhängiger Einheiten, $\frac{1}{2}\phi(n) - 1$ (siehe z.B. Weiss, S. 267, Proposition 7-6-1). Ramachandra stellt nun gerade $\frac{1}{2}\phi(n) - 1$ Einheiten zur Verfügung, die unabhängig sind.

Definition
Sei T_n die Menge aller P-Teiler von n. Sei ϵ_n eine beliebige, aber feste primitive n-te Einheitswurzel. Schließlich sei $\epsilon_d := \epsilon_n^{n/d}$. Für $\sigma_\nu \in G_n, \sigma_\nu > 1$ heißt die

zyklotomische Einheit

$$u_\nu := \prod_{d \in T_n} \frac{1-\epsilon_d^\nu}{1-\epsilon_d} = \prod_{d \in T_n} (1-\epsilon_d)^{\sigma_\nu - 1}$$

Ramachandra-Einheit.

Wir werden nun die Unabhängigkeit dieser Einheiten beweisen.

Satz 4 (Unabhängigkeit der Ramachandra-Einheiten)

Es seien für $\sigma_\nu > 1$ die u_ν wie oben definiert. Dann folgt aus

$$\prod_{\sigma_\nu > 1} u_\nu^{a_\nu} = 1,$$

daß $a_\nu = 0$ für alle $\sigma_\nu > 1$ ist.

Bevor der Satz bewiesen wird, noch ein Korollar, das auch die Torsionselemente berücksichtigt. Man erhält dabei aber nichts wesentlich Neues.

Korollar

Sei ϵ eine beliebige Einheitswurzel. Dann folgt aus

$$\epsilon \prod_{\sigma_\nu > 1} u_\nu^{a_\nu} = 1,$$

daß $a_\nu = 0$ für alle $\sigma_\nu > 1$ (und damit auch $\epsilon = 1$) ist.

Beweis des Korollars

Erhebt man letztgenannte Bedingung zu einer geeigneten k-ten Potenz, so daß $\epsilon^k = 1$ ist, gilt

$$\prod_{\sigma_\nu > 1} u_\nu^{k a_\nu} = 1,$$

und mit Satz 4 folgt $k a_\nu = 0$, also $a_\nu = 0$ für alle σ_ν.

QED.

Der Beweis von Satz 4 weicht von der ursprünglichen Version (vgl. Ramachandra, S. 172) dadurch ab, daß hier mit Gruppenringen gearbeitet wird, um das Lemma von Franz anwenden zu können.

Beweis des Satzes

Der Beweis wird mit Hilfe des Lemmas von Franz geführt. Dazu formen wir zunächst die Voraussetzung des Satzes um. Es gilt

$$\prod_{\sigma_\nu > 1} u_\nu^{a_\nu} = \prod_{\sigma_\nu > 1} \prod_{d \in T_n} (1-\epsilon_d)^{(\sigma_\nu - 1) a_\nu}$$

$$\begin{aligned} &= \prod_{d\in T_n}\prod_{\sigma_\nu>1}(1-\epsilon_d)^{(\sigma_\nu-1)a_\nu} \\ &= \prod_{d\in T_n}(1-\epsilon_d)^{g_+} = 1. \end{aligned}$$

Dabei ist g_+ als Element des Gruppenrings $\mathbb{Z}G_n$ definiert durch

$$g_+ := \sum_{\sigma_\nu>1} a_\nu(\sigma_\nu - 1).$$

Wir setzen

$$g := (1+\sigma_{-1})g_+,$$

und es ist dann auch

$$\prod_{d\in T_n}(1-\epsilon_d)^{g_+(1+\sigma_{-1})} = \prod_{d\in T_n}(1-\epsilon_d)^{g} = 1.$$

Schreibt man $g = \sum b_\nu\sigma_\nu$ mit Koeffizienten b_ν, so gilt für diese

$$b_\nu = \begin{cases} a_\nu & \text{falls} \quad \sigma_\nu > 1 \\ -\sum_{\sigma_\mu>1} a_\mu & \text{falls} \quad \sigma_\nu = 1 \\ a_{-\nu} & \text{falls} \quad \sigma_\nu < 0. \end{cases}$$

Insbesondere folgt aus $b_\nu = 0$, daß auch die a_ν verschwinden. Da außerdem g Augmentation 0 hat und $b_\nu = b_{-\nu}$ ist, genügt es, zum Beweis des Satzes folgende Proposition zu zeigen.

Proposition (verallgemeinertes Lemma von Franz)

Sei $g \in \Delta\mathbb{Z}G_n^+$. Es sei $\epsilon_d := \epsilon_n^{n/d}$ und ϵ_n eine primitive n-te Einheitswurzel. Dann folgt aus

$$\prod_{d\in T_n}(1-\epsilon_d)^{g} = 1, \qquad (*)$$

daß $g = 0$ ist.

Beweis der Proposition

Der Beweis wird mit Induktion nach der Anzahl der P-Teiler von n geführt. Ist $n = q$ Primzahlpotenz, so ist $T_q = \{q\}$, und $(*)$ ist gerade die Bedingung, die als Voraussetzung zum Lemma von Franz benötigt wird. Es folgt $g = 0$.

Für den Induktionsschluß schreiben wir $n = qt$, wobei $q = p^\alpha$ ein primer P-Teiler von n ist. Wir benutzen das Element N_q. Für dieses Element gilt (Abschnitt 1.2.5, Lemma 6), falls ϵ_d und ϵ_q primitive d-te beziehungsweise q-te Einheitswurzeln ($d \neq 1$) sind,

$$\begin{aligned} (1-\epsilon_d\epsilon_q)^{N_q} &= (1-\epsilon_d)^{\sigma_q(1-\sigma_p^{-1})} \\ (1-\epsilon_d)^{N_q} &= (1-\epsilon_d)^{\phi(q)} \\ (1-\epsilon_q)^{N_q} &= p. \end{aligned}$$

Wegen $\epsilon_{dq} = \epsilon_d^{\sigma_q^{-1}} \epsilon_q^{\sigma_d^{-1}}$ (Abschnitt 1.2.4, Lemma 4) folgt

$$\begin{aligned}
1 &= \prod_{d \in T_n} (1-\epsilon_d)^{gN_q} \\
&= (1-\epsilon_q)^{N_q g} \prod_{d \in T_t} ((1-\epsilon_d)^{N_q g} (1-\epsilon_{dq})^{N_q g}) \\
&= p^{\mathrm{aug}(g)} \prod_{d \in T_t} ((1-\epsilon_d)^{N_q g} (1-\epsilon_d^{\sigma_q^{-1}} \epsilon_q^{\sigma_d^{-1}})^{N_q g}) \\
&= p^{\mathrm{aug}(g)} \prod_{d \in T_t} \left((1-\epsilon_d)^{\phi(q)\, g(t)} (1-\epsilon_d)^{\sigma_q^{-1} \sigma_q (1-\sigma_p^{-1}) g(t)} \right) \\
&= \prod_{d \in T_t} (1-\epsilon_d)^{h_q g(t)}
\end{aligned}$$

mit $h_q = \phi(q) + 1 - \sigma_p^{-1}$. Wir haben im letzten Schritt ausgenutzt, daß $\mathrm{aug}(g) = 0$ vorausgesetzt wurde, so daß $p^{\mathrm{aug}(g)} = 1$ ist. Aus der Induktionsannahme folgt $h_q g(t) = 0$. Da h_q kein Nullteiler in $\mathbb{Z}\!\!\mathbb{Z} G_t$ ist (es gilt für jeden Charakter χ von G_t die Abschätzung $|\chi(h_q)| \geq \phi(q) + 1 - |\chi(\sigma_p^{-1})| = \phi(q) > 0$), folgt also $g(t) = 0$.

Hat man allgemein einen beliebigen P-Teiler $d \neq n$ von n, so ist $n = qrd$ mit einem primen P-Teiler q und einem eventuellen weiteren P-Teiler r. Nach dem oben Gezeigten folgt $g(rd) = 0$. Es ist also

$$(1-\epsilon_d)^g = (1-\epsilon_d)^{g(rd)} = 1.$$

In Gleichung $(*)$ eingesetzt ergibt sich auch für n

$$(1-\epsilon_n)^g = \prod_{d \in T_n} (1-\epsilon_d)^g = 1.$$

Als Quintessenz folgt für *jeden* P-Teiler d von n, daß

$$(1-\epsilon_d)^g = 1$$

ist, und mit dem Lemma von Franz folgt $g = 0$.

QED.

3.2 Explizite Konstruktion einer Basis

Ziel ist es, eine Basis für den torsionsfreien Teil aller zyklotomische Einheiten zu schaffen für den Fall, daß n von höchstens drei verschiedenen Primzahlen geteilt wird. Dies gelingt, indem Elemente aus dem Erzeugendensystem $E^{(n)}$ sukzessive entfernt und die jeweils entfernten Elemente mit Hilfe der übrigen, verbliebenen

dargestellt werden, bis gerade noch $\frac{1}{2}\phi(n)-1$ Elemente übrig bleiben. Natürlich ist dies keine Methode, die in allgemeinen abelschen Gruppen zum Erfolg führen muß (beispielsweise wird $(\mathbb{Z},+)$ von den Elementen 2 und 3 erzeugt, und hier erhält man offensichtlich keine Basis, indem man eines der beiden Elemente wegläßt). Wir werden aber sehen, daß dieser Ansatz für die Gruppe der zyklotomischem Einheiten fruchtet. Im folgenden wird immer $n \not\equiv 2 \bmod 4$ vorausgesetzt. Dies bedeutet beim Arbeiten in zyklotomischen Körpern keine Einschränkung, da wegen $\epsilon_{2u} = -\epsilon_u$ für u ungerade $\mathbb{Q}[\epsilon_{2u}] = \mathbb{Q}[\epsilon_u]$ ist.

3.2.1 Konstruktion einer Basis im Fall $n = q$

Satz 5 (Basis im Fall $n = q$)
Sei $n = q = p^\alpha$ Primzahlpotenz. Dann ist

$$B_q := \{(1-\epsilon_q)^{\sigma_\nu - 1} \mid \sigma_\nu > 1\}$$

eine Basis von $C^{(n)}$.

Beweis
Es besteht B_q aus genau $\frac{1}{2}\phi(q) - 1$ Elementen, und wegen $1 - \epsilon_q^\nu \stackrel{\text{tor}}{=} 1 - \epsilon_q^{-\nu}$ liegen auch die Elemente $(1-\epsilon_q)^{\sigma_\nu - 1}$ für $\sigma_\nu < -1$ in $< B_q >$. Dies sind schon alle Einheiten aus $E^{(q)}$.

QED.

3.2.2 Konstruktion einer Basis im Fall $n = qr$

Seien q und r zwei Primzahlpotenzen. Nach dem Chinesischen Restsatz ist

$$G_n \cong G_q \times G_r.$$

Für ein Element $\sigma_\nu \in G_n$ schreiben wir dementsprechend $\sigma_\nu = (x, y)$ mit $x \in G_q$ und $y \in G_r$. Sei ϵ_n eine feste n-te Einheitswurzel. Wir stellen $\epsilon_n = \epsilon_q \epsilon_r$ als Produkt einer primitiven q-ten und r-ten Einheitswurzel dar und schreiben

$$\epsilon_n^{(x,y)} := \epsilon_n^\nu = \epsilon_q^x \epsilon_r^y.$$

Satz 6 (Basis im Fall $n = qr$)
Sei $n = qr$ das Produkt zweier Primzahlpotenzen, dann ist

$$\begin{aligned} B_{qr} := \quad & B_q \cup B_r \\ \cup \quad & \{1 - \epsilon_n^{(x,y)} \mid x > 1, y > 1\} \end{aligned}$$

$$\cup \quad \{1-\epsilon_n^{(x,y)} \mid x>0, y<0\}$$

eine Basis von $C^{(n)}$.

Beweis

Wir bestimmen zunächst die Anzahl der Elemente in B_{qr}. Dazu machen wir folgende Aufstellung:

Menge :	Anzahl :
B_q	$\frac{1}{2}\phi(q)-1$
B_r	$\frac{1}{2}\phi(r)-1$
$\{1-\epsilon_n^{(x,y)} \mid x>1, y>1\}$	$(\frac{1}{2}\phi(q)-1)(\frac{1}{2}\phi(r)-1)$
$\{1-\epsilon_n^{(x,y)} \mid x>0, y<0\}$	$\frac{1}{2}\phi(q)\frac{1}{2}\phi(r)$.

Das ergibt summa summarum $\#B_{qr} = \frac{1}{2}\phi(q)-1+\frac{1}{2}\phi(r)-1+(\frac{1}{2}\phi(q)-1)(\frac{1}{2}\phi(r)-1)+\frac{1}{2}\phi(q)\frac{1}{2}\phi(r) = \frac{1}{2}\phi(q)\phi(r)-1 = \frac{1}{2}\phi(n)-1$ Elemente. Die Anzahl stimmt also. Die Elemente aus $E^{(n)}$, von denen wir jetzt zeigen müssen, daß sie durch Elemente aus B_{qr} dargestellt werden können, sind die $1-\epsilon_n^{(x,y)}$ mit

a) $x<0, y>0$,

b) $x=1, y>1$,

c) $x>1, y=1$,

d) $x=1, y=1$,

e) $x<0, y<0$.

Dies ist an Hand folgender Tabelle klar:

	$x=1$	$x>1$	$x<-1$	$x=-1$
$y=1$	d	c	a	a
$y>1$	b	B	a	a
$y<-1$	B	B	e	e
$y=-1$	B	B	e	e

Dabei sind mit B die Elemente bezeichnet, für die $1-\epsilon_n^{(x,y)}$ in der Basis liegt, die Buchstaben a-e beziehen sich auf die oben angeführten Fälle a-e.

Zu a: Sei $x<0$ und $y>0$. Es ist $1-\epsilon_n^{(x,y)} \overset{\text{tor}}{=} 1-\epsilon_n^{(-x,-y)}$, da wegen des Chinesischen Restsatzes $-(x,y)=(-x,-y)$ gilt. Die Elemente mit $x<0$ und $y>0$ werden also durch diejenigen mit $x>0$ und $y<0$ erzeugt.

Zu b: Sei $y > 1$ fest. Wir schreiben $q = p^\alpha$ mit einer Primzahl p. Es sei mit $\hat{q}$ die Zahl $\hat{q} := p^{\alpha-1}$ bezeichnet. Für das Element N_q galt

$$(1 - \epsilon_q \epsilon_r^y)^{N_q} = (1 - \epsilon_r^y)^{\sigma_q - \sigma_{\hat{q}}}.$$

Da $N_q = \sum_{\nu \equiv 1 \bmod r} \sigma_\nu$ ist, schreiben wir dies als

$$\prod_{x \in G_q} (1 - \epsilon_q^x \epsilon_r^y) = (1 - \epsilon_r^y)^{\sigma_q - \sigma_{\hat{q}}}.$$

Man kann dies anschaulich so interpretieren, daß das Produkt über Elemente gebildet wird, die in obiger Tabelle längs einer horizontalen Linie liegen. (Analog entspricht die durch N_r induzierte Relation der Bildung des Produkts längs einer Vertikalen.) Klammern wir aus dem Produkt auf der linken Seite den Faktor zu $x = 1$ aus und schreiben den Rest auf die rechte Seite, so erhalten wir

$$1 - \epsilon_n^{(1,y)} = (1 - \epsilon_r^y)^{\sigma_q - \sigma_{\hat{q}}} \prod_{x \in G_q \setminus \{\sigma_1\}}^{-1} (1 - \epsilon_q^x \epsilon_r^y)$$

als Darstellung von $1 - \epsilon_n^{(1,y)}$ durch Elemente, von denen wir schon wissen, daß sie aus $< B_{qr} >$ sind. (Wegen $\mathrm{aug}(\sigma_q - \sigma_{\hat{q}}) = 0$ liegt $(1 - \epsilon_r^y)^{\sigma_q - \sigma_{\hat{q}}}$ in $< B_r > \subseteq < B_{qr} >$.)

Zu c: Der Fall $x > 1$ und $y = 1$ ist absolut symmetrisch zum Fall b, indem man die Rollen von q und r vertauscht.

Zu d: Den Fall $x = 1$ und $y = 1$ können wir analog zu b abhandeln, wenn wir dort $y = 1$ setzen. Wir erhalten

$$1 - \epsilon_n = (1 - \epsilon_r)^{\sigma_q - \sigma_{\hat{q}}} \prod_{x \in G_q \setminus \{\sigma_1\}}^{-1} (1 - \epsilon_q^x \epsilon_r).$$

Von den Elementen $1 - \epsilon_q^x \epsilon_r$ mit $x > 1$ wissen wir jetzt aus c, daß sie alle in $< B_{qr} >$ liegen.

Zu e: Die Elemente $1 - \epsilon_n^{(x,y)}$ mit $x < 0$ und $y < 0$ werden genauso wie in a auf Grund von $1 - \epsilon_n^{(x,y)} \overset{\text{tor}}{=} 1 - \epsilon_n^{(-x,-y)}$ erzeugt. Daß diejenigen mit $x > 0$ und $y > 0$ in $< B_{qr} >$ liegen, folgt aus b,c und d.

QED.

