# Kapitel 2

# Algebra

## 2.1 Darstellung endlicher Gruppen

Wir setzen eine gewisse Vertrautheit mit der elementaren Gruppentheorie voraus. Sei $G$ eine endliche Gruppe. Wir schreiben alle Gruppen multiplikativ. 1 ist das Einselement, $|G|$ die Ordnung, d.h. die Anzahl der Elemente, von $G$.

**Beispiele:**

**1)** Die zyklische Gruppe $C_n$ der Ordnung $n$. Sie wird erzeugt von einem Element $q$ mit $q^n = 1$, so daß also $C_n = \{1, q, \ldots, q^{n-1}\}$. $C_n$ ist abelsch.

**2)** Die Gruppe $S_n$ der Permutationen von $n$ Elementen. Sie hat die Ordnung $n!$ und ist nicht abelsch. $S_n$ heißt die symmetrische Gruppe. Eine Permutation kann gerade oder ungerade sein. Die Untergruppe $A_n$ der geraden Permutationen heißt alternierende Gruppe.

**3)** Die Diedergruppe $D_n$. Sie wird erzeugt von Rotationen $r$ um den Winkel $2\pi/n$ und durch eine Spiegelung $s$ an einer Geraden. Sie besteht also aus den Elementen $1, r, \ldots, r^{n-1}$, $s$, $sr, \ldots, sr^{n-1}$ und hat also die Ordnung $2n$. Es ist $r^n = 1$, $s^2 = 1$. $D_n$ ist nur für $n = 1, 2$ abelsch.

**Definition 2.1.1** *Sei $G$ eine endliche Gruppe und $V$ ein $d$-dimensionaler Vektorraum über $\mathbb{C}$. $GL(V)$ sei die Gruppe der linearen invertierbaren Abbildungen $V \to V$.*

Ein Homomorphismus $\rho : G \to GL(V)$ heißt Darstellung von $G$ in $V$. Ist $\rho$ injektiv, so heißt die Darstellung treu. $d$ heißt der Grad von $\rho$. Zwei Darstellungen $\rho$, $\rho'$ von $G$ in $V$ bzw. $V'$ heißen äquivalent, wenn es eine lineare invertierbare Abbildung $\tau : V \to V'$ gibt, so daß $\rho' = \tau\rho\tau^{-1}$.

**Beispiele:**

**1)** $\rho(s) = 1$ für alle $s$ heißt Einheitsdarstellung.

**2)** Die reguläre Darstellung $\rho_{\text{reg}}$ wird wie folgt definiert. Sei $\{e_t : t \in G\}$ eine Basis von $V$. Dann setzt man

$$\rho_{\text{reg}}(s)e_t = e_{st}$$

(linksreguläre Darstellung). Es ist also

$$\begin{aligned}\rho_{\text{reg}}(s)\sum_{t\in G} x_t e_t &= \sum_{t\in G} x_t \rho_{\text{reg}}(s) e_t \\ &= \sum_{t\in G} x_t e_{st} \\ &= \sum_{t\in G} x_{s^{-1}t} e_t \ .\end{aligned}$$

$\rho_{\text{reg}}$ übt also auf die Komponenten $x_t$ die Permutation $t \to s^{-1}t$ aus. Der Grad von $\rho_{\text{reg}}$ ist $|G|$. $\rho_{\text{reg}}$ ist treu.

**3)** Sei $G = C_n = \{1, q, \ldots, q^{n-1}\}$ und $\omega$ eine $n$-te Einheitswurzel, also $\omega^n = 1$. Dann ist

$$\rho(q^k) = \omega^k \quad , \quad k = 0, 1, \ldots, n-1$$

eine Darstellung von $C_n$ in $\mathbb{C}$, der Grad also 1. $\rho$ ist genau dann treu, wenn $\omega$ eine primitive $n$-te Einheitswurzel ist, d.h. wenn $\omega^m \neq 1$ für $0 < m < n$. Sind $\omega_1$, $\omega_2$ verschiedene $n$-te Einheitswurzeln, so sind die zugehörigen Darstellungen nicht äquivalent.

Wir berechnen die reguläre Darstellung von $C_n$. Mit $e_k = e_{q^k}$, $x_k = x_{q^k}$ haben wir

$$\rho_{\text{reg}}(s^\ell) \sum_{k=0}^{n-1} x_k e_k = \sum_{k=0}^{n-1} x_{k-\ell} e_k \ , \qquad \ell = 0, \ldots, n-1 \ ,$$

wobei $k - \ell$ modulo $n$ genommen wird.

