Charaktere

Vortrag zum Seminar zur Funktionentheorie, 28.01.2008

Elisabeth Peternell

Zu den wichtigsten Dirichletschen Reihen gehören die L-Reihen, welche insbesondere gewöhnliche Dirichletsche Reihen darstellen, wobei deren Koeffizientenfolgen jeweils durch einen sogenannten Dirichletschen Charakter definiert sind. Es ist also wichtig, zunächst Kenntnisse über Eigenschaften und Verhalten solcher Charaktere zu erlangen.

§1 Die Charaktergruppe

(1.1) Definition (Charakter)
Sei G eine Gruppe und $\mathbb{C}^\times$ die multiplikative Gruppe von $\mathbb{C}$. Ein Homomorphismus

$$\chi : G \to \mathbb{C}^\times$$

heißt *Charakter* auf G. ◇

(1.2) Lemma
Die Menge

$$\widehat{G} := \{\chi, \chi \text{ ist Charakter auf } G\}$$

ist eine abelsche Gruppe mit der Verknüpfung $\widehat{G} \times \widehat{G} \to \widehat{G}$ definiert durch

$$(\chi_1\chi_2)(g) := \chi_1(g)\chi_2(g), \qquad \text{für alle } \chi_1, \chi_2 \in \widehat{G} \text{ und } g \in G$$

und inversem Element χ^{-1} definiert durch

$$\chi^{-1}(g) := (\chi(g))^{-1}, \qquad \text{für alle } \chi \in \widehat{G} \text{ und } g \in G.$$

$\widehat{G}$ wird auch als Charaktergruppe bezeichnet. ◇

Beweis
Die Abbildungen $\chi_1\chi_2$ und χ^{-1} sind offensichtlich Homomorphismen von G nach $\mathbb{C}^\times$. Einfaches Nachrechnen der Gruppenaxiome, wobei sich $\chi_0 \equiv 1$ als neutrales Element ergibt, liefert die Behauptung.

Im Folgenden werden wir nur endliche abelsche Gruppen betrachten. Um die Handhabung mit endlichen abelschen Gruppen zu erleichtern, notieren wir die

(1.3) Bemerkung
Sei G eine endliche abelsche Gruppe, dann existieren nach dem Hauptsatz über endlich erzeugte abelsche Gruppen $n_1, \dots, n_p \in \mathbb{N}$, so dass

$$G \cong (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_p\mathbb{Z}),$$

das heißt es existieren $g_1, \dots, g_p \in G$ mit $\operatorname{ord} g_k = n_k$, so dass

$$G = \langle g_1 \rangle \langle g_2 \rangle \cdots \langle g_p \rangle$$

und

$$\langle g_k \rangle \cap \prod_{\substack{j=1 \\ j \neq k}}^{n} \langle g_j \rangle = \{1\}, \qquad \text{für alle } 1 \leq k \leq p.$$

Man schreibt auch

$$G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_p \rangle \ .$$

Für $g \in G$ existiert demnach zu jedem $j \in \{1, \dots, p\}$ ein eindeutig bestimmtes $r_j \in \{0, \dots, n_j - 1\}$ mit $g = g_1^{r_1} \cdot g_2^{r_2} \cdots g_p^{r_p}$. ◇

Wir kommen zum ersten

(1.4) Satz
Sei G eine endliche abelsche Gruppe, dann gilt:

$$G \cong \widehat{G}.$$

Insbesondere ist $|G| = |\widehat{G}|$. ◇

Beweis
Sei $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_p \rangle$ mit den Bezeichnungen aus (1.3). Ist $\chi \in \widehat{G}$, so gilt

$$1 = \chi(1) = \chi(g_j^{n_j}) = \chi(g_j)^{n_j}, \qquad \text{für alle } 1 \leq j \leq p,$$

das heißt $\chi(g_j)$ ist eine n_j-te Einheitswurzel in $\mathbb{C}^\times$, also

$$\chi(g_j) = \exp\left(\frac{2\pi i k_j}{n_j}\right) \text{ für ein } 0 \leq k_j < n_j.$$

Definiere für $1 \leq j \leq p$ den Homomorphismus $\chi_j \in \widehat{G}$ mit

$$\chi_j(g_k) = \begin{cases} \exp\left(\frac{2\pi i}{n_j}\right), & \text{falls } k = j \\ 0, & \text{sonst.} \end{cases}$$

Sei $g \in G$ beliebig mit der eindeutigen Darstellung $g = g_1^{r_1} \cdot g_2^{r_2} \cdots g_p^{r_p}$. Damit ist

$$\begin{aligned}\chi(g) &= \chi(g_1^{r_1} \cdot g_2^{r_2} \cdots g_p^{r_p}) \\ &= \chi(g_1)^{r_1}\chi(g_2)^{r_2} \cdots \chi(g_p)^{r_p} \\ &= \exp\Big(\frac{2\pi i k_1}{n_1}\Big)^{r_1} \cdots \exp\Big(\frac{2\pi i k_p}{n_p}\Big)^{r_p} \\ &= \chi_1(g_1^{r_1})^{k_1} \cdots \chi_p(g_p^{r_p})^{k_p}, \\ &= \chi_1^{k_1}(g) \cdots \chi_p^{k_p}(g).\end{aligned}$$

Es ist also

$$\chi = \chi_1^{k_1} \cdots \chi_p^{k_p}. \qquad (*)$$

Sei nun $\Psi : G \to \widehat{G}$ der Homomorphismus definiert durch

$$\Psi(g_j) = \chi_j, \qquad \text{für alle } 1 \leq j \leq p.$$

Wegen $(*)$ ist Ψ surjektiv.

Sei $g \in \operatorname{Kern}\Psi$ mit

$$g = \prod_{j=1}^{p} g_j^{r_j}$$

für bestimmte $r_j \in \{0, \ldots, n_j - 1\}$. Dann gilt

$$1 \equiv \Psi(g) = \prod_{j=1}^{p} \Psi(g_j)^{r_j} = \prod_{j=1}^{p} \chi_j^{r_j}.$$

Für alle $j_0 \in \{1, \ldots, p\}$ ist also

$$1 = \prod_{j=1}^{p} \chi_j^{r_j}(g_{j_0}) = \chi_{j_0}^{r_{j_0}}(g_{j_0}) = \exp\Big(\frac{2\pi i r_{j_0}}{n_{j_0}}\Big),$$

was genau dann der Fall ist, wenn $r_{j_0} = 0$ für alle $1 \leq j_0 \leq p$ gilt. Es folgt $g = 1$, also Kern Ψ =1, was die Injektivität von Ψ zeigt. Demnach ist Ψ ein Isomorphismus zwischen G und $\widehat{G}$. □

§ 2 Dirichletsche Charaktere

Nun kommen wir zu den Koeffizientenfolgen, die eine L-Reihe ausmachen.

Zunächst einige

(2.1) Bemerkungen

(i) Die Abbildung

$$\mathbb{Z} \to \mathbb{Z}_N, \qquad x \mapsto \underline{x} := x + N\mathbb{Z}$$

ist ein Ringhomomorphismus, wobei $\mathbb{Z}_N$ den Ring $\mathbb{Z}/N\mathbb{Z}$ bezeichne.

(ii) Sei $\mathbb{Z}_N^\times$ die multiplikative Gruppe von $\mathbb{Z}_N$, dann gilt:

$$\underline{x} \in \mathbb{Z}_N^\times \Leftrightarrow \mathrm{ggT}\,(x, N) = 1.$$

(iii) Die *Eulersche φ-Funktion* wird definiert durch

$$\varphi : \mathbb{N} \to \mathbb{N} \qquad \varphi(N) := |\mathbb{Z}_N^\times|.$$

Es gilt

$$\varphi(N) = N \prod_{p|N} \Big(1 - \frac{1}{p}\Big).$$

◇

Beweis

(i) Nachrechnen.

(ii) „⇒“ Sei $\underline{x} \in \mathbb{Z}_N^\times$. Angenommen es gilt $\mathrm{ggT}\,(x, N) = d \neq 1$; dann ist $x = db$ und $N = dc$ für bestimmte $b, c \in \mathbb{Z}\backslash\{0\}$. Das führt wegen

$$\underline{0} \neq \underline{c} = \underline{x}^{-1}\underline{x}\,\underline{c} = \underline{x^{-1}xc} = \underline{x^{-1}dbc} = \underline{x^{-1}bN} = \underline{0}$$

zum Widerspruch.

