Dirichletsche Charaktere

Vortrag zum Seminar zur Funktionentheorie, 21.05.2012

Sebastian Schönitz

Dieser Vortrag verfolgt das Ziel, Primzahlen strukturell aus den natürlichen Zahlen herauszufiltern. Diese „Filter“ werden in dem nächsten Vortrag dazu genutzt, die Verteilung der Primzahlen, die den Rest k bei der Division durch N aufweisen, zu bestimmen.

§ 1 Homomorphismen zur Gruppenbeschreibung

In diesem Abschnitt wollen wir Homomorphismen dazu nutzen, um mit ihnen bestimmte Eigenschaften von Gruppen zu charakterisieren. Damit kommen wir gleich auf den Begriff des Charakters.

(1.1) Definition (Charakter)
Sei $(G, \cdot)$ eine Gruppe. Wir nennen einen Gruppenhomomorphismus $\chi : G \to \mathbb{C}^*$ einen *abelschen Charakter*, wobei $(\mathbb{C}^*, \cdot)$ die Gruppe ist, in die abgebildet wird.

Aus der Definition folgen eine interessante Eigenschaft.

(1.2) Lemma
Sei $(G, \cdot)$ eine Gruppe und χ ein zur Gruppe gehörender abelscher Charakter. Dann ist $(\chi(G), \cdot)$ eine abelsche Gruppe.

Beweis
Das Bild von χ ist automatisch eine Untergruppe von $(\mathbb{C}^*, \cdot)$, weil χ ein Gruppenhomomorphismus ist. Da $(\mathbb{C}^*, \cdot)$ eine abelsche Gruppe ist, gilt dies auch für jede Untergruppe.$\square$

Damit man ein kleines Gefühl dafür bekommt, was ein Charakter ist, geben wir hier ein paar Beispiele an.

(1.3) Beispiele
(i) Ist G eine Gruppe, so ist $\mathrm{triv} : G \to \mathbb{C}^*$, $g \mapsto 1$ ein abelscher Charakter.
(ii) Für $G = \mathrm{GL}_n(\mathbb{C})$ ist $\chi : G \to \mathbb{C}^*$, $g \mapsto \det g$ ein abelscher Charakter.
(iii) Für $G = S_n$ ist sgn: $G \to \mathbb{C}^*$, $\pi \mapsto \operatorname{sgn} \pi$ ein abelscher Charakter.

Beweis
(i) Es ist sofort klar, dass $\mathrm{triv}(e) = 1$ und für alle $g, h \in G$ gilt: $\mathrm{triv}(gh) = 1 = 1 \cdot 1 = \mathrm{triv}(g)\mathrm{triv}(h)$.

(ii) Es gilt, dass die Determinante der Einheitsmatrix gleich 1 ist. Da die Determinante eine multilineare Abbildung ist, ist sie ein Homomorphismus und als Einschränkung auf eine Gruppe auch ein Gruppenhomomorphismus.

(iii) Es gilt $sgn(id) = 1$. Außerdem gilt für $\pi, \tau \in S_n : \ sgn(\pi \circ \tau) = sgn(\psi) \cdot sgn(\tau)$. $\square$

(1.4) Lemma
Sei die Menge $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$ aller abelschen Charaktere von G gegeben und $\cdot$ eine Verknüpfung definiert als $(\chi \cdot \psi)(g) := \chi(g) \cdot \psi(g)$, für alle g aus G und alle χ, ψ aus $\widehat{G}$. So ist $(\widehat{G}, \cdot)$ eine Gruppe und wird die zu G *duale Gruppe* genannt. Diese ist außerdem abelsch.

Beweis
Seien $\chi, \psi, \xi \in \widehat{G}$. Wir wollen als erstes die Assoziativität zeigen.

$$((\chi \cdot \psi) \cdot \xi)(g) = (\chi \cdot \psi)(g) \cdot \xi(g) = \chi(g) \cdot \psi(g) \cdot \xi(g) = \chi(g) \cdot (\psi \cdot \xi)(g) = (\chi \cdot (\psi \cdot \xi))(g)$$

Jetzt wollen wir die Existenz des neutralen Elements zeigen.

$$(\mathrm{triv} \cdot \chi)(g) = \mathrm{triv}(g) \cdot \chi(g) = 1 \cdot \chi(g) = \chi(g) = \chi(g) \cdot 1 = \chi(g) \cdot \mathrm{triv}(g) = (\chi \cdot \mathrm{triv})(g)$$

Sei $\chi'(g) := \frac{1}{\chi(g)}$. Da $\chi(g) \neq 0$ für alle $g \in G$, ist χ' wohldefiniert. Wir wollen zeigen, dass dies ein Homomorphismus ist.

- $\chi'(e) = \frac{1}{\chi(e)} = 1$.
- Seien $g, h \in G$. es gilt nun: $\chi'(gh) = \frac{1}{\chi(gh)} = \frac{1}{\chi(g)} \cdot \frac{1}{\chi(h)} = \chi'(g) \cdot \chi'(h)$.

Jetzt müssen wir noch zeigen, dass χ' das Inverse von χ ist. Sei dazu $g \in G$.

$$(\chi' \cdot \chi)(g) = \chi'(g) \cdot \chi(g) = \frac{\chi(g)}{\chi(g)} = 1 = \chi(g) \cdot \chi'(g) = (\chi(g) \cdot \chi')(g)$$

Damit haben wir eingesehen, dass es sich bei $\widehat{G}$ tatsächlich um eine Gruppe handelt. Jetzt soll die Kommutativität gezeigt werden. Sei dazu $g \in \mathbb{C}^*$ beliebig und $\chi, \psi \in \widehat{G}$. Wir nutzen aus, dass $\mathbb{C}^*$ abelsch ist und dann gilt

$$(\chi \cdot \psi)(g) = \chi(g) \cdot \psi(g) = \psi(g) \cdot \chi(g) = (\psi \cdot \chi)(g). \qquad \square$$

(1.5) Satz
Sei G eine Gruppe. Dann ist $\widehat{G}$ eine linear unabhänge Teilmenge des $\mathbb{C}$-Vektorraums $\mathbb{C}^G$.

