3. Zahlentheoretische Funktionen.

Sei Φ die Menge der Abbildungen $\mathbb{N} \to \mathbb{C}$, derartige Abbildungen nennt man *zahlentheoretische Funktionen.*

Zahlentheoretische Funktionen, an denen wir interessiert sind:

$$\begin{array}{llll} I(n) = 0 & \text{für} & n > 1 \quad \text{und} & I(1) = 1 \\ U(n) = 1 & \text{für} & n \geq 1 & \\ E(n) = n & \text{für} & n \geq 1 & \end{array}$$

$$\begin{aligned} \tau(n) &= (\text{Anzahl der Teiler von } n) \\ \sigma(n) &= (\text{Summe der Teiler von } n) \end{aligned}$$

Ganz wichtig ist die Eulersche ϕ-Funktion, die in 2.3 eingeführt wurde, aber auch die Möbius-Funktion μ, siehe 3.5.

3.1. Die Faltung.

Wir definieren auf Φ ein Produkt $*$ (*Dirichlet-Produkt, Faltung*) auf folgende Weise: Seien $f, g \in \Phi$. Setze

$$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = \sum_{d_1 d_2 = n} f(d_1)g(d_2)$$

(dabei bedeutet die letzte Summenbildung, dass über alle Paare $(d_1, d_2) \in \mathbb{N}^2$ summiert werden soll, für die $d_1 d_2 = n$ gilt). Beispielsweise gilt:

$$\boxed{\tau = U * U, \quad \sigma = E * U.}$$

3.1.1. *Die Menge Φ ist bezüglich $*$ eine kommutative Halbgruppe mit neutralem Element I.*

Beweis: Übungsaufgabe! Zum Assoziativgesetz sollte man anmerken: Seien f, g, h zahlentheoretische Funktionen. Dann ist $(f * g * h)(n) = \sum_{d_1,d_2,d_3} f(d_1)g(d_2)h(d_3)$, wobei man über alle Tripel (d_1, d_2, d_3) mit $d_1 d_2 d_3 = n$ summiert.

Zusatz (Übungsaufgabe): Nehmen wir zusätzlich noch auf Φ die punktweise Addition als Addition, so erhalten wir einen kommutativen Ring.

3.1.2. *Eine Funktion $f \in \Phi$ ist genau dann bezüglich $*$ invertierbar, wenn $f(1) \neq 0$ gilt.*

Beweis: Sei $f * g = I$. Dann ist $1 = I(1) = f(1)g(1)$, da $n = 1$ nur den einzigen Teiler $d = 1$ hat. Aus $f(1)g(1) = 1$ folgt, dass $f(1)$ nicht Null sein kann. Umgekehrt

sei nun f eine zahlentheoretische Funktion mit $f(1) \neq 0$. Wir definieren eine zahlentheoretische Funktion g induktiv wie folgt: sei $g(1) = f(1)^{-1}$. Sei nun $n \geq 2$ und seien schon die Werte $g(1), \ldots, g(n-1)$ definiert. Wir setzen

$$g(n) = -f(1)^{-1} \sum\nolimits_{d|n, d<n} g(d) f(\tfrac{n}{d})$$

(die Summierung erfolgt also über alle Teiler d von n mit $d < n$; für derartige Zahlen d ist ja $g(d)$ schon definiert). Auf diese Weise erhalten wir eine Funktion g mit $g(1)f(1) = 1 = I(1)$ und

$$I(n) = 0 = g(n)f(1) + \sum\nolimits_{d|n, d<n} g(d) f(\tfrac{n}{d}) = (g * f)(n)$$

für $n \geq 2$. Es ist also $g = f^{-1}$.

Folgerung. *Die zahlentheoretischen Funktionen f mit $f(1) \neq 0$ bilden bezüglich der Faltung eine abelsche Gruppe.*

3.2. Multiplikative Funktionen.

Wir interessieren uns vor allem für "multiplikative" Funktionen: Wie schon im Abschnitt 2.9 notiert, heißt eine Funktion $f \in \Phi$ *multiplikativ*, falls f nicht die Nullfunktion ist und falls gilt: Sind n, n' teilerfremd, so ist $f(nn') = f(n)f(n')$.

Gilt $f(nn') = f(n)f(n')$ für alle Paare n, n' natürlicher Zahlen, so heißt f *stark multiplikativ* (oder auch "vollständig multiplikativ").

> Noch einmal die **Warnung:** In der Algebra würde man eine Funktion nur dann "multiplikativ" nennen, wenn die Regel $f(nn') = f(n)f(n')$ für **alle** n, n' gilt, nicht nur für teilerfremde Paare, wenn sie also stark multiplikativ ist.

Offensichtlich gilt für f multiplikativ: *Kennt man die Werte $f(p^e)$, für alle Primzahlen p und alle natürlichen Zahlen e, so kennt man f,* denn für $n = p_1^{e_1} \cdots p_t^{e_t}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_t$ gilt

$$f(p_1^{e_1} \cdots p_t^{e_t}) = f(p_1^{e_1}) \cdots f(p_t^{e_t}).$$

Umgekehrt kann man eine multiplikative Funktion g dadurch definieren, dass man beliebige Werte $g(p^e)$ (für p Primzahl, $e \in \mathbb{N}$) wählt, und diese Abbildung multiplikativ fortsetzt:

$$g(p_1^{e_1} \cdots p_t^{e_t}) = g(p_1^{e_1}) \cdots g(p_t^{e_t})$$

(für paarweise verschiedene Primzahlen $p_1, \ldots, p_t$ und alle $e_i \in \mathbb{N}$).

Ist f multiplikativ, so ist $f(1) = 1$..

Beweis: Wäre $f(1) = 0$, so wäre f wegen $f(1 \cdot n) = f(1)f(n)$ die Nullfunktion, dies ist ausgeschlossen; aus $f(1) = f(1 \cdot 1) = f(1)f(1)$ und $f(1) \neq 0$ folgt aber $f(1) = 1$.

