Vorlesung Analytische Zahlentheorie

SoSe '22, Uhu
K. Halupczok

AnZ 24: Charaktere

Stichworte: Gruppencharakter, Dirichletcharakter, Hauptcharakter, Orthogonalitätsrelationen, Grundeigenschaften von Charakteren, Charaktergruppe $\cong (\mathbb{Z}/q\mathbb{Z})^*$, Charaktertafeln

---

24.1. **Einleitung:** Auf der Menge $(\mathbb{Z}/q\mathbb{Z})^* := \{\overbrace{a \bmod q}^{\text{oder: } a(q)} : (a,q)=1\} = \{a+q\mathbb{Z} : (a,q)=1\}$ der reduzierten Restklassen mod q ist durch die wohldefinierte Multiplikation $(a+q\mathbb{Z})\cdot(b+q\mathbb{Z}) := ab+q\mathbb{Z}$ eine Gruppe definiert (assoziativ, neutr. El. ist $1+q\mathbb{Z}$, inverses El. von $a+q\mathbb{Z}$ ist $b+q\mathbb{Z}$, wo $a\cdot b + r\cdot q = 1$ für $b,r\in\mathbb{Z}$ ist, und schreiben $a^{-1}+q\mathbb{Z}$ für die inverse Restklasse von a mod q. Diese kann als Lsg. der Gleichung $ab+rq=1$ mit dem euklidischen Algorithmus berechnet werden). Homomorphismen von $((\mathbb{Z}/q\mathbb{Z})^*,\cdot)$ nach $(\mathbb{C},\cdot)$ können auf $\mathbb{Z}$ fortgesetzt werden und heißen dann Dirichletcharaktere. Sie sind das richtige Werkzeug, um die Einschränkung von (nat.) Zahlenangaben auf Restklassen $a \bmod q$ (schreiben auch $a(q)$) mathematisch gewinnbringend zu beschreiben. Die naheliegende Betrachtung von $\sum_{n\equiv a(q)} \frac{\Lambda(n)}{n^s}$ führt nämlich zu Schwierigkeiten, da $f(n) = \begin{cases}\Lambda(n), & n\equiv a(q),\\ 0, & \text{sonst},\end{cases}$ keine simplen Faltungseigenschaften hat.

24.2. **Def.:** Sei $q\in\mathbb{N}$ und $\tilde\chi$ ein Charakter der Gruppe $((\mathbb{Z}/q\mathbb{Z})^*,\cdot)$, d.h. $\tilde\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}$ sei Gruppenhomomorphismus auf die Gruppe $(\mathbb{C}\setminus\{0\},\cdot)$, d.h. $\forall \underline{u},\underline{v}\in(\mathbb{Z}/q\mathbb{Z})^*$ gelte $\tilde\chi(\underline{u}\underline{v}) = \tilde\chi(\underline{u})\cdot\tilde\chi(\underline{v})$.

- Die durch Fortsetzung von $\tilde\chi$ auf $\mathbb{Z}$, d.h. $\chi(n) := \begin{cases}\tilde\chi(n+q\mathbb{Z}), & \text{falls } (n,q)=1,\\ 0, & \text{sonst},\end{cases}$ entstehende vollständig multiplikative zahlentheoretische Funktion $\chi:\mathbb{Z}\to\mathbb{C}$, heißt Dirichletcharakter mod q. [$\chi(nm)=\chi(n)\chi(m)$ für alle $n,m\in\mathbb{N}$ ist dann klar]
- Ist $\tilde\chi$ der triviale Charakter von $(\mathbb{Z}/q\mathbb{Z},\cdot)^*$, d.h. $\tilde\chi(\underline{u})=1$ für alle $\underline{u}\in(\mathbb{Z}/q\mathbb{Z})^*$, so heißt χ der Hauptcharakter mod q und wird mit χ_0 bezeichnet (so dass also $\chi_0(n)=1$ für $(n,q)=1$ und $\chi_0(n)=0$ für $(n,q)>1$ gilt).