3.2.3 Konstruktion einer Basis im Fall $n = qrs$

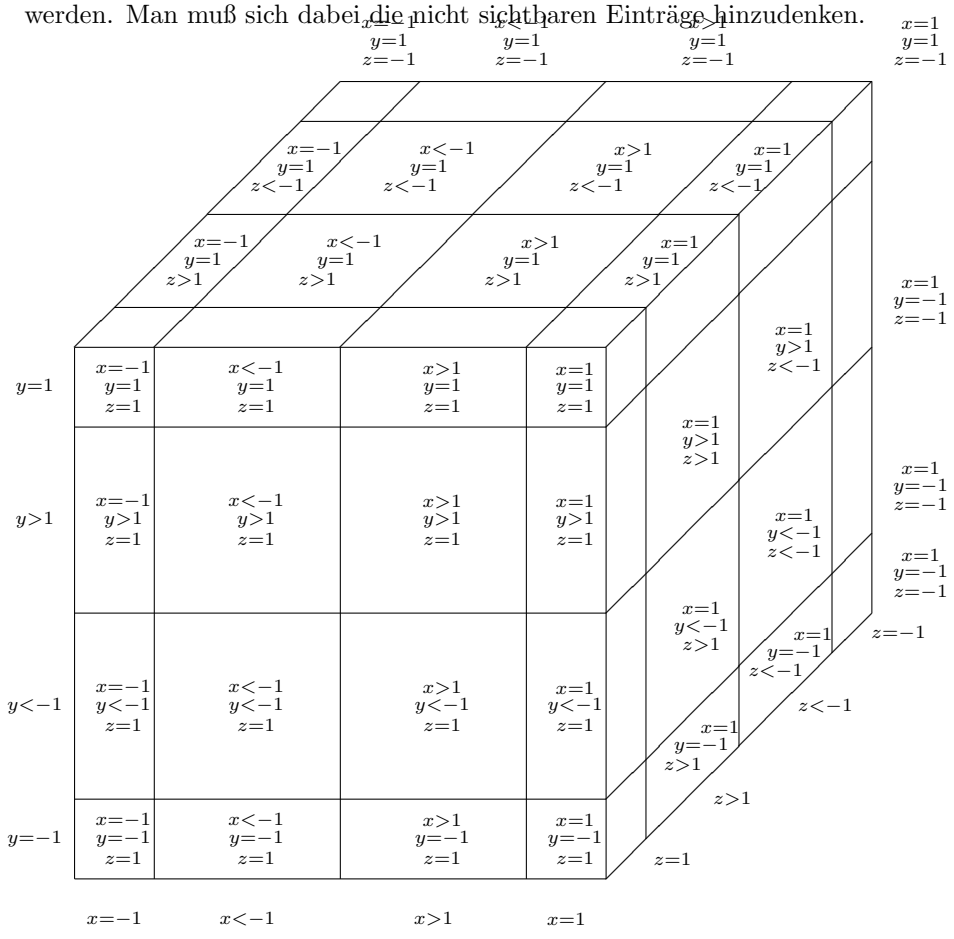
Seien nun q, r, s drei teilerfremde Primzahlpotenzen. Es gilt wie im Fall $n = qr$ nach dem Chinesischen Restsatz

$$G_n \cong G_q \times G_r \times G_s.$$

Wir schreiben demnach ein Element $\sigma_\nu \in G_n$ als Tripel $(x, y, z) \in G_q \times G_r \times G_s$ und definieren

$$1 - \epsilon_n^{(x,y,z)} := 1 - \epsilon_n^\nu = 1 - \epsilon_q^x \epsilon_r^y \epsilon_s^z.$$

Das folgende Diagramm ist als "dreidimensionale Tabelle" zu interpretieren, in die alle Elemente $(x, y, z) \in G_n$ eingetragen sind. Die Beschriftung der Quader gibt eine gewisse Übersicht über die Teilmengen von G_n, mit denen wir arbeiten werden. Man muß sich dabei die nicht sichtbaren Einträge hinzudenken.



Wir führen die Kurzschreibweise $\{x > 0, y > 0, z > 0\}$ für die Menge $\{1 - \epsilon_n^{(x,y,z)} \mid x > 0, y > 0, z > 0\}$ usw. ein. Betrachtet man dann die vier disjunkten Mengen

$$\begin{aligned} M_0 &:= \{x > 0, y > 0, z > 0\}, \\ M_x &:= \{x < 0, y > 0, z > 0\}, \\ M_y &:= \{x > 0, y < 0, z > 0\}, \\ M_z &:= \{x > 0, y > 0, z < 0\}, \end{aligned}$$

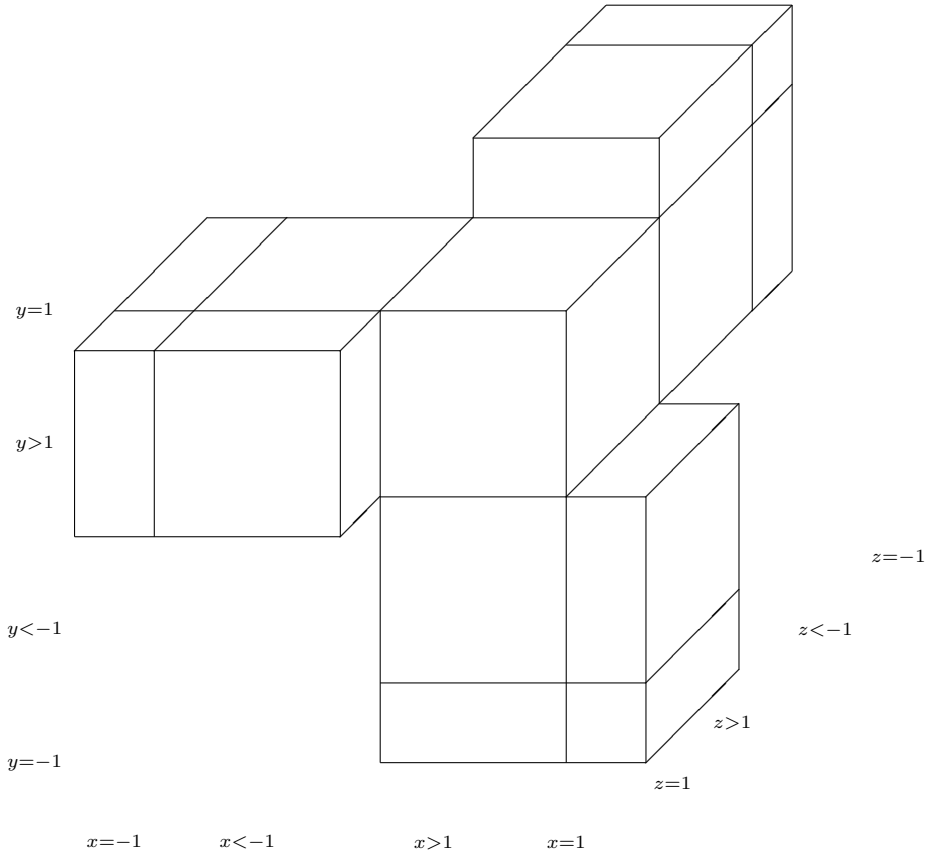
so liegt modulo Torsion jedes Element $1 - \epsilon_n^{(x,y,z)}$ in einer dieser Mengen (da $-(x, y, z) = (-x, -y, -z)$ ist). Die Basis ergibt sich nun, indem aus jeder dieser vier Mengen gewisse Elemente, für die $x = \sigma_1$, $y = \sigma_1$ oder $z = \sigma_1$ ist, weggelassen werden.

Satz 7 (Basis im Fall $n = qrs$)
Sei $n = qrs$ das Produkt dreier Primzahlpotenzen q, r und s. Dann ist

$$\begin{aligned} B_{qrs} := \quad & B_{qr} \cup B_{qs} \cup B_{rs} \\ \cup \quad & \{1 - \epsilon_n^{(x,y,z)} \mid x > 1, y > 1, z > 1\} \\ \cup \quad & \{1 - \epsilon_n^{(x,y,z)} \mid x < 0, y > 1, z > 0\} \\ \cup \quad & \{1 - \epsilon_n^{(x,y,z)} \mid x > 0, y < 0, z > 1\} \\ \cup \quad & \{1 - \epsilon_n^{(x,y,z)} \mid x > 1, y > 0, z < 0\} \end{aligned}$$

eine Basis von $C^{(n)}$.

Zeichnet man in dem dreidimensionalen Diagramm nur diejenigen Quader ein, die durch diese Mengen charakterisiert werden, so ergibt sich folgendes Bild:



Beweis

Wir werden, soweit es geht, in Analogie zum Fall $n = qr$ argumentieren, allerdings jetzt prinzipiell modulo Torsion rechnen. Das heißt, wenn wir gezeigt haben, daß ein Element $1 - \epsilon_n^{(x,y,z)}$ durch andere Elemente erzeugt werden kann, folgt direkt, daß auch das Element $1 - \epsilon_n^{(-x,-y,-z)}$ erzeugt werden kann.

Zunächst sind die Elemente in B_{qrs} zu zählen. Dabei ist zu beachten, daß B_{qr}, B_{qs} und B_{rs} paarweise nicht disjunkt sind. Es gilt vielmehr $B_{qr} \cap B_{qs} = B_q$, $B_{qr} \cap B_{rs} = B_r$ und $B_{rs} \cap B_{qs} = B_s$. Macht man die Mengen disjunkt, so lautet die Aufstellung:

Menge :	Anzahl :
$B_{qr} \setminus B_q$	$\frac{1}{2}\phi(q)\phi(r) - 1 - (\frac{1}{2}\phi(q) - 1)$
$B_{qs} \setminus B_s$	$\frac{1}{2}\phi(q)\phi(s) - 1 - (\frac{1}{2}\phi(s) - 1)$

$$\begin{array}{rl}
B_{rs} \setminus B_r & \frac{1}{2}\phi(r)\phi(s) - 1 - (\frac{1}{2}\phi(r) - 1) \\
\{x > 1, y > 1, z > 1\} & (\frac{1}{2}\phi(q) - 1)(\frac{1}{2}\phi(r) - 1)(\frac{1}{2}\phi(s) - 1) \\
\{x < 0, y > 1, z > 0\} & \frac{1}{2}\phi(q)(\frac{1}{2}\phi(s) - 1)\frac{1}{2}\phi(s) \\
\{x > 0, y < 0, z > 1\} & \frac{1}{2}\phi(q)\frac{1}{2}\phi(r)(\frac{1}{2}\phi(s) - 1) \\
\{x > 1, y > 0, z < 0\} & (\frac{1}{2}\phi(q) - 1)\frac{1}{2}\phi(r)\frac{1}{2}\phi(s).
\end{array}$$

Diese Terme rechnen wir aus:

$$\begin{array}{rcl}
\frac{1}{2}\phi(q)\phi(r) - 1 - (\frac{1}{2}\phi(q) - 1) & = & \frac{1}{2}\phi(q)\phi(r) - \frac{1}{2}\phi(q) \\
\frac{1}{2}\phi(q)\phi(s) - 1 - (\frac{1}{2}\phi(s) - 1) & = & \frac{1}{2}\phi(q)\phi(s) - \frac{1}{2}\phi(s) \\
\frac{1}{2}\phi(r)\phi(s) - 1 - (\frac{1}{2}\phi(r) - 1) & = & \frac{1}{2}\phi(r)\phi(s) - \frac{1}{2}\phi(s) \\
(\frac{1}{2}\phi(q) - 1)(\frac{1}{2}\phi(r) - 1)(\frac{1}{2}\phi(s) - 1) & = & \frac{1}{8}\phi(q)\phi(r)\phi(s) - \frac{1}{4}\phi(q)\phi(r) \\
 & & -\frac{1}{4}\phi(q)\phi(s) - \frac{1}{4}\phi(r)\phi(s) \\
 & & +\frac{1}{2}\phi(q) + \frac{1}{2}\phi(r) + \frac{1}{2}\phi(s) - 1 \\
\frac{1}{2}\phi(q)(\frac{1}{2}\phi(r) - 1)\frac{1}{2}\phi(s) & = & \frac{1}{8}\phi(q)\phi(r)\phi(s) - \frac{1}{4}\phi(q)\phi(s) \\
\frac{1}{2}\phi(q)\frac{1}{2}\phi(r)(\frac{1}{2}\phi(s) - 1) & = & \frac{1}{8}\phi(q)\phi(r)\phi(s) - \frac{1}{4}\phi(q)\phi(r) \\
(\frac{1}{2}\phi(q) - 1)\frac{1}{2}\phi(r)\frac{1}{2}\phi(s) & = & \frac{1}{8}\phi(q)\phi(r)\phi(s) - \frac{1}{4}\phi(r)\phi(s),
\end{array}$$

und die Summe beträgt tatsächlich $\frac{1}{2}\phi(q)\phi(r)\phi(s) - 1 = \frac{1}{2}\phi(n) - 1$.

Es sei wieder $q = p^\alpha$ und $\hat{q} = p^{\alpha-1}$. Analog seien die Zahlen $\hat{s}$ zu s und $\hat{r}$ zu r definiert. Wir werden, soweit es geht, mit der von N_q induzierten Formel argumentieren, die in diesem Fall

$$(1 - \epsilon_r^y \epsilon_s^z)^{(\sigma_q - \sigma_{\hat{q}})} = \prod_{x \in G_q} (1 - \epsilon_q^x \epsilon_r^y \epsilon_s^z)$$

lautet. Das Produkt auf der rechten Seite wird, wenn man es an Hand des Diagramms interpretiert, über alle Elemente längs einer waagerechten Geraden gebildet. Analoge Formeln gelten natürlich, indem man die Rollen von s und q bzw. r und q vertauscht.

Wir wollen uns zuerst eine Übersicht verschaffen, welche Elemente wir erzeugen müssen. Sie entsprechen gerade jenen Quadern, die im zweiten Diagramm fehlen. Wir bezeichnen die Mengen sukzessive mit A_1, A_2, usw. In dieser Reihenfolge werden wir denn auch vorgehen. Außerdem wird der Übersichtlichkeit

wegen angegeben, aus welcher der Mengen M_0, M_x, M_y, M_z die A_i sind:

$$\begin{array}{lcll} A_1 & := & \{x=1, y>1, z>1\} & \subset M_0, \\ A_2 & := & \{x>1, y=1, z>1\} & \subset M_0, \\ A_3 & := & \{x>1, y>1, z=1\} & \subset M_0, \\ A_4 & := & \{x<-1, y=1, z>0\} & \subset M_x, \\ A_5 & := & \{x>0, y<-1, z=1\} & \subset M_y, \\ A_6 & := & \{x=1, y>0, z<-1\} & \subset M_z, \\ A_7 & := & \{x>1, y=1, z=1\} & \subset M_0, \\ A_8 & := & \{x=1, y>1, z=1\} & \subset M_0, \\ A_9 & := & \{x=1, y=1, z>1\} & \subset M_0, \\ A_{10} & := & \{x=-1, y=1, z>1\} & \subset M_x, \\ A_{11} & := & \{x>1, y=-1, z=1\} & \subset M_y, \\ A_{12} & := & \{x=1, y>1, z=-1\} & \subset M_z \end{array}$$

und schließlich

$$\begin{array}{rcl} A_{13} := & & \{x=1, y=1, z=1)\} \cup \{x=-1, y=1, z=1)\} \\ & \cup & \{x=1, y=-1, z=1)\} \cup \{x=1, y=1, z=-1)\}. \end{array}$$

Wir werden später sehen, daß die einzige Menge, die wirklich Schwierigkeiten macht, die Menge A_{13} ist. Wir wollen noch den Mengen, die Basiselemente enthalten und nicht in einer der Mengen B_{qr}, B_{qs} oder B_{rs} liegen, einen Namen geben, und zwar definieren wir

$$\begin{array}{lcll} B_0 & := & \{x>1, y>1, z>1\} & \subset M_0, \\ B_x & := & \{x<0, y>1, z>0\} & \subset M_x, \\ B_y & := & \{x>0, y<0, z>1\} & \subset M_y, \\ B_z & := & \{x>1, y>0, z<0\} & \subset M_z. \end{array}$$

Schließlich werden wir zu einer gegebenen Menge M mit M^- die Menge bezeichnen, die gerade die Elemente mit entgegengesetzten Vorzeichen in x, y und z enthält, wie sie in M zu finden sind. Zum Beispiel ist B_0^- die Menge $\{x < -1, y < -1, z < -1\}$ usw. Es gilt dann gerade, daß M und M^- modulo Torsion die gleichen Elemente enthalten.
Alle Relationen, die unten auftauchen, sind eine Folgerung der Relationen, die von den Elementen N_q, N_r oder N_s induziert werden. Die Elemente in den A_i werden wie folgt erzeugt:

A_1: Seien $y > 1$ und $z > 1$ beliebig, aber fest. Es gilt

$$\begin{array}{rcl} 1-\epsilon_n^{(1,y,z)} & = & (1-\epsilon_r^y\epsilon_s^z)^{\sigma_q-\sigma_{\hat{q}}} \quad \prod_{x>1}^{-1}(1-\epsilon_n^{(x,y,z)}) \quad \prod_{x<0}^{-1}(1-\epsilon_n^{(x,y,z)}). \\ & & \in < B_{rs} > \qquad\qquad \in B_0 \qquad\qquad \in B_x \end{array}$$

A_2, A_3: Die Elemente aus A_2 und A_3 erhält man analog zu den Elementen aus A_1, indem man die Rollen von q, r und s vertauscht. Man beachte, daß die gesamte Konstruktion symmetrisch in q, r und s ist.

A_4: Seien $x < -1$ und $z > 0$ beliebig, aber fest. Es gilt

$$\begin{array}{rcl} 1-\epsilon_n^{(x,1,z)} & = & (1-\epsilon_q^x\epsilon_s^z)^{\sigma_r-\sigma_{\hat{r}}} \prod_{y>1}^{-1}(1-\epsilon_n^{(x,y,z)}) \prod_{y<0}^{-1}(1-\epsilon_n^{(x,y,z)}). \\ & & \in < B_{qs} > \quad \in B_x \quad \in B_z^- \end{array}$$

A_5, A_6: Dieses geht wieder symmetrisch zur Menge A_4.

A_7: Sei jetzt $x > 1$ beliebig, aber fest. Man erhält

$$\begin{array}{rcl} 1-\epsilon_n^{(x,1,1)} & = & (1-\epsilon_q^x\epsilon_r)^{\sigma_s-\sigma_{\hat{s}}} \prod_{z>1}^{-1}(1-\epsilon_n^{(x,1,z)}) \prod_{z<0}^{-1}(1-\epsilon_n^{(x,1,z)}). \\ & & \in < B_{qr} > \quad \in A_2 \quad \in B_z \end{array}$$

A_8, A_9: Symmetrisch zu A_7.

A_{10}: Sei jetzt $z > 1$ beliebig, aber fest. Man erhält

$$\begin{array}{rcl} 1-\epsilon_n^{(-1,1,z)} = & (1-\epsilon_q^{-1}\epsilon_s^z)^{\sigma_r-\sigma_{\hat{r}}} \prod_{y>1}^{-1}(1-\epsilon_n^{(-1,y,z)}) \prod_{y<0}^{-1}(1-\epsilon_n^{(-1,y,z)}). \\ & \in < B_{qs} > \quad \in B_x \quad \in A_6^- \end{array}$$

A_{11}, A_{12}: Symmetrisch zu A_{10}.

A_{13}: Die Menge $A_{13} \cup A_{13}^-$ wird gerade durch die Würfel an den Ecken des Diagramms dargestellt. Mit dieser Anschauung ist es intuitiv einsichtig, daß wir zunächst keine von den Elementen N_q, N_r oder N_s induzierte Relation zur Darstellung von Elementen aus A_{13} benutzen können. Die Anwendung einer dieser Relationen bedeutet nämlich, daß man alle Elemente entlang einer Parallelen zu einer der Kanten aufmultipliziert. Wenn wir das hier tun, stoßen wir immer auf *zwei* Elemente aus A_{13}. Wir können aber mit einem Trick eine Darstellung für $(1-\epsilon_n)^2$ herleiten, die ohne die anderen Elemente aus A_{13} auskommt. Wir werden diese dann so umformen, daß $(1-\epsilon_n)^2$ als Produkt von *Quadraten* von Elementen, die nicht aus A_{13} sind, dargestellt wird, und es ergibt sich so eine Relation für $1-\epsilon_n$. Die restlichen Elemente aus A_{13} erzeugen wir danach auf die übliche Weise mit Hilfe von $1-\epsilon_n$ und einer von N_q, N_r oder N_s induzierten Relation. Wir wollen diese Konstruktion als Lemma formulieren.

Lemma (Darstellung von $1-\epsilon_n$)
Seien die Bezeichnungen wie oben. Dann gibt es eine Darstellung von

$$1-\epsilon_n$$

als Produkt zyklotomischer Einheiten aus $E^{(n)}$, die aber nicht modulo Torsion in A_{13} liegen, die also nicht von der Form

$$1-\epsilon_q^{\pm 1}\epsilon_r^{\pm 1}\epsilon_s^{\pm 1}$$

(alle acht Kombinationen der Vorzeichen möglich) sind.

Beweis des Lemmas
Wir werden zunächst, wie es in der Vorbemerkung angedeutet wurde, eine Darstellung von $(1-\epsilon_n)^2$ herleiten, die nur aus Quadraten besteht. Zur besseren Übersicht wird der Beweis in vier Schritten durchgeführt. Im ersten Schritt werden wir in $\mathbb{Z}[\epsilon_n] = \mathbb{Z}[\epsilon_{qrs}]$ arbeiten, im nächsten Schritt im Ring $\mathbb{Z}[\epsilon_{qr}]$ und im dritten Schritt in $\mathbb{Z}[\epsilon_q]$. Dabei werden wir symmetrisch in q, r und s rechnen, so daß wir die Rechnungen in $\mathbb{Z}[\epsilon_{qr}]$ auch analog in $\mathbb{Z}[\epsilon_{rs}]$ und $\mathbb{Z}[\epsilon_{qs}]$ führen können und die Rechnungen in $\mathbb{Z}[\epsilon_q]$ analog in $\mathbb{Z}[\epsilon_r]$ und $\mathbb{Z}[\epsilon_s]$. Diese Überlegungen werden alle modulo Torsion geführt. Der Torsionsanteil wird schließlich im vierten Schritt diskutiert.

1.Schritt Wir betrachten wieder die vier Mengen

$$\begin{aligned} M_0 &:= \{x>0, y>0, z>0\},\\ M_x &:= \{x<0, y>0, z>0\},\\ M_y &:= \{x>0, y<0, z>0\},\\ M_z &:= \{x>0, y>0, z<0\}. \end{aligned}$$

Wenn wir das Produkt über alle Konjugierten von $1-\epsilon_n$ bilden, so ist dieses, da $1-\epsilon_n$ Einheit in $\mathbb{Z}[\epsilon_n]$ ist, gleich ± 1. Nun enthält $M^+ := M_0 \cup M_x \cup M_y \cup M_z$ *modulo Torsion* alle Elemente der Form $1-\epsilon_n^{(x,y,z)}$, und es sind jeweils $1-\epsilon_n^{(x,y,z)}$ und $1-\epsilon_n^{(-x,-y,-z)}$ modulo Torsion gleich. Es gilt also

$$\prod_{u\in M^+}^{2} u \overset{\text{tor}}{=} \prod_{(x,y,z)\in G_n} 1-\epsilon_n^{(x,y,z)} \overset{\text{tor}}{=} 1$$

und durch Wurzelziehen

$$\prod_{u\in M^+} u \overset{\text{tor}}{=} 1. \qquad (*)$$

Es genügt, eine Darstellung von

$$\prod_{u\in M_0}^{2} u$$

durch Quadrate zu finden, da alle Elemente aus M_0 außer $1-\epsilon_n$ nicht in A_{13} liegen.

Die Elemente N_q, N_r und N_s liefern die drei Gleichungen

$$\begin{aligned}\prod_{u\in M_0} u \prod_{u\in M_x} u &= \prod_{\substack{y>0\\ z\le 0}} 1-\epsilon_r^y\epsilon_s^z)^{\sigma_q-\sigma_{\hat{q}}},\\ \prod_{u\in M_0} u \prod_{u\in M_y} u &= \prod_{\substack{x>0\\ z\le 0}} 1-\epsilon_q^x\epsilon_s^z)^{\sigma_r-\sigma_{\hat{r}}},\\ \prod_{u\in M_0} u \prod_{u\in M_z} u &= \prod_{\substack{x>0\\ y\le 0}} 1-\epsilon_q^x\epsilon_r^y)^{\sigma_s-\sigma_{\hat{s}}}.\end{aligned}$$

Diese multiplizieren wir auf und erhalten unter Verwendung von $(*)$ die in allen drei Zahlen q, r und s symmetrische Darstellung

$$\begin{aligned}\prod_{u\in M_0}^{2} u &\overset{\text{tor}}{=} \prod_{u\in M_0}^{2} u \prod_{u\in M_0} u \prod_{u\in M_x} u \prod_{u\in M_y} u \prod_{u\in M_z} u\\ &= \prod_{\substack{x>0\\ y\le 0}} 1-\epsilon_q^x\epsilon_r^y)^{\sigma_s-\sigma_{\hat{s}}} \prod_{\substack{y>0\\ z\le 0}} 1-\epsilon_r^y\epsilon_s^z)^{\sigma_q-\sigma_{\hat{q}}} \prod_{\substack{x>0\\ z\le 0}} 1-\epsilon_q^x\epsilon_s^z)^{\sigma_r-\sigma_{\hat{r}}}.\end{aligned}$$

2.Schritt Wir definieren zunächst

$$u_{x,y} := 1-\epsilon_q^x\epsilon_r^y.$$

Es ist also

$$\begin{aligned}\prod_{\substack{x>0\\ y\le 0}} 1-\epsilon_q^x\epsilon_r^y)^{\sigma_s-\sigma_{\hat{s}}} &= \prod_{\substack{x>0\\ y\le 0}} \left((1-\epsilon_q^{sx}\epsilon_r^{sy})(1-\epsilon_q^{\hat{s}x}\epsilon_r^{\hat{s}y})^{-1}\right)\\ &= \prod_{\substack{x>0\\ y\le 0}} u_{sx,sy} \prod_{\substack{x>0\\ y>0}}^{-1} u_{\hat{s}x,\hat{s}y}.\end{aligned}$$

Es bezeichne nun $\tilde{s}$ die Primzahl, für die $\tilde{s}^\alpha = s$ für ein $\alpha\in\mathbb{N}$ gilt (es ist also $\tilde{s}\hat{s}=s$) und $\sigma := \sigma_{\tilde{s}}$. Wir definieren Q_s und R_s durch

$$Q_s := \prod_{x>0,\sigma x>0}^{-1} 1-\epsilon_q^{sx})^{\sigma_r-\sigma_{\hat{r}}}$$

und

$$R_s := \prod_{y>0,\sigma y>0}^{-1} 1-\epsilon_r^{sy})^{\sigma_q-\sigma_{\hat{q}}}.$$

Dabei bedeutet die Schreibweise $x>0,\sigma x>0$, daß das Produkt über alle $x\in G_q$, die die beiden Bedingungen $x>0$ und $\sigma x>0$ erfüllen, gebildet wird. Entsprechendes gilt für y.

Mit Hilfe dieser Elemente Q_s und R_s werden die durch N_q beziehungsweise N_r induzierten Relationen angewendet. Und zwar gilt

$$Q_s \prod_{\substack{x>0,\,\tau x>0\\ y<0}} \iota_{sx,sy} \;=\; \prod_{\substack{x>0,\,\sigma x>0\\ y<0}} u_{sx,sy} \;=\; (\cdots)^2 \prod_{\substack{x>0,\,\tau x>0\\ y<0}} \iota_{sx,sy}$$

und

$$R_s \prod_{\substack{x<0,\,\tau x<0\\ y>0}} \iota_{sx,sy} \;=\; \prod_{\substack{x>0,\,\sigma x>0\\ y>0}} u_{sx,sy} \;=\; (\cdots)^2 \prod_{\substack{x<0,\,\tau x<0\\ y>0}} \iota_{sx,sy}.$$

Die Schreibweise $(\cdots)^2$ soll andeuten, daß an dieser Stelle irgendwelche quadratische Terme stehen. Da die folgende Rechnung nur modulo Torsion interessiert, ist es erlaubt, in einem Produkt bei allen "x" und "y" gleichzeitig das Vorzeichen zu wechseln. Um zu verdeutlichen, wo dies benutzt wurde, steht an diesen Stellen "$\overset{\text{tor}}{=}$". Dort, wo nur "$=$" steht, handelt es sich um echte Gleichheit. So ergibt sich

$$\begin{aligned}
R_sQ_s \prod_{\substack{x>0,\,\tau x>0\\ y<0}} \iota_{sx,sy} &= R_sQ_s \prod_{\substack{x>0,\,\tau x>0\\ y<0}} \iota_{sx,sy} \prod_{\substack{x>0,\,\tau x<0\\ y<0}} \iota_{sx,sy} \\
&= (\cdots)^2\, R_s \prod_{\substack{x>0,\,\tau x>0\\ y<0}} \iota_{sx,sy} \prod_{\substack{x>0,\,\tau x<0\\ y<0}} \iota_{sx,sy} \\
&\overset{\text{tor}}{=} (\cdots)^2\, R_s \prod_{\substack{x<0,\,\tau x<0\\ y<0}} \iota_{sx,sy} \prod_{\substack{x>0,\,\tau x<0\\ y<0}} \iota_{sx,sy} \\
&= (\cdots)^2\, R_s \prod_{\substack{\sigma x<0\\ y<0}} \iota_{sx,sy} \\
&= (\cdots)^2\, R_s \prod_{\substack{\sigma x<0\\ y>0}} \iota_{sx,sy} \prod_{\substack{\sigma x<0\\ y<0}} \iota_{sx,sy} \\
&= (\cdots)^2 \prod_{\substack{\sigma x>0\\ y>0}} \iota_{sx,sy} \prod_{\substack{\sigma x<0\\ y<0}} \iota_{sx,sy} \\
&\overset{\text{tor}}{=} (\cdots)^2 \prod_{\substack{\sigma x>0\\ y>0}} \iota_{sx,sy} \prod_{\substack{\sigma x<0\\ y<0}} \iota_{sx,sy} \\
&= (\cdots)^2 \prod_{\substack{\sigma x>0\\ \sigma y>0}} \iota_{sx,sy}.
\end{aligned}$$

Mit der Variablentransformation $\sigma x \to x$ folgt, da $\sigma = \sigma_{\tilde{s}}$ und $\tilde{s}\hat{s} = s$ ist,

$$R_sQ_s \prod_{\substack{x>0,\,\tau x>0\\ y<0}} \iota_{sx,sy} \;\overset{\text{tor}}{=}\; (\cdots)^2 \prod_{\substack{x>0,\,\tau x>0\\ \sigma y>0}} \iota_{sx,sy} \;=\; (\cdots)^2 \prod_{\substack{x>0,\,\tau x>0\\ y<0}} \iota_{\hat{s}x,\hat{s}y},$$

somit

$$\prod_{\substack{x>0,\,\tau x>0\\ y<0}} \iota_{sx,sy} \prod_{\substack{x>0\\ y<0}}^{-1} u_{\hat{s}x,\hat{s}y} \;\overset{\text{tor}}{=}\; (\cdots)^2\; Q_s^{-1}R_s^{-1}.$$

Führen wir den 2. Schritt analog für (q,s) und (r,s) statt (q,r) durch (mit analogen Bezeichnungen), so erhält man als Zwischenergebnis aus den Schritten 1 und 2

$$(1-\epsilon_n)^2 \overset{\text{tor}}{=} (\cdots)^2\, Q_s^{-1}R_s^{-1}Q_r^{-1}S_r^{-1}R_q^{-1}S_q^{-1}.$$

Im dritten Schritt werden wir uns also um die Terme Q_s, R_s usw. kümmern.

3. Schritt Da die Argumentation symmetrisch in q, r und s ist, beschränken wir uns darauf, in $\mathbb{Z}[\epsilon_q]$ zu arbeiten. Es seien $\tilde{s}, \hat{s}$ und $\tilde{r}, \hat{r}$ wie im 2. Schritt definiert, also $s = \tilde{s}^\alpha$ mit $\tilde{s}$ Primzahl, $\hat{s} = \tilde{s}^{\alpha-1}$ und analog für $\tilde{r}$ und $\hat{r}$. Weiter sei $\sigma := \sigma_{\tilde{s}}$ und $\rho := \sigma_{\tilde{r}}$ Mit der Bezeichnung

$$v_x := 1 - \epsilon_q^{\hat{s}\hat{r}x}$$

ist

$$\begin{aligned} Q_r^{-1} &= \prod_{x>0,\rho x>0} (1-\epsilon_q^{rx})^{\sigma_s - \sigma_{\hat{s}}} \\ &= \prod_{x>0,\rho x>0} \left((1-\epsilon_q^{rsx})(1-\epsilon_q^{r\hat{s}x})^{-1}\right) \overset{\text{tor}}{=} \prod_{x>0,\rho x>0} v_{\sigma\rho x} \prod_{x>0,\rho x>0}^{-1} v_{\rho x} \end{aligned}$$

und

$$\begin{aligned} Q_s^{-1} &= \prod_{x>0,\sigma x>0} (1-\epsilon_q^{sx})^{\sigma_r - \sigma_{\hat{r}}} \\ &= \prod_{x>0,\sigma x>0} \left((1-\epsilon_q^{srx})(1-\epsilon_q^{s\hat{r}x})^{-1}\right) \overset{\text{tor}}{=} \prod_{x>0,\sigma x>0} v_{\rho\sigma x} \prod_{x>0,\sigma x>0}^{-1} v_{\sigma x}. \end{aligned}$$

Es ist zu zeigen, daß $Q_r^{-1}Q_s^{-1}$ Quadrat ist. Dazu betrachten wir die vier Mengen

$$\begin{aligned} D_1 &:= \rho & \{x \in G_q \mid x>0 \text{ und } \rho x>0\}, \\ D_2 &:= \sigma\rho & \{x \in G_q \mid x>0 \text{ und } \rho x>0\}, \\ D_3 &:= \sigma & \{x \in G_q \mid x>0 \text{ und } \sigma x>0\}, \\ D_4 &:= \rho\sigma & \{x \in G_q \mid x>0 \text{ und } \sigma x>0\}, \end{aligned}$$

und es ist

$$Q_r^{-1}Q_s^{-1} = \prod_{\sigma_a \in D_1} v_a \prod_{\sigma_a \in D_2}^{-1} v_a \prod_{\sigma_a \in D_3} v_a \prod_{\sigma_a \in D_4}^{-1} v_a.$$

Da $v_a \overset{\text{tor}}{=} v_{-a}$ ist, ist zu zeigen, daß, falls $\sigma_a \in G_q$ gegeben ist, σ_a oder σ_{-a} in genau zwei, gar keiner oder in allen vier Mengen D_1, D_2, D_3 und D_4 vorkommt. Wir schreiben $\sigma_b := \rho^{-1}\sigma^{-1}\sigma_a$. Es gilt:

$$\begin{aligned} \sigma_a \in D_1 &\Leftrightarrow \sigma\sigma_b > 0 \quad \text{und} \quad \sigma_a > 0, \\ \sigma_a \in D_2 &\Leftrightarrow \sigma_b > 0 \quad \text{und} \quad \rho\sigma_b > 0, \\ \sigma_a \in D_3 &\Leftrightarrow \rho\sigma_b > 0 \quad \text{und} \quad \sigma_a > 0, \\ \sigma_a \in D_4 &\Leftrightarrow \sigma_b > 0 \quad \text{und} \quad \sigma\sigma_b > 0. \end{aligned}$$

Wir verwenden zur Übersicht eine Tabelle. Der Eintrag σ_a in der Spalte D_i bedeutet dabei, daß σ_a mit den in der ersten Spalte angegebenen Eigenschaften

in der Menge D_i vorkommt. Da v_a mit v_{-a} identifiziert wird, sind jeweils die beiden Zeilen mit σ_a und σ_{-a} zusammengefaßt.

				D_1	D_2	D_3	D_4
$\sigma_b > 0$	$\rho\sigma_b > 0$	$\sigma\sigma_b > 0$	$\sigma_a > 0$	σ_a	σ_a	σ_a	σ_a
$\sigma_b < 0$	$\rho\sigma_b < 0$	$\sigma\sigma_b < 0$	$\sigma_a < 0$				
$\sigma_b < 0$	$\rho\sigma_b > 0$	$\sigma\sigma_b > 0$	$\sigma_a > 0$	σ_a		σ_a	
$\sigma_b > 0$	$\rho\sigma_b < 0$	$\sigma\sigma_b < 0$	$\sigma_a < 0$				
$\sigma_b > 0$	$\rho\sigma_b < 0$	$\sigma\sigma_b > 0$	$\sigma_a > 0$	σ_a			σ_a
$\sigma_b < 0$	$\rho\sigma_b > 0$	$\sigma\sigma_b < 0$	$\sigma_a < 0$				
$\sigma_b < 0$	$\rho\sigma_b < 0$	$\sigma\sigma_b > 0$	$\sigma_a > 0$	σ_a			
$\sigma_b > 0$	$\rho\sigma_b > 0$	$\sigma\sigma_b < 0$	$\sigma_a < 0$		σ_a		
$\sigma_b > 0$	$\rho\sigma_b > 0$	$\sigma\sigma_b < 0$	$\sigma_a > 0$		σ_a	σ_a	
$\sigma_b < 0$	$\rho\sigma_b < 0$	$\sigma\sigma_b > 0$	$\sigma_a < 0$				
$\sigma_b < 0$	$\rho\sigma_b > 0$	$\sigma\sigma_b < 0$	$\sigma_a > 0$			σ_a	
$\sigma_b > 0$	$\rho\sigma_b < 0$	$\sigma\sigma_b > 0$	$\sigma_a < 0$				σ_a
$\sigma_b > 0$	$\rho\sigma_b < 0$	$\sigma\sigma_b < 0$	$\sigma_a > 0$				
$\sigma_b < 0$	$\rho\sigma_b > 0$	$\sigma\sigma_b > 0$	$\sigma_a < 0$				
$\sigma_b < 0$	$\rho\sigma_b < 0$	$\sigma\sigma_b < 0$	$\sigma_a > 0$				
$\sigma_b > 0$	$\rho\sigma_b > 0$	$\sigma\sigma_b > 0$	$\sigma_a < 0$		σ_a		σ_a

Da in jeder der Zeilen die σ_a paarweise vorkommen, folgt die Behauptung.