Beweis
Für alle $\chi \in \widehat{G}$ gilt $\chi(e) = 1 \neq 0$. Damit ist $\{\chi\}$ immer linear unabhängig. Es sei

$$\sum_{i=1}^{n} a_i \chi_i = 0$$

mit $a_i \in \mathbb{C} \setminus \{0\}$ und $\chi_i \neq \chi_j$ für $i \neq j$ und n minimal gewählt. Damit wissen wir sofort, dass n größer als 1 ist. Wir wählen $g \in G$ so, dass $\chi_1(g) \neq \chi_2(g)$. Dies gibt es, da $\chi_1 \neq \chi_2$. Sei nun $h \in G$. Wir wissen nun wegen unserer Voraussetzung, dass

$$\sum_{i=1}^{n} (a_i \chi_i(g) \chi_i)(h) = \sum_{i=1}^{n} a_i \chi_i(g) \chi_i(h) = \sum_{i=1}^{n} a_i \chi_i(gh) = 0.$$

Somit erhalten wir

$$\sum_{i=1}^{n} a_i \chi_i(g) \chi_i = 0$$

und bekommen damit

$$0 = \sum_{i=1}^{n} a_i \chi_i(g) \chi_i - \chi_1(g) \sum_{i=1}^{n} a_i \chi_i = \sum_{i=2}^{n} a_i (\chi_i(g) - \chi_1(g)) \chi_i,$$

und wegen $\chi_2(g) - \chi_1(g) \neq 0$ haben wir einen Widerspruch zur Minimalität von n. □

(1.6) Lemma
Sei $(G, \cdot)$ eine zyklische Gruppe der Ordnung n. Ein abelscher Charakter χ ist durch $\chi(g)$ eindeutig bestimmt, wobei $G = \langle g \rangle$.

Beweis
Wir wissen, dass G die Gestalt $G = \langle g \rangle = \{g^k;\, 0 \leq k < n\}$ hat. Da χ ein abelscher Charakter ist, folgt aus den Eigenschaften für Gruppenhomomorphismen, dass

$$\chi(g^k) = \chi(\prod_{i=1}^{k} g) = \prod_{i=1}^{k} \chi(g) = \chi(g)^k$$

gilt und damit erhalten wir folgende Darstellung für die 1 in $\mathbb{C}$:

$$1 = \chi(e) = \chi(g^n) = \chi(g)^n.$$

Damit ist $\chi(g)$ eine n-te Einheitswurzel.

Sei μ eine n-te Einheitswurzel, dann legt man mit $\chi(g^k) = \mu^k$ für alle $k \in \mathbb{Z}$ einen Homommorphismus fest, da

$$\chi(g^0) = \mu^0 = 1$$

und

$$\chi(g^l) = \mu^l = \prod_{k=1}^{l} \mu = \prod_{k=1}^{l} \chi(g) = \chi(g)^k$$

gilt. Damit ist die Isomorphie folgender Gruppen sofort klar:

$$G \cong \mathbb{Z}/n\mathbb{Z} \cong \{\mu \in \mathbb{C};\ \mu^n = 1\} \cong \widehat{G}$$ □

Wir wollen dieses Lemma dazu nutzten, um das gleiche Ergebnis für allgemeine abelsche Gruppen zu bekommen.

(1.7) Satz
Sei G eine endliche abelsche Gruppe. Dann gilt:

a) G ist isomorph zu $\widehat{G}$.

b) Zu jedem $g \in G\backslash\{e\}$ existiert ein $\chi \in \widehat{G}$ mit $\chi(g) \neq 1$.

Beweis

a) Im Folgenden Lemma 1.6, wo wir das Resultat a) schon für zyklische Gruppen bewiesen haben. Wir stellen die Gruppe G nun als Produkt zyklischer Gruppen dar, denn nach dem Hauptsatz über endliche abelsche Gruppen, gibt es $n_1, \ldots, n_r \in \mathbb{N}$, so dass
$$G \cong (\mathbb{Z}/n_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/n_r\mathbb{Z}) \text{ mit } n = \text{ord } G = n_1 \cdot \ldots \cdot n_r.$$
Damit können wir G anders schreiben, da es $g_1, \ldots, g_r \in G$ gibt, mit
$$G = \{g_1^{m_1} \cdot \ldots g_r^{m_r};\ m_j \in \mathbb{Z}\}$$
und
$$g_1^{m_1} \cdot \ldots \cdot g_r^{m_r} = g_1^{k_1} \cdot \ldots \cdot g_r^{k_r} \Leftrightarrow m_j \equiv k_j \mod n_j,\ j = 1, \ldots, r.$$
Ist χ abelscher Charakter, so wird er durch die Werte $\chi(g_j)$, $1 \leq j \leq r$ eindeutig festgelegt, denn es gilt
$$\chi(g) = \chi(g_1^{m_1} \cdot \ldots \cdot g_r^{m_r}) = \chi(g_1^{m_1}) \cdot \ldots \cdot \chi(g_r^{m_r}) = \chi(g_1)^{m_1} \cdot \ldots \cdot \chi(g_r)^{m_r}$$
Wegen
$$1 = \chi(e) = \chi(g_j^{n_j}) = \chi(g_j)^{n_j}$$
ist $\chi(g_j)$ eine n_j-te Einheitswurzel. Analog zu Lemma 1.6, können wir durch jedes r-Tupel $(\mu_1, \ldots, \mu_r) \in \mathbb{C}^{*r}$ mit $\mu_j^{n_j} = 1$ mit
$$\chi(g_1^{m_1} \cdot \ldots \cdot g_r^{m_r}) = \mu_1^{m_1} \cdot \ldots \cdot \mu_r^{m_r}$$

einen abelschen Charakter festlegen, denn es gilt

$$\begin{aligned}\chi(g_1^{m_1}\cdot\ldots\cdot g_r^{m_r}) &= \mu_1^{m_1}\cdot\ldots\cdot\mu_r^{m_r} = \left(\prod_{l=1}^{m_1}\mu_1\right)\cdot\ldots\cdot\left(\prod_{l=1}^{m_r}\mu_r\right)\\ &= \left(\prod_{l=1}^{m_1}\chi(g_1)\right)\cdot\ldots\cdot\left(\prod_{l=1}^{m_r}\chi(g_r)\right) = \chi(g)^{m_1}\cdot\ldots\cdot\chi(g_r)^{m_r}\end{aligned}$$

und zusätzlich

$$\chi(e) = \chi(g_1^0\cdot\ldots\cdot g_r^0) = \mu_1^0\cdot\ldots\cdot\mu_r^0 = 1.$$

Damit sind analog zu Lemma 1.6 folgende Gruppen isomorph

$$G \cong \mathbb{Z}/n_1\mathbb{Z}\times\ldots\times\mathbb{Z}/n_r\mathbb{Z} \cong \{(\mu_1,\ldots,\mu_r)\in\mathbb{C}^{*r};\ \mu_j^{n_j}=1,\ 1\le j\le r\} \cong \widehat{G}.$$

b) Sei $g = g_1^{m_1}\cdot\ldots\cdot g_r^{m_r}\in G\setminus\{e\}$. Dann gibt es ein j mit $m_j\not\equiv 0 \mod n_j$. Wähle

$$\mu_j = e^{2\pi i/n_j},\ \mu_k = 1 \text{ für } k\neq j.$$

Damit gilt für den Charakter χ, der durch Potenzen dieser Einheitswurzeln festgelegt wurde

$$\chi(g) = e^{2\pi i\cdot m_j/n_j}\neq 1, \text{ da } m_j\not\equiv 0 \mod n_j.$$

□

(1.8) Korollar
Sei G eine endliche abelsche Gruppe. Dann ist

$$\varepsilon : G\to\widehat{\widehat{G}},\ g\mapsto\varepsilon_g,\ \varepsilon_g(\chi) := \chi(g)$$

ein Gruppenisomorphismus.

Beweis
Seien $\chi,\psi\in\widehat{G}$. Wir wissen, dass χ und ψ Homomorphismen sind und deshalb gilt für alle $g\in G$:

$$\varepsilon_g(\chi\cdot\psi) = (\chi\cdot\psi)(g) = \chi(g)\cdot\psi(g) = \varepsilon_g(\chi)\cdot\varepsilon_g(\psi).$$

Und damit ergibt sich, dass $\varepsilon_g\in\widehat{\widehat{G}}$. Nun gilt

$$\varepsilon_e(\chi) = \chi(e) = 1.$$

Durch das Anwenden der Homomorphieeigenschaft von χ, gilt für $g,h\in G$:

$$\varepsilon_{gh}(\chi) = \chi(gh) = \chi(g)\cdot\chi(h) = \varepsilon_g(\chi)\cdot\varepsilon_h(\chi).$$

Damit ist $\varepsilon_{gh} = \varepsilon_g \cdot \varepsilon_h$. Wir haben nun gesehen, dass ε ein Gruppenhomomorphismus ist. Für $g \in \text{Kern}\ \varepsilon$ gilt $\chi(g) = 1$ für alle $\chi \in \widehat{G}$. Aus Satz 1.7 folgt $h = e$ und damit ist ε injektiv. Wir wissen, da G eine endliche abelsche Gruppe ist, dass $\widehat{G}$ auch eine endliche abelsche Gruppe ist. Mit dem Satz 1.7 bekommen wir

$$\text{ord}\ G = \text{ord}\ \widehat{G} = \text{ord}\ \widehat{\widehat{G}} < \infty.$$

So sehen wir, dass ε surjektiv ist und damit ist ε ein Gruppenisomorphismus. □

Im folgenden Satz geben wir Orthogonalitätsrelationen an. Weil wir hier eigentlich ein spezielles Skalarprodukt für Charaktere vorliegen haben, heißen diese Identitäten Orthogonalitätsrelationen.

(1.9) Satz (Orthogonalitätsrelationen)
Sei G eine abelsche Gruppe der Ordnung $n \in \mathbb{N}$.

a) Für $\chi \in \widehat{G}$ gilt

$$\sum_{g \in G} \chi(g) = \begin{cases} n, & \text{falls } \chi \equiv 1, \\ 0, & \text{sonst.} \end{cases}$$

b) Für $g \in G$ gilt

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} n, & \text{falls } g = e, \\ 0, & \text{sonst.} \end{cases}$$

Beweis
a)
$\chi \equiv 1$: $\sum\limits_{g \in G} \chi(g) = \sum\limits_{g \in G} 1 = n$, da $|G| = n$

$\chi \not\equiv 1$: Es muss ein $h \in G$ existieren mit $\chi(h) \neq 1$ und damit $\chi(h) - 1 \neq 0$, da sonst $\chi \equiv 1$ wäre. Außerdem wissen wir, da für $l \in G$ die Abbildung $G \to G$, $g \mapsto lg$ ein Gruppenisomorphismus ist, wobei $g \mapsto l^{-1}g$ die Umkehrabbildung darstellt, und χ ein Gruppenhomomorphismus ist, dass

$$(\chi(h) - 1) \cdot \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) - \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g) - \sum_{g \in G} \chi(g) = 0$$

gilt. Damit ergibt sich, wegen $\chi(h) - 1 \neq 0$, dass $\sum_{g \in G} \chi(g) = 0$.

b) Wir können jetzt a) benutzen. Wir setzten $g \in G$ beliebig fest. Dann ist ε_g ein abelscher Charakter von $\widehat{G}$. Somit erhalten wir

$$\sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \varepsilon_g(\chi) = \begin{cases} n, & \text{falls } \varepsilon_g \equiv 1, \text{ d.h. } g = e, \\ 0, & \text{sonst.} \end{cases}$$

□

§ 2 L-Reihen

Wir möchten jetzt unseren Charaktere so konstruieren, dass er aus den ganzen Zahlen diejenigen Zahlen heraussucht, die einen bestimmten Rest haben. Wir werden danach mit diesen speziellen Charakteren Dirichletsche Reihen beziehungsweise L-Reihen bilden, in deren Darstellung nur noch Primzahlen mit bestimmten Teilungseigenschaften vorkommen.