**4)** Sei $G = S_n$. Die alternierende Darstellung

$$\rho_{\text{alt}}(\pi) = \begin{cases} \phantom{-}1 & , \ \pi \text{ gerade }, \\ -1 & , \ \pi \text{ ungerade} \end{cases}$$

ist vom Grad 1 und für $n > 2$ nicht treu. Die natürliche Darstellung von $S_n$ ist wie folgt definiert. Seien $e_1, \ldots, e_n$ die Einheitsvektoren in $\mathbb{C}$ und $v = \sum_{i=1}^n x_i e_i$. Dann ist

$$\rho_{\text{nat}}(\pi) v = \sum_{i=1}^{n} x_i e_{\pi(i)} \ .$$

Der Grad von $\rho_{\text{nat}}$ ist $n$, und $\rho_{\text{nat}}$ ist treu.

**5)** Sei $G = D_n$ und $n$ gerade. Für $D_n$ haben wir 5 verschiedene Typen von Darstellungen

| | $\rho(r^k)$ | $\rho(sr^k)$ | Grad($\rho$) | Bemerkungen |
|---|---|---|---|---|
| $\rho_1$ | 1 | 1 | 1 | Einheitsdarstellung |
| $\rho_2$ | 1 | $-1$ | 1 | |
| $\rho_3$ | $(-1)^k$ | $(-1)^k$ | 1 | |
| $\rho_4$ | $(-1)^k$ | $(-1^{k+1}$ | 1 | |
| $\rho_5^h$ | $\begin{pmatrix} \omega^{hk} & 0 \\ 0 & \omega^{-hk} \end{pmatrix}$ | $\begin{pmatrix} 0 & \omega^{-hk} \\ \omega^{hk} & 0 \end{pmatrix}$ | 2 | $\omega = e^{2\pi i/n}$ , $h = 1, \ldots, \frac{n}{2} - 1$ . |

Die Beschränkung auf $h < \frac{n}{2}$ ist sinnvoll, weil $\rho_5^h$, $\rho_5^{n-h}$ äquivalent sind. Wegen $\omega_n = 1$ ist nämlich

$$\begin{aligned}
\rho_5^{n-h}(r^k) &= \begin{pmatrix} \omega^{(n-h)k} & 0 \\ 0 & \omega^{-(n-h)k} \end{pmatrix} = \begin{pmatrix} \omega^{-hk} & 0 \\ 0 & \omega^{hk} \end{pmatrix} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \omega^{hk} & 0 \\ 0 & \omega^{-hk} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
&= \tau \rho_5^h(r^k) \tau^{-1} , \\
\rho_5^{n-h}(sr^k) &= \begin{pmatrix} 0 & \omega^{(n-h)k} \\ \omega^{-(n-h)k} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \omega^{-hk} \\ \omega^{hk} & 0 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \omega^{hk} \\ \omega^{-hk} & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
&= \tau \rho_5^h(sr^k) \tau_{-1}
\end{aligned}$$

für alle $k$ mit der nichtsingulären Matrix $T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

**Definition 2.1.2** *Eine Darstellung $\rho$ von $G$ in $V$ heißt reduzibel, wenn es einen echten Unterraum $V_1$ von $V$ gibt mit $\rho(s)V_1 \subseteq V_1$ für alle $s \in G$. $V_1$ heißt dann invarianter Unterraum von $\rho$.*

*Ist $\rho$ nicht reduzibel, so nennt man $\rho$ irreduzibel.*

**Beispiele:**

**1)** Die Einheitsdarstellung ist für $d > 1$ reduzibel. Darstellungen vom Grad 1 sind stets irreduzibel.

**2)** $\rho_{\text{reg}}$ ist für $|G| > 1$ reduzibel, denn $(1, \ldots, 1)$ spannt einen echten invarianten Unterraum auf.