4.Schritt Wir haben nun die Existenz einer Darstellung von $(1-\epsilon_n)^2$ modulo Torsion durch Quadrate hergeleitet. Das heißt, es gilt für irgendeine Einheitswurzel ϵ die Relation

$$(1-\epsilon_n)^2 = \epsilon\,(\cdots)^2\,.$$

Dabei steht $(\cdots)^2$ für irgendwelche Elemente aus $C^{(n)}$. Es ist zu zeigen, daß ϵ ein Quadrat eines Elementes aus $C^{(n)}$ ist. Dies ist aber trivialerweise der Fall wegen

$$\epsilon = ((1-\epsilon_n)(\cdots))^2 \in \left(C^{(n)}\right)^2.$$

Mit Hilfe der Schritte 1-4 erhalten wir also

$$(1-\epsilon_n)^2 \stackrel{\text{tor}}{=} \prod u_i^2$$

mit zyklotomischen Einheiten u_i, die nicht in A_{13} liegen. Die gesuchte Darstellung von $1-\epsilon_n$ ist somit

$$1-\epsilon_n \stackrel{\text{tor}}{=} \prod u_i.$$

QED.

3.3 Beispiele

Die Rechnungen im vorherigen Abschnitt sind so explizit, daß es möglich ist, ein Computerprogramm zu erstellen, das eine solche Basis berechnet. Ein solches in SIMATH geschriebenes Programm befindet sich kommentiert im Anhang. Die folgenden Beispiele wurden mit diesem Programm berechnet. Es wird immer nur Gleichheit modulo Torsion geliefert. Um den Torsionsanteil zu bestimmen, muß man die Terme auf eine Seite bringen und in $\mathbb{Q}[\epsilon_n]$ ausrechnen.

3.3.1 $n = 27 = 3^3$

Die ist ein Beispiel für den Fall, daß n Primzahlpotenz ist.

Sei ϵ_{27} eine beliebige, aber feste primitive 27-te Einheitswurzel und $\epsilon_9 := \epsilon_{27}^3$. Eine Basis besteht aus den Elementen

$$\begin{aligned}
&(1-\epsilon_{27}^{13})\,(1-\epsilon_{27})^{-1},\ (1-\epsilon_{27}^{11})\,(1-\epsilon_{27})^{-1},\ (1-\epsilon_{27}^{10})\,(1-\epsilon_{27})^{-1},\\
&(1-\epsilon_{27}^{8})\,(1-\epsilon_{27})^{-1},\ (1-\epsilon_{27}^{7})\,(1-\epsilon_{27})^{-1},\ (1-\epsilon_{27}^{5})\,(1-\epsilon_{27})^{-1},\\
&(1-\epsilon_{27}^{4})\,(1-\epsilon_{27})^{-1},\ (1-\epsilon_{27}^{2})\,(1-\epsilon_{27})^{-1}.
\end{aligned}$$

Die Darstellung der anderen Elemente durch Basiselemente sieht wie folgt aus (dabei ist die Reihenfolge der Faktoren auf der rechten Seite diejenige, die das Programm liefert):

$$\begin{aligned}
(1-\epsilon_9^{2})\,(1-\epsilon_9)^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{27}^{7})\,(1-\epsilon_{27}^{11})\,(1-\epsilon_{27}^{2})\\
&\quad (1-\epsilon_{27}^{8})^{-1}(1-\epsilon_{27}^{10})^{-1}(1-\epsilon_{27})^{-1}\\
(1-\epsilon_9^{4})\,(1-\epsilon_9)^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{27}^{5})\,(1-\epsilon_{27}^{13})\,(1-\epsilon_{27}^{4})\\
&\quad (1-\epsilon_{27}^{8})^{-1}(1-\epsilon_{27}^{10})^{-1}(1-\epsilon_{27})^{-1}\\
(1-\epsilon_9^{-4})\,(1-\epsilon_9)^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{27}^{13})\,(1-\epsilon_{27}^{5})\,(1-\epsilon_{27}^{4})\\
&\quad (1-\epsilon_{27}^{8})^{-1}(1-\epsilon_{27}^{10})^{-1}(1-\epsilon_{27})^{-1}\\
(1-\epsilon_9^{-2})\,(1-\epsilon_9)^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{27}^{11})\,(1-\epsilon_{27}^{7})\,(1-\epsilon_{27}^{2})\\
&\quad (1-\epsilon_{27}^{8})^{-1}(1-\epsilon_{27}^{10})^{-1}(1-\epsilon_{27})^{-1}\\
(1-\epsilon_{27}^{-13})\,(1-\epsilon_{27})^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{27}^{13})\,(1-\epsilon_{27})^{-1}\\
(1-\epsilon_{27}^{-11})\,(1-\epsilon_{27})^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{27}^{11})\,(1-\epsilon_{27})^{-1}\\
&\ \ \vdots\\
(1-\epsilon_{27}^{-2})\,(1-\epsilon_{27})^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{27}^{2})\,(1-\epsilon_{27})^{-1}
\end{aligned}$$

3.3.2 $n = 32 = 2^5$

Dieser Fall erscheint hier, um zu zeigen, daß auch Potenzen von 2 keine Schwierigkeiten bereiten. Sei ϵ_{32} eine beliebige, aber feste primitive 32-te Einheitswurzel, $\epsilon_{16} := \epsilon_{32}^2$ und $\epsilon_8 := \epsilon_{32}^4$. Eine Basis ist in diesem Fall

$$(1-\epsilon_{32}^{15})\,(1-\epsilon_{32})^{-1},\ (1-\epsilon_{32}^{13})\,(1-\epsilon_{32})^{-1},\ (1-\epsilon_{32}^{11})\,(1-\epsilon_{32})^{-1},$$
$$(1-\epsilon_{32}^{9})\,(1-\epsilon_{32})^{-1},\ (1-\epsilon_{32}^{7})\,(1-\epsilon_{32})^{-1},\ (1-\epsilon_{32}^{5})\,(1-\epsilon_{32})^{-1},$$
$$(1-\epsilon_{32}^{3})\,(1-\epsilon_{32})^{-1}.$$

Die Darstellung der anderen Erzeugenden lautet wie folgt:

$$\begin{aligned}
(1-\epsilon_8^{3})\,(1-\epsilon_8)^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{32}^{11})\,(1-\epsilon_{32}^{5})\,(1-\epsilon_{32}^{13})\\
&\quad (1-\epsilon_{32}^{3})\,(1-\epsilon_{32}^{9})^{-1}(1-\epsilon_{32}^{7})^{-1}\\
&\quad (1-\epsilon_{32}^{15})^{-1}(1-\epsilon_{32})^{-1}\\
(1-\epsilon_8^{-3})\,(1-\epsilon_8)^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{32}^{11})\,(1-\epsilon_{32}^{5})\,(1-\epsilon_{32}^{13})\\
&\quad (1-\epsilon_{32}^{3})\,(1-\epsilon_{32}^{9})^{-1}(1-\epsilon_{32}^{7})^{-1}\\
&\quad (1-\epsilon_{32}^{15})^{-1}(1-\epsilon_{32})^{-1}\\
(1-\epsilon_{16}^{3})\,(1-\epsilon_{16})^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{32}^{13})\,(1-\epsilon_{32}^{3})\,(1-\epsilon_{32}^{15})^{-1}\\
&\quad (1-\epsilon_{32})^{-1}\\
(1-\epsilon_{16}^{5})\,(1-\epsilon_{16})^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{32}^{11})\,(1-\epsilon_{32}^{5})\,(1-\epsilon_{32}^{15})^{-1}\\
&\quad (1-\epsilon_{32})^{-1}\\
(1-\epsilon_{16}^{7})\,(1-\epsilon_{16})^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{32}^{9})\,(1-\epsilon_{32}^{7})\,(1-\epsilon_{32}^{15})^{-1}\\
&\quad (1-\epsilon_{32})^{-1}\\
(1-\epsilon_{16}^{-7})\,(1-\epsilon_{16})^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{32}^{9})\,(1-\epsilon_{32}^{7})\,(1-\epsilon_{32}^{15})^{-1}\\
&\quad (1-\epsilon_{32})^{-1}\\
(1-\epsilon_{16}^{-5})\,(1-\epsilon_{16})^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{32}^{11})\,(1-\epsilon_{32}^{5})\,(1-\epsilon_{32}^{15})^{-1}\\
&\quad (1-\epsilon_{32})^{-1}\\
(1-\epsilon_{16}^{-3})\,(1-\epsilon_{16})^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{32}^{13})\,(1-\epsilon_{32}^{3})\,(1-\epsilon_{32}^{15})^{-1}\\
&\quad (1-\epsilon_{32})^{-1}\\
(1-\epsilon_{32}^{-15})\,(1-\epsilon_{32})^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{32}^{15})\,(1-\epsilon_{32})^{-1}\\
(1-\epsilon_{32}^{-13})\,(1-\epsilon_{32})^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{32}^{13})\,(1-\epsilon_{32})^{-1}\\
&\ \ \vdots\\
(1-\epsilon_{32}^{-3})\,(1-\epsilon_{32})^{-1} &\overset{\text{tor}}{=} (1-\epsilon_{32}^{3})\,(1-\epsilon_{32})^{-1}
\end{aligned}$$

3.3.3 $n = 35 = 5 \cdot 7$

Ein Beispiel mit zwei P-Teilern. Seien ϵ_5 und ϵ_7 primitive 5-te beziehungsweise 7-te Einheitswurzeln. Eine Basis ist hier

$$\begin{array}{ccc} 1-\epsilon_5^2\epsilon_7^{-1}, & 1-\epsilon_5^2\epsilon_7^{-2}, & 1-\epsilon_5^2\epsilon_7^{-3}, \\ 1-\epsilon_5^2\epsilon_7^{3}, & 1-\epsilon_5^2\epsilon_7^{2}, & 1-\epsilon_5\epsilon_7^{-1}, \\ 1-\epsilon_5\epsilon_7^{-2}, & 1-\epsilon_5\epsilon_7^{-3}, & (1-\epsilon_5^2)\,(1-\epsilon_5)^{-1}, \\ (1-\epsilon_7^3)\,(1-\epsilon_7)^{-1}, & (1-\epsilon_7^2)\,(1-\epsilon_7)^{-1}. & \end{array}$$

Die anderen Elemente werden folgendermaßen erzeugt (dabei werden hier, um Platz zu sparen, nur solche Elemente berücksichtigt, die nicht schon modulo Torsion gleich einem Basiselement sind):

$$\begin{aligned} 1-\epsilon_5\epsilon_7 &\overset{\text{tor}}{=} (1-\epsilon_5\epsilon_7^{-1})^{-1}(1-\epsilon_5^2\epsilon_7^{-2})\,(1-\epsilon_5^2\epsilon_7^{-3}) \\ &\quad (1-\epsilon_5^2\epsilon_7^{3})\,(1-\epsilon_5^2\epsilon_7^{2})\,(1-\epsilon_5^2) \\ &\quad (1-\epsilon_5)^{-1}(1-\epsilon_7)^{-1}(1-\epsilon_7^2) \\ 1-\epsilon_5\epsilon_7^2 &\overset{\text{tor}}{=} (1-\epsilon_5\epsilon_7^{-2})^{-1}(1-\epsilon_5^2\epsilon_7^{-2})^{-1}(1-\epsilon_5^2\epsilon_7^{2})^{-1} \\ &\quad (1-\epsilon_7^2)^{-1}(1-\epsilon_7^3) \\ 1-\epsilon_5\epsilon_7^3 &\overset{\text{tor}}{=} (1-\epsilon_5\epsilon_7^{-3})^{-1}(1-\epsilon_5^2\epsilon_7^{-3})^{-1}(1-\epsilon_5^2\epsilon_7^{3})^{-1} \\ &\quad (1-\epsilon_7^3)^{-1}(1-\epsilon_7) \\ 1-\epsilon_5^2\epsilon_7 &\overset{\text{tor}}{=} (1-\epsilon_5^2\epsilon_7^{-1})^{-1}(1-\epsilon_5^2\epsilon_7^{-2})^{-1}(1-\epsilon_5^2\epsilon_7^{-3})^{-1} \\ &\quad (1-\epsilon_5^2\epsilon_7^{3})^{-1}(1-\epsilon_5^2\epsilon_7^{2})^{-1}(1-\epsilon_5^2)^{-1} \\ &\quad (1-\epsilon_5) \\ 1-\epsilon_5^{-2}\epsilon_7^{-1} &\overset{\text{tor}}{=} (1-\epsilon_5^2\epsilon_7^{-1})^{-1}(1-\epsilon_5^2\epsilon_7^{-2})^{-1}(1-\epsilon_5^2\epsilon_7^{-3})^{-1} \\ &\quad (1-\epsilon_5^2\epsilon_7^{3})^{-1}(1-\epsilon_5^2\epsilon_7^{2})^{-1}(1-\epsilon_5^2)^{-1} \\ &\quad (1-\epsilon_5) \\ 1-\epsilon_5^{-1}\epsilon_7^{-3} &\overset{\text{tor}}{=} (1-\epsilon_5\epsilon_7^{-3})^{-1}(1-\epsilon_5^2\epsilon_7^{-3})^{-1}(1-\epsilon_5^2\epsilon_7^{3})^{-1} \\ &\quad (1-\epsilon_7^3)^{-1}(1-\epsilon_7) \\ 1-\epsilon_5^{-1}\epsilon_7^{-2} &\overset{\text{tor}}{=} (1-\epsilon_5\epsilon_7^{-2})^{-1}(1-\epsilon_5^2\epsilon_7^{-2})^{-1}(1-\epsilon_5^2\epsilon_7^{2})^{-1} \\ &\quad (1-\epsilon_7^2)^{-1}(1-\epsilon_7^3) \\ 1-\epsilon_5^{-1}\epsilon_7^{-1} &\overset{\text{tor}}{=} (1-\epsilon_5\epsilon_7^{-1})^{-1}(1-\epsilon_5^2\epsilon_7^{-2})\,(1-\epsilon_5^2\epsilon_7^{-3}) \\ &\quad (1-\epsilon_5^2\epsilon_7^{3})\,(1-\epsilon_5^2\epsilon_7^{2})\,(1-\epsilon_5^2) \\ &\quad (1-\epsilon_5)^{-1}(1-\epsilon_7)^{-1}(1-\epsilon_7^2) \end{aligned}$$

3.3.4 $n = 60 = 2^2 \cdot 3 \cdot 5$

60 ist die kleinste natürliche Zahl mit drei P-Teilern und inkongruent 2 modulo 4. Es sei ϵ_d für $d = 3,\ 4,\ 5$ eine primitive d-te Einheitswurzel. Eine Basis gemäß

unserer Konstruktion ist in diesem Fall

$$1-\epsilon_4^{-1}\epsilon_5^2,\ 1-\epsilon_4^{-1}\epsilon_5,\ 1-\epsilon_4\epsilon_3^{-1}\epsilon_5^2,$$
$$1-\epsilon_4\epsilon_3^{-1},\ 1-\epsilon_3\epsilon_5^{-1},\ 1-\epsilon_3\epsilon_5^{-2},$$
$$(1-\epsilon_5^2)\,(1-\epsilon_5)^{-1}.$$

a) Erzeugende, die nicht in $E^{(n)}$ liegen (ϵ_2 ist natürlich gleich -1, wird hier aber trotzdem ϵ_2 geschrieben):

$$\begin{aligned}
1-\epsilon_2\epsilon_5 &\overset{\text{tor}}{=} (1-\epsilon_5)^{-1}(1-\epsilon_5^2)\\
1-\epsilon_2\epsilon_5^2 &\overset{\text{tor}}{=} (1-\epsilon_5^2)^{-1}(1-\epsilon_5)\\
1-\epsilon_2\epsilon_5^{-2} &\overset{\text{tor}}{=} (1-\epsilon_5^2)^{-1}(1-\epsilon_5)\\
1-\epsilon_2\epsilon_5^{-1} &\overset{\text{tor}}{=} (1-\epsilon_5)^{-1}(1-\epsilon_5^2)\\
1-\epsilon_2\epsilon_3\epsilon_5 &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-1})^{-1}(1-\epsilon_3\epsilon_5^{-2})^{-1}(1-\epsilon_5^2)^{-1}\\
&\quad\ (1-\epsilon_5)\\
1-\epsilon_2\epsilon_3\epsilon_5^2 &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-1})\,(1-\epsilon_3\epsilon_5^{-2})^{-1}\\
1-\epsilon_2\epsilon_3\epsilon_5^{-2} &\overset{\text{tor}}{=} (1-\epsilon_5)^{-2}(1-\epsilon_3\epsilon_5^{-1})^{-1}(1-\epsilon_3\epsilon_5^{-2})\\
&\quad\ (1-\epsilon_5^2)^2\\
1-\epsilon_2\epsilon_3\epsilon_5^{-1} &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-1})\,(1-\epsilon_3\epsilon_5^{-2})\,(1-\epsilon_5^2)^{-1}\\
&\quad\ (1-\epsilon_5)\\
1-\epsilon_2\epsilon_3^{-1}\epsilon_5 &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-1})\,(1-\epsilon_3\epsilon_5^{-2})\,(1-\epsilon_5^2)^{-1}\\
&\quad\ (1-\epsilon_5)\\
1-\epsilon_2\epsilon_3^{-1}\epsilon_5^2 &\overset{\text{tor}}{=} (1-\epsilon_5)^{-2}(1-\epsilon_3\epsilon_5^{-1})^{-1}(1-\epsilon_5^2)^2\\
&\quad\ (1-\epsilon_3\epsilon_5^{-2})\\
1-\epsilon_2\epsilon_3^{-1}\epsilon_5^{-2} &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-1})\,(1-\epsilon_3\epsilon_5^{-2})^{-1}\\
1-\epsilon_2\epsilon_3^{-1}\epsilon_5^{-1} &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-1})^{-1}(1-\epsilon_3\epsilon_5^{-2})^{-1}(1-\epsilon_5^2)^{-1}\\
&\quad\ (1-\epsilon_5)
\end{aligned}$$

Bemerkung: Es gilt $1-\epsilon_2\epsilon_3 = 1+\epsilon_3 = -\epsilon_3^2 \overset{\text{tor}}{=} 1$, so daß dieser und ähnliche Fälle in obiger Liste nicht auftauchen.

b) Erzeugende aus einer der Mengen $E^{(12)}$, $E^{(15)}$ oder $E^{(20)}$:

$$\begin{aligned}
(1-\epsilon_5^{-2})\,(1-\epsilon_5)^{-1} &\overset{\text{tor}}{=} (1-\epsilon_5^2)\,(1-\epsilon_5)^{-1}\\
1-\epsilon_4\epsilon_3 &\overset{\text{tor}}{=} (1-\epsilon_4\epsilon_3^{-1})^{-1}\\
1-\epsilon_4^{-1}\epsilon_3 &\overset{\text{tor}}{=} 1-\epsilon_4\epsilon_3^{-1}\\
1-\epsilon_4^{-1}\epsilon_3^{-1} &\overset{\text{tor}}{=} (1-\epsilon_4\epsilon_3^{-1})^{-1}
\end{aligned}$$

$$
\begin{aligned}
1-\epsilon_4\epsilon_5 &\overset{\text{tor}}{=} (1-\epsilon_4\epsilon_5^{-1})^{-1}(1-\epsilon_5^2)^{-1}(1-\epsilon_5)\\
1-\epsilon_4\epsilon_5^2 &\overset{\text{tor}}{=} (1-\epsilon_4\epsilon_5^{-2})^{-1}(1-\epsilon_5)^{-1}(1-\epsilon_5^2)\\
1-\epsilon_4^{-1}\epsilon_5 &\overset{\text{tor}}{=} 1-\epsilon_4\epsilon_5^{-1}\\
1-\epsilon_4^{-1}\epsilon_5^2 &\overset{\text{tor}}{=} 1-\epsilon_4\epsilon_5^{-2}\\
1-\epsilon_4^{-1}\epsilon_5^{-2} &\overset{\text{tor}}{=} (1-\epsilon_4\epsilon_5^{-2})^{-1}(1-\epsilon_5)^{-1}(1-\epsilon_5^2)\\
1-\epsilon_3\epsilon_5 &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-1})^{-1}(1-\epsilon_5)^{-1}(1-\epsilon_5^2)\\
1-\epsilon_3\epsilon_5^2 &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-2})^{-1}(1-\epsilon_5^2)^{-1}(1-\epsilon_5)\\
1-\epsilon_3^{-1}\epsilon_5 &\overset{\text{tor}}{=} 1-\epsilon_3\epsilon_5^{-1}\\
1-\epsilon_3^{-1}\epsilon_5^2 &\overset{\text{tor}}{=} 1-\epsilon_3\epsilon_5^{-2}\\
1-\epsilon_3^{-1}\epsilon_5^{-2} &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-2})^{-1}(1-\epsilon_5^2)^{-1}(1-\epsilon_5)\\
1-\epsilon_3^{-1}\epsilon_5^{-1} &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-1})^{-1}(1-\epsilon_5)^{-1}(1-\epsilon_5^2)
\end{aligned}
$$

c) sonstige Erzeugende:

$$
\begin{aligned}
1-\epsilon_4\epsilon_3\epsilon_5 &\overset{\text{tor}}{=} (1-\epsilon_5)^{-1}(1-\epsilon_5^2)\,(1-\epsilon_3\epsilon_5^{-1})\\
&\quad (1-\epsilon_4\epsilon_3^{-1}\epsilon_5^2)\,(1-\epsilon_4\epsilon_3^{-1})\,(1-\epsilon_4^{-1}\epsilon_5^2)^{-1}\\
1-\epsilon_4\epsilon_3\epsilon_5^2 &\overset{\text{tor}}{=} (1-\epsilon_4\epsilon_3^{-1}\epsilon_5^2)^{-1}(1-\epsilon_5^2)^{-1}(1-\epsilon_5)\\
&\quad (1-\epsilon_4^{-1}\epsilon_5^2)\,(1-\epsilon_4^{-1}\epsilon_5)\\
1-\epsilon_4\epsilon_3\epsilon_5^{-2} &\overset{\text{tor}}{=} (1-\epsilon_4\epsilon_3^{-1}\epsilon_5^2)^{-1}(1-\epsilon_3\epsilon_5^{-1})^{-1}(1-\epsilon_3\epsilon_5^{-2})^{-1}\\
&\quad (1-\epsilon_5^2)^{-1}(1-\epsilon_5)\\
1-\epsilon_4\epsilon_3\epsilon_5^{-1} &\overset{\text{tor}}{=} (1-\epsilon_4\epsilon_3^{-1}\epsilon_5^2)\,(1-\epsilon_3\epsilon_5^{-2})\,(1-\epsilon_5^2)\\
&\quad (1-\epsilon_5)^{-1}(1-\epsilon_4^{-1}\epsilon_5)^{-1}(1-\epsilon_4\epsilon_3^{-1})\\
1-\epsilon_4\epsilon_3^{-1}\epsilon_5 &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-1})^{-1}(1-\epsilon_4\epsilon_3^{-1}\epsilon_5^2)^{-1}(1-\epsilon_4\epsilon_3^{-1})^{-1}\\
&\quad (1-\epsilon_4^{-1}\epsilon_5)\,(1-\epsilon_5)^{-1}(1-\epsilon_5^2)\\
1-\epsilon_4\epsilon_3^{-1}\epsilon_5^{-2} &\overset{\text{tor}}{=} (1-\epsilon_4\epsilon_3^{-1}\epsilon_5^2)\,(1-\epsilon_3\epsilon_5^{-1})\,(1-\epsilon_3\epsilon_5^{-2})\\
&\quad (1-\epsilon_4^{-1}\epsilon_5^2)^{-1}(1-\epsilon_4^{-1}\epsilon_5)^{-1}\\
1-\epsilon_4\epsilon_3^{-1}\epsilon_5^{-1} &\overset{\text{tor}}{=} (1-\epsilon_5)\,(1-\epsilon_5^2)^{-1}(1-\epsilon_4\epsilon_3^{-1}\epsilon_5^2)^{-1}\\
&\quad (1-\epsilon_4\epsilon_3^{-1})^{-1}(1-\epsilon_4^{-1}\epsilon_5^2)\,(1-\epsilon_3\epsilon_5^{-2})^{-1}\\
1-\epsilon_4^{-1}\epsilon_3\epsilon_5 &\overset{\text{tor}}{=} (1-\epsilon_5)\,(1-\epsilon_5^2)^{-1}(1-\epsilon_4\epsilon_3^{-1}\epsilon_5^2)^{-1}\\
&\quad (1-\epsilon_4\epsilon_3^{-1})^{-1}(1-\epsilon_4^{-1}\epsilon_5^2)\,(1-\epsilon_3\epsilon_5^{-2})^{-1}\\
1-\epsilon_4^{-1}\epsilon_3\epsilon_5^2 &\overset{\text{tor}}{=} (1-\epsilon_4\epsilon_3^{-1}\epsilon_5^2)\,(1-\epsilon_3\epsilon_5^{-1})\,(1-\epsilon_3\epsilon_5^{-2})\\
&\quad (1-\epsilon_4^{-1}\epsilon_5^2)^{-1}(1-\epsilon_4^{-1}\epsilon_5)^{-1}\\
1-\epsilon_4^{-1}\epsilon_3\epsilon_5^{-2} &\overset{\text{tor}}{=} 1-\epsilon_4\epsilon_3^{-1}\epsilon_5^2
\end{aligned}
$$

$$
\begin{aligned}
1-\epsilon_4^{-1}\epsilon_3\epsilon_5^{-1} &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-1})^{-1}(1-\epsilon_4\epsilon_3^{-1}\epsilon_5^{2})^{-1}(1-\epsilon_4\epsilon_3^{-1})^{-1}\\
&\quad (1-\epsilon_4^{-1}\epsilon_5)\,(1-\epsilon_5)^{-1}(1-\epsilon_5^{2})\\
1-\epsilon_4^{-1}\epsilon_3^{-1}\epsilon_5 &\overset{\text{tor}}{=} (1-\epsilon_4\epsilon_3^{-1}\epsilon_5^{2})\,(1-\epsilon_3\epsilon_5^{-2})\,(1-\epsilon_5^{2})\\
&\quad (1-\epsilon_5)^{-1}(1-\epsilon_4^{-1}\epsilon_5)^{-1}(1-\epsilon_4\epsilon_3^{-1})\\
1-\epsilon_4^{-1}\epsilon_3^{-1}\epsilon_5^{2} &\overset{\text{tor}}{=} (1-\epsilon_4\epsilon_3^{-1}\epsilon_5^{2})^{-1}(1-\epsilon_3\epsilon_5^{-1})^{-1}(1-\epsilon_3\epsilon_5^{-2})^{-1}\\
&\quad (1-\epsilon_5^{2})^{-1}(1-\epsilon_5)\\
1-\epsilon_4^{-1}\epsilon_3^{-1}\epsilon_5^{-2} &\overset{\text{tor}}{=} (1-\epsilon_4\epsilon_3^{-1}\epsilon_5^{2})^{-1}(1-\epsilon_5^{2})^{-1}(1-\epsilon_5)\\
&\quad (1-\epsilon_4^{-1}\epsilon_5^{2})\,(1-\epsilon_4^{-1}\epsilon_5)\\
1-\epsilon_4^{-1}\epsilon_3^{-1}\epsilon_5^{-1} &\overset{\text{tor}}{=} (1-\epsilon_5)^{-1}(1-\epsilon_5^{2})\,(1-\epsilon_3\epsilon_5^{-1})\\
&\quad (1-\epsilon_4\epsilon_3^{-1}\epsilon_5^{2})\,(1-\epsilon_4\epsilon_3^{-1})\,(1-\epsilon_4^{-1}\epsilon_5^{2})^{-1}
\end{aligned}
$$

3.3.5 Weitere Fälle

Eine Auflistung, wie sie in den vorherigen Abschnitten durchgeführt wurde, ist natürlich auch für größere Zahlen n mit höchstens drei P-Teilern möglich. Sie bringt allerdings nichts substantiell Neues. Hauptsächlich ist die Basisdarstellung von $1-\epsilon_n = 1-\epsilon_q\epsilon_r\epsilon_s$ interessant, da diese zu einer Relation innerhalb der zyklotomischen Einheiten führt, die nicht direkt durch N_q, N_r oder N_s geliefert wird. Im Fall $n = 105 = 3\cdot 5\cdot 7$ lautet diese Relation:

$$
\begin{aligned}
1-\epsilon_3\epsilon_5\epsilon_7 &\overset{\text{tor}}{=} (1-\epsilon_3^{-1}\epsilon_7^{3})^{-1}(1-\epsilon_7^{2})^{-1}(1-\epsilon_7)\\
&\quad (1-\epsilon_5^{2}\epsilon_7^{3})^{-1}(1-\epsilon_5^{2}\epsilon_7^{-2})^{-1}(1-\epsilon_5\epsilon_7^{-1})\\
&\quad (1-\epsilon_3\epsilon_5^{-2}\epsilon_7^{2})\,(1-\epsilon_5^{2}\epsilon_7^{-1})^{-1}(1-\epsilon_3\epsilon_5^{-1}\epsilon_7^{2})\\
&\quad (1-\epsilon_3\epsilon_5^{-2}\epsilon_7^{3})\,(1-\epsilon_5^{2}\epsilon_7^{2})^{-2}(1-\epsilon_5\epsilon_7^{-3})\\
&\quad (1-\epsilon_3\epsilon_5^{-1}\epsilon_7^{3})\,(1-\epsilon_5^{2})^{-2}(1-\epsilon_3\epsilon_5^{-1})\\
&\quad (1-\epsilon_3^{-1}\epsilon_5^{2}\epsilon_7)\,(1-\epsilon_3^{-1}\epsilon_7^{2})^{-1}(1-\epsilon_5)^{2}.
\end{aligned}
$$

Im Fall $n = 900 = 2^2\cdot 3^2\cdot 5^2$, das kleinste Beispiel, in dem alle Primfaktoren mindestens quadratisch vorkommen, ist die Darstellung von $1-\epsilon_4\epsilon_9\epsilon_{25}$:

$$
\begin{aligned}
1-\epsilon_4\epsilon_9\epsilon_{25} &\overset{\text{tor}}{=} (1-\epsilon_4^{-1}\epsilon_{25}^{7})^{-1}(1-\epsilon_4^{-1}\epsilon_{25}^{6})\,(1-\epsilon_9^{2}\epsilon_{25}^{4})^{-1}\\
&\quad (1-\epsilon_9^{2}\epsilon_{25}^{-4})^{-1}(1-\epsilon_9\epsilon_{25}^{-4})^{-1}(1-\epsilon_4\epsilon_9^{-4}\epsilon_{25}^{2})\\
&\quad (1-\epsilon_4\epsilon_9^{-2}\epsilon_{25}^{2})\,(1-\epsilon_4\epsilon_9^{-1}\epsilon_{25}^{2})\,(1-\epsilon_{25}^{7})^{-1}\\
&\quad (1-\epsilon_9^{2}\epsilon_{25}^{6})^{-1}(1-\epsilon_9^{4}\epsilon_{25}^{6})^{-1}(1-\epsilon_9^{2}\epsilon_{25}^{-6})^{-1}\\
&\quad (1-\epsilon_9\epsilon_{25}^{-6})^{-1}(1-\epsilon_4\epsilon_9^{-4}\epsilon_{25}^{3})\,(1-\epsilon_4\epsilon_9^{-2}\epsilon_{25}^{3})\\
&\quad (1-\epsilon_4\epsilon_9^{-1}\epsilon_{25}^{3})\,(1-\epsilon_4\epsilon_9^{-4}\epsilon_{25}^{4})\,(1-\epsilon_4\epsilon_9^{-2}\epsilon_{25}^{4})\\
&\quad (1-\epsilon_4\epsilon_9^{-1}\epsilon_{25}^{4})\,(1-\epsilon_4\epsilon_9^{-4}\epsilon_{25}^{6})\,(1-\epsilon_4\epsilon_9^{-2}\epsilon_{25}^{6})
\end{aligned}
$$

$$
\begin{aligned}
&(1-\epsilon_4\epsilon_9^{-1}\epsilon_{25}^{6})\,(1-\epsilon_4\epsilon_9^{-4}\epsilon_{25}^{7})\,(1-\epsilon_{25}^{2})^{-1}\\
&(1-\epsilon_{25}^{9})\,(1-\epsilon_9^{4}\epsilon_{25}^{3})\,(1-\epsilon_9\epsilon_{25}^{-3})\\
&(1-\epsilon_4\epsilon_9^{-2}\epsilon_{25}^{7})\,(1-\epsilon_4\epsilon_9^{-1}\epsilon_{25}^{7})\,(1-\epsilon_4^{-1}\epsilon_{25}^{3})^{-1}\\
&(1-\epsilon_4\epsilon_9^{-4}\epsilon_{25}^{8})\,(1-\epsilon_{25}^{4})^{2}(1-\epsilon_9^{4}\epsilon_{25}^{7})\\
&(1-\epsilon_9\epsilon_{25}^{-7})\,(1-\epsilon_4\epsilon_9^{-2}\epsilon_{25}^{8})\,(1-\epsilon_4\epsilon_9^{-1}\epsilon_{25}^{8})\\
&(1-\epsilon_4^{-1}\epsilon_{25}^{2})\,(1-\epsilon_4\epsilon_9^{-4}\epsilon_{25}^{9})\,(1-\epsilon_{25})^{-1}\\
&(1-\epsilon_9^{4}\epsilon_{25}^{11})\,(1-\epsilon_9\epsilon_{25}^{-11})\,(1-\epsilon_4\epsilon_9^{-2}\epsilon_{25}^{9})\\
&(1-\epsilon_4\epsilon_9^{-1}\epsilon_{25}^{9})\,(1-\epsilon_4^{-1}\epsilon_{25})^{-1}(1-\epsilon_4^{-1}\epsilon_{25}^{8})\\
&(1-\epsilon_4\epsilon_9^{-4}\epsilon_{25}^{11})\,(1-\epsilon_4\epsilon_9^{-2}\epsilon_{25}^{11})\,(1-\epsilon_4\epsilon_9^{-1}\epsilon_{25}^{11})\\
&(1-\epsilon_4^{-1}\epsilon_{25}^{11})\,(1-\epsilon_4\epsilon_9^{-4}\epsilon_{25}^{12})\,(1-\epsilon_4\epsilon_9^{-2}\epsilon_{25}^{12})\\
&(1-\epsilon_9^{4})\,(1-\epsilon_9^{2}\epsilon_{25}^{2})^{-1}(1-\epsilon_4\epsilon_9^{-1}\epsilon_{25}^{12})\\
&(1-\epsilon_4^{-1}\epsilon_9^{2}\epsilon_{25})\,(1-\epsilon_{25}^{6})^{-1}(1-\epsilon_9)^{-1}\\
&(1-\epsilon_4\epsilon_9^{-2})\,(1-\epsilon_4^{-1}\epsilon_9^{4}\epsilon_{25})\,(1-\epsilon_9^{2}\epsilon_{25}^{8})^{-1}\\
&(1-\epsilon_9^{2}\epsilon_{25}^{12})^{-1}(1-\epsilon_9^{2}\epsilon_{25}^{-9})^{-1}(1-\epsilon_9^{2}\epsilon_{25}^{-1})^{-1}\\
&(1-\epsilon_{25}^{3})\,(1-\epsilon_9^{2}\epsilon_{25}^{-2})^{-1}.
\end{aligned}
$$

Anhang A

Es sei m eine natürliche Zahl und χ ein Charakter modulo m ungleich dem Hauptcharakter. Es wird das Nichtverschwinden von $\mathrm{L}(1,\chi)$ hergeleitet. Dazu betrachten wir für ein reelles $s \geq 1$ die unendliche Reihe

$$\mathrm{L}(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

Zur Konvergenz der Reihe und zum Nichtverschwinden dieser Funktion im Punkte 1 gibt es in der Literatur zahlreiche Beweise. Als "Standardbeweis" hat sich ein Beweis herausgebildet, der mit Hilfe von Sätzen aus der Funktionentheorie arbeitet. In diesem Anhang wird nun ein Beweis geführt, der ohne wesentlichen Einstieg in die Funktionentheorie auskommt. Es wird statt dessen mit Idealen zyklotomischer Körper gerechnet. Ein solcher Beweis, der die Eigenschaften zyklotomischer Körper benutzt, erscheint im Zusammenhang mit dieser Arbeit angemessener als ein mit Hilfe von Funktionentheorie geführter. Die folgenden Lemmata sind bis auf Lemma 2, das im Kern auf einen Artikel von Zassenhaus zurückgeht, Standardargumente, wie sie im Zusammenhang mit der L-Funktion öfters verwendet werden. *Lemma 1*

Es sei χ ein Charakter modulo m, aber nicht der Hauptcharakter. Dann konvergiert $\mathrm{L}(s,\chi)$ für $s \geq 1$ und ist in $s = 1$ eine rechtsstetige Funktion.

Beweis

Wir zeigen zuerst, daß $\mathrm{L}(s,\chi)$ für $s \geq 1$ konvergiert und es eine positive Zahl c_1 gibt, so daß für alle $K \in \mathbb{N}$ und $s \geq 1$ die Abschätzung

$$\left|\sum_{n=K}^{\infty} \frac{\chi(n)}{n^s}\right| \quad \leq \quad \frac{c_1}{K}$$

gilt. Dazu benutzen wir das Abelsche Lemma (vgl. Serre, S. 109, Lemma 2):

Seien zu zwei natürlichen Zahlen M und N für $M \leq n \leq N$ Zahlen a_n und b_n gegeben. Dann ist

$$\sum_{n=M}^{N} a_n b_n = \sum_{n=M}^{N-1} ((\sum_{\nu=M}^{n} a_\nu)(b_n - b_{n+1})) + b_N \sum_{\nu=M}^{N} a_\nu.$$

Dies folgt aus

$$\begin{aligned}\text{r.S.} &= \sum_{n=M}^{N}\sum_{\nu=M}^{n} a_\nu b_n - \sum_{n=M}^{N-1}\sum_{\nu=M}^{n} a_\nu b_{n+1} = \sum_{n=M}^{N}\sum_{\nu=M}^{n} a_\nu b_n - \sum_{n=M+1}^{N}\sum_{\nu=M}^{n-1} a_\nu b_{n+1} \\ &= \sum_{n=M+1}^{N} \underbrace{(\sum_{\nu=M}^{n} a_\nu - \sum_{\nu=M}^{n-1} a_\nu)}_{=a_n} b_n + a_M b_M = \sum_{n=M}^{N} a_n b_n.\end{aligned}$$

Es gilt, da χ nicht Hauptcharakter ist,

$$\sum_{a=1}^{m} \chi(a) = 0.$$

Allgemeiner folgt daraus, da $\chi(a+m) = \chi(a)$ ist, sogar

$$\sum_{a=km+1}^{(k+1)m} \chi(a) = 0$$

mit k aus $\mathbb{Z}$ beliebig. Man erhält damit für zwei natürliche Zahlen M und N

$$|\sum_{n=M}^{N} \chi(n)| \leq c_1$$

mit einer positiven Zahl c_1 unabhängig von M und N.
Sei nun $K \in \mathbb{N}$. Wendet man auf

$$\sum_{n=K}^{N} \frac{\chi(n)}{n^s}$$

das Abelsche Lemma mit $a_n := \chi(n)$ und $b_n := \dfrac{1}{n^s}$ an und schätzt die auftretenden Summen durch c_1 ab, so erhält man

$$|\sum_{n=K}^{N} \frac{\chi(n)}{n^s}| = |\sum_{n=K}^{N-1} \left((\sum_{\nu=K}^{n} \chi(\nu))(\frac{1}{n^s} - \frac{1}{(n+1)^s}) \right) + \frac{1}{N^s} \sum_{\nu=K}^{N} \chi(\nu)|$$
$$\leq c_1 |\sum_{n=K}^{N-1} (\frac{1}{n^s} - \frac{1}{(n+1)^s})| + c_1 \frac{1}{N^s} \leq c_1 \left((\frac{1}{K^s} - \frac{1}{N^s}) + \frac{1}{N^s} \right) \leq \frac{c_1}{K},$$

für $s \geq 1$ und alle $N \in \mathbb{N}$, und es folgt die Konvergenz von $\mathrm{L}(s,\chi)$ nach dem Cauchyschen Konvergenzkriterium.

Es bleibt zu zeigen, daß $\mathrm{L}(s,\chi)$ für einen Charakter χ ungleich dem Hauptcharakter eine in $s=1$ rechtsstetige Funktion ist. Mit anderen Worten für jedes $\delta > 0$ ist ein $s_0 > 1$ zu finden, so daß $|\mathrm{L}(1,\chi) - \mathrm{L}(s,\chi)| < \delta$ gilt für $1 < s < s_0$. Für $K \in \mathbb{N}$ beliebig folgt aus der Dreiecksungleichung

$$\begin{aligned} |\mathrm{L}(1,\chi) - \mathrm{L}(s,\chi)| &\leq |\sum_{n=K}^{\infty} \frac{\chi(n)}{n}| + |\sum_{n=K}^{\infty} \frac{\chi(n)}{n^s}| + |\sum_{n=1}^{K-1} \frac{\chi(n)}{n} - \sum_{n=1}^{K-1} \frac{\chi(n)}{n^s}| \\ &\leq \frac{2c_1}{K} + |\sum_{n=1}^{K-1} \frac{\chi(n)}{n} - \sum_{n=1}^{K-1} \frac{\chi(n)}{n^s}|. \end{aligned}$$

Man betrachtet nun diese Ungleichung für ein K, für das der erste Term kleiner als $\delta/2$ wird, und wählt s_0 genügend dicht an 1, so daß auch der zweite Term für $1 < s < s_0$ kleiner $\delta/2$ wird.

QED.

Wir werden in den nächsten drei Lemmata zeigen, daß es eine positive Konstante c gibt, so daß für alle $s > 1$ die Abschätzung $\mathrm{L}(s, \chi) \geq c$ gilt. Auf Grund der eben bewiesenen Stetigkeit folgt dann $\mathrm{L}(1, \chi) \geq c$.

Für ein Ideal $\mathrm{A} \trianglelefteq \mathbb{Z}[\epsilon_m]$ sei die Norm $N(\mathrm{A})$ definiert als die Anzahl der Elemente in $\mathbb{Z}[\epsilon_m]/\mathrm{A}$. Es gilt für zwei Ideale A und B, daß $N(\mathrm{A}) \cdot N(\mathrm{B}) = N(\mathrm{A} \cdot \mathrm{B})$ ist, und es ist $N(\mathrm{A}) = |N(\alpha)|$, falls $\mathrm{A} = (\alpha)$ Hauptideal ist. Die Norm $N(\alpha)$ ist dabei das Produkt über alle Konjugierten von α (siehe z.B. Ireland, Rosen, S. 203, Prop. 14.1.1 und Prop. 14.1.3). Wir definieren für $s > 1$ die Dirichletsche Zeta-Funktion durch

$$\zeta(s) := \sum_{\mathrm{A}} \frac{1}{N(\mathrm{A})^s},$$

wobei die Summe über alle Ideale $\mathrm{A} \neq (0)$ von $\mathbb{Z}[\epsilon_n]$ gebildet wird.

Lemma 2

Es existiert eine positive Konstante c_2, so daß für alle $s > 1$ die Abschätzung

$$\zeta(s) \geq c_2 \sum_{n=1}^{\infty} \frac{1}{n^s}$$

gilt.

Beweis

Der Beweis geht auf Zassenhaus zurück und beruht auf der expliziten Konstruktion von genügend vielen Hauptidealen.

Sei $k := \phi(m)$. Die Einheitswurzeln ϵ_m^i bilden dann für $0 \leq i \leq k-1$ eine Basis von $\mathbb{Z}[\epsilon_m]$. Für eine natürliche Zahl t betrachten wir die Menge

$$\begin{aligned} B_t \quad := \quad & \{\xi \in \mathbb{Z}[\epsilon_m] \,|\, \xi = \sum_{i=0}^{k-1} a_i \epsilon_m^i,\ a_i \in \mathbb{Z}, \\ & |a_0 - \frac{3}{4} t^{1/k}| < \frac{1}{4k} t^{1/k},\ |a_i| < \frac{1}{4k} t^{1/k} \text{ für } 0 < i < k\}. \end{aligned}$$

Einen Punkt $(a_0, \ldots, a_{k-1})$, für den $\xi = \sum a_i \epsilon_m^i$ in B_t liegt, kann man sich als Gitterpunkt innerhalb eines k-dimensionalen Würfels der Kantenlänge $\frac{1}{4k} t^{1/k}$ vorstellen.

Für jedes a_i hat man mindestens $2 \cdot \frac{1}{4k} t^{1/k} - 3$ Wahlmöglichkeiten, also gilt

$$\# B_t \geq (\frac{1}{2k} t^{1/k} - 3)^k \geq c_3 t$$

für $t > t_0$ mit geigneten positiven Konstanten c_3 und t_0.
Schätzt man die Norm einer Zahl ξ aus B_t ab, so erhält man (mit σ seien die Automorphismen von $\mathbb{Q}[\epsilon_m]$ bezeichnet)

$$\begin{aligned} |N(\xi)| &= |\prod_\sigma \sigma(\xi)| = \prod_\sigma |\sum_i a_i \sigma(\epsilon_m^i)| \\ &\leq \prod_\sigma \sum_i |a_i| = (\sum_i |a_i|)^k \leq (t^{1/k}(\frac{3}{4} + \frac{1}{4k} + (k-1)\cdot\frac{1}{4k}))^k = t. \end{aligned}$$

Hierin wurde a_0 durch $\frac{3}{4} + \frac{1}{4k}$ und die $k-1$ restlichen a_i durch $\frac{1}{4k}$ abgeschätzt. Es gilt also für jedes $\xi \in B_t$, daß

$$|N(\xi)| \leq t$$

ist.
Wir zeigen, daß die von zwei verschiedenen Zahlen $\xi = \sum a_i \epsilon_m^i$ und $\xi' = \sum a_i' \epsilon_m^i$ aus B_t erzeugten Ideale verschieden sind:
Zunächst erhält man für $i = 0, \ldots, k-1$ die Abschätzungen

$$|a_i - a_i'| < \frac{1}{2k} t^{1/k}$$

und

$$|\sum_{i=0}^{k-1} a_i \epsilon_m^i| \geq |a_0| - \sum_{i=1}^{k-1} |a_i| \geq t^{1/k}(\frac{3}{4} - \frac{1}{4k} - (k-1)\frac{1}{4k}) = \frac{1}{2} t^{1/k},$$

so daß

$$|N(\frac{\xi'}{\xi} - 1)| = \frac{|N(\xi' - \xi)|}{|N(\xi)|} \leq \prod_\sigma \frac{\sum |a_i' - a_i|}{|\sum a_i \epsilon_m^i|} < \frac{k\frac{1}{2k} t^{1/k}}{\frac{1}{2} t^{1/k}} = 1 \qquad (*)$$

ist. Erzeugen nun ξ und ξ' das gleiche Ideal, so gilt $\xi' \in (\xi)$, und es ist dann $N(\xi'/\xi - 1) \in \mathbb{Z}$. Nach $(*)$ folgt $N(\xi'/\xi - 1) = 0$, also $\xi' = \xi$.
Bezeichnet $C(t)$ die Anzahl aller Ideale $\mathrm{A} \neq (0)$ mit $N(\mathrm{A}) \leq t$, so folgt

$$C(t) \geq \#B_t \geq c_3 t \text{ für } \ t > t_0.$$

Da wegen $N(1) = 1$ zusätzlich $C(t) \geq 1$ für $t \geq 1$ ist, folgt

$$C(t) \geq c_2 t$$

mit $c_2 := \min\{1/t_0, c_3\}$.

Man erhält schließlich ($C(0) = 0$):

$$\begin{aligned}
&\sum_{0<N(\mathrm{A})\le t} \frac{1}{N(\mathrm{A})^s} = \sum_{n=1}^{t} \frac{C(n) - C(n-1)}{n^s} \\
&= \sum_{n=1}^{t} \frac{C(n)}{n^s} - \sum_{n=0}^{t-1} \frac{C(n)}{(n+1)^s} = \frac{C(t)}{t^s} + \sum_{n=1}^{t-1} C(n)(\frac{1}{n^s} - \frac{1}{(n+1)^s}) \\
&\ge c_1(\frac{t}{t^s} + \sum_{n=1}^{t-1}(\frac{n}{n^s} - \frac{n+1}{(n+1)^s} + \frac{1}{(n+1)^s})) \\
&= c_1(\frac{t}{t^s} + 1 - \frac{t}{t^s} + \sum_{n=1}^{t-1} \frac{1}{(n+1)^s}) = c_1 \sum_{n=1}^{t} \frac{1}{n^s}.
\end{aligned}$$

Mit $t \to \infty$ folgt die Behauptung.

QED.

Lemma 3

Es gibt eine positive Konstante c_4, so daß für $s > 1$ die Abschätzung

$$c_4 + \phi(m) \sum_{p \equiv 1(m)} \frac{1}{p^s} \ge \log \zeta(s)$$

gilt.

Beweis

Wir führen den Beweis in drei Schritten. 1. Schritt

Es gilt für ein zu (m) teilerfremdes Primideal $\mathrm{P} \trianglelefteq \mathbb{Z}[\epsilon_m]$

$$N(\mathrm{P}) \equiv 1 \bmod m.$$

Man betrachte dazu die multiplikative Gruppe des Körpers $\mathbb{Z}[\epsilon_m]/\mathrm{P}$, die gerade $N(\mathrm{P})-1$ Elemente enthält, und die Menge $\Psi_m := \{\epsilon_m^a, a = 0, \ldots, m-1\}$ der m-ten Einheitswurzeln. Die Bildmenge von Ψ_m unter der kanonischen Abbildung $\kappa : \mathbb{Z}[\epsilon_m] \to \mathbb{Z}[\epsilon_m]/\mathrm{P}$ bildet eine Untergruppe in $(\mathbb{Z}[\epsilon_m]/\mathrm{P})^*$. Ist κ eingeschränkt auf Ψ_m injektiv, so hat man $m|N(\mathrm{P}) - 1$, und die Behauptung ist gezeigt.

Die Injektivität von κ ergibt sich wie folgt: Da $\prod_\epsilon (x - \epsilon) = x^m - 1 = (x - 1)(x^{m-1} + \cdots + x + 1)$ ist, wobei ϵ ganz Ψ_m durchläuft, erhält man durch Division von $x - 1$ und Einsetzen von $x = 1$, daß $\prod_{\epsilon \ne 1}(1 - \epsilon) = m$ ist. Nimmt man an, daß $\kappa|\Psi_m$ nicht injektiv ist, so existiert ein $\epsilon \ne 1$ mit $\kappa(\epsilon) = 1$, und da κ Homomorphismus ist, wird

$$\kappa(m) = \kappa(\prod_{\epsilon \ne 1}(1 - \epsilon)) = \prod_{\epsilon \ne 1}(1 - \kappa(\epsilon)) = 0,$$

also $m \in \mathrm{P}$, was ein Widerspruch zur Voraussetzung ist.

2. Schritt

Die Anzahl der Primideale P *mit* $N(\mathrm{P}) = p^f$ *ist kleiner als* $\phi(m)$.

Dies folgt sofort aus der Primidealzerlegung von (p). Denn aus $N(\mathrm{P}) = p^f$ folgt $p \in \mathrm{P}$, so daß also P in der (eindeutigen) Zerlegung $(p) = \mathrm{P}_1 \cdot \ldots \cdot \mathrm{P}_g$ in Primideale als Faktor enthalten ist. Bildet man jetzt die Norm auf beiden Seiten, so erhält man

$$p^{\phi(m)} = N((p)) = N(\mathrm{P}_1) \cdot \ldots \cdot N(\mathrm{P}_g) \geq p^g,$$

also $g \leq \phi(m)$.

3. Schritt

Da jedes Ideal $\mathrm{A} \neq (0)$ von $\mathbb{Z}[\epsilon_n]$ eine eindeutige Zerlegung in Primideale besitzt, erhalten wir für die Dirichletsche Zeta-Funktion die Darstellung (wir können die Reihe beliebig umordnen, weil alle Summanden positiv sind)

$$\begin{aligned} \zeta(s) &= \sum_A \frac{1}{N(\mathrm{A})^s} = \prod_{\mathrm{P\ prim}} (1 + \frac{1}{N(\mathrm{P})^s} + \frac{1}{N(\mathrm{P})^{2s}} + \cdots) \\ &= \prod_{\mathrm{P\ prim}} \frac{1}{1 - 1/N(\mathrm{P})^s}. \end{aligned} \qquad (*)$$

Weiter hat man die Abschätzung

$$\begin{aligned} \sum_{\nu=2}^{\infty} \frac{1}{\nu N(\mathrm{P})^{\nu s}} &\leq \sum_{\nu=2}^{\infty} \frac{1}{N(\mathrm{P})^{\nu s}} = \frac{1}{N(\mathrm{P})^{2s}} \sum_{\nu=0}^{\infty} \frac{1}{N(\mathrm{P})^{\nu s}} \\ &\leq \frac{1}{N(\mathrm{P})^{2s}} \sum_{\nu=0}^{\infty} \frac{1}{2^\nu} = \frac{2}{N(\mathrm{P})^{2s}}. \end{aligned} \qquad (**)$$

Logarithmiert man nun $(*)$, setzt die Taylorentwicklung von $\log(1-x) = -\sum x^\nu/\nu$ ein und schätzt diese mit $(**)$ ab, erhält man

$$\begin{aligned} \log \zeta(s) &= \log \prod_{\mathrm{P\ prim}} \frac{1}{1 - 1/N(\mathrm{P})^s} = \sum_{\mathrm{P\ prim}} \log(1 - \frac{1}{N(\mathrm{P})^s})^{-1} \\ &= \sum_{\mathrm{P\ prim}} \sum_{\nu=1}^{\infty} \frac{1}{\nu N(\mathrm{P})^{\nu s}} \leq \sum_{\mathrm{P\ prim}} (\frac{1}{N(\mathrm{P})^s} + \frac{2}{N(\mathrm{P})^{2s}}) \\ &\leq \phi(m)(\sum_{p \equiv 1 \bmod m} \frac{1}{p^s} + \sum_p \frac{3}{p^2}) + c_5. \end{aligned}$$

Die letzte Ungleichung ist dabei folgendermaßen begründet: Falls $N(\mathrm{P}) = p$ und P teilerfremd zu (m), so ist nach dem 1. Schritt $p \equiv 1 \bmod m$. Ist $N(\mathrm{P}) = p^f$ eine höhere Primzahlpotenz (also $f \geq 2$), so wird $N(\mathrm{P})^s$ großzügig mit p^2 abgeschätzt. Aus dem 2. Schritt wissen wir, daß jede Primzahl höchstens $\phi(m)$-mal als Norm eines Primideals auftritt, was zum Faktor $\phi(m)$ vor der Summe

führt. Schließlich sei die endliche Summe über alle zu (m) nicht teilerfremden Primideale durch c_5 abgeschätzt.