„⇐“ Sei $\mathrm{ggT}\,(x, N) = 1$, dann existieren nach dem erweiterten euklidischen Algorithmus $a, b \in \mathbb{Z}$ mit $1 = ax + bN$ und damit $\underline{1} = \underline{ax + bN} = \underline{a}\,\underline{x}$. Daher gilt $\underline{x} \in \mathbb{Z}_N^\times$.

(iii) Ist $N = p^k$ für eine Primzahl p, dann gelten für $1 \leq x \leq p^k$ die Äquivalenzen:

$$\mathrm{ggT}\,(x, N) = 1 \Leftrightarrow p \not| x \Leftrightarrow x \notin \{0, p, 2p, \ldots, p^{k-1}p\},$$

also

$$\varphi(p^k) = |\mathbb{Z}_{p^k}^\times| = p^k - p^{k-1}.$$

Für $N \in \mathbb{N}$ sei $N = p_1^{k_1} \cdots p_n^{k_n}$ die Primfaktorzerlegung von N mit p_j paarweise verschieden. Dann gilt wegen des Chinesischen Restsatzes (vgl.(3.5)):

$$\varphi(N) = \varphi(p_1^{k_1}) \cdots \varphi(p_n^{k_n}) = N \prod_{p|N} \Big(1 - \frac{1}{p}\Big).$$

□

(2.2) Definition (Dirichletscher Charakter (mod N))
Ein *Dirichletscher Charakter (*mod N*)* ist ein Charakter

$$\chi : \mathbb{Z}_N^\times \to \mathbb{C}^\times.$$

Die diesem Homomorphismus zugeordnete Funktion definiert durch

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

nennt man ebenfalls Dirichletschen Charakter. Mit G_N sei die Charaktergruppe von $\mathbb{Z}_N^\times$ bezeichnet. Wir schreiben auch $\chi \in G_N$ falls mit χ die Fortsetzung eines Dirichletschen Charakters (mod N) gemeint ist. ◇

Offensichtlich ist folgendes

(2.3) Lemma
Die Fortsetzung von $\chi \in G_N$ auf $\mathbb{Z}$ ist streng multiplikativ und durch die Werte von χ auf $\mathbb{Z}_N^\times$ eindeutig bestimmt. ◇

Beweis
Da $n \mapsto \underline{n}$ ein Ringhomomorphismus von $\mathbb{Z}$ nach $\mathbb{Z}_N$ und χ auf $\mathbb{Z}_N^\times$ ein Gruppenhomomorphismus ist, folgt die Behauptung sofort. □

Zur Bestimmung aller Dirichletschen Charaktere auf $\mathbb{Z}_N^\times$ dient das

(2.4) Lemma
Die Anzahl der Dirichletschen Charaktere auf $\mathbb{Z}_N^\times$ ist gegeben durch

$$|G_N| = |\mathbb{Z}_N^\times| = \varphi(N).$$

◇

Beweis
Folgt aus (2.1)(iii). □

Zur Veranschaulichung dienen die

(2.5) Beispiele

(i) Sei $N \in \mathbb{N}$ und $\chi_0 : \mathbb{Z} \to \mathbb{C}^\times$ mit

$$\chi(n) = \begin{cases} 1, & \text{falls } \operatorname{ggT}(n, N) = 1 \\ 0, & \text{sonst} \end{cases}$$

ist ein Dirichletscher Charakter $(\bmod N)$ und heißt Hauptcharakter.

(ii) Sei χ ein Dirichletscher Charakter $(\bmod N)$, dann ist $\overline{\chi}$ definiert durch

$$\overline{\chi}(g) := \overline{\chi(g)}$$

ein Dirichletscher Charakter $(\bmod N)$. Zu $g \in \mathbb{Z}_N^\times$ existiert ein $q \in \mathbb{Q}$ mit $\chi(g) = \exp(2\pi i q)$, also gilt

$$\overline{\chi}(g) = \overline{\exp(2\pi i q)} = \exp(-2\pi i q) = \chi^{-1}(g).$$

Demnach ist $\overline{\chi} = \chi^{-1}$.

(iii) Sei $N = 8$; dann gilt $G_8 = \{\varepsilon_j \mid 1 \le j \le 4\}$ mit

$\underline{n}$	$\underline{1}$	$\underline{3}$	$\underline{5}$	$\underline{7}$
$\varepsilon_1(\underline{n})$	1	1	1	1
$\varepsilon_2(\underline{n})$	1	1	−1	−1
$\varepsilon_3(\underline{n})$	1	−1	−1	1
$\varepsilon_4(\underline{n})$	1	−1	1	−1

Beweis
Es ist $|G_8| = \varphi(8) = 2^3 - 2^2 = 4$, also existieren genau vier Charaktere. Weiter ist $\mathbb{Z}_8^\times = \langle \underline{3} \rangle \times \langle \underline{5} \rangle$. Die Charaktere sind also jeweils eindeutig durch die Werte von $\underline{3}$ und $\underline{5}$ bestimmt. Da $\underline{3} \cdot \underline{5} = \underline{7}$ gilt, ist leicht nachzurechnen, dass die angegebenen Abblidungen Charaktere auf $\mathbb{Z}_8^\times$ sind.

(iv) **Das Legendre-Symbol**

Für $p \in \mathbb{P} := \{n \in \mathbb{N} \mid n \text{ ist Primzahl}\}$ definiere

$$\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \mathbb{C},$$

$$\left(\frac{n}{p}\right) = \begin{cases} 0, & \text{falls } p \mid n \\ 1, & \text{falls } p \nmid n \text{ und } n \equiv_p x^2 \text{ für ein } x \in \mathbb{Z}\backslash\{0\} \\ -1, & \text{sonst.} \end{cases}$$

Dann ist $\left(\frac{\cdot}{p}\right)$ ein Dirichletscher Charakter $(\mathrm{mod}\, p^r)$ für jedes $r \in \mathbb{N}$ und heißt *Legendre-Symbol*.

Beweis
Es ist zu zeigen:

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \qquad \forall m, n \in \mathbb{Z}.$$

Für $m \equiv_p 0$ und $m \equiv_p 1$ ist die Aussage klar.

Sei also $p \neq 2$. Da $\mathbb{Z}_p$ ein Körper ist, ist $\mathbb{Z}_p^\times$ zyklisch. Es existiert demnach ein $a \in \mathbb{Z}$ mit $\langle a + p\mathbb{Z}\rangle = \mathbb{Z}_p^\times$.

Es gilt:

$$m \equiv_p x^2 \text{ für ein } x \in \mathbb{Z} \Leftrightarrow m \equiv_p a^r \text{ für ein } r \in \mathbb{N}_0 \text{ mit } 2|r.$$

Ist $m \equiv_p a^r$ mit $2|r$, dann wähle $x = a^{\frac{r}{2}}$.

Sei $m \equiv_p x^2$, dann ist $x + p\mathbb{Z} \in \mathbb{Z}_p^\times = \langle a + p\mathbb{Z}\rangle$, also ist $x \equiv_p a^k$ für ein $k \in \mathbb{N}_0$. Es folgt

$$m \equiv px^2 \equiv_p (a^k)^2 \equiv_p a^{2k}.$$

Für $n, m \in \mathbb{Z}$ mit $n \equiv_p a^r$ und $m \equiv_p a^k$ ist also

$$mn \equiv_p a^{k+r} \equiv_p a^{2q} \text{ für ein } q \in \mathbb{N} \Leftrightarrow k + r \equiv_2 0.$$

Somit ist mn eine Quadratzahl $\mathrm{mod}\, p$ genau dann wenn m und n Quadratzahlen $\mathrm{mod}\, p$ sind oder wenn m und n beide keine Quadratzahlen $\mathrm{mod}\, p$ sind, was äquivalent zu

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$$

ist. □

Für das Legendre-Symbol notieren wir die folgenden Eigenschaften:

(2.6) Lemma (Eigenschaften des Legendre-Symbols)
Seien $p, q \in \mathbb{P}, p \neq 2 \neq q$; dann gilt

(i) $\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right), & \text{falls } q \equiv_4 p \equiv_4 3 \\ \left(\frac{q}{p}\right), & \text{sonst,} \end{cases}$

(ii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,

(iii) $\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{falls } p \equiv_8 1 \text{ und } p \equiv_8 7 \\ -1, & \text{falls } p \equiv_8 3 \text{ und } p \equiv_8 5. \end{cases}$ ◇

Beweis

(i) Folgt aus dem Reziprozitätsgesetz.