**Satz 2.1.3** *Sei $V = V_1 \oplus \ldots \oplus V_r$, und seien $\rho_i$ Darstellungen von $G$ in $V_i$. Dann ist*

$$\rho(s)v = \sum_{i=1}^{r} \rho_i(s)v_i \quad \textit{für} \quad v = \sum_{i=1}^{r} v_i \, , \quad v_i \in V_i$$

*eine Darstellung von $G$ in $V$ mit den invarianten Unterräumen $V_i$.*

**Beweis:** Natürlich ist $\rho : G \to GL(V)$ ein Homomorphismus. Ist $v \in V_i$, so ist auch $\rho(s)v \in V_i$.

□

**Definition 2.1.4** *Die Darstellung $\rho$ aus Satz 2.1.3 heißt direkte Summe von $\rho_1, \ldots, \rho_r$. Man schreibt $\rho = \rho_1 + \ldots + \rho_r$.*

Wir wollen nun Darstellungen durch Matrizen beschreiben. Sei $v_1, \ldots, v_d$ eine Basis von $V$. $\rho(s)$ wird dann beschrieben durch eine $(d,d)$-Matrix $R(s)$, d.h.

$$\rho(s)v = \sum_{i=1}^{d} y_i v_i \quad \text{für} \quad v = \sum_{i=1}^{d} x_i v_i$$

mit $y = R(s)x$. Natürlich gilt $R(st) = R(s)R(t)$. $R$ ist nichts anderes als eine Darstellung von $G$ in $\mathbb{C}^d$.

Sei nun $V_1$ invarianter Unterraum von $\rho$ der Dimension $m$ mit Basis $v_1, \ldots, v_m$. Dann hat $R$ die Gestalt

$$R(s) = \begin{pmatrix} R_{11}(s) & R_{12}(s) \\ 0 & R_{22}(s) \end{pmatrix}$$

mit einer $(m,m)$-Matrix $R_{11}(s)$ und einer $(d-m, d-m)$-Matrix $R_{22}(s)$. Ist $R_{12} = 0$, so ist $\rho = \rho_1 + \rho_2$ mit den durch $R_{11}$, $R_{22}$ beschriebenen Darstellungen $\rho_1$, $\rho_2$. Sind allgemeiner $\rho_1, \ldots, \rho_r$ Darstellungen von $G$ in $V_1, \ldots, V_r$, welche von den Matrizen $R_1, \ldots, R_r$ beschrieben werden, so wird $\rho = \rho_1 + \ldots + \rho_r$ durch die Matrix

$$R = \begin{pmatrix} R_1 & & 0 \\ & \ddots & \\ 0 & & R_r \end{pmatrix}$$

beschrieben.

**Satz 2.1.5** *Sei $\rho$ eine Darstellung von $G$ in $V$. Dann gibt es ein Skalarprodukt in $V$, bezüglich dem $\rho$ unitär ist.*

**Beweis:** Sei $( \, , \, )$ irgendein Skalarprodukt in $V$, und sei

$$\langle u, v\rangle = \frac{1}{|G|} \sum_{s\in G} (\rho(s)u, \rho(s)v) \; .$$

Dann ist auch $\langle \, , \, \rangle$ ein Skalarprodukt in $V$, und es gilt

$$\begin{aligned}
\langle \rho(t)u, \rho(t)v\rangle &= \frac{1}{|G|} \sum_{s\in G} \langle \rho(s)\rho(t)u, \rho(s)\rho(t)v\rangle \\
&= \frac{1}{|G|} \sum_{s\in G} \langle \rho(st)u, \rho(st)v\rangle \\
&= \frac{1}{|G|} \sum_{s\in G} \langle \rho(s)u, \rho(s)v\rangle \\
&= \langle u, v\rangle \; .
\end{aligned}$$

Also ist $\rho$ bezüglich $\langle \, , \, \rangle$ unitär.

□

**Satz 2.1.6** *Jede Darstellung einer Gruppe ist eine direkte Summe irreduzibler Darstellungen dieser Gruppe.*

**Beweis:** Sei $\rho$ eine Darstellung von $G$ in $V$. Ohne Beschränkung der Allgemeinheit können wir annehmen, daß $\rho$ bezüglich eines Skalarprodukts $\langle \, , \, \rangle$ in $V$ unitär ist. Ist $\rho$ irreduzibel, sind wir fertig. Andernfalls besitzt $\rho$ einen invarianten Unterraum $V_1 \neq \{0\}, \neq V$. Sei $V_2$ das orthogonale Komplement von $V_1$ in $V$ bezüglich des Skalarprodukts $\langle \, , \, \rangle$. Wir zeigen, daß auch $V_2$ invarianter Unterraum von $\rho$ ist. Sei dazu $v \in V_2$. Für jedes $u \in V_1$ ist

$$\begin{aligned}
\langle \rho(s)v, u\rangle &= \langle \rho(s)v, \rho(s)\rho(s^{-1})u\rangle = \langle v, \rho(s^{-1})u\rangle \\
&= 0 \; ,
\end{aligned}$$

denn mit $u$ ist auch $\rho(s^{-1})u \in V_1$. Also ist $\rho(s)v \in V_2$. Es sind also $V_1$, $V_2$ invariante Unterräume von $\rho$, und es ist $V = V_1 \oplus V_2$. Die Restriktionen