Da $\sum_p \frac{1}{p^2}$ konvergiert, folgt die Behauptung mit $c_4 := \phi(m) \sum_p \frac{3}{p^2} + c_5$.

QED.

Lemma 4

Es gilt für $s > 1$ die Abschätzung

$$\log |\prod_\chi \mathrm{L}(s,\chi)| \geq \phi(m) \sum_{p \equiv 1(m)} \frac{1}{p^s}.$$

Das Produkt wird dabei über alle Charaktere χ modulo m gebildet.

Beweis

Wir haben für die L-Funktion die Darstellung als Eulerprodukt gemäß

$$\mathrm{L}(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \,\mathrm{prim}} (1 + \frac{\chi(p)}{p^s} + \frac{\chi(p)^2}{p^{2s}} + \cdots) = \prod_{p \,\mathrm{prim}} \frac{1}{1 - \chi(p)/p^s},$$

und es folgt

$$\begin{aligned} \log \prod_\chi \mathrm{L}(s,\chi) &= \sum_\chi \sum_p -\log(1 - \frac{\chi(p)}{p^s}) = \sum_\chi \sum_p \sum_{\nu=1}^{\infty} \frac{\chi(p)^\nu}{\nu p^{\nu s}} \\ &= \sum_{p^\nu} (\frac{1}{\nu p^{\nu s}} \sum_\chi \chi(p^\nu)) = \phi(m) \sum_{p^\nu \equiv 1 \bmod m} \frac{1}{\nu p^{\nu s}}, \end{aligned}$$

da

$$\sum_\chi \chi(a) = \begin{cases} \phi(m) & \text{falls } a \equiv 1 \bmod m \\ 0 & \text{sonst.} \end{cases}$$

Genaugenommen wird die Rechnung, da wir es hier mit dem komplexen Logarithmus zu tun haben, modulo $2\pi i$ geführt. Für ein komplexes z ist $\log(z) = \log|z| + i \arg(z)$. Es folgt

$$\log |\prod_\chi \mathrm{L}(s,\chi)| = \phi(m) \sum_{p^\nu \equiv 1 \bmod m} \frac{1}{\nu p^{\nu s}},$$

da der Term auf der rechten Seite reell ist.

Lassen wir nun in der Summe alle Summanden bis auf diejenigen mit $\nu = 1$ weg, so ergibt sich

$$\log |\prod_\chi \mathrm{L}(s,\chi)| \geq \phi(m) \sum_{p \equiv 1 \bmod m} \frac{1}{p^s}.$$

QED.

Satz 8 ($\mathrm{L}(1,\chi) \neq 0$*)*
Sei χ ein Charakter modulo m, aber nicht der Hauptcharakter. Es gilt für die Dirichletsche L-Funktion

$$\mathrm{L}(1,\chi) \neq 0.$$

Beweis
Es genügt, da $\mathrm{L}(s,\chi)$ nach Lemma 1 für einen Charakter χ ungleich dem Hauptcharakter eine im Punkte 1 rechtsstetige Funktion ist, zu zeigen, daß es eine positive Konstante c_6 gibt, so daß für alle $s > 1$ die Abschätzung

$$|\mathrm{L}(s,\chi)| \geq c_6 > 0$$

gilt.
Nach den Lemmata 3 und 4 hat man mit der Konstanten c_4 aus Lemma 3, daß

$$c_4 + \log|\prod_{\chi} \mathrm{L}(s,\chi)| \geq \log\zeta(s)$$

ist, also

$$e^{c_4}|\prod_{\chi} \mathrm{L}(s,\chi)| \geq \zeta(s).$$

Mit Lemma 2 und der dort definierten Konstanten c_2 folgt

$$e^{c_4}|\prod_{\chi} \mathrm{L}(s,\chi)| \geq \zeta(s) \geq c_2 \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Bezeichnet χ_1 den Hauptcharakter, so ist

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \geq \sum_{n=1}^{\infty} \frac{\chi_1(n)}{n^s} = \mathrm{L}(s,\chi_1),$$

da $\chi_1(n)$ als Werte nur 0 und 1 annimmt. Man erhält schließlich

$$e^{c_4}|\prod_{\chi\neq\chi_1} \mathrm{L}(s,\chi)| \geq c_2 > 0.$$

Weil $\mathrm{L}(s,\chi)$ für $\chi \neq \chi_1$ auf einem kompakten Intervall $[1, 1+\delta]$ stetig ist, ist die Funktion dort beschränkt, so daß dort also

$$|\mathrm{L}(s,\chi)| < c_7$$

für eine positive Konstante c_7 gilt (c_7 kann unabhängig von χ gewählt werden). Man erhält für einen festen Charakter $\hat{\chi}$

$$c_7^{\phi(m)-2} e^{c_4} |\mathrm{L}(s,\hat{\chi})| \geq e^{c_4} \prod_{\chi \neq \chi_1} |\mathrm{L}(s,\chi)| \geq c_2 > 0,$$

also

$$|\mathrm{L}(s,\hat{\chi})| \geq c_2 c_7^{2-\phi(m)} e^{-c_4} =: c_6 > 0.$$

QED.

Weitere Literatur zu diesem Thema:

Sätze, in denen das Nichtverschwinden der L-Funktion mittels Funktionentheorie bewiesen wird, finden sich bei

- *J.– P. Serre:* Cours d'arithmétique, Presses Universitaires de France, Paris 1970, S. 118, Proposition 12,
- *G. Frey:* Elementare Zahlentheorie, Vieweg, Braunschweig 1984, S. 111, Lemma 4.

Eine umfassende Darstellung dieses Themas mit verschiedenen Beweisen findet sich bei

- *H. Hasse:* Zahlentheorie, Akademie Verlag, Berlin 1963, S. 238-283.

Hasse bringt auch Verweise auf weitere Veröffentlichungen mit alternativen Beweisen zum Nichtverschwinden der L-Funktion im Punkte 1.

Anhang B

Das folgende Programm liefert bei Eingabe von n eine Basis und die Darstellung durch Erzeugende. Es ist innerhalb des Computeralgebrasystems SIMATH geschrieben. Insbesondere wird dessen Listenverwaltung genutzt. Die einzelnen Funktionen sind innerhalb des Listings erklärt. Das Programm liefert eine Ausgabe, die innerhalb eines in LaTeX geschriebenen Textes verwendet werden kann. An das Programm schließt sich ein Beispiel einer Originalausgabe für die Eingabe $n = 15$ an.

```
#include<_simath.h>
#define cyc int

/* qB := \bar{q}, qT :=  \tilde{q}  etc.  */

static single q = 0, qT = 0, qB = 0;
static single r = 0, rT = 0, rB = 0;
static single s = 0, sT = 0, sB = 0;

static list L_111 = 0;

/*C
        cycinit( n )

    "cyclotomic unit initialisation"

    single cycinit( n )   single n;
    a = cycinit( n );

    Es werden die statischen Variablen q, r, s usw.
    initialisiert.
    Diese Funktion MUSS vor jeder anderen aufgerufen werden.
    Falls n mehr als 3 verschiedene Primfaktoren besitzt
    oder kongruent 2 mod 4 ist, wird a=0, sonst a=1.
    Wird die Funktion mit n = 0 aufgerufen, so werden die
    Werte fuer q, r und s explizit vom Benutzer abgefragt.
C*/

cycinit(n)
    single n;
{

    single lL, e;
    list L;
```

```
    bind(L);

    L_111 = 0;

    if (n == 0) {
        printf(" q, r, s = ?\n");
        q = getsi();
        r = getsi();
        s = getsi();
        n = q * r * s;
        printf("n = %d\n", n);
    }
/* Abfrage: n = 2 mod 4       */
    if (iaval(2, n) == 1) {
        return (0);
    }
    L = sfact(n);
    L = ifel(L);


    lL = llength(L);
/* Abfrage: n mehr als drei P-Teiler */
    if (lL > 6) {
        return (0);
    }
    if (L != _0) {
        sT = lfirst(L);
        L = lred(L);
        e = lfirst(L);
        L = lred(L);
    } else
        sT = 1, e = 1;

    s = sexp(sT, e);
    sB = s / sT;

    if (L != _0) {
        rT = lfirst(L);
        L = lred(L);
        e = lfirst(L);
        L = lred(L);
    } else
        rT = 1, e = 1;
```

```
    r = sexp(rT, e);
    rB = r / rT;
    if (L != _0) {
        qT = lfirst(L);
        L = lred(L);
        e = lfirst(L);
        L = lred(L);
    } else
        qT = 1, e = 1;

    q = sexp(qT, e);
    qB = q / qT;

    return (1);
}

/* unwichtige Hilfsfunktion: */
/*C
    u_decomp(u, tT, ptR, puu)

    "u decomposition"

    single u_decomp(u, tT, ptR, puu) single u, tT, *ptR, *puu;
    s = u_decomp(u, tT, ptR, puu);
    Es muss gelten: tT teilt u, tT ist Primzahl.
    Es gilt: u = tT * *ptR * *puu
C*/

single u_decomp(u, tT, ptR, puu)
    single u, tT, *ptR, *puu;
{
    single w;

    w = iaval(tT, u);

    *ptR = sexp(tT, w - 1);
    *puu = u / (*ptR * tT);
    return (1);
}


/* Interne Darstellung eines Elements als Liste:
( exponent, x, y, z ) <=> ( 1 - e_qˆx e_rˆy e_sˆz )ˆexponent  */
```

```
/*C
        cycevalo( C )

    "cyclotomic unit evaluation once"

    list cycevalo( C )   cyc C;
    L = cycevalo( C );

    Die zyklotomische Einheit C wird einmal gemaess
    den Relationen aus der Diplomarbeit entwickelt.
    Ist also L = ( A1, A2,... ,An ), dann gilt
    C = A1 * A2 * ... * An.
C*/

list cycevalo(C)
    cyc C;
{
    single e, x, y, z;
    single xx, yy, zz;
    single xE, yE, zE;

/*     xE := x Ergebnis      */

    single qR, rR, sR;

/* qR : restliche q - Potenz   */

    cyc E;
    single i;

    list L;

    init(L, E);
    bind(C);

    e = lfirst(C);
    x = lsecond(C);
    y = lthird(C);
    z = lfourth(C);

/* Entwicklung von Elementen, die nicht in E^(n) liegen */
    if (x && x % qT == 0) {
        u_decomp(x, qT, &qR, &xx);
        L = _0;
```

```
        yE = mshoms(r, y * qT);
        zE = mshoms(s, z * qT);
        for (i = 0; i < qT; i++) {
            xE = xx * qR + i * qB;
            xE = mshoms(q, xE);
            E = list4(e, xE, yE, zE);
            L = lcomp(E, L);
        }
    } else if (y && y % rT == 0) {
        u_decomp(y, rT, &rR, &yy);
        L = _0;
        xE = mshoms(q, x * rT);
        zE = mshoms(s, z * rT);
        for (i = 0; i < rT; i++) {
            yE = yy * rR + i * rB;
            yE = mshoms(r, yE);
            E = list4(e, xE, yE, zE);
            L = lcomp(E, L);
        }
    } else if (z && z % sT == 0) {
        u_decomp(z, sT, &sR, &zz);
        L = _0;
        xE = mshoms(q, x * sT);
        yE = mshoms(r, y * sT);
        for (i = 0; i < sT; i++) {
            zE = zz * sR + i * sB;
            zE = mshoms(s, zE);
            E = list4(e, xE, yE, zE);
            L = lcomp(E, L);
        }
    }
/* ''Ab hier koennen wir uns auf P-Teiler beschraenken'' */

/* Normierung auf zwei Komponenten > 0  bei qrs
   bzw. Auswahl einer der Mengen x>0 y<0 usw. bei zwei
P-Teilern etc.                                          */
/* Torsionsanteil                                       */
    else if ((x <= 0 && y <= 0 && z <= 0) ||
         (x > 0 && y < 0 && z < 0) ||
         (x < 0 && y > 0 && z < 0) ||
         (x < 0 && y < 0 && z > 0) ||

         (x == 0 && y < 0 && z >= 0) ||
         (x < 0 && y >= 0 && z == 0) ||
```

```
         (x >= 0 && y == 0 && z < 0)
        ) {
        E = list4(e, -x, -y, -z);
        L = list1(E);
    }

/* Durch N_q induzierte Relationen   */

    else if ((x == 1 && y > 0 && z == 0) ||
         (x == 1 && y == 0 && z > 0) ||
         (x == 1 && y > 1 && z > 1) ||    /* A_1  */
         (x == 1 && y > 0 && z < -1) ||    /* A_6  */
         (x == 1 && y == 1 && z > 1) ||    /* A_9  */
         (x == 1 && y > 1 && z == -1)    /* A_12 */
        ) {

        yE = mshoms(r, q * y);
        zE = mshoms(s, q * z);
        C = list4(e, 0, yE, zE);
        L = list1(C);

        yE = mshoms(r, qB * y);
        zE = mshoms(s, qB * z);

        C = list4(-e, 0, yE, zE);
        L = lcomp(C, L);

        for (i = 2; i < q; i++)
            if (i % qT) {
                xE = mshoms(q, i);
                C = list4(-e, xE, y, z);
                L = lcomp(C, L);
            }
    }

/* Durch N_r induzierte Relationen        */

    else if ((x > 0 && y == 1 && z == 0) ||
         (x == 0 && y == 1 && z > 0) ||
         (x > 1 && y == 1 && z > 1) ||    /* A_2 */
         (x < -1 && y == 1 && z > 0) ||    /* A_4 */
         (x > 1 && y == 1 && z == 1) ||    /* A_7 */
         (x == -1 && y == 1 && z > 1)    /* A_10 */
        ) {
```

```
        xE = mshoms(q, r * x);
        zE = mshoms(s, r * z);

        C = list4(e, xE, 0, zE);
        L = list1(C);

        xE = mshoms(q, rB * x);
        zE = mshoms(s, rB * z);

        C = list4(-e, xE, 0, zE);
        L = lcomp(C, L);

        for (i = 2; i < r; i++)
            if (i % rT) {
                yE = mshoms(r, i);
                C = list4(-e, x, yE, z);
                L = lcomp(C, L);
            }
    }

/* Durch N_s induzierte Relationen  */

    else if ((x > 0 && y == 0 && z == 1) ||
         (x == 0 && y > 0 && z == 1) ||
         (x > 1 && y > 1 && z == 1) ||    /* A_3   */
         (x > 0 && y < -1 && z == 1) ||    /* A_5   */
         (x == 1 && y > 1 && z == 1) ||    /* A_8   */
         (x > 1 && y == -1 && z == 1)    /* A_11  */
        ) {
        xE = mshoms(q, s * x);
        yE = mshoms(r, s * y);

        C = list4(e, xE, yE, 0);
        L = list1(C);

        xE = mshoms(q, sB * x);
        yE = mshoms(r, sB * y);

        C = list4(-e, xE, yE, 0);
        L = lcomp(C, L);

        for (i = 2; i < s; i++)
            if (i % sT) {
```

```
                zE = mshoms(s, i);
                C = list4(-e, x, y, zE);
                L = lcomp(C, L);
            }
    }
/* Die  Menge A_13                  */
    else if (x == -1 && y == 1 && z == 1) {

        yE = mshoms(r, q * y);
        zE = mshoms(s, q * z);
        C = list4(e, 0, yE, zE);
        L = list1(C);

        yE = mshoms(r, qB * y);
        zE = mshoms(s, qB * z);

        C = list4(-e, 0, yE, zE);
        L = lcomp(C, L);

        for (i = -2; i > -q; i--)
            if (i % qT) {
                xE = mshoms(q, i);
                C = list4(-e, xE, y, z);
                L = lcomp(C, L);
            }
    } else if (x == 1 && y == -1 && z == 1) {

        xE = mshoms(q, r * x);
        zE = mshoms(s, r * z);

        C = list4(e, xE, 0, zE);
        L = list1(C);

        xE = mshoms(q, rB * x);
        zE = mshoms(s, rB * z);

        C = list4(-e, xE, 0, zE);
        L = lcomp(C, L);

        for (i = -2; i > -r; i--)
            if (i % rT) {
                yE = mshoms(r, i);
                C = list4(-e, x, yE, z);
                L = lcomp(C, L);
```

```
            }
    } else if ((x == 1 && y == 1 && z == -1)) {

        xE = mshoms(q, s * x);
        yE = mshoms(r, s * y);

        C = list4(e, xE, yE, 0);
        L = list1(C);

        xE = mshoms(q, sB * x);
        yE = mshoms(r, sB * y);

        C = list4(-e, xE, yE, 0);
        L = lcomp(C, L);

        for (i = -2; i > -s; i--)
            if (i % sT) {
                zE = mshoms(s, i);
                C = list4(-e, x, y, zE);
                L = lcomp(C, L);
            }
    }
/* Das 111 - Element     */

    else if ((x == 1 && y == 1 && z == 1)) {
        single j, k;
        list M;

 /*    Zunaechst Darstellung von ( 2, 1, 1, 1 )      */
/*     (zuerst  nur  durch irgendeine Liste  L)     */

        init(M);
        if (L_111 != 0)
            M = L_111;
        else {
            L = _0;
            for (i = 1; i <= q / 2; i++)
                if (i % qT)
                    for (j = 1; j <= r / 2; j++)
                        if (j % rT)
                            for (k = 1; k <= s / 2; k++)
           if (k % sT && !(i == 1 && j == 1 && k == 1)) {
                                    C = list4(-2, i, j, k);
                                    L = lcomp(C, L);
```

```
                        }
            for (i = 1; i <= q / 2; i++)
                if (i % qT)
                    for (j = 1; j <= r / 2; j++)
                        if (j % rT) {
                            xE = mshoms(q, s * i);
                            yE = mshoms(r, s * j);
                            C = list4(1, xE, yE, 0);
                            L = lcomp(C, L);

                            xE = mshoms(q, sB * i);
                            yE = mshoms(r, sB * j);
                            C = list4(-1, xE, yE, 0);
                            L = lcomp(C, L);
                        }
            for (i = 1; i <= q / 2; i++)
                if (i % qT)
                    for (k = 1; k <= s / 2; k++)
                        if (k % sT) {
                            xE = mshoms(q, r * i);
                            zE = mshoms(s, r * k);
                            C = list4(1, xE, 0, zE);
                            L = lcomp(C, L);

                            xE = mshoms(q, rB * i);
                            zE = mshoms(s, rB * k);
                            C = list4(-1, xE, 0, zE);
                            L = lcomp(C, L);
                        }
            for (j = 1; j <= r / 2; j++)
                if (j % rT)
                    for (k = 1; k <= s / 2; k++)
                        if (k % sT) {
                            yE = mshoms(r, q * j);
                            zE = mshoms(s, q * k);
                            C = list4(1, 0, yE, zE);
                            L = lcomp(C, L);

                            yE = mshoms(r, qB * j);
                            zE = mshoms(s, qB * k);
                            C = list4(-1, 0, yE, zE);
                            L = lcomp(C, L);
                        }
/* Entwicklung von L: */
```

```
            M = lcyceval(L);
            L_111 = M;
        }
        L = _0;
/* Division jedes Exponenten durch 2, um Darstellung von  */
/* ( 1, 1, 1, 1 ) zu erhalten                             */
        while (M != _0) {
            single ee;

            C = lfirst(M);
            M = lred(M);

            ee = lfirst(C);

            xE = lsecond(C);
            yE = lthird(C);
            zE = lfourth(C);

            ee = ee / 2;

            C = list4(e * ee, xE, yE, zE);
            L = lcomp(C, L);
        }
    }
/* C ist Basiselement (das heisst nicht entwickelbar) */
    else
        L = list1(C);

    return (L);
}

/*C
        lcyccollect( L )

    "list of cyclotomic units collection"

    list lcyccollect( L )   cyc L;
    K = lcyccollect( L );

    Es werden gleiche Elemente in L zu einem
    Element zusammengefasst, dabei wird
    der Exponent veraendert. Ist der Exponent
    dieses Elementes Null, wird es weggelassen.
    Kommt jedes Element in L genau einmal vor,
```

```
    ist K = L.
C*/

list lcyccollect(L)
    list L;
{
    list N, K;
    cyc C, D, E;
    single exp;

    bind(L);
    init(N, K, C, D, E);

    K = _0;
    while (L != _0) {
        C = lfirst(L);
        exp = lfirst(C);
        C = lred(C);
        N = lred(L);
        L = _0;
        while (N != _0) {
            D = lfirst(N);
            N = lred(N);

            if (oequal(lred(D), C)) {
                exp += lfirst(D);
            } else
                L = lcomp(D, L);
        }
        L = linv(L);
        if (exp)
            K = lcomp(lcomp(exp, C), K);
    }
    return (linv(K));
}


/*C
        lcycevalo( L )

    "list of cyclotomic units evaluation once"

    list lcycevalo( L )   list L;
    K = lcycevalo( L );
```

```
    Fuer jedes Element C in L wird
    cycevalo( C ) aufgerufen, und die Ergebnisse
    werden in eine Liste geschrieben.
C*/

list lcycevalo(L)
    list L;
{

    list K, M;
    cyc C;

    bind(L);
    init(K, M, C);

    K = _0;

    while (L != _0) {
        C = lfirst(L);
        L = lred(L);

        M = cycevalo(C);
        K = lconc(K, M);
    }
    return (K);
}

/*C
        lcyceval( L )

    "list of cyclotomic units evaluation"

    list lcyceval( L )   list L;
    K = lcyceval( L );

    L wird als Produkt von Basiselementen
    dargestellt.
    K enthaelt diese Basiselemente.
C*/

list lcyceval(L)
    list L;
{
```

```
    list M;
    single i = 0;

    bind(L);
    init(M);

    while (!oequal(L, M)) {
        M = L;
        L = lcycevalo(L);
        L = lcyccollect(L);
    }
    return (L);
}

/*C
        cyceval( C )

    "cyclotomic unit evaluation"

    list cyceval( C )   cyc C;
    K = cyceval( C );

    C wird als Produkt von Basiselementen
    dargestellt.
    K enthaelt diese Basiselemente.
C*/

list cyceval(C)
    cyc C;
{
    int L;

    bind(C);

    L = lcyceval(list1(C));
    return (L);
}


/*C
        iscycbasel( C )

    "is cyclotomic unit base element ?"
```

```
    single  iscycbasel( C )   cyc C;
    a = iscycbasel( C );
    a = 1 falls C Basiselement ist,
    a = 0 sonst.

C*/


iscycbasel(C)
    cyc C;
{
    list L;
    cyc D;

    bind(C, D);
    init(L);
    L = cycevalo(C);
    D = lfirst(L);

    if (oequal(C, D))
        return (1);
    else
        return (0);
}


/*C
        cycbasecons( )

    "cyclotomic units base construction"

    list  cycbasecons();
    L = cycbasecons();

    L ist eine Liste, die alle Basiselemente enthaelt.
    Achtung: ( e, 2, 0, 0 ) muss als Einheit
    ( ( e, 2, 0, 0 ), ( -e, 1, 0, 0 ) ) usw.
    interpretiert werden.
C*/



list cycbasecons()
{
```

```
    single i, j, k;
    single phi, anz, zae;
    single x, y, z;
    cyc C;
    list L;

    init(C, L);

    zae = 0;
    phi = iphi(q) * iphi(r) * iphi(s);
    anz = phi / 2 - 1;
    L = _0;

    for (i = 0; i < q; i++)
        for (j = 0; j < r; j++)
            for (k = 0; k < s; k++)
                if (i + j + k > 1) {
                    x = mshoms(q, i);
                    y = mshoms(r, j);
                    z = mshoms(s, k);
                    C = list4(1, x, y, z);
                    if (iscycbasel(C)) {
                        zae++;
                        L = lcomp(C, L);
                    }
                }
    return (L);
}

/* Es folgen diverse Prozeduren, um einen Ausdruck in
TeX-Code zu ermoeglichen */

/* x = pp * xx mit p teilt nicht xx */

spsep(p, x, pp, xx)
    single x, p, *pp, *xx;
{
    *pp = 1;
    *xx = x;
    while (!(*xx % p)) {
        *xx /= p;
        *pp *= p;
    }
    return (0);
```

```
}

putepsTeX(sub, pot)
    single sub, pot;
{
    if (sub == 1 || pot == 0)
        printf("  ");
    else if (pot == 1)
        printf("\\ep_{%2d} ", sub);
    else
        printf("\\ep_{%2d}^{%2d} ", sub, pot);
    return (0);
}

putcycTeX(C, klammer)
    cyc C;
    single klammer;
{

    single x, y, z, e, xx, yy, zz, qq, rr, ss;

    bind(C);

    e = lfirst(C);
    x = lsecond(C);
    y = lthird(C);
    z = lfourth(C);

    LN_SIZE = BASIS;

    if (x)
        spsep(qT, x, &qq, &xx);
    else
        qq = q, xx = 1;
    if (y)
        spsep(rT, y, &rr, &yy);
    else
        rr = r, yy = 1;
    if (z)
        spsep(sT, z, &ss, &zz);
    else
        ss = s, zz = 1;
    if (klammer || e != 1)
        printf("(");
```

```
    else
        printf(" ");
    printf("1 - ");
    putepsTeX(q / qq, xx);
    putepsTeX(r / rr, yy);
    putepsTeX(s / ss, zz);
    if (e != 1)
        printf(")^{%2d}", e);
    else if (klammer)
        printf(")\\; ");
    else
        printf("\\; ");

    printf("%% (%d,%d,%d ) \n", x, y, z);
    return (0);
}



putlcycTeX(L)
    list L;
{
    cyc C;
    single klammer, x, y, z, e, h, zaehl;

    bind(L);
    init(C);

    if (llength(L) <= 1)
        klammer=0;
    else
        klammer=1;

    zaehl=0;
    while (L != _0) {
        C = lfirst(L);
        L = lred(L);
                if ( !(zaehl % 3) && zaehl ) {
                printf("\\\\ & & %% \n");
                }
        zaehl++;
        putcycTeX(C, klammer);
    }
    return (0);
```

```
}

TeXlcyceval(K)
    list K;
{
    list L;
    single n;

    bind(K);
    init(L);
    L = lcyceval(K);
    putlcycTeX(K);
    printf(" &\\eqt &\n");
    putlcycTeX(L);
    printf("\\\\ \n" );

    return (0);
}

#define ppot( P, X ) ( spsep( P, X, &NUM, &DUM ), NUM )

/* Hauptprogramm                                    */
main()
{
    list L;
    single n;
    cyc C, D;

    single u, e, i, j, k, x, y, z;

    init(L, C, D, L_111);



    printf("n = ? \n");
    n = getsi();
    printf(" n = %d\n", n);
    cycinit(n);

    printf("%%    BASIS:     \n%% \n");

    L = cycbasecons();

        printf("\\begin{eqnarray*} & & %%   \n");
```

```
    putlcycTeX(L);
    printf("\\end{eqnarray*} %%   \n");

    printf("\\par   %%   \n");
    printf("\\begin{eqnarray*} %%   \n");
    for (i = 0; i < q; i++)
     for (j = 0; j < r; j++)
      for (k = 0; k < s; k++) if (i + j + k > 0) {
       x = mshoms(q, i);
       y = mshoms(r, j);
       z = mshoms(s, k);

       C = list4(1, x, y, z);
       if ( !x && !y ) D = list4(-1, x, y, ppot( sT, z) );
       else if ( !x && !z ) D = list4(-1, x,   ppot( rT, y), z );
       else if ( !y && !z ) D = list4(-1, ppot( qT, x), y, z );
       else D = _0;
       if ( D == _0 ) L = list1( C );
       else L = list2( C, D );
       if (!iscycbasel(C)) {
            TeXlcyceval(L);
             printf("%%\n%%\n");
            }
       }
    printf("\\end{eqnarray*} %%   \n");
    printf("\n\n ok.\n");
}
```