Ist f multiplikativ, so gilt

$$\boxed{f(m)f(n) = f((m,n))f(mn/(m,n)),}$$

dabei bezeichnet (m,n) wieder den größten gemeinsamen Teiler von m und n, und $mn/(m,n)$ ist das kleinste gemeinsame Vielfache von m und n.

Beweis: Sind e, e' reelle Zahlen, so gilt $\{e,e'\} = \{\min(e,e'), \max(e,e')\}$. Schreiben wir m,n in der Form $m = p_1^{e_1}\cdots p_t^{e_t}$, $n = p_1^{e_1'}\cdots p_t^{e_t'}$ mit paarweise verschiedenen Primzahlen $p_1,\ldots,p_t$ und nicht-negativen ganzen Zahlen e_i, e_i', so ist

$$(m,n) = p_1^{\min(e_1,e_1')}\cdots p_t^{\min(e_t,e_t')} \quad \text{und} \quad mn/(m,n) = p_1^{\max(e_1,e_1')}\cdots p_t^{\max(e_t,e_t')}.$$

Es ist also

$$f(m)f(n) = \prod_i p_i^{e_i+e_i'} = \prod_i p_i^{\min\{e_i,e_i'\}+\max\{e_i,e_i'\}} = f((m,n))f((mn/(m,n)).$$

3.2.1. Satz. *Sind f,g muliplikativ, ist ist auch $f*g$ multiplikativ.*

Beweis: Seien n_1, n_2 teilerfremde natürliche Zahlen. Ist d ein Teiler von n_1n_2, so lässt sich d eindeutig in der Form $d = d_1d_2$ mit $d_1|n_1$ und $d_2|n_2$ schreiben (es ist $d_1 = (d,n_1)$ und $d_2 = (d,n_2)$). Da n_1, n_2 teilerfremde Zahlen sind, sind auch die Zahlen d_1, d_2 teilerfremd. Entsprechend sind auch die Zahlen n_1/d_1 und n_2/d_2 teilerfremd.

$$\begin{aligned}
(f*g)(n_1n_2) &= \sum_{d|n_1n_2} f(d)g\big(\frac{n_1n_2}{d}\big) \\
&= \sum_{d_1,d_2} f(d_1d_2)g\big(\frac{n_1}{d_1}\frac{n_2}{d_2}\big) \\
&\underset{(*)}{=} \sum_{d_1,d_2} f(d_1)f(d_2)g\big(\frac{n_1}{d_1}\big)g\big(\frac{n_2}{d_2}\big) \\
&= \Big(\sum_{d_1} f(d_1)g\big(\frac{n_1}{d_1}\big)\Big)\Big(\sum_{d_2} f(d_2)g\big(\frac{n_2}{d_2}\big)\Big) \\
&= (f*g)(n_1)\cdot(f*g)(n_2),
\end{aligned}$$

dabei gilt das Gleichheitszeichen mit $(*)$, weil f und g multiplikativ sind.

Beachte: Sind die Funktionen f,g vollständig multiplikativ, so ist $f*g$ multiplikativ, meist aber **nicht** vollständig multiplikativ. Beispiel: die Funktion U ist vollständig multiplikativ. Aber $\tau := U*U$ ist nicht vollständig multiplikativ ($\tau(n)$ ist die Anzahl der Teiler von n, und es ist $\tau(2) = 2$, und $\tau(4) = 3 \neq 2^2 = \tau(2)^2$).

3.2.2. Satz. *Ist f multiplikativ, so ist auch f^{-1} multiplikativ.*

Beweis. Definiere g wie folgt: Es sei $g(p^j) = f^{-1}(p^j)$ für jede Primzahl p und $j \in \mathbb{N}$ (nach Voraussetzung ist f invertierbar), und wir setzen diese Abbildung multiplikativ fort. Auf diese Weise erhalten wir eine multiplikative Funktion g. Da f, g multiplikativ sind, ist nach 3.2.1 auch $f * g$ multiplikativ. Wir zeigen: $f * g = I$. Da die beiden Funktionen $f * g$ und I multiplikativ sind, brauchen wir nur $(f * g)(p^e) = I(p^e)$ für Primzahlpotenzen p^e zu zeigen. Es ist

$$\begin{aligned}(f * g)(p^e) &= \sum\nolimits_{0 \le e' \le e} f(p^{e'}) g(p^{e-e'}) \\ &\underset{(*)}{=} \sum\nolimits_{0 \le e' \le e} f(p^{e'}) f^{-1}(p^{e-e'}) \\ &= (f * f^{-1})(p^e) = I(p^e),\end{aligned}$$

dabei gilt $(*)$, da $p^{e-e'}$ eine p-Potenz ist, und die Abbildungen g und f^{-1} nach der Definition von g auf p-Potenzen übereinstimmen.

Folgerung. *Die multiplikativen zahlentheoretischen Funktionen bilden bezüglich der Faltung eine Gruppe.*

Die Funktionen I, U, E sind offensichtlich multiplikativ, also sind auch τ und σ multiplikativ.

3.2.3. Stark multiplikative Funktionen. Es sei daran erinnert, dass man eine zahlentheoretische Funktion f *stark multiplikativ* nennt, wenn f nicht die Nullfunktion ist und $f(n_1 n_2) = f(n_1) f(n_2)$ für alle natürlichen Zahlen n_1, n_2 gilt. Natürlich gilt: *Stark multiplikative Funktionen sind eindeutig bestimmt durch die Werte $f(p)$ mit p Primzahl.*

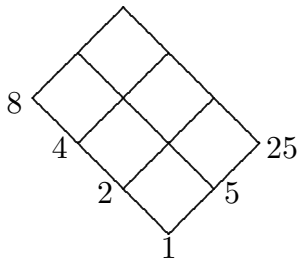
Warnung: Sind f, g stark multiplikativ, so braucht weder $f * g$ noch f^{-1} stark multiplikativ zu sein. Beispiele: U ist stark multiplikativ, aber $\tau = U * U$ ist nicht stark multiplikativ (denn $\tau(2) = 2$, $\tau(4) = 3$). In 3.5 berechnen wir $\mu = U^{-1}$ und werden sehen, dass auch μ nicht multiplikativ ist ($\mu(2) = -1$, $\mu(4) = 0$).