(ii) 1. Ergänzungssatz.

(iii) 2. Ergänzungssatz. □

Wir wenden uns nun zwei Sätzen zu, die für Konvergenzuntersuchung von L-Reihen wichtig sind. Man benötigt dafür zunächst das

(2.7) Lemma

Sei G eine Gruppe und $a \in G$; dann ist die Abbildung $G \to G$, $g \mapsto ag$ bijektiv. ◇

Beweis

Die Umkehrabbildung ist $G \to G$, $g \mapsto a^{-1}g$. □

(2.8) Satz

Sei χ ein Dirichletscher Charakter $\bmod N$; dann gilt:

$$\sum_{\underline{n} \in (\mathbb{Z}_N)} \chi(n) = \begin{cases} \varphi(N), & \text{falls } \chi = \chi_0 \\ 0, & \text{sonst.} \end{cases}$$

◇

Beweis

(1) Sei $\chi = \chi_0$; dann ist

$$\begin{aligned} \sum_{\underline{n} \in (\mathbb{Z}_N)} \chi(n) &= \sum_{\underline{n} \in (\mathbb{Z}_N^\times)} \chi_0(n) \\ &= \sum_{\underline{n} \in (\mathbb{Z}_N^\times)} 1 = |\mathbb{Z}_N^\times| = \varphi(N). \end{aligned}$$

(2) Sei $\chi \neq \chi_0$, dann existiert ein $\underline{m} \in \mathbb{Z}_N^\times$ mit $\chi(m) \neq 1$. Es gilt

$$\begin{aligned} \underbrace{(1 - \chi(m))}_{\neq 0} \Big(\sum_{\underline{n} \in (\mathbb{Z}_N)} \chi(n) \Big) &= \sum_{\underline{n} \in (\mathbb{Z}_N^\times)} \chi(\underline{n}) - \sum_{\underline{n} \in (\mathbb{Z}_N^\times)} \chi(\underline{m}\,\underline{n}) \\ &\overset{(2.7)}{=} \sum_{\underline{n} \in (\mathbb{Z}_N^\times)} \chi(\underline{n}) - \sum_{\underline{n} \in (\mathbb{Z}_N^\times)} \chi(\underline{n}) \\ &= 0. \end{aligned}$$

Es folgt

$$\sum_{\underline{n}\in(\mathbb{Z}_N)} \chi(n) = 0.$$

□

(2.9) Korollar
Seien χ_1, χ_2 Dirichletsche Charaktere $(\mathrm{mod}\, N)$, dann ist:

$$\frac{1}{\varphi(N)} \sum_{\underline{n}\in(\mathbb{Z}_N)} \chi_1(n)\overline{\chi}_2(n) = \begin{cases} 1, & \text{falls } \chi_1 = \chi_2 \\ 0, & \text{sonst.} \end{cases}$$

◇

Beweis
Nach (2.5)(ii) ist $\overline{\chi}_2 = \chi_2^{-1}$. Demnach gilt

$$\chi_0 = \chi_1\overline{\chi}_2 = \chi_1\chi_2^{-1} \Leftrightarrow \chi_1 = \chi_2.$$

Damit folgt die Behauptung aus (2.8). □

(2.10) Satz
Für $n \in \mathbb{Z}$ gilt:

$$\sum_{\chi\in(G_N)} \chi(n) = \begin{cases} \varphi(N), & \text{falls } \underline{n} = \underline{1} \\ 0, & \text{sonst.} \end{cases}$$

◇

Beweis
(1) Sei $\underline{n} = 1$. Es ist $\chi(\underline{1}) = 1$ für jedes $\chi \in G_N$ und somit

$$\sum_{\chi\in(G_N)} \chi(n) = \sum_{\chi\in(G_N)} 1 = |G_N| \overset{(1.4)}{=} \varphi(N).$$

(2) Für $\mathrm{ggT}\,(n, N) \neq 1$ ist die Aussage klar.

(3) Sei also $N \geq 3$ und $\underline{n} \in \mathbb{Z}_N^\times \backslash \{1\}$; dann existiert ein $\chi_1 \in G_N$ mit $\chi_1 \neq \chi_0$ und $\chi(n) \neq 1$. Demnach gilt:

$$\begin{aligned} \underbrace{\big(1 - \chi_1(n)\big)}_{\neq 0}\Big(\sum_{\chi\in(G_N)} \chi(n)\Big) &= \sum_{\chi\in(G_N)} \chi(\underline{n}) - \sum_{\chi\in(G_N)} \chi_1(\underline{n})\chi(\underline{n}) \\ &\overset{(2.7)}{=} \sum_{\chi\in(G_N)} \chi(\underline{n}) - \sum_{\chi\in(G_N)} \chi(\underline{n}) \\ &= 0. \end{aligned}$$

Es folgt

$$\sum_{\chi\in(G_N)} \chi(n) = 0.$$

□

(2.11) Korollar
Seien $a, b \in \mathbb{Z}$; dann gilt

$$\frac{1}{\varphi(N)} \sum_{\chi \in (G_N)} \chi(a)\overline{\chi}(b) = \begin{cases} 1, & \text{falls } \underline{a} = \underline{b} \text{ und } \operatorname{ggT}(a, N) = 1 \\ 0, & \text{sonst.} \end{cases}$$

◇

Beweis
Für $\operatorname{ggT}(a, N) \neq 1$ ist die Aussage klar. Für $\underline{a}$,$\underline{b} \in \mathbb{Z}_N^\times$ gilt:

$$\chi(a)\overline{\chi}(b) = \chi(\underline{a})\chi^{-1}(\underline{b}) = \chi(\underline{a})\chi(\underline{b}^{-1}) = \chi(\underline{a}\,\underline{b}^{-1}).$$

Außerdem ist

$$\underline{a}\,\underline{b}^{-1} = 1 \Leftrightarrow \underline{a} = \underline{b}.$$

Die Behauptung folgt damit aus (2.10). □

§ 3 Primitive Charaktere

Nun kommen wir zu primitiven und insbesondere reellen primitiven Dirichletschen Charakteren, die beim Auffinden von Nullstellen der L-Reihen bedeutsam werden.

(3.1) Bemerkung
Sei $\widetilde{N} \in \mathbb{N}$ mit $\widetilde{N}|N$. Dann ist die Reduktion

$$R_{N,\widetilde{N}} : \mathbb{Z}_N^\times \to \mathbb{Z}_{\widetilde{N}}^\times, \qquad x + N\mathbb{Z} \mapsto x + \widetilde{N}\mathbb{Z}$$

ein surjektiver Gruppenhomomorphismus.
Insbesondere ist dann $\widetilde{\chi} \circ R_{N,\widetilde{N}}$ für $\widetilde{\chi} \in G_{\widetilde{N}}$ ein Dirichletscher Charakter $(\operatorname{mod} N)$. ◇

(3.2) Definition
Seien $\chi \in G_N$ und $\widetilde{\chi} \in G_{\widetilde{N}}$, so dass $N \neq \widetilde{N}$ mit $\widetilde{N}|N$ und

$$\chi = \widetilde{\chi} \circ R_{N,\widetilde{N}}. \qquad (*)$$

(i) χ heißt der von $\widetilde{\chi}$ *induzierte Charakter*.

(ii) χ heißt *imprimitiv*, falls χ eine solche Zerlegung $(*)$ besitzt und *primitiv* sonst.◇

Offensichtlich ist folgende

(3.3) Bemerkung
Für jedes $\chi \in G_N$ existiert eine kleinste Zahl $\widetilde{N}$ und ein $\widetilde{\chi} \in G_{\widetilde{N}}$, so dass $\chi = \widetilde{\chi} \circ R_{N,\widetilde{N}}$ und $\widetilde{\chi}$ primitiv ist. Die Zahl $\widetilde{N}$ heißt *Führer* von χ. Die Beziehung $\chi = \widetilde{\chi} \circ R_{N,\widetilde{N}}$ impliziert jedoch nicht die Gleichheit der Fortsetzungen von χ und auf $\widetilde{\chi}$ auf ganz $\mathbb{Z}$. ◇

Zur Veranschaulichung dienen die

(3.4) Beispiele

(i) Für $N \neq 1$ ist χ_0 nie primitiv, da $\chi_0 = \widetilde{\chi_0} \circ R_{N,1}$ mit $\widetilde{\chi_0} \equiv 1$. (Es gilt $\mathbb{Z}_1^\times = \{1\}$.)

(ii) Sei χ ein Dirichletscher Charakter (mod 12) bestimmt durch

n	1	2	3	4	5	6	7	8	9	10	11	12
$\chi(n)$	1	0	0	0	-1	0	1	0	0	0	-1	0

Auf $(\mathbb{Z}_{12}^\times)$ gilt $\chi = \sigma \circ R_{12,3}$ mit dem durch $\sigma(2+3\mathbb{Z}) = -1$ eindeutig bestimmten $\sigma \in G_3$, also wird χ von σ induziert. Offensichtlich ist σ primitiv und somit ist der Führer von χ gleich 3. Für die Fortsetzung auf $\mathbb{Z}$ gilt jedoch $\chi \neq \sigma$, da $0 = \chi(2) \neq \sigma(2) = -1$. ◇

Wichtig für das weitere Vorgehen ist folgender

(3.5) Satz (Chinesischer Restsatz)
Ist $N = m_1 \cdots m_n$ mit $m_j \in \mathbb{N}$ paarweise teilerfremd, dann ist

$$\begin{aligned} \pi = (\pi_1, \ldots, \pi_n) : (\mathbb{Z}_N) &\to (\mathbb{Z}_{m_1}) \times \cdots \times (\mathbb{Z}m_n) \\ \pi(x + N\mathbb{Z}) &= (\pi_1(x + N\mathbb{Z}), \ldots, \pi_n(x + N\mathbb{Z})) \\ &= (x + m_1\mathbb{Z}, \ldots, x + m_n\mathbb{Z}) \end{aligned}$$

ein Ringisomorphismus, wobei Addition und Multiplikation in $(\mathbb{Z}_{m_1}) \times \cdots \times (\mathbb{Z}_{m_n})$ komponentenweise definiert ist. Insbesondere ist π auf $\mathbb{Z}_N^\times$ ein Gruppenisomorphismus. ◇

Beweis
Bekannt aus der Algebra. □

Wie die folgende Bemerkung zeigt, lässt sich jeder Dirichletscher Charakter als Produkt von Dirichletschen Charakteren mod p^r beschränken, wobei p eine Primzahl und r eine natürliche Zahl ist.

(3.6) Bemerkung
Ist $\chi \in G_N$ und $N = m_1 \cdots m_n$ mit $m_j \in \mathbb{N}$ paarweise teilerfremd, so gilt

$$\chi(x) = \sigma_1(x) \cdots \sigma_n(x)$$

für gewisse $\sigma_j \in G_{m_j}$ und für alle $x \in \mathbb{Z}$. ◇

Beweis
Definiere für σ_j durch

$$\sigma_j : \mathbb{Z}_{m_j}^{\times} \to \mathbb{C}^{\times}$$
$$\sigma_j(y + m_j\mathbb{Z}) := \chi(\pi^{-1}(1, \ldots, 1, y + m_j\mathbb{Z}, 1 \ldots, 1)), \qquad \text{für alle } 1 \leq j \leq n,$$

wobei π der Isomorphismus aus (3.5) ist. Damit ist $\sigma_j \in G_{m_j}$ für alle $1 \leq j \leq n$. Für $\underline{x} \in \mathbb{Z}_N^{\times}$ gilt

$$\begin{aligned}
\chi(\underline{x}) &= \chi(\pi^{-1}(\pi(\underline{x}))) \\
&= \chi(\pi^{-1}(\pi_1(\underline{x}), \ldots, \pi_n(\underline{x}))) \\
&= \prod_{j=1}^{n} \chi(\pi^{-1}(1, \ldots, 1, \pi_j(\underline{x}), 1, \ldots, 1)) \\
&= \prod_{j=1}^{n} \sigma_j \circ \pi_j(\underline{x}),
\end{aligned}$$

also ist $\chi(x + N\mathbb{Z}) = \sigma_1(x + m_1\mathbb{Z}) \cdots \sigma_n(x + m_n\mathbb{Z})$ für alle $\underline{x} \in \mathbb{Z}_N^{\times}$. Aus der Äquivalenz

$$\text{ggT}\,(x, N) = 1 \Leftrightarrow \text{ggT}\,(x, m_j) = 1 \text{ für alle } 1 \leq j \leq n$$

folgt die Gleichheit $\chi(x) = \sigma_1(x) \cdots \sigma_n(x)$ für alle $x \in \mathbb{Z}$. □

Erleichterung bei der Untersuchung von primitiven Dirichletschen Charakteren verschafft das

(3.7) Lemma
Mit den Bezeichnungen aus (3.6) gilt:

$$\chi \text{ ist imprimitiv } \Leftrightarrow \sigma_j \text{ imprimitiv für mindestens ein } j.$$ ◇

Beweis
Es ist $\chi(x+N\mathbb{Z}) = \sigma_1(x+m_1\mathbb{Z})\cdots\sigma_n(x+m_n\mathbb{Z})$. Ist χ imprimitiv, so existiert ein $\widetilde{N} \in \mathbb{N}$ mit $\widetilde{N} = \widetilde{m}_1\cdots\widetilde{m}_n$ und $\widetilde{m}_j | m_j$ für alle $1 \leq j \leq n$, so dass $N \neq \widetilde{N}$ und $\chi = \widetilde{\chi}\circ R_{N,\widetilde{N}}$ für ein $\widetilde{\chi} \in G_{\widetilde{N}}$. Sei ohne Einschränkung $m_1 \neq \widetilde{m}_1$. Nach (3.6) ist

$$\widetilde{\chi}(y+\widetilde{N}\mathbb{Z}) = \prod_{j=1}^{n}\widetilde{\sigma}_j(y+\widetilde{m}_j\mathbb{Z}), \qquad \text{für alle } y+\widetilde{N}\mathbb{Z} \in \mathbb{Z}_{\widetilde{N}}^{\times},$$

für entsprechende $\widetilde{\sigma}_j \in G_{m_j}$. Sei nun

$$x+m_1\mathbb{Z} \in \mathbb{Z}_{m_1}^{\times} \text{ und } y+N\mathbb{Z} := \pi^{-1}(x+m_1\mathbb{Z},1,\ldots,1).$$

Wegen (3.5) gilt also

$$y \equiv_{m_j} \begin{cases} x, & \text{falls } j=1 \\ 1, & \text{sonst} \end{cases}$$

und daher

$$\begin{aligned}\sigma_1(x+m_1\mathbb{Z}) &= \chi(\pi^{-1}(x+m_1\mathbb{Z},1,\ldots,1)) = \chi(y+N\mathbb{Z}) \\ &= \widetilde{\chi}(y+\widetilde{N}\mathbb{Z}) = \prod_{j=1}^{n}\widetilde{\sigma}_j(y+\widetilde{m}_j\mathbb{Z}) \\ &= \widetilde{\sigma}_1(y+\widetilde{m}_1\mathbb{Z}) \\ &= \widetilde{\sigma}_1(x+\widetilde{m}_1\mathbb{Z}).\end{aligned}$$

Das bedeutet, dass σ_1 von $\widetilde{\sigma}_1$ induziert wird und somit imprimitiv ist.

Gilt hingegen $\sigma_j(x+m_j\mathbb{Z}) = \widetilde{\sigma}_j(x+\widetilde{m}_j\mathbb{Z})$ für alle $x+m_j\mathbb{Z} \in \mathbb{Z}_{m_j}^{\times}$ und für alle $1 \leq j \leq n$ mit $m_1 \neq \widetilde{m}_1$, dann definiere für $\widetilde{N} = \widetilde{m}_1\cdots\widetilde{m}_n$

$$\widetilde{\chi}(y+\widetilde{N}\mathbb{Z}) := \prod_{j=1}^{n}\widetilde{\sigma}_j(y+\widetilde{m}_j\mathbb{Z}).$$

Nach (3.6) ist $\widetilde{\chi} \in G_{\widetilde{N}}$ und es folgt

$$\chi(x+N\mathbb{Z}) = \prod_{j=1}^{n}\sigma_j(x+m_j\mathbb{Z}) = \prod_{j=1}^{n}\widetilde{\sigma}_j(x+\widetilde{m}_j\mathbb{Z}) = \widetilde{\chi}(x+\widetilde{N}\mathbb{Z})$$

aus der Wohldefiniertheit von $\widetilde{\chi}$. Daher wird χ von $\widetilde{\chi}$ induziert und ist somit imprimitiv, da $\widetilde{N} \neq N$ wegen $\widetilde{m}_1 \neq m_1$ gilt. □

Zur Bestimmung der Anzahl der primitiven Dirichletschen Charaktere auf einer Gruppe notieren wir das

(3.8) Lemma
Sei $N = p_1^{r_1} \cdots p_n^{r_n}$ die Primfaktorzerlegung von N, dann ist die Anzahl der primitiven Dirichletschen Charaktere auf $\mathbb{Z}_N^\times$ gegeben durch

$$\prod_{j=1}^{n} \Big(\varphi(p_j^{r_j}) - \varphi(p_j^{r_j-1}) \Big).$$

◇

Beweis
Sei zunächst $n = 1$. Ein Homomorphismus $\chi \in G_{p^r}$ ist genau dann imprimitiv, wenn ein $\sigma \in G_{p^{r-1}}$ existiert mit $\chi = \sigma \circ R_{p^r,p^{r-1}}$. Außerdem folgt aus $\sigma_1, \sigma_2 \in G_{p^{r-1}}$ mit $\sigma_1 \neq \sigma_2$, dass $\sigma_1 \circ R_{p^r,p^{r-1}} \neq \sigma_2 \circ R_{p^r,p^{r-1}}$ gilt und daher existieren genau

$$|G_{p^r}| - |G_{p^{r-1}}| = \varphi(p^r) - \varphi(p^{r-1})$$

primitive Dirichletsche Charaktere. Für $n > 1$ folgt die Behauptung mit (3.7), da demnach χ genau dann primitiv ist wenn alle σ_j dies sind, wobei σ_j definiert ist wie in (3.6) mit $m_j = p_j^{r_j}$. □

Zur Bestimmung der Periodenmenge eines Dirichletschen Charakters dient das

(3.9) Lemma
Sei $\chi \in G_M$ und $M = p_1^{r_1} \cdots p_n^{r_n}$ die Primfaktorzerlegung von M mit $r_j \in \mathbb{N}$. Weiter sei N der Führer von χ mit $N = p_1^{k_1} \cdots p_n^{k_n}$, dann ist die Periodenmenge P_χ von χ auf $\mathbb{Z}$ gegeben durch

$$P_\chi = r\mathbb{Z}, \text{ wobei } r = \prod_{j=1}^{n} p_j^{\max\{1,k_j\}}.$$

◇

Beweis
Sei d die minimale Periode. Da P_χ eine Untergruppe von $(\mathbb{Z}, +)$ sein muss, gilt daher $P_\chi = d\mathbb{Z}$. Es ist also die Gleichheit von d und r zu zeigen. Sei χ zunächst primitiv, also $M = N$. Angenommen es gilt $d < N = r$. Wegen $N \in P_\chi = d\mathbb{Z}$ wird N von d geteilt. Definiere $\sigma(x + d\mathbb{Z}) := \chi(x + N\mathbb{Z})$ für $x + d\mathbb{Z} \in \mathbb{Z}_d^\times$. Da d eine Periode von χ ist, ist σ wohldefiniert, also ein Dirichletscher Charakter $(\mathrm{mod}\, d)$ und es gilt $\chi = \sigma \circ R_{N,d}$, was ein Widerspruch zur Primitivität von χ ist. Es folgt $d = N = r$.

Sei nun $M > N$, das heißt $\chi = \sigma \circ R_{M,N}$ auf $\mathbb{Z}_M^\times$ für ein passendes $\sigma \in G_N$. Nach dem ersten Fall ist N minimale Periode von χ auf $\mathbb{Z}_M^\times$ und daher wird d von N geteilt. Angenommen, es gibt ein $j \in \{1, \ldots, n\}$, so dass p_j nicht d teilt. Es ist

$$p_j + d + N\mathbb{Z} = p_j + N\mathbb{Z} \in \mathbb{Z}_N^\times.$$

Man erhält dann einen Widerspruch durch

$$0 \neq \sigma(p_j + d + N\mathbb{Z}) = \chi(p_j + d + M\mathbb{Z})\chi(p_j + d) = \chi(p_j) = 0.$$

Es folgt $d \geq r$. Weiter ist

$$\underline{x} \in \mathbb{Z}_M^\times \Leftrightarrow \underline{x} + \underline{r} \in \mathbb{Z}_M^\times,$$

da gilt

$$\begin{aligned} \operatorname{ggT}(x, M) = 1 &\Leftrightarrow x + p_k + \mathbb{Z} = x + r + p_k + \mathbb{Z} \neq 0 \text{ für alle } 1 \leq k \leq n \\ &\Leftrightarrow \operatorname{ggT}(x + r, M) = 1. \end{aligned}$$

Für $\underline{x} \in \mathbb{Z}_M^\times$ ist demnach

$$\chi(x + r) = \sigma(x + r + N\mathbb{Z}) = \sigma(x + N\mathbb{Z}) = \chi(x)$$

und für $\underline{y} \notin \mathbb{Z}_M^\times$ ist

$$\chi(y) = 0 = \chi(y + r).$$

Demnach ist $r \in P_\chi$, also $r \leq d$ und damit $r = d$. □

§ 4 Primitive reelle Charaktere

Interessant sind die primitiven reellen Dirichletschen Charaktere. Eine zentrale Rolle in diesem Paragraphen spielen die sogenannten Grundzahlen:

(4.1) Definition
Sei D eine ganze Zahl, welche eine der beiden Eigenschaften erfüllt:

(i) $D \equiv_4 1$ und D quadratfrei oder

(ii) $D \equiv_4 0$ und $\frac{D}{4}$ quadratfrei, sowie $\frac{D}{4} \equiv_4 2$ oder $\frac{D}{4} \equiv_4 3$.

Die Zahl D heißt *Grundzahl* oder *Fundamentaldiskriminante*. ◇

(4.2) Definition
Sei D eine Grundzahl, dann definiere

$$\chi_D : \mathbb{Z} \to \mathbb{C} \quad \text{durch}$$

(i) $\chi_D(p) = \left(\frac{D}{p}\right)$, für alle $2 \neq p \in \mathbb{P}$

(ii) $\chi_D(2) = \begin{cases} 0, & \text{falls } D \equiv_4 0 \\ 1, & \text{falls } D \equiv_8 1 \\ -1, & \text{falls } D \equiv_8 5 \end{cases}$

(iii) $\chi_D(-1) = \begin{cases} 1, & \text{falls } D > 0 \\ -1 & \text{falls } D < 0 \end{cases}$

(iv) $\chi_D(mn) = \chi_D(m)\chi_D(n)$; für alle $m, n \in \mathbb{Z}$

(v) $\chi_D(0) = 0$, ◇

wobei $\left(\frac{D}{p}\right)$ das Legendre-Symbol bezeichne.

Wir wollen zeigen, dass jede dieser Abbildungen die Fortsetzung eines primitiven Dirichletschen Charakter ist, und dass umgekehrt jede Fortsetzung eines primitiven Dirichletschen Charakters eine solche Abbildung ist. Zur Vorbereitung dient das

(4.3) Lemma

(i) Für $r > 1$, $p \in \mathbb{P}$ ist die Abbildung ψ definiert durch

$$\psi : \mathbb{Z}_{p^r}^\times \to \mathbb{Z}_{p^r}^\times, \qquad g \mapsto g^p$$

ein Gruppenhomomorphismus mit

$$\operatorname{Kern} \psi = \{ap^{r-1} + 1 + p^r\mathbb{Z}; 0 \leq a < p\}.$$

(ii) $\mathbb{Z}_{p^r}^\times$ ist zyklisch für $2 \neq p \in \mathbb{P}$, $r \in \mathbb{N}$.