(2.1) Definition
Sei $N \in \mathbb{N}$. Eine Abbildung $\chi : \mathbb{Z} \to \mathbb{C}$ heißt DIRICHLET*scher Charakter* $\mod N$, wenn es einen abelschen Charakter χ' von $(\mathbb{Z}/N\mathbb{Z})^*$ gibt, so dass

$$\chi(k) = \begin{cases} \chi'(k + N\mathbb{Z}), & \text{falls } \mathrm{ggT}(k, N) = 1, \\ 0, & \text{sonst.} \end{cases}$$

(2.2) Lemma
Die Anzahl der DIRICHLETschen Charaktere $\mod N$ ist durch $\varphi(N)$ gegeben.

Beweis
Wir wissen, dass $|(\mathbb{Z}/N\mathbb{Z})^*| = \varphi(N)$ gilt. Da N endlich ist, wissen wir wegen 1.6, dass die Anzahl der abelschen Charaktere auch $\varphi(N)$ ist. Und damit gibt es genau so viele DIRICHLETsche Charaktere $\mod N$. □

(2.3) Beispiele
Wir wollen die DIRICHLETschen Charaktere $\mod N$ für $N = 1, 2, 3, 4, 5, 6, 8$ betrachten. Zuerst bestimmen wir, wie viele es jeweils gibt: $\varphi(1) = 1$, $\varphi(2) = 2^1 - 2^0 = 1$, $\varphi(3) = 3^1 - 3^0 = 2$, $\varphi(4) = 2^2 - 2^1 = 2$, $\varphi(5) = 5^1 - 5^0 = 4$, $\varphi(6) = (2^1 - 2^0)(3^1 - 3^0) = 2$,$\varphi(8) = 2^3 - 2^2 = 4$. Außerdem wissen, dass $\chi(k) = 0$ für $\mathrm{ggT}(k, N) \neq 1$. Wir wollen nun in einer Tabelle die DIRICHLETschen Charaktere $\mod N$ kompakt darstellen. Wir geben dabei zuerst das N an und dann schreiben wir in die erste Zeile die Restklassenvertreter, die teilerfremd zu N sind. In jeder weiteren Zeile, geben wir für die unterschiedlichen χ die Bilder der teilerfremden Restklassen unter χ an. Wegen Satz 1.9 müssen bis auf die erste Zeilensumme, alle Zeilensummen 0 sein. Dann wissen wir, dass die 1 immer auf die 1 abgebildet wird. Außerdem muss jedes Bild einer φ-ten Einheitswurzel entsprechen. Dies wissen wir aus Satz 1.7. So ergeben sich sofort die Werte für die Fälle $N = 1, 2, 3, 4, 6$. Und für die Fälle $n = 5, 8$ muss man dann für die entsprechenden Möglichkeiten noch die Homomorphieeigenschaften nachrechen. So gelangt man zu folgenden Charaktertafeln:

$N=1$	1
χ_1	1

$N=2$	1
χ_1	1

$N=3$	1	2
χ_1	1	1
χ_2	1	-1

$N=4$	1	3
χ_1	1	1
χ_2	1	-1

$N=5$	1	2	3	4
χ_1	1	1	1	1
χ_2	1	i	$-i$	-1
χ_3	1	-1	-1	1
χ_4	1	$-i$	i	1

$N=6$	1	5
χ_1	1	1
χ_2	1	-1

$N=8$	1	3	5	7
χ_1	1	1	1	1
χ_2	1	-1	-1	1
χ_3	1	-1	1	-1
χ_4	1	1	-1	-1

(2.4) Lemma
Sei $N \in \mathbb{N}$. Eine Abbildung $\chi : \mathbb{Z} \to \mathbb{C}$ ist genau dann ein DIRICHLETscher Charakter mod N, wenn gilt:

(i) $\chi(k) = 0 \Leftrightarrow \mathrm{ggT}(k, N) > 1$.

(ii) $\chi(kn) = \chi(k) \cdot \chi(n)$ für alle $k, n \in \mathbb{Z}$.

(iii) $\chi(k) = \chi(n)$, falls $k \equiv n \mod N$.

Beweis

$\Rightarrow$ (i) Ist $\mathrm{ggT}(k, N) \neq 1$, so folgt aus der Definition $\chi(k) = 0$. Ist $\mathrm{ggT}(k, N) = 1$, so folgt, da χ' ein abelscher Charakter ist und damit ungleich 0, dass $\chi(k) \neq 0$. Ist $\chi(k) \neq 0$, so muss $\mathrm{ggT}(k, N) = 1$ gelten.

(ii) Ist $\mathrm{ggT}(k, N) \neq 1$ oder $\mathrm{ggT}(n, N) \neq 1$, so folgt $\mathrm{ggT}(kn, N) \neq 1$. Also $\chi(k) \cdot \chi(n) = \chi(kn) = 0$. Ist nun $\mathrm{ggT}(k, N) = 1$ und $\mathrm{ggT}(n, N) = 1$, so folgt $\mathrm{ggT}(kn, N) = 1$ und dann gilt:
$\chi(k) \cdot \chi(n) = \chi'(k + N\mathbb{Z}) \cdot \chi'(n + N\mathbb{Z}) = \chi'(kn + kN\mathbb{Z} + nN\mathbb{Z} + N\mathbb{Z}N\mathbb{Z})$
$= \chi'(kn + N\mathbb{Z}) = \chi(kn)$

(iii) Ist $k \equiv n \mod N$ so ist $\chi'(k + N\mathbb{Z}) = \chi'(n + N\mathbb{Z})$ und auch $\mathrm{ggT}(k, N) = \mathrm{ggT}(n, N)$ und damit ist $\chi(k) = \chi(n)$.

$\Leftarrow$ Sei $k \in \mathbb{Z}$ mit $\mathrm{ggT}(k, N) = 1$, so sei $\chi'(k + N\mathbb{Z}) := \chi(k) \in \mathbb{C}^*$. Sei nun $n \in \mathbb{Z}$ mit $n \equiv k \mod N$. Damit folgt $\mathrm{ggT}(n, N) = 1$, so gilt mit (i), dass $\chi'(k + N\mathbb{Z}) \neq 0$. Mit (iii) folgt $\chi'(k + N\mathbb{Z}) = \chi'(n + N\mathbb{Z})$, womit die Wohldefiniertheit gezeigt ist.