3.3. Die Funktion τ. Es ist $\tau(p^e) = e + 1$, also gilt

$$\boxed{\tau(p_1^{e_1} \cdots p_t^{e_t}) = \prod_{i=1}^{t} (e_i + 1)}$$

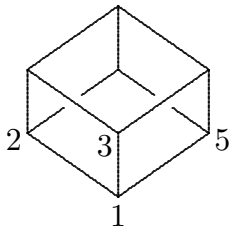
(falls $p_1, \ldots, p_t$ paarweise verschiedene Primzahlen sind).

Beispiel 1. $\tau(200) = \tau(2^3 5^2) = 4 \cdot 3 = 12$. Zugehöriges Schokoladen-Bild:



Die Teiler bilden ein Rechtecksraster, beschriftet wurden nur die beiden unteren Kanten (hier findet man alle Primpotenzteiler) — die weitere Beschriftung erhält man durch die jeweiligen Produkt-Bildungen. Ganz allgemein gilt: Ist $n = p_1^{e_1} p_2^{e_2}$ mit Primzahlen $p_1 \neq p_2$, so bilden die Teiler ein derartiges Rechteck.

Beispiel 2. $\tau(2 \cdot 3 \cdot 5) = 2 \cdot 2 \cdot 2 = 8$. Zugehöriges Würfelbild:



3.4. Die Funktion σ. Es ist

$$\boxed{\sigma(p^e) = \frac{p^{e+1} - 1}{p - 1}}$$

,

Beweis: Die Zahl p^e hat die Teiler $p^{e'}$ mit $0 \leq e' \leq e$ und deren Summe ist

$$\sum\nolimits_{0 \leq e' \leq e} p^{e'} = 1 + p + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1}.$$

Insbesondere ist $\sigma(2^e) = 2^{e+1} - 1$, und natürlich ist $\sigma(p) = p + 1$.

Also gilt: $\sigma(n) = \prod_{p^e || n} \frac{p^{e+1}-1}{p-1}$, dabei schreibt man $p^e || n$ falls p^e aber nicht p^{e+1} ein Teiler von n ist, falls also p^e die höchste p-Potenz ist, die n teilt.

3.5. Die Möbius-Transformierte $f * U$ von f.

Ist f eine beliebige zahlentheoretische Funktion, so betrachtet man oft $f * U$ und nennt dies die Möbius-Transformierte zu f (oder auch die "summatorische" Funktion zu f); es ist

$$(f * U)(n) = \sum_{d|n} f(d),$$

es wird hier also die Summe der Werte $f(d)$ für alle Teiler d von n gebildet.

Beispiele:
(1) $U * U = \tau$,
(2) $E * U = \sigma$,
(3) $\phi * U = E$ (siehe 2.3.2).

Ist f multiplikativ, und sind $p_1 < p_2 < \cdots < p_t$ Primzahlen und $e_1, \ldots, e_t$ natürliche Zahlen, so gilt

$$(f * U)(p_1^{e_1} \cdots p_1^{e_1}) = \prod_{i=1}^{t} \big(f(1) + f(p_i) + f(p_i^2) + \cdots + f(p_i^{e_i})\big)$$

Die Funktion U ist nach 3.1.2 invertierbar. Setze $\mu = U^{-1}$, man nennt dies die *Möbius'sche Umkehrfunktion.* Die Funktion μ wird vor allem wegen der trivialerweise geltenden Formel

$$f = (f * U) * \mu$$

gebraucht — diese Formel besagt: *Kennt man die Möbius-Transformierte $f * U$ von f, so kann man durch Faltung mit μ die Funktion f zurück gewinnen.* Andere Formulierung:

$$\text{Ist} \quad F(n) = \sum\nolimits_{d|n} f(d), \quad \text{so ist} \quad f(n) = \sum\nolimits_{d|n} F(d)\mu(\frac{n}{d}).$$

3.5.1. *Die Funktion $\mu = U^{-1}$ ist multiplikativ* (wegen 3.2.2).

3.5.2. Wir berechnen die Werte $\mu(p^e)$. Es ist $\mu(p) = -1$ und $\mu(p^e) = 0$ für $e > 1$.

Beweis: Es ist $\mu(1) = 1$. Für $e \geq 1$ gilt

$$0 = I(p^e) = (U * \mu)(p^e) = \sum\nolimits_{0 \leq i \leq e} \mu(p^i).$$

Für $e = 1$ liefert dies $0 = \mu(1) + \mu(p) = 1 + \mu(p)$, also $\mu(p) = -1$. Für $e \geq 2$ sehen wir:

$$0 = \sum\nolimits_{0 \leq i \leq e} \mu(p^i) \qquad \text{und auch} \qquad 0 = \sum\nolimits_{0 \leq i < e} \mu(p^i),$$

also ist $\mu(p^e) = 0$.

Also erhalten wir die Formel:

$$\mu(n) = \begin{cases} 0 & \text{falls } n \text{ nicht quadratfrei,} \\ (-1)^t & \text{falls } n = p_1 \cdots p_t \text{ mit paarweise verschiedenen Primzahlen } p_i. \end{cases}$$

dabei schließt die zweite Zeile auch den Fall $n = 1$, also $t = 0$ ein: Es ist $\mu(1) = 1$.

3.6. Die Eulersche ϕ-Funktion.

Erinnerung: Die Eulersche ϕ-Funktion ist folgendermaßen definiert:

$$\phi(n) = (\text{Anzahl der Zahlen } 1 \leq m \leq n \text{ mit } (m, n) = 1)$$

3.6.1. *Es ist*

$$\phi * U = E.$$

Dies haben wir in 2.3.2. gezeigt!

3.6.2. Folgerung: *ϕ ist multiplikativ.*

Beweis: Es gilt $\phi = E * \mu$, und E und μ sind multiplikativ.

Wir haben die Multiplikativität der ϕ-Funktion schon im Teil 2 gezeigt. Hier haben wir einen neuen Beweis.

3.7. Restklassen-Charaktere.

3.7.1. Charaktere einer endlichen abelschen Gruppe G.

Definition: Sei G eine (multiplikativ geschriebene) abelsche Gruppe der Ordnung h. Ein Charakter von G ist ein Gruppen-Homomorphismus $G \to \mathbb{C}^*$. Den Charakter χ_0 mit $\chi_0(g) = 1$ für alle $g \in G$ nennt man den *trivialen* Charakter. Ist χ ein Charakter mit $\chi(g) \in \mathbb{R}$, für alle $g \in G$, so nennt man χ einen *reellen* Charakter. Beachte: Für jeden Charakter χ und $g \in G$ gilt: $\chi(g)$ *ist eine h-te Einheitswurzel*. Insbesondere gilt: Genau dann ist χ reell, wenn χ nur die Werte 1 und -1 annimmt.

Satz (Orthogonalitätsrelation I). Sei G eine Gruppe der Ordnung h. Dann gilt für jeden Charakter χ

$$\sum_{g\in G}\chi(g)=\begin{cases} h & \text{falls } \chi=\chi_0\\ 0 & \chi\neq\chi_0\end{cases}$$

Beweis: Es ist $\chi_0(g)=1$ für alle $g\in G$, und demnach $\sum_\chi \chi_0(g)=h$. Sei nun $\chi\neq\chi_0$. Dann gibt es $g'\in G$ mit $\chi(g)\neq 1$. Es ist

$$(\chi(g')-1)\sum_g\chi(g)=\sum_g\chi(g')\chi(g)-\sum_g\chi(g)=0.$$

Einerseits ist nämlich $\chi(g')\chi(g)=\chi(g'g)$, andererseits gilt: Durchläuft g alle Elemente der Gruppe G, so auch $g'g$, also ist die Summe $\sum_g\chi(g')\chi(g)=\sum_g\chi(g'g)$ nur eine Umordnung der Summe $\sum_g\chi(g)$.

3.7.2. Die Charaktergruppe $\widehat{G}$ einer endlichen abelschen Gruppe G.

Satz. *Sei G eine abelsche Gruppe der Ordnung h. Die Menge der Charaktere von G bildet bezüglich punktweiser Multiplikation eine abelsche Gruppe $\widehat{G}$ der Ordnung h. Zu jedem $1\neq x\in G$ gibt es einen Charakter χ mit $\chi(x)\neq 1$.*

Beweis: Dass $\widehat{G}$ bezüglich der punktweisen Multiplikation eine abelsche Gruppe ist, ist leicht zu sehen. Für die weiteren Behauptungen brauchen wir folgendes Lemma:

Fortsetzungslemma. *Sei G endliche abelsche Gruppe, sei U eine Untergruppe und $g\in G$ sodass sich jedes Element aus G in der Form ug^t mit $t\in\mathbb{N}$ schreiben lässt. Sei r minimal mit $g^r\in U$. Dann ist $|G|=|U|r$. Ist $\chi\colon U\to\mathbb{C}^*$ ein Charakter von U, und z eine r-te Wurzel von $\chi(g^r)$, so erhalten wir durch $\chi'(ug^s)=\chi(u)z^s$ eine Fortsetzung von χ auf G, und jede Fortsetzung erhält man auf diese Weise.*

Beachte: (a) Da g endliche Ordnung hat, gibt es $t\in\mathbb{N}$ mit $g^t=1$, also gibt es r.
(b) Da $\chi(g^r)$ eine von Null verschiedene komplexe Zahl ist, und jede von Null verschiedene komplexe Zahl genau r r-te Wurzeln besitzt, sieht man, dass χ' genau r Fortsetzungen besitzt.

Beweis des Lemmas. Wir zeigen als erstes: *Jedes Element $h\in G$ lässt sich eindeutig in der Form ug^s mit $u\in U$ und $0\leq s<r$ schreiben.* Nach Voraussetzung sind die Elemente von G von der Form ug^t mit $u\in U$ und $t\in\mathbb{N}$. Schreibe $t=ar+s$ mit $a\in\mathbb{N}_0$ und $0\leq s<r$. Dann ist $ug^t=ug^{ar+s}=u(g^r)^ag^s=u'g^s$ mit $u'=u(g^r)^a\in U$. Eindeutigkeit: Sei $h\in G$ auf zwei Weisen geschrieben: $h=u_1g^{s_1}=u_2g^{s_2}$ mit $u_1,u_2\in U$ und $0\leq s_1<r$, $0\leq s_2<r$. Wir können annehmen $s_1\leq s_2$. Aus $u_1g^{s_1}=u_2g^{s_2}$ folgt $(u_2)^{-1}u_1=g^{s_2-s_1}$ und es ist $0\leq s_2-s_1<r$. Wir sehen also, dass $g^{s_2-s_1}$ zu U gehört. Die Minimalität von r liefert $s_2-s_1=0$, also $s_2=s_1$ und demnach auch $u_1=u_2$.

Wir sehen insbesondere, dass G die disjunkte Vereinigung $\bigcup_{s=0}^{r-1} Ug^s$ ist, und natürlich haben die Teilmengen Ug^s von G alle die Kardinalität $|U|$, daher folgt $|G| = |U|r$ (wir erhalten hier also eine Partition von G wie im Beweis des Satzes von Lagrange).

Sei nun $\chi' \in \widehat{G}$ eine Fortsetzung von χ (also $\chi'|U = \chi$). Es ist $(\chi'(g))^r = \chi'(g^r) = \chi(g^r)$, also ist $z = \chi'(g)$ eine r-te Wurzel von $\chi(g^r)$. Für ein Element ug^t mit $u \in U$ und $g \in \mathbb{N}$ gilt $\chi'(ug^t) = \chi'(u)(\chi'(g))^t = \chi(u)z^t$, also hat χ' die genannte Form.

Umgekehrt gilt aber auch: Ist z eine r-te Wurzel von $\chi(g^r)$, so definiere χ' durch

$$\chi'(ug^s) = \chi(u)z^s$$

für $u \in U$ und $0 \leq s < r$. Da alle Elemente von G eindeutig in der Form ug^s mit $u \in U$ und $0 \leq s < r$ geschrieben werden können, ist χ' wohldefiniert. Behauptung: dies ist ein Gruppen-Homomorphismus. Zu zeigen ist also $\chi'(u_1u_2g^{s_1+s_2}) = \chi'(u_1g^{s_1})\chi'(u_2g^{s_2})$. Dies ist klar, wenn $s_1 + s_2 < r$ gilt. Ist $s_1 + s_2 = r + s$ mit $0 \leq s$, so ist $\leq s < r$, also gilt

$$\begin{aligned}\chi'(u_1u_2g^{s_1+s_2}) &= \chi'(u_1u_2g^{r+s}) = \chi'(u_1u_2g^rg^s) = \chi(u_1)\chi(u_2)\chi(g^r)z^s \\ &= \chi(u_1)\chi(u_2)z^rz^s = \chi(u_1)\chi(u_2)z^{s_1+s_2} = \chi'(u_1g^{s_1})\chi'(u_2g^{s_2}).\end{aligned}$$

Nun der Beweis des Satzes, mit Induktion: Ist $G = 1$ ist nichts zu zeigen. Ist $G \neq 1$, so gibt es eine echte Untergruppe U und $g \in G$, sodass sich jedes Element aus G in der Form ug^t mit $t \in \mathbb{N}$ schreiben lässt. Sei r minimal mit $g^r \in U$. Nach Induktionsvoraussetzung besitzt U genau $|U|$ Charaktere. Jeder dieser Charaktere besitzt genau r Fortsetzungen. Also hat G genau $|U|r = |G|$ Charaktere.

Sei $x \neq 1$ in G. Ist $x \in U$, so gibt es einen Charakter χ von U mit $\chi(x) \neq 1$. Ist χ' eine beliebige Fortsetzung auf G, so ist $\chi'(x) = \chi(x) \neq 0$. Ist $x \notin U$, etwa $x = ug^s$ mit $1 \leq s < r$, so betrachte den trivialen Charakter χ_0 von U. Es ist $\chi(g^r) = 1$; die Fortsetzungen von χ_0 auf G werden durch r-te Einheitswurzeln gegeben. Sei z eine primitive r-te Einheitswurzel und χ' die zugehörige Fortsetzung. Dann ist $\chi'(ug^s) = \chi(u)z^s = 1 \cdot z^s = z^s \neq 1$.

Zusatz: Ist χ ein Charakter, so ist $\chi^{-1}(g) = \chi(g)^{-1} = \overline{\chi(g)}$, denn $|\chi(g)| = 1$ und für komplexe Zahlen c mit $|c| = 1$ gilt $c^{-1} = \overline{c}$.

> Zusatz: *Ist G zyklisch, so ist auch $\widehat{G}$ zyklisch.* Sei nämlich $|G| = n$ und $g \in G$ ein Element der Ordnung n. Wir konstruieren einen Charakter der Ordnung n wie folgt: Sei z eine primitive n-te Einheitswurzel. Dann gibt es, wie wir gesehen haben einen Charakter χ mit $\chi(g) = z$. Dieser Charakter hat aber offensichtlich die Ordnung n. Da $|\widehat{G}| = n$, folgt $\widehat{G} = \langle G \rangle$.
> Beachte: *Ist G zyklisch mit gerader Ordnung, so gibt es genau einen Charakter der Ordnung* 2, denn eine zyklische Gruppe gerader Ordnung hat genau ein Element der Ordnung 2.

3.7.3. Die Gruppe $\hat{\hat{G}}$. Sei G eine abelsche Gruppe. Dann ist auch $G' = \widehat{G}$ eine abelsche Gruppe und wir können $\widehat{G'}$ bilden, statt $\widehat{G'}$ schreibt man $\hat{\hat{G}}$. Offensichtlich gibt es eine kanonische Abbildung $G \to \hat{\hat{G}}$, nämlich die Auswertungsabbildung $g \mapsto (\chi \mapsto \chi(g))$ für $g \in G$ und $\chi \in \widehat{G}$, und diese kanonische Abbildung $G \to \hat{\hat{G}}$ ist ein Gruppen-Homomorphismus. All dies ist ganz analog zur Bildung des Dualraums V^* eines Vektorraums V, dabei ist die Auswertungsabbildung $V \to V^{**}$ ein injektiver Vektorraum-Homomorphismus. Entsprechend ist auch die Auswertungsabbildung $G \to \hat{\hat{G}}$ injektiv.

Korollar. *Ist G eine endliche abelsche Gruppe, so ist die kanonische Abbildung $G \to \hat{\hat{G}}$ ein Gruppen-Isomorphismus.*

Wir haben schon notiert, dass die Auswertungsabbildung $G \to \hat{\hat{G}}$ ein injektiver Gruppen-Homomorphismus ist. Da G und $\hat{\hat{G}}$ die gleiche Ordnung haben, ist die Auswertungsabbildung auch surjektiv.

Zusatz.
Struktursatz für endliche abelsche Gruppen: *Jede endliche abelsche Gruppe ist ein Produkt zyklischer Gruppen.* Beweis: Sei G endliche abelsche Gruppe, sei $g \in G$ ein Element mit maximaler Ordnung, etwa mit Ordnung r. Zur zyklischen Untergruppe $G' = \langle g \rangle$ gibt es einen Charakter χ', der $\widehat{G'}$ erzeugt. Setzen wir χ' auf G fort, so erhalten wir einen Charakter χ von G, dessen Ordnung größer oder gleich r ist. Wäre die Ordnung von χ echt größer als r, so erhielten wir mit dem gleichen Argument ein Element in $\hat{\hat{G}}$ mit Ordnung echt größer als r, aber $\hat{\hat{G}}$ ist isomorph zu G. Wir sehen also: Die Ordnung von χ ist gleich r. Das Bild von G unter χ ist eine Untergruppe von $\mathbb{C}^*$, also zyklisch, und demnach die zyklische Untergruppe von $\mathbb{C}^*$ der Ordnung r. Der Kern H von χ hat die Ordnung $\frac{1}{r}|G|$ und natürlich ist $\langle g \rangle \cap H = \{1\}$. Es folgt: G ist isomorph zu $\langle g \rangle \times H$. (Die Abbildung $\eta\colon \langle g \rangle \times H \to G$, mit $\eta(g^t, h) = g^t h$ ist ein Gruppen-Homomorphismus, der wegen $\langle g \rangle \cap H = \{1\}$ injektiv ist. Da die Gruppen $\langle g \rangle \times H$ und G die gleiche Ordnung haben, ist η auch surjektiv, also ein Isomorphismus.)

Kennt man diesen Struktursatz, so kann man sich sehr viel besser die Struktur von $\widehat{G}$ vorstellen: Wir schreiben $G = G_1 \times \cdots \times G_s$ als Produkt zyklischer Gruppen G_i und sehen $\widehat{G} = \widehat{G_1} \times \cdots \times \widehat{G_s}$. Für jede dieser zyklischen Gruppen G_i wissen wir, dass $\widehat{G_i}$ wieder zyklisch, also zu G_i isomorph ist. Es folgt: $\widehat{G}$ ist zu G isomorph. Aber es muss betont werden, dass es keinen kanonischen Isomorphismus zwischen G und $\widehat{G}$ gibt, denn schon für eine zyklische Gruppe G der Ordnung r hängt die Angabe eines Isomorphismus $G \to \widehat{G}$ von der Auswahl eines erzeugenden Elements von g und der Auswahl einer primitiven r-ten Einheitswurzel in $\mathbb{C}$ ab.

3.7.4. Orthogonalitätsrelation II. Es gilt für jedes $g \in G$

$$\boxed{\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} h & \text{falls} \quad g = 1 \\ 0 & \qquad\quad g \neq 1 \end{cases}}$$

Beweis: Ist $g = 1$, so ist $\chi(g) = 1$ für alle χ, und demnach $\sum_\chi \chi(1) = h$. Sei nun $g \neq 1$. Zu g gibt es einen Charakter ψ mit $\psi(g) \neq 1$. Es ist

$$(\psi(g) - 1) \sum_\chi \chi(g) = \sum_\chi \psi(g)\chi(g) - \sum_\chi \chi(g) = 0.$$

Einerseits ist nämlich $\psi(g)\chi(g) = (\psi\chi)(g)$, andererseits gilt: Durchläuft χ alle Elemente der Gruppe $\widehat{G}$, so auch $\psi\chi$, also ist die Summe $\sum_\chi \psi(g)\chi(g)$ nur eine Umordnung der Summe $\sum_\chi \chi(g)$.

Folgerung. Es gilt für $g, g' \in G$.

$$\sum_{\chi \in \widehat{G}} \frac{\chi(g')}{\chi(g)} = \begin{cases} h & \text{falls} \quad g = g' \\ 0 & \qquad\quad g \neq g' \end{cases}$$

Beweis: $\frac{\chi(g')}{\chi(g)} = \chi(g'g^{-1})$.

3.7.5. Restklassen-Charaktere. Sei nun $G = U(\mathbb{Z}/k, \cdot)$. Ist χ ein Charakter von G, so erhalten wir eine zahlentheoretische Funktion, die ebenfalls mit χ bezeichnet wird, auf folgende Weise:

$$\chi(n) = \begin{cases} \chi(\overline{n}) & \text{falls} \quad (n,k) = 1 \\ 0 & \text{sonst} \end{cases}.$$

Man nennt diese Abbildung $\chi\colon \mathbb{N} \to \mathbb{C}$ einen Restklassen-Charakter modulo k.

Lemma. *Alle Restklassen-Charaktere sind stark multiplikativ.*

Beweis: Sei χ ein Restklassen-Charakter modulo k und $n_1, n_2 \in \mathbb{N}$. Ist $(k, n_1 n_2) > 1$, so gilt auch $(k, n_i) > 1$ für mindestens ein i, also gilt $\chi(n_1 n_2) = 0$ und auch $\chi(n_1)\chi(n_2) = 0$. Ist dagegen $(k, n_1) = 1$ und $(k, n_2) = 1$, so verwendet man, dass $\chi\colon U(\mathbb{Z}/k, \cdot) \to \mathbb{C}^*$ ein Gruppen-Homomorphismus ist:

$$\chi(n_1 n_2) = \chi(\overline{n_1 n_2}) = \chi(\overline{n_1} \cdot \overline{n_2}) = \chi(\overline{n_1})\chi(\overline{n_2}) = \chi(n_1)\chi(n_2).$$

Sei $k \in \mathbb{N}$. Eine zahlentheoretische Funktion $f\colon \mathbb{N} \to \mathbb{C}$ ist genau dann eine Restklassen-Charakter modulo k wenn die folgenden drei Eigenschaften gelten:

(i) *Genau dann ist $f(n) = 0$, wenn $(n, k) = 1$ gilt.*
(ii) *Ist $n \equiv n' \mod k$, so ist $f(n) = f(n')$.*
(iii) *Die Funktion f ist stark multiplikativ.*

Beweis: Übungsaufgabe.

Es gibt genau $\phi(k)$ Restklassen-Charaktere modulo k.

Beweis: Sei $G = U(\mathbb{Z}/k, \cdot)$. Wir wissen $|G| = \phi(k)$, also ist auch $|\widehat{G}| = \phi(k)$.

Ist χ ein Restklassen-Charakter modulo k, so ist jeder von Null verschiedene Wert $\chi(n)$ eine $\phi(k)$-te Einheitswurzel.

Beweis: Ist $n \in \mathbb{N}$ mit $(n, k) = 1$, so ist die Ordnung von $\overline{n} \in U(\mathbb{Z}/k, \cdot)$ ein Teiler von $\phi(k)$, also $\overline{n}^{\phi(k)} = \overline{1}$. Es folgt $\chi(n)^{\phi(k)} = \chi(n^{\phi}(k)) = \chi(1) = 1$.

Für jedes k gibt es den Restklassen-Charakter $\chi_0^{(k)}$ mit

$$\chi_0^{(k)}(n) = \begin{cases} 1 & \text{falls} \quad (n,k) = 1 \\ 0 & \text{sonst} \end{cases},$$

man nennt ihn den *Hauptcharakter*, die übrigen Restklassen-Charaktere nehmen auch Werte ungleich Null und Eins an. Ein Restklassen-Charakter, der nur reelle Werte (also $0, 1, -1$) annimmt, heißt *reeller* Charakter.

Ist p ungerade Primzahl, so liefert das Legendre-Symbol $\left(\frac{\cdot}{p}\right)$ den einzigen vom Hauptcharakter verschiedenen reellen Restklassen-Charakter modulo p. Beachte: In 2.11.5 haben wir gesehen, dass $\left(\frac{\cdot}{p}\right)$ einen Gruppen-Homomorphismus $U(\mathbb{Z}/p, \cdot) \to (\{1, -1\}, \cdot) \subset \mathbb{C}^*$, also einen Charakter, liefert.

Beispiele.

- $k = 1$. Es ist $\phi(1) = 1$, also gibt es genau einen Restklassen-Charakter χ modulo 1, nämlich die Funktion $\chi_0^{(1)}$ mit $\chi_0^{(1)}(n) = 1$ für alle n, also $\chi_0^{(1)} = U$.

χ \ n	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
$\chi_0^{(1)}$	1	1	1	1	1	1	1	1	1	1	1	

- $k = 2$. Es ist $\phi(2) = 1$, also gibt es genau einen Restklassen-Charakter χ modulo 2, den Hauptcharakter $\chi_0^{(2)}$ (mit $\chi_0^{(2)}(2n+1) = 1$ und $\chi_0^{(2)}(2n) = 0$).

χ \ n	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
$\chi_0^{(2)}$	1	0	1	0	1	0	1	0	1	0	1	

- $k = 3$. Neben dem Hauptcharakter $\chi_0^{(3)}$ gibt es einen weiteren Charakter $\chi_1^{(3)}$ mit

$$\chi_1^{(3)}(n) = \begin{cases} 1 & n \equiv 1 \mod 3, \\ 0 & n \equiv 0 \mod 3 \end{cases}$$

Insgesamt hat man:

$\chi \diagdown n$	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
$\chi_0^{(3)}$	1	1	0	1	1	0	1	1	0	1	1	
$\chi_1^{(3)}$	1	-1	0	1	-1	0	1	-1	0	1	-1	

- $k = 4$. Es ist $\phi(4) = 2$, also gibt es genau einen vom Hauptcharakter verschiedenen Restklassen-Charakter $\chi_1^{(4)}$ modulo 4, nämlich

$$\chi_1^{(4)}(n) = \begin{cases} 1 & \\ -1 & \text{für} \\ 0 & \end{cases} \begin{array}{l} n \equiv 1 \mod 4, \\ n \equiv 3 \mod 4, \\ n \equiv 0 \mod 2 \end{array}$$

$\chi \diagdown n$	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
$\chi_0^{(4)}$	1	0	1	0	1	0	1	0	1	0	1	
$\chi_1^{(4)}$	1	0	-1	0	1	0	-1	0	1	0	-1	

Natürlich gilt $\chi_0^{(4)} = \chi_0^{(2)}$ (die Hauptcharaktere für alle echten Zweierpotenzen k stimmen überein).

- $k = 5$. Es ist $\phi(5) = 4$, also gibt es neben dem Hauptcharakter genau drei weitere Restklassen-Charaktere $\chi_1^{(5)}, \chi_2^{(5)}, \chi_3^{(5)}$ modulo 5. Hier tauchen zum ersten Mal nicht-reelle Zahlen als Funktionswerte auf, nämlich i und $-i$. Beachte, dass 2 eine Primitivwurzel modulo 5 ist, daher können wir Restklassen-Charaktere $\chi_t^{(5)}$ durch $\chi_t^{(5)}(2) = i^t$ definieren.

$\chi \diagdown n$	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
$\chi_0^{(5)}$	1	1	1	1	0	1	1	1	1	0	1	
$\chi_1^{(5)}$	1	i	$-i$	-1	0	1	i	$-i$	-1	0	i	
$\chi_2^{(5)}$	1	-1	-1	1	0	1	-1	-1	1	0	-1	
$\chi_3^{(5)}$	1	$-i$	i	-1	0	1	$-i$	i	-1	0	$-i$	

- $k = 6$. Es ist $\phi(6) = 2$, also gibt es neben dem Hauptcharakter wieder nur einen weiteren Restklassen-Charakter modulo 6

$\chi \diagdown n$	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
$\chi_0^{(6)}$	1	0	0	0	1	0	1	0	0	0	1	
$\chi_1^{(6)}$	1	0	0	0	-1	0	1	0	0	0	-1	

- $k = 7$. Es ist $\phi(7) = 6$. Sei ζ eine primitive 6-te Einheitswurzel. Beachte, dass 3 eine Primitivwurzel modulo 7 ist. Es gibt die folgenden sechs Restklassen-Charaktere $\chi_t^{(7)}$ modulo 7 (mit $0 \le t \le 5$), die durch $\chi_t^{(7)}(3) = \zeta^t$ definiert sind:

$\chi \diagdown n$	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
$\chi_0^{(7)}$	1	1	1	1	1	1	0	1	1	1	1	
$\chi_1^{(7)}$	1	ζ^2	ζ	ζ^4	ζ^5	ζ^3	0	1	ζ^2	ζ	ζ^4	
$\chi_2^{(7)}$	1	ζ^4	ζ^2	ζ^2	ζ^4	1	0	1	ζ^4	ζ^2	ζ^2	
$\chi_3^{(7)}$	1	1	ζ^3	1	ζ^3	ζ^3	0	1	1	ζ^3	1	
$\chi_4^{(7)}$	1	ζ^2	ζ^4	ζ^4	ζ^2	1	0	1	ζ^2	ζ^4	ζ^4	
$\chi_5^{(7)}$	1	ζ^4	ζ^5	ζ^2	ζ	ζ^3	0	1	ζ^4	ζ^5	ζ^2	

  Wegen $\zeta^3 = -1$ ist $\chi_3^{(7)}$ ein reeller Charakter.

- $k = 8$. Es ist $\phi(8) = 4$, also gibt es genau 4 Restklassen-Charaktere. Dies ist der erste Fall, in dem $G = U(\mathbb{Z}/n, \cdot)$ nicht zyklisch ist. Alle nicht-trivialen Elemente in G haben Ordnung 2, also haben auch die nicht-trivialen Elemente in $\widehat{G}$ die Ordnung 2. Es folgt, dass alle Restklassen-Charaktere reell sind. Die Gruppe G wird von den Restklassen $\overline{3}$ und $\overline{5}$ erzeugt wird. Wir erhalten alle Restklassen-Charaktere χ, indem wir $\chi(3) = \pm 1$ und $\chi(5) = \pm 1$ setzen.

$\chi \diagdown n$	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
$\chi_0^{(8)}$	1	0	1	0	1	0	1	0	1	0	1	
$\chi_1^{(8)}$	1	0	-1	0	1	0	-1	0	1	0	-1	
$\chi_2^{(8)}$	1	0	1	0	-1	0	-1	0	1	0	1	
$\chi_3^{(8)}$	1	0	-1	0	-1	0	1	0	1	0	-1	

- $k = 9$. Es ist $\phi(9) = 6$. Die Gruppe $G = U(\mathbb{Z}/9, \cdot)$ ist wieder zyklisch, sie wird von $\overline{2}$ erzeugt. Sei ζ eine primitive 6-te Einheitswurzel, so können wir die 6 Restklassen-Charaktere durch $\chi_i^{(9)}(2) = \zeta^t$ definieren. Wir notieren hier nur die Werte von $\chi_1^{(9)}$.

$\chi \diagdown n$	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
$\chi_1^{(9)}$	1	ζ	0	ζ^2	ζ^5	0	ζ^4	ζ^3	0	1	ζ	

Orthogonalitätsrelation I (Umformulierung für Restklassen-Charaktere modulo k). Sei χ ein Restklassen-Charakter modulo k. Dann gilt:

$$\sum_{l=1}^{k-1} \chi(l) = \begin{cases} \phi(k) & \text{falls} \quad \chi = \chi_0 \\ 0 & \qquad\quad \chi \neq \chi_0. \end{cases}$$

Orthogonalitätsrelation II (Umformulierung für Restklassen-Charaktere modulo k). Seien $l, l' \in \mathbb{N}$ mit $(k, l) = 1$. Dann gilt:

$$\sum_{\chi} \chi(l) = \begin{cases} \phi(k) & \text{falls} \quad l \equiv 1 \mod k, \\ 0 & \qquad\quad l \not\equiv 1 \mod k, \end{cases}$$

dabei wird über alle Restklassen-Charaktere modulo k summiert.

Natürlich gibt es auch die Version, die statt eines Werts $\chi(l)$ den Quotienten $\frac{\chi(l')}{\chi(l)}$ betrachtet: Seien $l, l' \in \mathbb{N}$ mit $(k, l) = 1$. Dann gilt:

$$\sum_{\chi} \frac{\chi(l')}{\chi(l)} = \begin{cases} \phi(k) & \text{falls} \quad l' \equiv l \mod k, \\ 0 & \qquad\quad l' \not\equiv l \mod k, \end{cases}$$

dabei wird über alle Restklassen-Charaktere modulo k summiert.

Beweis: Ist auch $(l', k) = 1$, so sind die Restklassen von l und l' beide in $G = U(\mathbb{Z}/k, \cdot)$, und wir wenden die Orthogonalitätsrelation an, andernfalls ist $\chi(l') = 0$ nach Definition.

Ausblick. Warum sind wir an Restklassen-Charakteren interessiert? Wie wir wissen, divergiert die Reihe $\sum_n \frac{1}{n}$ die wir uns gerne als (unendliches) Produkt der geometrischen Reihen $\sum_t \frac{1}{p^t} = \frac{1}{1-p^{-1}}$ vorstellen würden. Statt der Reihe $\sum_n \frac{1}{n}$ betrachtet man für $s > 1$ die konvergente Reihe $\sum_n \frac{1}{n^s}$ und erhält auf diese Weise die Funktion $\zeta(s) = \sum_n \frac{1}{n^s}$.

Ist nun $k > 1$ und χ ein Restklassen-Charakter modulo k, der nicht der Hauptcharakter ist, so werden wir sehen, dass die Reihe $\sum_n \frac{\chi(n)}{n}$ immer konvergiert, auch hier können wir den Exponenten s einbauen und die Funktion $L(s, \chi) = \sum_n \frac{\chi(n)}{n^s}$ betrachten, man nennt dies eine *Dirichlet-Reihe*. Hervorzuheben ist, dass die Dirichlet-Reihen schon 1837 eingeführt wurden (eben von Dirichlet), die Arbeit von Riemann, nach der die Riemann'schen ζ-Funktion benannt ist, wurde erst 1859 publiziert.