(iii) Für $n \in \mathbb{Z}$, $r \geq 3$ gilt $n \equiv_{2^r} x^2$ für ein $x \in \mathbb{Z} \Leftrightarrow n \equiv_8 1$.

(iv) $\mathbb{Z}_{2^r}^\times = \langle \underline{3} \rangle \times \langle -\underline{1} \rangle$, für $r \geq 3$ ◇

Beweis

(i) Die Homomorphieeigenschaften und die Beziehung

$$\operatorname{Kern}\psi \supseteq \{ap^{r-1}+1+p^r\mathbb{Z}; a \in \mathbb{Z}\}$$

sind klar. Man zeigt
$\operatorname{Kern}\psi \subseteq \{ap^{r-1}+1+p^r\mathbb{Z}; a \in \mathbb{Z}\}$ durch vollständige Induktion:

Sei $r = 2$ und $x + p^2\mathbb{Z} \in \operatorname{Kern}\psi$ mit $x = mp + y$, wobei $0 \leq y < p$ gilt. Es ist zu zeigen, dass $y = 1$ ist. Es gilt:

$$x^p \equiv_{p^2} \sum_{j=0}^{p} \binom{p}{j} m^j p^j y^{p-j} \equiv_{p^2} y^p.$$

Da $x \in \operatorname{Kern}\psi$ gilt, wird $y^p - 1$ von p^2 geteilt und somit ist auch

$$\begin{aligned} &0 \equiv_p (y^p - 1) \equiv_p (y-1)^p \\ &\Rightarrow p|(y-1) \\ &\Rightarrow y = 1. \end{aligned}$$

Sei nun $r \geq 3$ und $x + p^r\mathbb{Z} = mp^{r-1} + y + p^r\mathbb{Z} \in \operatorname{Kern}\psi$ mit $x = mp^{r-1} + y$ und $0 \leq y < p^{r-1}$. Da der Ausdruck $\binom{p}{j} m^j p^{j(r-1)}$ für $j \geq 1$ von p^r geteilt wird, gilt

$$\begin{aligned} &(mp^{r-1}+y)^p \equiv_{p^r} \sum_{j=0}^{p} \binom{p}{j} m^j p^{j(r-1)} y^{p-j} \equiv_{p^r} y^p \\ &\Rightarrow p^r|(y^p-1) \\ &\Rightarrow p^{r-1}|(y^p-1), \end{aligned}$$

also ist $y + p^{r-1}\mathbb{Z} \in \operatorname{Kern}\psi^*$, wobei ψ^* der Homomorphismus

$$\psi^* : \mathbb{Z}^\times_{p^{r-1}} \to \mathbb{Z}^\times_{p^{r-1}}, \qquad g \mapsto g^p$$

ist. Nach Induktionsvoraussetzung ist $y \equiv_{p^{r-1}} ap^{r-2} + 1$, also $y = bp^{r-2} + 1$ für gewisse $a, b \in \mathbb{Z}$ und somit gilt:

$$x^p \equiv_{p^r} (bp^{r-2}+1)^p \equiv_{p^r} \sum_{j=0}^{p} \binom{p}{j} b^j p^{j(r-2)} \equiv_{p^r} bp^{r-1} + 1,$$

da p^r die Ausdrücke $p^{j(r-2)}$ für $j \geq 3$ und $\binom{p}{2} p^{2(r-2)}$ teilt. Daher ist

$$x + p^r\mathbb{Z} \in \{ap^{r-1} + 1 + p^r\mathbb{Z}; 0 \leq a < p\}.$$

(ii) Die Behauptung folgt mit Induktion nach r:

Für $r = 1$ ist $\mathbb{Z}_{p^r}$ ist ein Körper und damit $\mathbb{Z}_{p^r}^\times$ zyklisch.

Sei $r \geq 1$: Definiere

$$\pi : \mathbb{Z}_{p^r}^\times \to \mathbb{Z}_{p^{r-1}}^\times, \qquad x + p^r\mathbb{Z} \mapsto x + p^{r-1}\mathbb{Z}.$$

Dann ist π ein ist surjektiver Gruppenhomomorphismus mit Kern $\pi = \text{Kern}\,\psi$, wobei ψ der Homomorphismus aus (i) ist. Nach dem Homomorphiesatz gilt

$$\text{Bild}\,\psi \cong \mathbb{Z}_{p^r}^\times/\text{Kern}\,\psi = \mathbb{Z}_{p^r}^\times/\text{Kern}\,\pi \cong \text{Bild}\,\pi = \mathbb{Z}_{p^{r-1}}^\times.$$

Demnach ist $\text{Bild}\,\psi \cong \mathbb{Z}_{p^{r-1}}^\times$ vermöge eines Isomorphismus ϕ. Nach Induktionsvoraussetzung ist $\mathbb{Z}_{p^{r-1}}^\times = \langle g \rangle$ für ein $g \in \mathbb{Z}_{p^{r-1}}^\times$ und es gilt $\phi^{-1}(g) = \psi(x) = x^p$ für ein $x \in \mathbb{Z}_{p^r}^\times$. Somit ist $\text{ord}\,x^p = \text{ord}\,g = p^{r-2}(p-1)$ und es folgt

$$\text{ord}\,x = p \cdot p^{r-2}(p-1) = |\mathbb{Z}_{p^r}^\times|,$$

das heißt $\langle x \rangle = \mathbb{Z}_{p^r}^\times$.

(iii) Sei $n \equiv_{2^r} x^2$ für ein $x \in \mathbb{Z}$ und $r \geq 3$. Es existiert ein $a \in \{1, 3, -1, -3\}$ mit $x \equiv_8 a$ und somit gilt $n \equiv_8 x^2 \equiv_8 a^2 \equiv_8 1$.

Die Rückrichtung zeigt man mit Induktion nach r:

Sei $r > 3$ und $n \equiv_8 1$. Nach Induktionsvoraussetzung existieren u, $x \in \mathbb{Z}$ mit $x^2 = n + u2^{r-1}$. Für $y := x + u2^{r-2}$ ist

$$y^2 = x^2 + xu2^{r-1} + u^2 2^{2r-4} = n + u2^{r-1}(1 + x) + u^2 2^{2r-4}.$$

Da x wegen $x^2 \equiv_8 n \equiv_8 1$ ungerade ist, wird $(x + 1)$ von 2 und 2^{2r-4} von 2^r geteilt, also ist $y^2 \equiv_{2^r} n$.

(iv) Für $r = 3$ folgt die Behauptung durch leichtes Nachrechnen.

Für $r > 3$ sei $U := \{\underline{x}_1^2, \ldots, \underline{x}_n^2; \quad \underline{x}_j \in \mathbb{Z}_{2^r}^\times\}$ die Menge der Quadratzahlen in $\mathbb{Z}_{2^r}^\times$ und $x_1 \equiv_8 a$ mit $a \in \{1, 3, -1, -3\}$. Es folgt

$$ax_1 \equiv_8 a^2 \equiv_8 1$$

und damit nach (iii)

$$\underline{a}\,\underline{x}_1 = \underline{x}_j^2 \qquad \text{für ein } 1 \leq j \leq n.$$

Ist $j = 1$, so folgt $\underline{x}_1 = \underline{a}$. Andernfalls ist

$$\underline{x}_1 = \underline{a}^{-1}\underline{x}_j^2.$$

Es gilt also $\underline{x}_1 \in \langle -\underline{1}, \underline{3}, \underline{x}_2^2, \ldots, \underline{x}_n^2 \rangle$. Analoges Vorgehen für $j = 2, \ldots, n$ liefert

$$\mathbb{Z}_{2^r}^\times = \langle -\underline{1}, \underline{3} \rangle.$$

Weiter ist $3^k \equiv_8 1$ oder $3^k \equiv_8 3$ für $k \in \mathbb{N}$ und somit $-\underline{1} \notin \langle \underline{3} \rangle$ (da $r > 3$). Also $\langle \underline{3} \rangle \cap \langle -\underline{1} \rangle = \{1\}$ und damit $\mathbb{Z}_{2^r}^\times = \langle \underline{3} \rangle \times \langle -\underline{1} \rangle$. □

Nun können wir folgende Aussage beweisen:

(4.4) Satz
Ist D eine Grundzahl, dann definiert χ_D wie in (4.2) einen primitiven Dirichletschen Charakter $(\mathrm{mod}|D|)$. Außerdem ist jeder primitive reelle Dirichletsche Charakter einer der Charaktere χ_D. ◇

Beweis
Betrachte zunächst Charaktere modulo N mit $N = p^r$ für $p \in \mathbb{P}$, $r \in \mathbb{N}$.