Mit (ii) folgt die Gruppenhomomorphismeneigenschaft und damit wissen wir, dass χ' ein abelscher Charakter ist. Und damit ist χ wegen (i) ein DIRICHLETscher Charakter. □

(2.5) Bezeichnung

1. $n \pmod N$ bedeutet, dass n ein beliebiges Vertretersystem von $\mathbb{Z}/N\mathbb{Z}$ durchläuft.
2. $\chi \pmod N$ bedeutet, dass χ alle DIRICHLETschen Charakter $\bmod N$ durchläuft.
3. Wir bezeichnen mit

$$\chi_0 : \mathbb{Z} \to \mathbb{C},\ n \mapsto \begin{cases} 1, & \text{falls } \operatorname{ggT}(n, N) = 1, \\ 0, & \text{sonst,} \end{cases}$$

den *Hauptcharakter* $\bmod N$, der dem trivialen Charakter auf $(\mathbb{Z}/N\mathbb{Z})^*$ entspricht.

(2.6) Satz
Sei $N \in \mathbb{N}$.

a) Ist χ ein DIRICHLETscher Charakter $\pmod N$, so gilt

$$\sum_{n \pmod N} \chi(n) = \begin{cases} \varphi(N), & \text{falls } \chi = \chi_0, \\ 0, & \text{falls } \chi \neq \chi_0. \end{cases}$$

b) Sind χ_1, χ_2 DIRICHLETsche Charaktere $\pmod N$, so gilt

$$\frac{1}{\varphi(N)} \sum_{n \pmod N} \chi_1(n)\overline{\chi_2(n)} = \begin{cases} 1, & \text{falls } \chi_1 = \chi_2, \\ 0, & \text{falls } \chi_1 \neq \chi_2. \end{cases}$$

c) Für $n \in \mathbb{Z}$ gilt

$$\sum_{\chi \pmod N} \chi(n) = \begin{cases} \varphi(N), & \text{falls } n \equiv 1 \pmod N, \\ 0, & \text{falls } n \not\equiv 1 \pmod N. \end{cases}$$

d) Für $k, n \in \mathbb{Z}$ mit $\operatorname{ggT}(n, N) = 1$ gilt

$$\frac{1}{\varphi(N)} \sum_{\chi \pmod N} \chi(k)\overline{\chi(n)} = \begin{cases} 1, & \text{falls } k \equiv n \pmod N, \\ 0, & \text{falls } k \not\equiv n \pmod N. \end{cases}$$

Beweis
Zuerst sei bemerkt, dass die Einheiten in $\mathbb{Z}/N\mathbb{Z}$, diejenigen Elemente sind, die teilerfremd zu N sind, d. h. $\underline{k} \in \mathbb{Z}/N\mathbb{Z}$ mit $\operatorname{ggT}(k, N) = 1$. Wir wissen damit, dass es davon $\varphi(N)$ Elemente gibt und daraus folgt $\operatorname{ord}(\mathbb{Z}/N\mathbb{Z})^* = \varphi(N)$.

a)

$$\sum_{n \,(\mathrm{mod}\ N)} \chi(n) \overset{2.1}{=} \sum_{k \in (\mathbb{Z}/N\mathbb{Z})^*} \chi'(k) \overset{1.9}{=} \begin{cases} \varphi(N), & \text{falls } \chi' \equiv 1, \text{ d. h. } \chi = \chi_0 \\ 0, & \text{sonst.} \end{cases}$$

b) Hat man zwei DIRICHLETsche Charaktere $\pmod N$, etwa χ_1, χ_2, so ist $\chi_1\chi_2$ wieder ein DIRICHLETscher Charakter $\pmod N$, da χ_1', χ_2' beide in der dualen Gruppe von $(\mathbb{Z}/N\mathbb{Z})^*$ liegen. Nun müssen wir zeigen, dass $\chi_1\overline{\chi_2} = \chi_0$ genau dann gilt, wenn $\chi_1 = \chi_2$. Seien χ_1', χ_2' die zugehörigen abelschen Charaktere von $(\mathbb{Z}/N\mathbb{Z})^*$. Es gilt wegen Lemma 1.6, dass ein $x \in \mathbb{Q}$ existiert mit $\chi_2'(g) = \exp(2\pi i x)$ und somit gilt für alle $g \in (\mathbb{Z}/N\mathbb{Z})^*$

$$\overline{\chi_2'(g)} = \overline{\exp(2\pi i x)} = \exp(-2\pi i x) = \chi_2'^{-1}(g).$$

Wenn nun $\chi_1' = \chi_2'$ gilt, dann folgt $\chi_1'(g)\overline{\chi_2'(g)} = 1$ und damit $\chi_1\overline{\chi_2} = \chi_0$. Gilt $\chi_1' \neq \chi_2'$ so sieht man sofort, dass ein g existiert mit $\chi_1'(g)\overline{\chi_2'(g)} \neq 1$ und damit $\chi_1\overline{\chi_2} \neq \chi_0$. So erhalten wir mit a) die Behauptung.

c) Mit Lemma 2.2 und $\chi(n) = 1$ für $n \equiv 1 \mod N$ folgt sofort die Behauptung.

d) Statt $\overline{\chi(n)}$ zu schreiben, wissen wir, dass ein n' existiert mit $nn' \equiv 1 \mod N$. Da $k \equiv n \mod N$, folgt $kn' \equiv 1 \mod N$. Und damit gilt

$$\begin{aligned} \sum_{\chi \,(\mathrm{mod}\ N)} \chi(k)\overline{\chi(n)} &= \sum_{\chi' \in \widehat{(\mathbb{Z}/N\mathbb{Z})^*}} \chi'(\underline{k})\overline{\chi'(\underline{n})} = \sum_{\chi' \in \widehat{(\mathbb{Z}/N\mathbb{Z})^*}} \chi'(\underline{k})\chi'(\underline{n})^{-1} \\ &= \sum_{\chi' \in \widehat{(\mathbb{Z}/N\mathbb{Z})^*}} \chi'(\underline{k})\chi'(\underline{n}^{-1}) = \sum_{\chi' \in \widehat{(\mathbb{Z}/N\mathbb{Z})^*}} \chi'(\underline{k})\chi'(\underline{n}') \\ &= \sum_{\chi \,(\mathrm{mod}\ N)} \chi(k)\chi(n') = \sum_{\chi \,(\mathrm{mod}\ N)} \chi(kn'). \end{aligned}$$

Mit c) folgt nun die Behauptung. □

(2.7) Definition
Ist χ ein DIRICHLETscher Charakter $\pmod N$, so heißt

$$L(\chi, s) := D_\chi(s) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$$

die DIRICHLETsche L-Reihe zum DIRICHLETscher Charakter.