Beim Start des mit Hilfe der SIMATH-Oberfläche compilierten Programms und mit der Eingabe $n = 15$ wird folgende Ausgabe geliefert:

```
n = ?
 n = 15
%    BASIS:
%
\begin{eqnarray*} & & %
(1 -   \ep_{ 3} \ep_{ 5}^{-1} )\; % (0,1,-1 )
(1 -   \ep_{ 3} \ep_{ 5}^{-2} )\; % (0,1,-2 )
(1 -     \ep_{ 5}^{ 2} )\; % (0,0,2 )
\end{eqnarray*} %
\par   %
\begin{eqnarray*} %
(1 -     \ep_{ 5}^{-2} )\; % (0,0,-2 )
(1 -     \ep_{ 5} )^{-1}% (0,0,1 )
```

```
 &\eqt &
(1 -     \ep_{ 5}^{ 2} )\; % (0,0,2 )
(1 -     \ep_{ 5} )^{-1}% (0,0,1 )
\\
%
%
(1 -     \ep_{ 5}^{-1} )\; % (0,0,-1 )
(1 -     \ep_{ 5} )^{-1}% (0,0,1 )
 &\eqt &
\\
%
%
 1 -   \ep_{ 3} \ep_{ 5} \; % (0,1,1 )
 &\eqt &
(1 -   \ep_{ 3} \ep_{ 5}^{-1} )^{-1}% (0,1,-1 )
(1 -     \ep_{ 5} )^{-1}% (0,0,1 )
(1 -     \ep_{ 5}^{ 2} )\; % (0,0,2 )
\\
%
%
 1 -   \ep_{ 3} \ep_{ 5}^{ 2} \; % (0,1,2 )
 &\eqt &
(1 -   \ep_{ 3} \ep_{ 5}^{-2} )^{-1}% (0,1,-2 )
(1 -     \ep_{ 5}^{ 2} )^{-1}% (0,0,2 )
(1 -     \ep_{ 5} )\; % (0,0,1 )
\\
%
%
(1 -   \ep_{ 3}^{-1}   )\; % (0,-1,0 )
(1 -   \ep_{ 3}   )^{-1}% (0,1,0 )
 &\eqt &
\\
%
%
 1 -   \ep_{ 3}^{-1} \ep_{ 5} \; % (0,-1,1 )
 &\eqt &
 1 -   \ep_{ 3} \ep_{ 5}^{-1} \; % (0,1,-1 )
\\
%
%
 1 -   \ep_{ 3}^{-1} \ep_{ 5}^{ 2} \; % (0,-1,2 )
 &\eqt &
 1 -   \ep_{ 3} \ep_{ 5}^{-2} \; % (0,1,-2 )
\\
```

```
%
%
 1 -   \ep_{ 3}^{-1} \ep_{ 5}^{-2} \; % (0,-1,-2 )
 &\eqt &
(1 -   \ep_{ 3} \ep_{ 5}^{-2} )^{-1}% (0,1,-2 )
(1 -     \ep_{ 5}^{ 2} )^{-1}% (0,0,2 )
(1 -     \ep_{ 5} )\; % (0,0,1 )
\\
%
%
 1 -   \ep_{ 3}^{-1} \ep_{ 5}^{-1} \; % (0,-1,-1 )
 &\eqt &
(1 -   \ep_{ 3} \ep_{ 5}^{-1} )^{-1}% (0,1,-1 )
(1 -     \ep_{ 5} )^{-1}% (0,0,1 )
(1 -     \ep_{ 5}^{ 2} )\; % (0,0,2 )
\\
%
%
\end{eqnarray*} %


 ok.


*** 0  GC in    0.0  Sekunden haben     0 Zellen angefordert. ***
*** Es sind noch   15799  Zellen in insgesamt  1  Block frei. ***
*** Blockgroesse BL_SIZE: 16383;  Stackgroesse ST_SIZE:  500. ***
*** Es  wurden       0.33   Sekunden  Rechenzeit  verbraucht. ***
```

Die Anweisung `\eqt` muß als Anweisung definiert werden, die die Interpretation "Gleichheit modulo Torsion" zuläßt (in unserem Fall " $\overset{\text{tor}}{=}$ "). Die Anweisung `\ep` ist eine Abkürzung für `\epsilon` (ϵ). In der Darstellung der Basis wird statt der vollständigen Formulierung $(1-\epsilon_5^2)\,(1-\epsilon_5)^{-1}$ nur $(1-\epsilon_5^2)$ ausgegeben. Der zu der obigen Ausgabe gehörige geTEX-te Text sieht wie folgt aus (dabei wurden die ersten Zeilen sowie die Schlußmeldung weggelassen, ansonsten ist der Rest unredigiert):

$$(1-\epsilon_3\epsilon_5^{-1})\,(1-\epsilon_3\epsilon_5^{-2})\,(1-\epsilon_5^2)$$

$$\begin{aligned}(1-\epsilon_5^{-2})\,(1-\epsilon_5)^{-1} &\overset{\text{tor}}{=} (1-\epsilon_5^2)\,(1-\epsilon_5)^{-1}\\ (1-\epsilon_5^{-1})\,(1-\epsilon_5)^{-1} &\overset{\text{tor}}{=}\end{aligned}$$

$$
\begin{aligned}
1-\epsilon_3\epsilon_5 &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-1})^{-1}(1-\epsilon_5)^{-1}(1-\epsilon_5^2)\\
1-\epsilon_3\epsilon_5^2 &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-2})^{-1}(1-\epsilon_5^2)^{-1}(1-\epsilon_5)\\
(1-\epsilon_3^{-1})\,(1-\epsilon_3)^{-1} &\overset{\text{tor}}{=}\\
1-\epsilon_3^{-1}\epsilon_5 &\overset{\text{tor}}{=} 1-\epsilon_3\epsilon_5^{-1}\\
1-\epsilon_3^{-1}\epsilon_5^2 &\overset{\text{tor}}{=} 1-\epsilon_3\epsilon_5^{-2}\\
1-\epsilon_3^{-1}\epsilon_5^{-2} &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-2})^{-1}(1-\epsilon_5^2)^{-1}(1-\epsilon_5)\\
1-\epsilon_3^{-1}\epsilon_5^{-1} &\overset{\text{tor}}{=} (1-\epsilon_3\epsilon_5^{-1})^{-1}(1-\epsilon_5)^{-1}(1-\epsilon_5^2)
\end{aligned}
$$

Literaturverzeichnis

Bass, Hyman: The Dirichlet unit theorem, induced characters and Whitehead groups of finite groups. In: Topology (1966), Vol. 4, 391-410.

Endl, Kurt/Luh, Wolfgang: Analysis III, eine integrierte Darstellung. Akademische Verlagsgesellschaft, Wiesbaden 1976.

Franz, Wolfgang: Über die Torsion einer Überdeckung. In: Journal für die reine und angewandte Mathematik 173 (1935), 245-254.

Frey, Gerhard: Elementare Zahlentheorie. Vieweg, Braunschweig 1984.

Hasse, Helmut: Zahlentheorie. Akademie Verlag, Berlin 1963.

Ireland, Kenneth/Rosen, Michael: A classical Introduction to Modern Number Theory. Springer-Verlag, New-York 1982.

Karpilovsky, Gregory: Commutative group algebras. Marcel Dekker, inc., New York 1983.

Lang, Serge: Algebra. Addison-Wesley Publishing Company, Reading, Massachusetts 1974.

Ramachandra, K.: On the units of cyclotomic fields. In: Acta Arithmetica 12 (1966), 165-173.

Serre, Jean-Pierre: Cours d'arithmétique. Presses Universitaires de France, Paris 1970.

Washington, Lawrence C.: Introduction to Cyclotomic Fields. Springer-Verlag, New York 1982.

Weiss, E.: Algebraic number theory. McGraw-Hill, New York 1963.

Zassenhaus, Hans: Über die Existenz von Primzahlen in arithmetischen Progressionen. In: Commentarii Mathematici Helvetici 22 (1949), S.232-259.