Behauptung 1: Für $2 \neq p$ gilt:

$$\chi \text{ ist ein primitiver reeller Dirichletscher Charakter } (\mathrm{mod}\, p^r) \Leftrightarrow r = 1 \text{ und } \chi = \left(\frac{\cdot}{p}\right).$$

Beweis: Nach (4.3)(ii) gilt $\mathbb{Z}_{p^r}^\times = \langle g \rangle$ für ein $g \in \mathbb{Z}_{p^r}^\times$. Ist $\chi \neq \chi_0$ reell, dann gilt $\chi(g) = -1$, also existiert höchstens ein primitiver reeller Dirichletscher Charakter. Die Abbildung

$$\mathbb{Z} \to \mathbb{Z}, \qquad n \mapsto \left(\frac{n}{p}\right)$$

ist ein reeller Dirichletscher Charakter $(\mathrm{mod}\, p^r)$ und offensichtlich nur für $r = 1$ primitiv (vgl. (2.5)(iv)).

Behauptung 2: Es existieren genau drei primitive reelle Dirichletsche Charaktere in

$$\bigcup_{r \in \mathbb{N}} G_{2^r}.$$

Beweis: Sei also $p = 2$ und

(1) $r = 1$: Es gilt $\mathbb{Z}_2^\times = \{1\} \Rightarrow \chi_0$ ist einziger Charakter und nicht primitiv.

(2) $r = 2$: Es ist $\mathbb{Z}_4^\times = \langle 3 + 4\mathbb{Z} \rangle$ und somit

$$\alpha_1 : \mathbb{Z}_4^\times \to \mathbb{C}^\times, \qquad 3 + 4\mathbb{Z} \mapsto -1$$

der einzige von χ_0 verschiedene Charakter. Er ist offensichtlich reell und primitiv.

(3) $r = 3$: Nach (2.5)(iii) sind alle Charaktere auf G_8 reell, wobei die Identität ε_1, sowie ε_4 nicht primitiv sind, da $\varepsilon_4 = \alpha_1 \circ R_4$ gilt. Weiter sind ε_2 und ε_3 primitiv, da sonst $\varepsilon_j(\underline{3}) = \varepsilon_j(\underline{7})$ gelten müsste, wegen $\underline{3} \equiv_4 \underline{7}$.

(4) Sei schließlich $r > 3$: Nach (4.3)(iv) gilt $\mathbb{Z}_{2^r}^\times = \langle \underline{3} \rangle \times \langle -\underline{1} \rangle$. Damit ist ein Dirichletscher Charakter $(\mathrm{mod} 2^r)$ eindeutig durch die Werte von $\underline{3}$ und $-\underline{1}$ bestimmt. Da es für diese Werte im primitiven reellen Fall genau zwei Möglichkeiten für jedes Erzeugerelement gibt, existieren genau vier reelle Dirichletsche Charaktere $(\mathrm{mod} 2^r)$.

Für $j = 1, \ldots, 4$ sind $\varepsilon_j \circ R_8$ paarweise verschiedene Charaktere auf $\mathbb{Z}_{2^r}^\times$. Damit gilt für $\chi \in G_{2^r}$ reell, dass $\chi = \varepsilon_j \circ R_{N,8}$ für ein j, also ist χ nicht primitiv.

Es folgt *Behauptung 2* mit den Charakteren α_1, ε_2, ε_3.

Behauptung 3: Zu jedem primitiven Dirichletschen Charakter $\chi \,(\mathrm{mod}\, p^r)$ existiert eine Grundzahl D mit $\chi_D = \chi$, welche in folgender Weise bestimmt wird:

(i) Es ist $\left(\frac{\cdot}{p}\right) = \chi_D$ mit $D = (-1)^{\frac{p-1}{2}} p$, für $p \neq 2$,

(ii) $\alpha_1 = \chi_{-4}$,

(iii) $\varepsilon_2 = \chi_{-8}$,

(iv) $\varepsilon_3 = \chi_8$.

Beweis:

(i) Sei zunächst $p \neq 2$ eine Primzahl mit $p \equiv_4 1$; dann gilt

$$(-1)^{\frac{p-1}{2}} p = p$$

und es ist die Gleichheit

$$\left(\frac{x}{p}\right) = \chi_p(x), \qquad \text{für alle } x \in \mathbb{Z}$$

zu zeigen. Ist $x \notin \{2, p\}$ eine Primzahl; dann gilt

$$\left(\frac{x}{p}\right) \overset{(2.6)(i)}{=} \left(\frac{p}{x}\right) = \chi_p(x).$$

Weiter ist $p \equiv_8 1$ oder $p \equiv_8 5$ und daher

$$\begin{aligned}\chi_p(2) &= \begin{cases} 1, & \text{falls } p \equiv_8 1 \\ -1, & \text{falls } p \equiv_8 5 \end{cases} \\ &\overset{(2.6)(iii)}{=} \left(\frac{2}{p}\right)\end{aligned}$$

und außerdem

$$\chi_p(-1) = 1 = (-1)^{\frac{p-1}{2}} \overset{(2.6)(ii)}{=} \left(\frac{-1}{p}\right).$$

Für $x \in \{0, p\}$ gilt

$$\chi_p(x) = 0 = \left(\frac{x}{p}\right).$$

Aus der strengen Multiplikativität beider Abblidungen folgt nun

$$\left(\frac{x}{p}\right) = \chi_p(x), \qquad \text{für alle } x \in \mathbb{Z}.$$

Sei nun $p \equiv_4 3$, also ist

$$(-1)^{\frac{p-1}{2}} p = -p$$

und es ist die Gleichheit

$$\chi_{-p}(x) = \left(\frac{x}{p}\right), \qquad \text{für alle } x \in \mathbb{Z}$$

zu zeigen. Ist $p \neq x$ eine Primzahl mit $x \equiv_4 3$, dann gilt

$$\begin{aligned}\chi_{-p}(x) &= \left(\frac{-p}{x}\right) \\ &= \left(\frac{-1}{x}\right)\left(\frac{p}{x}\right) \\ &= (-1)^{\frac{p-1}{2}}(-1)\left(\frac{x}{p}\right) \\ &= \left(\frac{x}{p}\right).\end{aligned}$$

Ist $p \neq x$ eine Primzahl mit $x \equiv_4 1$, so folgt

$$\begin{aligned}\chi_{-p}(x) &= \left(\frac{-p}{x}\right)\\ &= \left(\frac{-1}{x}\right)\left(\frac{p}{x}\right)\\ &= (-1)^{\frac{p-1}{2}}\left(\frac{x}{p}\right)\\ &= \left(\frac{x}{p}\right).\end{aligned}$$

Weiter ist $-p \equiv_8 1$ oder $p \equiv_8 5$ und daher

$$\begin{aligned}\chi_{-p}(2) &= \begin{cases}1, & \text{falls } -p \equiv_8 1\\ -1, & \text{falls } -p \equiv_8 5\end{cases}\\ &\overset{(2.6)(iii)}{=} \left(\frac{2}{p}\right)\end{aligned}$$

und außerdem

$$\chi_p(-1) = -1 = (-1)^{\frac{p-1}{2}} \overset{(2.6)(ii)}{=} \left(\frac{-1}{p}\right).$$

Für $x \in \{0, p\}$ gilt

$$\chi_p(x) = 0 = \left(\frac{x}{p}\right)$$

Aus der strengen Multiplikativität beider Abblidungen folgt nun

$$\left(\frac{x}{p}\right) = \chi_{-p}(x), \qquad \text{für alle } x \in \mathbb{Z}.$$

(ii) Es gilt $\chi = \alpha_1$. Sei $2 \neq x$ eine Primzahl; dann ist

$$\begin{aligned}\chi_{-4}(x) &= \left(\frac{-4}{x}\right)\\ &= \left(\frac{-1}{x}\right)\left(\frac{2}{x}\right)^2\\ &\overset{(2.6)(ii)}{=} (-1)^{\frac{p-1}{2}}\\ &= \begin{cases}1, & \text{falls } x \equiv_4 1\\ -1, & \text{falls } x \equiv_4 3\end{cases}\\ &= \alpha_1(x),\end{aligned}$$

sowie

$$\chi_{-4}(2) = 0 = \alpha_1(2)$$

und

$$\chi_{-4}(-1) = -1 = \alpha_1(-1).$$

Also ist wieder mit der strengen Multiplikativität der beiden Abbildungen $\chi_{-4} = \alpha_1$.