(2.8) Beispiele
Seien χ_{-4}, χ_{-3} wie folgt definiert

$$\chi_{-4} = \begin{cases} 1, & \text{falls } n \equiv 1 \mod 4, \\ -1, & \text{falls } n \equiv 3 \mod 4, \\ 0, & \text{falls } n \text{ gerade}, \end{cases}$$
$$\chi_{-3} = \begin{cases} 1, & \text{falls } n \equiv 1 \mod 3, \\ -1, & \text{falls } n \equiv 2 \mod 3, \\ 0, & \text{falls } n \equiv 0 \mod 3. \end{cases}$$

Weiter seien $r(n) := |\{(a,b) \in \mathbb{Z} \times \mathbb{Z};\ a^2 + b^2 = n\}|$,
$\tilde{r}(n) := |\{(a,b) \in \mathbb{Z} \times \mathbb{Z};\ a^2 + ab + b^2 = n\}|$. Dann gilt für $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$:
a)

$$\sum_{n=1}^{\infty} r(n) n^{-s} = 4\zeta(s) L(\chi_{-4}, s),$$

b)

$$\sum_{n=1}^{\infty} \tilde{r}(n) n^{-s} = 6\zeta(s) L(\chi_{-3}, s).$$

Beweis
a) Haben wir gezeigt, dass $\frac{1}{4} r(n) = \sum\limits_{d|n} \chi_{-4}(d)$, wissen wir

$$\sum_{n=1}^{\infty} \frac{1}{4} r(n) n^{-s} = \sum_{n=1}^{\infty} \left(\sum_{d|n} \chi_{-4}(d) \right) n^{-s}$$

Wir dürfen die Faltungsformel für alle s mit $\mathrm{Re}(s) > 1$ wie folgt anwenden

$$\zeta(s) L(\chi - 4, s) = \sum_{a=1}^{\infty} a^{-s} \cdot \sum_{b=1}^{\infty} \chi_{-4}(b) b^{-s} = \sum_{n=1}^{\infty} \left(\sum_{d|n} \chi_{-4}(d) \right) n^{-s}.$$

Also müssen wir jetzt noch $\frac{1}{4} r(n) = \sum\limits_{d|n} \chi_{-4}(d)$ zeigen.
Ein sehr elementarer Beweis kann bei [3] auf den Seiten 57-60 nachgelesen werden. Der Charakter χ_{-4} ist eine (streng) multiplikative zahlentheoretische Funktion. Außerderm gilt, dass sich eine Primzahl $p \in \mathbb{Z}$ in $\mathbb{Z}[i]$ auf drei verschiedene Arten zerlegt:

- $\chi_{-4}(p) = 1$: So gilt $p = q\overline{q}$ und $q, \overline{q}$ sind nicht-assoziierte Primelemente in $\mathbb{Z}[i]$.

- $\chi_{-4}(p) = -1$: So ist p prim in $\mathbb{Z}[i]$.
- $\chi_{-4}(p) = 0$: So gilt $p = uq^2$ mit u Einheit und Primelement q in $\mathbb{Z}[i]$.

Die Einheiten in $\mathbb{Z}[i]$ sind $\pm i, \pm 1$. Außerdem ist jedes irreduzibles Element in $\mathbb{Z}$ auch prim. Dies kann alles ausführlich in [4] nachgelesen werden. Es gilt

$$\begin{aligned} r(n) &= \left|\{(a,b) \in \mathbb{Z} \times \mathbb{Z};\ a^2 + b^2 = n\}\right| = |\{(a,b) \in \mathbb{Z} \times \mathbb{Z};\ (a+ib)(a-ib) = n\}| \\ &= \left|\{(a,b) \in \mathbb{Z} \times \mathbb{Z};\ |a+ib|^2 = n\}\right| = \left|\{x \in \mathbb{Z}[i];\ |x|^2 = n\}\right| \end{aligned}$$

Uns interessieren nun die Anzahl der verschiedenen $x \in \mathbb{Z}[i]$ mit $x\overline{x} = n$. Wir wissen, ist x eine Lösung unseres Problems, so auch $-x, ix$ und $-ix$. Wir sehen uns also jetzt $\frac{1}{4}r(n)$ an. Ist $n = 1$, so sieht man sofort, dass $\frac{1}{4}r(n) = \frac{1}{4}\left|\{\pm i, \pm 1\}\right| = 1$ gilt. Ist $n = a \cdot b$ mit $\mathrm{ggT}(a,b) = 1$, so sind a und b teilerfremd und man sieht sofort ein, dass wir $\frac{1}{4}r(n) = \frac{1}{4}r(a) \cdot \frac{1}{4}r(b)$. Denn wir sehen uns $y, z \in \mathbb{Z}[i]$ mit $|y|^2 = a$ und $|z|^2 = b$ an, so dass $|x|^2 = n = a \cdot b = |y|^2 \cdot |z|^2$ gilt. Damit bekommen wir die Multiplikativität der von $\frac{1}{4}r(n)$. Jetzt müssen wir uns nur noch anschauen, wie $\frac{1}{4}r(p^l)$ mit $p \in \mathbb{P}$ aussieht. Für denn Fall $n = 2$ gilt $2 = u \cdot q^2$ mit $u \in \mathbb{Z}[i]$ Einheit und $q \in \mathbb{Z}[i]$ Primelement. Damit gilt $p^l = u_1 \cdot u_l (q^2)^l$. Da das Produkt $u_1 \cdot u_l$ nur einen von vier möglichen Werten annehmen kann, folgt $\frac{1}{4}r(p^l) = \prod_{k=1}^{l} \frac{1}{4}r(p) = \prod_{k=1}^{l} 1 = 1 = \sum_{d|2^l} \chi_{-4}(d)$. Die Begründung für eine Primzahl $p \equiv 3 \mod 4$ ist ähnlich. Da wir aus [2] wissen, dass dann nur eine gerade Potenz von p durch ein $|x|^2$ darstellbar ist, bekommen wir für $n = p^2$ die vier Möglichkeiten $x = p, -p, ip, -ip$. Für jede gerade Potenz $2l$ bekommen wir die Möglichkeiten $x = p^l, -p^l, ip^l, -ip^l$ heraus. Damit ist ersichtlich, dass $\sum_{d|p^l} \chi_{-4}(d) = \frac{1}{2}(1 + (-1)^{l+1}) = \frac{1}{4}r(p^l)$.
Jetzt fehlt nur noch der Fall $p \equiv 1 \mod 4$. Wir wollen jetzt zeigen, dass $x = q, -q, iq, -iq, \overline{q}, -\overline{q}, i\overline{q}, -i\overline{q}$ Lösungen sind. Da $|q\overline{q}|^2 = p^2$, müssen $|q|^2 = p$ und $|\overline{q}|^2 = p$ sein, da das Ergebnis eine nichtnegative ganze Zahl sein muss und p^2 nur die Teiler $1, p, p^2$ hat. Da aber keine Zahl eine Einheit ist und $|q\overline{q}|^2 = |q|^2|\overline{q}|^2$, haben wir unsere Lösungen bekommen.
Nun habe p^l die Lösungen $\pm \prod_{k=1}^{r} q \prod_{j=r+1}^{l} \overline{q}, \pm \prod_{k=1}^{r} q \prod_{j=r+1}^{l} \overline{q},\ 0 \le r \le l$. Für p^{l+1} sieht man ganz schnell, dass mit Multiplikation von q oder $\overline{q}$ nur vier Lösungen mehr ergeben, nämlich für den Fall, dass wir $\overline{q}$ an die Lösungen mit $r = 0$ ranmultiplizieren, denn man weiß, dass es weiterhin immer vier Darstellungen gibt wo die Anzahl der $\overline{q}$ gleich m ist mit $0 \le m \le l$. So bekommt man $\frac{1}{4}r(p^l) = l + 1 = \sum_{d|p^l} \chi_{-4}(d)$. Da $\frac{1}{4}r(n)$ multiplikativ ist, haben wir durch das Beweisen für die verschiedenen Primzahlpotenzen nun auch die Identität gezeigt.

b) Analog brauchen wir nur, dass $\frac{1}{6}\tilde{r}(p^l) = \sum_{d|p^l} \chi_{-3}(d)$. Dann nehmen wir statt $\mathbb{Z}[i]$ den Ring $\mathbb{Z}[\frac{1}{2}(1 + i\sqrt{3})]$. Danach geht der Beweis durch die Faltungsformel wie in a). □

(2.9) Proposition
Sei χ_0 der Hauptcharakter $\pmod N$. Dann gilt:

$$\sigma_a(\chi_0) = \sigma_b(\chi_0) = 1$$

und

$$L(\chi_0, s) = \left(\prod_{\substack{p|N \\ p\in\mathbb{P}}} (1-p^{-s}) \right) \cdot \zeta(s) = \prod_{\substack{p|N \\ p\in\mathbb{P}}} (1-p^{-s})^{-1} \neq 0$$

für alle $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$. Die L-Reihe $L(\chi_0, s)$ besitzt eine meromorphe Fortsetzung in die rechte Halbebene $\{s \in \mathbb{C};\, \mathrm{Re}(s) > 0\}$ und ist dort holomorph bis auf einen einfachen Pol bei $s = 1$ mit dem Residuum $\frac{\varphi(N)}{N}$.

Beweis
Es gilt wegen $|\chi_0(n)| \leq 1$ für $\sigma := \mathrm{Re}(s) > 1$

$$\left| \sum_{n=1}^{\infty} \chi_0(n) n^{-s} \right| \leq \sum_{n=1}^{\infty} |\chi_0(n)||n^{-s}| \leq \sum_{n=1}^{\infty} |n^{-s}| \overset{[1](3.4)}{\leq} 1 + \frac{1}{\sigma - 1}.$$

Damit kovergiert die Reihe für $\mathrm{Re}(s) > 1$ absolut. Es bekannt, dass $\chi_0(n) = 1$ für alle n mit $\mathrm{ggT}(n, N) = 1$ und sonst 0 ist. Somit gilt

$$\sum_{n=1}^{rN} \chi_0(n) n^{-1} \geq \sum_{n=0}^{r-1} \chi_0(1+nN)(1+nN)^{-s}.$$

Damit folgt

$$\sum_{n=1}^{rN} \chi_0(n) n^{-1} \geq \sum_{n=0}^{r-1} \chi_0(1+nN)(1+nN)^{-s} \geq \sum_{n=0}^{r-1} \frac{1}{1+nN} \geq \frac{1}{N} \sum_{m=1}^{r} \frac{1}{m} \xrightarrow[r\to\infty]{} \infty.$$

Damit divergiert die Reihe für $s = 1$ und damit gilt $\sigma_a(\chi_0) = \sigma_b(\chi_0) = 1$.
Wir nutzen nun aus, dass χ_0 streng multiplikativ ist, da für χ_0' gilt, dass es streng multiplikativ ist, wie wir in Satz 1.7 gesehen haben. Somit ist die Existenz eines EULER-Produktes durch [1](4.15) und $\sigma_a = 1$ für $\mathrm{Re}(s) > 1$ gesichert. Wir folgern damit

$$\begin{aligned} L(\chi_0, s) &\overset{\text{Multiplikativität}}{=} \prod_{p\in\mathbb{P}} \left(\sum_{l=0}^{\infty} \chi_0(p^l) p^{-ls} \right) \overset{\text{strenge Multiplikativität}}{=} \prod_{p\in\mathbb{P}} \frac{1}{1-\chi_0(p)p^{-s}} \\ &= \prod_{\substack{p\nmid N \\ p\in\mathbb{P}}} \frac{1}{1-p^{-s}} \overset{[1](4.16)}{=} f(s) \cdot \zeta(s),\ f(s) = \prod_{p|N} (1-p^{-s}). \end{aligned}$$