24.3. **Bsp.:** Der einzige nichttriviale Charakter (d.h. $\chi\neq\chi_0$) mod 4 ist $\chi:\mathbb{Z}\to\mathbb{C}$, $\chi(n) = \begin{cases}1, & n\equiv 1(4),\\ -1, & n\equiv 3(4),\\ 0, & n \text{ gerade}.\end{cases}$
Der Hauptcharakter mod 4 ist $\chi_0(n) := \begin{cases}1, & 2\nmid n,\\ 0, & 2\mid n.\end{cases}$ Es gibt $\varphi(4)=2$ Charaktere mod 4.

24.4. **Satz:** Es gibt $\varphi(q)$ viele Dirichletcharaktere $\chi \bmod q$, wobei φ die Eulersche φ-Fkt. ist (d.h. $\varphi(q) := \#\{0 < a \le q;\ ggT(a,q) = 1\}$).

24.5. **Bem.:** • $q = 1 \Rightarrow \chi = \mathbb{1}$ (die Konstant-1-Fkt. auf $\mathbb{N}$). Haben ja $\varphi(1) = 1$.

• Behandeln im folgenden nur noch Dirichletcharaktere, schreiben dafür Charaktere (mod q).

Bew.: • Für $m \in (\mathbb{Z}/q\mathbb{Z})^*$ und ein χ mod q ist $\chi(m)$ eine $\varphi(q)$-te Einheitswurzel in $\mathbb{C}$, d.h. $\chi(m)^{\varphi(q)} = 1$, da $\varphi(q) = \#(\mathbb{Z}/q\mathbb{Z})^*$.

[Satz von Lagrange aus der Gruppentheorie $\rightsquigarrow$ G endl. $\Rightarrow \forall g \in G: g^{\#G} = e_G$ ($= $ neutr. El. in G).]

Damit existieren nur höchstens endlich viele Charaktere mod q.

• $\sum_{\chi(q)} \sum_{m(q)} \chi(m) = \sum_{m(q)} \chi_0(m) + \sum_{\chi \neq \chi_0} \sum_{m(q)} \chi(m) = \sum_{m(q)} \chi_0(m) = \varphi(q)$. (Alle Summen endlich!)
($\chi(q)$: durchläuft alle χ mod q; $\sum_{m(q)} \chi(m) = 0$ nach ONR 24.6.a)

• $\sum_{\chi(q)} \sum_{m(q)} \chi(m) = \sum_{\chi(q)} \chi(1) + \sum_{\chi(q)} \sum_{m \not\equiv 1(q)} \chi(m) \overset{\text{ONR } 24.6.b)}{=} \sum_{\chi(q)} 1$. (Summe $= 0$)

Also: $\sum_{\chi(q)} 1 = \varphi(q)$. □

Dabei haben wir bereits folgendes grundlegendes Ergebnis für Charaktere benutzt:

24.6. **Satz** (Orthogonalitätsrelationen / Kurz: ONR):

(a) **ONR 1. Art:** • $\sum_{n \bmod q} \chi(n) = \varphi(q)$, falls $\chi = \chi_0$, und $= 0$ sonst,

und • $\sum_{n \bmod q} \chi_1(n)\overline{\chi_2(n)} = \varphi(q)$ falls $\chi_1 = \chi_2$, und $= 0$ sonst.

(b) **ONR 2. Art:** • $\sum_{\chi \bmod q} \chi(n) = \varphi(q)$ falls $n \equiv 1 \bmod q$, und $= 0$ sonst,

und • $\sum_{\chi \bmod q} \chi(n_1)\overline{\chi(n_2)} = \varphi(q)$ falls $n_1 \equiv n_2 \bmod q$, und $= 0$ sonst.

Bew.: • Der 2. Teil der Aussage in (a) bzw. (b) folgt mit $\chi = \chi_1\bar{\chi}_2$ bzw. $n_1 n_2^{-1}$ aus dem 1. Teil.

• (a): $\chi = \chi_0$ klar, $\chi \neq \chi_0$: Betr. m mit $\chi(m) \neq 1$. Dann: $\sum_{n(q)} \chi(n) = \sum_{n(q)} \chi(nm) = \chi(m)\sum_{n(q)} \chi(n)$
$\Rightarrow \sum_{n(q)} \chi(n) = 0$ (nach Division durch $1 - \chi(m) \neq 0$).

• (b): $n \equiv 1\,(q)$ klar, $n \not\equiv 1\,(q)$: Betr. χ_1 mit $\chi_1(n) \neq 1$. Dann: $\sum_{\chi(q)} \chi(n) = \sum_{\chi(q)} \chi\chi_1(n) = \chi_1(n)\sum_{\chi(q)} \chi(n)$
$\Rightarrow \sum_{\chi(q)} \chi(n) = 0$ (nach Division durch $1 - \chi_1(n) \neq 0$). □

Wir halten noch weitere Grundeigenschaften der Charaktere fest.

24.7. **Satz:** (1) Die Charaktere χ mod q haben die Eigenschaften

(i) $|\chi(n)| = 1$ für $(n,q)=1$ und $\chi(n)=0$ für $(n,q)>1$,

(ii) χ ist vollständig multiplikativ, d.h. $\forall n,m \in \mathbb{Z}: \chi(nm) = \chi(n)\chi(m)$,

(iii) χ ist q-periodisch, d.h. $\forall n \in \mathbb{Z}: \chi(n+q) = \chi(n)$.

(2) Jede Funktion $f: \mathbb{Z} \to \mathbb{C}$ mit den Eigenschaften (ii), (iii) und $f(n)=0$ für $(n,q)>1$ und $f(n) \neq 0$ für $(n,q)=1$ ist ein Charakter mod q.

(3) Die Menge der Charaktere mod q wird durch $(\chi_1 \cdot \chi_2)(n) := \chi_1(n) \cdot \chi_2(n)$ zu einer abelschen Gruppe mit neutralem Element χ_0, und das Inverse zu χ ist $\overline{\chi}$ (mit $\overline{\chi}(n) := \overline{\chi(n)}$). Diese heißt Charaktergruppe mod q und ist isomorph zu $((\mathbb{Z}/q\mathbb{Z})^*, \cdot)$.

($\overline{\chi(n)}$: konjugiert komplexes)

Bew.: (1): (i) klar, da jede komplexe Einheitswurzel den Betrag 1 hat.

(ii) folgt aus der Fortsetzung auf die n mit $(n,q)>1$ durch den Wert 0.

(iii): Mit $n \in \mathbb{Z}$ liegt $n+q$ in derselben Restklasse mod q wie n, die Charakterwerte sind dann gleich.

(2): Sei f eine Fkt. wie angegeben. Dann wird durch $\xi(n+q\mathbb{Z}) := f(n)$, wo $(n,q)=1$, ein Homomorphismus auf $(\mathbb{Z}/q\mathbb{Z})^*$ definiert, und damit ein Charakter.

(3): Zur Struktur der Charaktergruppe im allgemeinen Fall:

Mit Charakteren χ_1, χ_2 ist auch $\chi_1 \cdot \chi_2$ ein solcher, klar. Auch, dass χ_0 neutrales Element ist. Mit χ ist auch $\overline{\chi}$ ein Charakter, und wegen $\chi(n) \cdot \overline{\chi(n)} = |\chi(n)|^2 = 1$ für jede komplexe Einheitswurzel ist $\overline{\chi}$ der inverse Charakter zu χ.

Zur Konstruktion des Isomorphismus von $X_q := \{\chi: \mathbb{Z} \to \mathbb{C};\ \chi \text{ char. mod } q\}$ nach $(\mathbb{Z}/q\mathbb{Z})^*$:

Sei $(\mathbb{Z}/q\mathbb{Z})^* \cong G_1 \times \dots \times G_r$ die Zerlegung in ein Produkt zyklischer Gruppen $G_1, \dots, G_r$ gemäß dem Hauptsatz über endliche abelsche Gruppen aus der Vorlesung Algebra.

Die erzeugende Elemente von $G_1, \dots, G_r$ seien $g_1, \dots, g_r$, und die Ordnungen seien $\#G_1 = m_1, \dots, \#G_r = m_r$.

Weiter seien $\eta_1, \dots, \eta_r$ primitive m_j-te Einheitswurzeln, etwa $\eta_j := e^{2\pi i/m_j}$, $1 \le j \le r$.

Jedes r-Tupel $(\omega_1, \dots, \omega_r)$ aus Einheitswurzeln ist schreibbar als $(\eta_1^{a_1}, \dots, \eta_r^{a_r})$, wo die $a_j \in \mathbb{Z}$ mit $0 \le a_j \le m_j - 1$, $1 \le j \le r$.

Dann wird durch $a \cong (g_1^{a_1}, \dots, g_r^{a_r}) \mapsto \xi \cong (\eta_1^{a_1}, \dots, \eta_r^{a_r})$ ein Isomorphismus zwischen $(\mathbb{Z}/q\mathbb{Z})^*$ und X_q definiert. □

24.8. Bsp.: $q=5$. Dann ist $(\mathbb{Z}/5\mathbb{Z})^*$ zyklisch, und $b=2$ ist Primitivwurzel, weil $1\equiv 2^0$, $2\equiv 2^1$, $3\equiv 2^3$, $4\equiv 2^2 \bmod 5$. Weiter ist $\eta = e^{2\pi i/4} = i$ primitive 4-te EW: $\eta = i$ erzeugt alle 4-ten EWn: $\eta^0=1$, $\eta^1=i$, $\eta^2=-1$, $\eta^3=-i$.
Die 4 Charaktere mod 5 entstehen, dass man $b=2$ die vier möglichen η-Potenzen zuordnet.
Die Charaktertafel (nur für $(a,5)=1$ angegeben) lautet damit

	$a=1$	$a=2$	$a=3$	$a=4$
$\chi_0 : (2\mapsto 1)$	1	1	1	1
$\chi_1 : (2\mapsto i)$	1	i	$-i$	-1
$\chi_2 : (2\mapsto -1)$	1	-1	-1	1
$\chi_3 : (2\mapsto -i)$	1	$-i$	i	-1

24.9. Bsp.: $q=12$. Mit $12=2^2\cdot 3$ ist $(\mathbb{Z}/12\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$. Dann ist $b_1=3$ Primitivwurzel mod 4, $b_2=2$ Primitivwurzel mod 3. Für die 4 El. von $(\mathbb{Z}/12\mathbb{Z})^*$ ist dann

$a=1 \hat{=} (3^0, 2^0)$, $a=5 \hat{=} (3^0, 2^1)$, $a=7 \hat{=} (3^1, 2^0)$, $a=11 \hat{=} (3^1, 2^1)$ in $(\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$.
($1\equiv 3^0 (4), 1\equiv 2^0 (3)$; $5\equiv 3^0 (4), 5\equiv 2^1 (3)$; $7\equiv 3^1 (4), 7\equiv 2^0 (3)$; $11\equiv 3^1 (4), 11\equiv 2^1 (3)$)

Die primitiven 2-ten Einheitswurzeln sind $\eta_1=-1$ und $\eta_2=-1$. Die Charaktertafel lautet dann

	$a=1$	$a=5$	$a=7$	$a=11$
$\chi_0 : (2,3)\mapsto(1,1)$	1	1	1	1
$\chi_1 : (2,3)\mapsto(1,-1)$	1	-1	1	-1
$\chi_2 : (2,3)\mapsto(-1,1)$	1	1	-1	-1
$\chi_3 : (2,3)\mapsto(-1,-1)$	1	-1	-1	1

Die Charaktere mod 12 sind also alle reellwertig. Reelle Charaktere sind solche, deren Bild reell ist, d.h. also nur Werte $\in\{1,-1,0\}$ besitzen. Sie werden später noch eine besondere Rolle spielen.

24.10. Bsp.: $q=p>2$ eine ungerade Primzahl. Dann wird das Legendresymbol $\left(\frac{\cdot}{p}\right)$ (bekannt aus elementarer ZT / Algebra / algebraischer ZT) durch die Fortsetzung $\left(\frac{a}{p}\right) := 0$ für a mit $p|a$ zu einem Charakter mod p. Dieser ist neben dem Hauptcharakter der einzige reelle Charakter mod p, denn die einzigen reellen $(p-1)$-ten EW sind $\eta=\pm 1$.

24.11. Bem.: Es wird im folgenden i.a. nicht darauf ankommen, die Werte der Charaktere im einzelnen zu kennen. Vielmehr sind die ONRen wichtig, die man in den Tafeln daran erkennt, dass die einzelnen Zeilen- und Spaltensummen (außer der ersten) Null ergeben.