(iii) Es gilt $\varepsilon_2 = \chi_{-8}$. Sei $2 \neq x$ eine Primzahl; dann ist

$$\begin{aligned}
\chi_{-8}(x) &= \left(\frac{-8}{x}\right) \\
&= \left(\frac{-1}{x}\right)\left(\frac{2}{x}\right)^3 \\
&= (-1)^{\frac{p-1}{2}}\left(\frac{2}{x}\right) \\
&= \begin{cases} 1, & \text{falls } x \equiv_8 1 \text{ oder } x \equiv_8 3 \\ -1, & \text{falls } x \equiv_8 5 \text{ oder } x \equiv_8 7 \end{cases} \\
&= \varepsilon_2(x).
\end{aligned}$$

Außerdem gilt

$$\chi_{-8}(2) = 0 = \varepsilon_2(2)$$

und

$$\chi_{-8}(-1) = -1 = \varepsilon_2(7) = \varepsilon_2(-1).$$

Also ist wieder mit der strengen Multiplikativität der beiden Abbildungen $\chi_{-8} = \varepsilon_2$.

(iv) Man zeigt $\chi_8 = \varepsilon_3$ analog.

Behauptung 4: Sind D_1, D_2 teilerfremde Grundzahlen; dann gilt

(i) $D_1 \cdot D_2$ ist wieder eine Grundzahl,

(ii) $\chi_{D_1 \cdot D_2} = \chi_{D_1}\chi_{D_2}$.

Beweis

(i) Ist $D_1 \equiv_4 0$, so folgt $D_1 \cdot D_2 \equiv_4 = 0$ und $D_2 \equiv_4 1$, da $\mathrm{ggT}(D_1, D_2) = 1$ gilt. Weiter sind $\frac{D_1}{4}$ und D_2 quadratfrei und damit auch $\frac{D_1 \cdot D_2}{4}$, da D_1 und D_2 teilerfremd sind. Außerdem folgt aus $D_2 \equiv_4 1$, dass $\frac{D_1 \cdot D_2}{4} \equiv_4 \frac{D_1}{4}$ gilt und damit ist $D_1 \cdot D_2$ eine Grundzahl.

Ist $D_1 \equiv_4 D_2 \equiv_4 1$, so gilt ebenfalls $D_1 \cdot D_2 \equiv_4 1$ und $D_1 \cdot D_2$ ist quadratfrei , da $\mathrm{ggT}(D_1, D_2) = 1$; also ist $D_1 \cdot D_2$ eine Grundzahl.

(ii) Ist $2 \neq x$ eine Primzahl, so gilt wegen der strengen Multiplikativität des Legendre-Symbols

$$\chi_{D_1 \cdot D_2}(x) = \left(\frac{D_1 \cdot D_2}{x}\right) = \left(\frac{D_1}{x}\right)\left(\frac{D_2}{x}\right) = \chi_{D_1}\chi_{D_2}.$$

Sei nun $x = 2$ und $D_1, D_2 \neq 0 (\mathrm{mod} 4)$. Dann ist

$$D_1 D_2 \equiv_8 1 \Leftrightarrow D_1 \equiv_8 D_2$$

und damit

$$\chi_{D_1 \cdot D_2}(2) = 1 = \chi_{D_1}(2)\chi_{D_2}(2).$$

Außerdem gilt

$$D_1 D_2 \equiv_8 5 \Leftrightarrow D_1 \equiv_8 1 \text{ und } D_2 \equiv_8 5$$

und damit

$$\chi_{D_1 \cdot D_2}(2) = -1 = \chi_{D_1}(2)\chi_{D_2}(2).$$

Weiter gilt

$$D_1 D_2 > 0 \Leftrightarrow \operatorname{sgn} D_1 = \operatorname{sgn} D_1 \Leftrightarrow \chi_{D_1 \cdot D_2}(-1) = 1 \Leftrightarrow \chi_{D_1}(-1)\chi_{D_2}(-1) = 1.$$

Aus der strengen Multiplikativität folgt dann die Gleichheit.

Behauptung 5: Sei nun N beliebig. Ist χ ein primitiver reeller Dirichletscher Charakter $(\mathrm{mod}\, N)$, dann existiert eine Grundzahl D mit $\chi_D = \chi$.

Beweis Ist $N = 1$, dann ist χ_0 einziger Charakter und insbesondere reell und primitv. Außerdem gilt offensichtlich $\chi_0 = \chi_1$ und 1 ist eine Grundzahl.

Sei $N = p_1^{r_1} \cdots p_n^{r_n}$ die Primfaktorzerlegung von N und χ ein primitiver reeller Dirichletscher Charakter $(\mathrm{mod}\, N)$. Nach (3.6) existieren $\sigma_j \in G_{p_j^{r_j}}$ für $1 \leq j \leq n$, so dass $\chi(x) = \sigma_1(x) \cdots \sigma_n(x)$ für alle $x \in \mathbb{Z}$. Nach (3.7) sind alle σ_j primitiv und nach *Behauptung 3* existiert zu jedem j eine Grundzahl D_j mit $\sigma_j = \chi_{D_j}$, wobei die D_j zudem paarweise teilerfremd sind. Nach *Behauptung 4* ist dann

$$\chi = \chi_{D_1} \cdots \chi_{D_n} = \chi_{D_1 \cdots D_n},$$

wobei $D_1 \cdots D_n$ eine Grundzahl ist.

Behauptung 6:

Ist D eine Grundzahl, dann ist $D = a_1 \cdots a_n$ mit a_j paarweise teilerfremd und

$$a_j \in \{1, -4, -8, 8, (-1)^{\frac{p-1}{2}} p, \quad 2 \neq p \in \mathbb{P}\}.$$

Beweis:

(1) Ist $D \equiv_4 1$, so folgt, da D quadratfrei ist:

$$D = \pm \prod_{\substack{p \in \mathbb{P} \\ p|D}} p.$$

Wegen $D \equiv_4 1$ ist, teilt 2 nicht D und es folgt für $D < 0$, dass

$$m := |\{p \in \mathbb{P}; p \text{ teilt } D, p \equiv_4 -1\}|$$

ungerade ist. Weiter gilt

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{falls } p \equiv_4 1 \\ -1, & \text{falls } p \equiv_4 -1. \end{cases}$$

Damit ist

$$\begin{aligned} \prod_{p|D} (-1)^{\frac{p-1}{2}} p &= \prod_{\substack{p|D \\ p \equiv_4 -1}} (-1)^{\frac{p-1}{2}} \prod_{p|D} p \\ &= (-1)^m \prod_{p|D} p \\ &= -\prod_{p|D} p \\ &= D, \end{aligned}$$

also ist D darstellbar als Produkt solcher a_j. Analoge Überlegungen führen zu dieser Darstellung für $D > 0$.

(2) Ist $D \equiv_4 0$, dann gilt $D = \pm 8m$ bzw. $D = -4m$ mit m quadratfrei und $m \equiv_4 1$, also ist m eine Grundzahl und die Behauptung folgt mit (i).

Ist also D eine Grundzahl mit $D = a_1 \cdots a_n$, so gilt nach *Behauptung 4*, dass

$$\chi_D = \chi_{a_1} \cdots \chi_{a_n}$$

ist und somit ist χ_D streng multiplikativ. Nach *Behauptung 1* und *Behauptung 2* sind die χ_{a_j} primitive Dirichletsche Charaktere (mod $|a_j|$) und nach (3.7) mit $\chi_{a_j} = \sigma_j$ ist χ_D ein primitiver Dirichletscher Charakter (mod $|D|$).

Damit ist dieser Satz bewiesen. □