$\rho_1$, $\rho_2$ von $\rho$ auf $V_1$, $V_2$ sind Darstellungen von $\rho$ in $V_1$, $V_2$, und es gilt $\rho = \rho_1 + \rho$. $\rho_1$, $\rho_2$ haben kleineren Grad als $\rho$.

Sind $\rho_1$, $\rho_2$ irreduzibel, so sind wir fertig. Andernfalls zerfallen $\rho_1$, $\rho_2$ ihrerseits in Darstellungen noch kleineren Grades. Durch Fortführen dieses Prozesses kommt man nach endlich vielen Schritten bei irreduziblen Darstellungen an.

□

**Definition 2.1.7** *Das Zerlegen einer Darstellung in irreduzible Darstellungen nach Satz 2.1.6 nennt man Ausreduzieren der Darstellung.*

**Beispiel:**

Ausreduzieren der regulären Darstellung $\rho_{\mathrm{reg}}$ von $C_n$. Bezüglich der Basis $e_0, \ldots, e_{n-1}$ in $V = \mathbb{C}^n$ gilt

$$\rho_{\mathrm{reg}}(s^\ell) \sum_{k=0}^{n-1} x_k e_k = \sum_{k=0}^{n-1} x_{k-\ell} e_k \ , \quad \ell = 0, \ldots, n-1 \ ,$$

wobei $k - \ell$ modulo $n$ zu verstehen ist. Sei $\omega_j$ eine $n$-te Einheitswurzel und $x^j = (1, \omega_j, \ldots, \omega_j^{n-1})$. Dann ist

$$\begin{aligned} \rho_{\mathrm{reg}}(s^\ell) x^j &= \sum_{k=0}^{n-1} \omega_j^{k-\ell} e_k = \omega_j^{-\ell} \sum_{k=0}^{n-1} \omega_j^k e_k \\ &= \omega_j^\ell x \ . \end{aligned}$$

Also ist $V_j = sp\langle x^j \rangle$ invarianter Unterraum von $\rho$, und $\rho_j(s^\ell) = \omega_j^\ell$ Darstellung von $C_n$ in $V_j$. Für $\omega_j = e^{2\pi i j/n}$, $j = 0, \ldots, n-1$ gilt $V = V_0 \oplus \ldots \oplus V_{n-1}$, weil $x^0, \ldots, x^{n-1}$ linear unabhängig sind (Van der Mond'sche Determinante). Also $\rho = \rho + \ldots + \rho_{n-1}$.

**Satz 2.1.8** *(Lemma von Schur) Seien $\rho_i$ irreduzible Darstellungen einer Gruppe in $V_i$, $i = 1, 2$. Sei $\tau : V_1 \to V_2$ linear. Es gelte $\tau\rho_1 = \rho_2\tau$. Dann gilt:*

*(i) Sind $\rho_1$, $\rho_2$ nicht äquivalent, so ist $\tau = 0$.*

*(ii) Ist $\rho_1 = \rho_2$, so ist $\tau = \lambda$ mit $\lambda \in \mathbb{C}$.*

**Beweis:**

**(i)** Wir zeigen zunächst, daß $W_1 = \tau^{-1}(0)$ invarianter Unterraum von $\rho_1$ ist. Ist nämlich $x \in W_1$, so ist auch $\tau\rho_1(s)x = \rho_2(s)\tau x = 0$.

Da $\rho_1$ irreduzibel ist, ist also entweder $W_1 = \{0\}$ oder $W_1 = V_1$. Im letzteren Fall sind wir fertig. Im ersten Fall ist $\tau$ injektiv. Wir zeigen, daß $W_2 = \tau V_1$ invarianter Unterraum von $\rho_2$ ist. Für $y \in W_2$ ist nämlich $\rho_2(s)y = \rho_2(s)\tau x = \tau\rho_1(s)x \in W_2$. Da $\rho_2$ irreduzibel ist, ist entweder $W_2 = \{0\}$ oder $W_2 = V_2$. Im ersten Fall ist $\tau = 0$, und wir sind fertig. