Gruppencharaktere

Lukas-Fabian Moser, SS 2013

Definition. Ist G eine endliche abelsche Gruppe, so ist ein *Charakter von G* ein Gruppenhomomorphismus $G \to \mathbb{C}^\times$. Ist m eine ganze Zahl, so ist ein *Charakter modulo m* ein Charakter von $(\mathbb{Z}/m\mathbb{Z})^\times$, also ein Gruppenhomomorphismus $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$.

Der „triviale“ Charakter, der also jedes Element der Gruppe auf $1 \in \mathbb{C}$ abbildet, heißt *Hauptcharakter*. Die Menge der Charaktere von G, notiert als $\widehat{G}$, bildet eine Gruppe mit der Verknüpfung, die durch punktweise Multiplikation gegeben ist, also $(\chi_1 \cdot \chi_2)(g) := \chi_1(g) \cdot \chi_2(g)$. In dieser sogenannten *Charaktergruppe* ist der Hauptcharakter das neutrale Element.

Proposition. *Die Charaktere modulo m entsprechen eineindeutig den zahlentheoretischen Funktionen $\chi : \mathbb{N} \to \mathbb{C}$ mit folgenden Eigenschaften:*

i) $\chi(a) = \chi(b)$, *falls* $a \equiv b \pmod{m}$.

ii) χ *ist vollständig multiplikativ.*

iii) $\chi(a) = 0$, *falls* $\mathrm{ggT}(a, m) \neq 1$.

iv) $\chi(a) \neq 0$, *falls* $\mathrm{ggT}(a, m) = 1$.

Häufig werden auch solche zahlentheoretischen Funktionen einfach als Charaktere modulo m bezeichnet.

Beweis. Ist eine Funktion $\chi : \mathbb{N} \to \mathbb{C}$ gegeben, so definiert χ wegen i) eine wohldefinierte Abbildung $\mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ (durch $[a] \mapsto \chi(a)$), deren Einschränkung auf die Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ wegen iv) nur Werte in $\mathbb{C}^\times$ annimmt und wegen ii) ein Gruppenhomomorphismus ist.

Ist umgekehrt $\varphi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ ein Gruppenhomomorphismus, so definieren wir eine Abbildung $\chi : \mathbb{N} \to \mathbb{C}$ durch die Vorschrift

$$\chi(a) := \begin{cases} 0 & \text{falls } \mathrm{ggT}(a, m) \neq 1, \\ \varphi([a]) & \text{falls } \mathrm{ggT}(a, m) = 1. \end{cases}$$

Dies ist eine wohldefinierte Abbildung, weil $[a] \in \mathbb{Z}/m\mathbb{Z}$ genau dann in $(\mathbb{Z}/m\mathbb{Z})^\times$ liegt, wenn $\mathrm{ggT}(a, m) = 1$ ist. Dann sind i), iii) und iv) nach Definition erfüllt; die vollständige Multiplikativität sieht man so: Sind a und b beide teilerfremd zu m, so auch ihr Produkt ab, und dann folgt $\chi(ab) = \varphi([ab]) = \varphi([a]) \cdot \varphi([b]) = \chi(a) \cdot \chi(b)$, weil χ ein Gruppenhomomorphismus ist. Besitzt dagegen a oder b einen gemeinsamen Teiler mit m, so auch ab, und damit verschwinden sowohl $\chi(ab)$ als auch $\chi(a) \cdot \chi(b)$.

Außerdem sind die konstruierten Zuordnungen beider Klassen von Abbildungen zueinander invers (!), woraus die Behauptung folgt. □

Der Satz ist Spezialfall des folgenden allgemeinen Satzes (angewandt für $G = (\mathbb{Z}/m\mathbb{Z})^\times$):

Satz. *Es ist* $\left|\widehat{G}\right| = |G|$*, die Gruppe* G *hat also ebensoviele Charaktere wie Elemente.*

Folgerung. *Die Anzahl der Charaktere modulo* m *ist genau* $\varphi(m)$*.*

Beweis des Satzes. Wir argumenieren in zwei Schritten:

i) Ist G sogar *zyklisch* von der Ordnung n, so entsprechen (laut einem Resultat der Algebravorlesung) die Homomorphismen $G \to \mathbb{C}^\times$ genau den Elementen von $\mathbb{C}^\times$, deren Ordnung ein Teiler von n ist (indem nämlich, nach Wahl eines Erzeugers $g \in G$ mit $G = \langle g \rangle$, ein Homomorphismus $\varphi : G \to \mathbb{C}^\times$ vollständig beschrieben ist durch das Bild $\varphi(g)$, und dessen Ordnung ist ein Teiler von n wegen $\varphi(g)^n = \varphi(g^n) = \varphi(e_G) = 1$). Dies sind aber genau die Lösungen der Gleichung $x^n = 1$ in $\mathbb{C}^\times$, also die n-ten Einheitswurzeln, von denen es genau n Stück gibt.

ii) Im allgemeinen Fall ist G nach dem Satz über die Struktur endlicher abelscher Gruppen isomorph zu einem Produkt zyklischer Gruppen:

$$G \cong G_1 \times \ldots \times G_n$$

mit endlichen zyklischen Gruppen G_i der Ordnung n_i. Wegen $|G| = g_1 \cdot \ldots \cdot g_n$ genügt es nun zu zeigen, daß die Anzahl der Homomorphismen $\left|\widehat{G}\right| = \prod_{i=1}^n \widehat{G_i}$ ist. Um das zu beweisen, genügt es (mittels eines induktiven Arguments), den Fall $n = 2$ zu betrachten, und dann hilft das nächste Lemma.

□

Lemma. *Sind* G_1, G_2, H *abelsche Gruppen, so entsprechen die Homomorphismen* $G_1 \times G_2 \to H$ *eineindeutig den Paaren von Homomorphismen* $G_1 \to H$ *und* $G_2 \to H$*.*

Beweis. In formaler Notation suchen wir eine bijektive Zuordnung zwischen den Mengen

$$\mathrm{Hom}(G_1 \times G_2, H) \quad \text{und} \quad \mathrm{Hom}(G_1, H) \times \mathrm{Hom}(G_2, H).$$

Ist $\varphi : G_1 \times G_2 \to H$ gegeben, so definieren wir $\varphi_1 : G_1 \to H$ durch $\varphi_1(g_1) := \varphi(g_1, e_{G_2})$ und $\varphi_2 : G_2 \to H$ durch $\varphi_2(g_2) := \varphi(e_{G_1}, g_2)$. Beides sind, wie man mühelos nachrechnen kann, Homomorphismen.

Sind umgekehrt $\varphi_1 : G_1 \to H$ und $\varphi_2 : G_2 \to H$ gegeben, so definieren wir $\varphi : G_1 \times G_2 \to H$ durch $\varphi(g_1, g_2) := \varphi_1(g_1) \cdot \varphi_2(g_2)$. Daß dies wieder ein Homomorphismus ist, ist mühelos nachzurechnen (wobei die Kommutativität von H wesentlich ist).

Beide Zuordnungen sind zueinander invers: Sind nämlich φ_1, φ_2 gegeben und φ definiert wie oben angegeben, so ist $\varphi(g_1, e_{G_2}) = \varphi_1(g_1) \cdot \varphi_2(e_{G_2}) = \varphi_1(g_1)$ und ebenso $\varphi(e_{G_1}, g_2) = \ldots = \varphi_2(g_2)$, wie behauptet. Ist umgekehrt φ gegeben und φ_1, φ_2 definiert wie ganz oben,[1], so gilt

$$\varphi_1(g_1) \cdot \varphi_2(g_2) = \varphi(g_1, e_{G_2}) \cdot \varphi(e_{G_1}, g_2) = \varphi((g_1, e_{G_2}) \cdot (e_{G_1}, g_2)) = \varphi(g_1, g_2),$$

was zu beweisen war. □

[1] Gleichung numerieren!

0.1 Satz (Orthogonalitätsrelationen)**.** *Es sei G eine endliche abelsche Gruppe.*

i) Für jeden Charakter χ von G gilt

$$\sum_{g\in G}\chi(g)=\begin{cases}|G| & \text{falls } \chi \text{ der Hauptcharakter ist,}\\ 0 & \text{sonst.}\end{cases}$$

ii) Für jedes Element $g\in G$ gilt

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

Beweis.

i) Ist χ der Hauptcharakter, so ist die Aussage klar wegen $\sum_{g\in G}1=|G|$. Andernfalls gibt es ein g_0 mit $\chi(g_0)\neq 1$. Aber es ist

$$\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(g_0\cdot g)=\chi(g_0)\cdot\sum_{g\in G}\chi(g),$$

da auch $g_0\cdot g$ für laufendes g alle Elemente von G durchläuft. Wegen $\chi(g_0)\neq 1$ muß dann die Summe verschwinden.

ii) Ist $g=e_G$, so ist die Aussage wiederum klar wegen $\chi(e_G)=1$ für jeden Charakter. Andernfalls gibt es nach dem nächsten Lemma einen Charakter χ_0 mit $\chi_0(g)\neq 1$. Nun gilt

$$\sum_{\chi\in\widehat{G}}\chi(g)=\sum_{\chi\in\widehat{G}}(\chi_0\cdot\chi)(g)=\chi_0(g)\cdot\sum_{\chi\in\widehat{G}}\chi(g),$$

da auch $\chi_0\cdot\chi$ mit laufendem χ alle Elemente der Charaktergruppe $\widehat{G}$ durchläuft. Wie im letzten Beweis muß dann aber wegen $\chi_0(g)\neq 1$ die Summe verschwinden.

□

Lemma. *Ist G eine endliche abelsche Gruppe, und ist $g\in G$ nicht das neutrale Element, so gibt es einen Charakter χ von G mit $\chi(g)\neq 1$.*

Beweis. Es sei $H=\langle g\rangle$ die von g erzeugte Untergruppe von G. Wir zählen die Charaktere von G und von G/H und betrachten das zu die „Einschränkungsabbildung“

$$r:\widehat{G/H}=\{\text{Charaktere von } G/H\}\to\{\text{Charaktere von } G\}=\widehat{G},$$

die aus einem Charakter $\chi: G/H\to\mathbb{C}^\times$ den Charakter $g\mapsto\chi([g])$ von G macht (also die komponierte Abbildung $G\to G/H\xrightarrow{\chi}\mathbb{C}^\times$).

Die Abbildung r ist injektiv (formal deswegen, weil die Projektion $G \to G/H$ surjektiv ist). Hat nun g die Eigenschaft, daß für jeden Charakter χ gilt $\chi(g) = 1$, so gilt auch $\chi(H) = 1$, so daß χ nach dem Homomorphiesatz einen Homomorphismus $G/H \to \mathbb{C}^\times$ definiert. In diesem Fall ist die Abbildung r also surjektiv und damit insgesamt bijektiv. Damit folgt aber $\left|\widehat{G/H}\right| = \left|\widehat{G}\right|$, also nach dem Satz über die Anzahl der Charaktere $|G/H| = |G|$, und das bedeutet $|H| = 1$, d.h. $g = e_G$. $\square$