Es ergibt sich, dass $f(s)$ eine ganze Funktion mit $f(s) \neq 0$ für alle s mit $\mathrm{Re}(s) > 0$ ist. Da $s = a + it$ mit $a \in \mathbb{R}^+$ und $t \in \mathbb{R}$ ist und es ein $l \in \mathbb{R}$ mit $e^l = p$ gibt, folgt $|p^{-s}| = |(e^l)^{a+it}| = |(e^l)^a||(e^l)^{it}| = |e^{la}| \neq 1$, da $la \neq 0$. Und da $\zeta(s) \neq 0$ für alle $\mathrm{Re}(s) > 1$, ist $L(\chi_0, s) = f(s) \cdot \zeta(s) \neq 0$ für alle $\mathrm{Re}(s) > 1$. Da wir aus [1](5.6) wissen, dass $\zeta(x)$ eine mereomorphe Fortsetzung für $\mathrm{Re}(s) > 0$ mit einzigem Pol in $s = 1$ hat, folgt sofort, dass dies auch für $L(\chi_0, s)$ gilt. Aus [2] wissen wir, dass $N \prod_{\substack{p|N \\ p\in\mathbb{P}}} \left(1 - \frac{1}{p}\right) = \varphi(N)$ gilt und bestimmen damit das Residuum an der Stelle $s = 1$:

$$\mathrm{Res}_{s=1} L(\chi_0, s) = f(1)\mathrm{Res}_{s=1}\zeta(s) = f(1) = \prod_{\substack{p|N \\ p\in\mathbb{P}}} \left(1 - \frac{1}{p}\right) = \frac{\varphi(N)}{N}$$

□

(2.10) Satz

Sei χ ein DIRICHLETscher Charakter $\pmod N$ und $\chi \neq \chi_0$. Dann gilt

$$\sigma_a(\chi) = 1 \quad \text{und} \quad \sigma_b(\chi) = 0.$$

$L(\chi, s)$ ist holomorph in der rechten Halbebene $\{s \in \mathbb{C};\ \mathrm{Re}(s) > 0\}$ und erfüllt

$$L(\chi, s) = \prod_{\substack{p\nmid N \\ p\in\mathbb{P}}} (1 - \chi(p)p^{-s})^{-1} \neq 0, \text{ für } \mathrm{Re}(s) > 1.$$

Beweis

Sei $x \in \mathbb{R}$, $x > 0$ mit $[x] = Nr + m$, $r \in \mathbb{N}_0$ und $0 \leq m < N$. Da $\chi \neq \chi_0$ ist $\sum_{n=1}^{N} \chi(n) = 0$ nach Satz 2.6. Damit bekommen wir

$$\left|\sum_{n\leq x} \chi(n)\right| = \left|\sum_{n=1}^{Nr} \chi(n) + \sum_{n=Nr+1}^{Nr+m} \chi(n)\right| = \left|\sum_{n=1}^{m} \chi(n)\right| \leq m \leq N.$$

Wir folgern

$$\left|\sum_{n\leq x} \chi(n)\right| = \mathcal{O}(x^0).$$

Nach [1](4.8) gilt

$$\sigma_b = \inf\{\alpha \in \mathbb{R};\ \sum_{n\leq x} \chi(n) = \mathcal{O}(x^\alpha)\} = 0,$$

da $D_\chi(0)$ nicht konvergiert, weil $\chi(n)n^{-0} = \chi(n)$ keine Nullfolge ist. Aus [1](4.4) folgern wir, dass für $\mathrm{Re}(s) > 0$ die DIRICHLET-Reihe $D_\chi(s) = L(\chi, s)$ holomorph ist. Genau wie im Beweis zur Proposition 2.9, können wir zeigen, dass $\sigma_a = 1$ ist. Jetzt nutzten wir aus, dass χ streng multiplikativ ist. Damit können wir für $\mathrm{Re}(s) > 1$ schreiben

$$
\begin{aligned}
L(\chi,s) &= \prod_{p\in\mathbb{P}}\left(\sum_{l=0}^{\infty}\chi(p^l)p^{-ls}\right) = \prod_{p\in\mathbb{P}}\left(\sum_{l=0}^{\infty}(\chi(p)p^{-s})^l\right) = \prod_{p\in\mathbb{P}}\frac{1}{1-\chi(p)p^{-s}} \\
&= \prod_{\substack{p\mid N\\ p\in\mathbb{P}}}\frac{1}{1-\chi(p)p^{-s}}\cdot\prod_{\substack{p\nmid N\\ p\in\mathbb{P}}}\frac{1}{1-\chi(p)p^{-s}} = \prod_{\substack{p\mid N\\ p\in\mathbb{P}}}\frac{1}{1}\cdot\prod_{\substack{p\nmid N\\ p\in\mathbb{P}}}\frac{1}{1-\chi(p)p^{-s}} \\
&= \prod_{\substack{p\nmid N\\ p\in\mathbb{P}}}\frac{1}{1-\chi(p)p^{-s}} \neq 0.
\end{aligned}
$$

□

Literatur

[1] Aloys Krieg. *Analytische Zahlentheorie*, Aachen

[2] Eva Zerz. *Elementare Zahlentheorie*, Aachen

[3] Volha Baranouskaya.
http://upload.wikimedia.org/wikiversity/de/a/a9/Summe_von_Quadraten_und_die_Anzahl_ihrer_Darstellungen.pdf,
Summe von Quadraten und die Anzahlihrer Darstellungen, Osnabrück

[4] T. Linkin, S. Krez.
http://www2.math.uni-paderborn.de/fileadmin/Mathematik/People/wedhorn/Lehre/LinkinKrez_Gau%C3%83_scheZahlen.pdf,
Gaußsche Zahlen, Paderborn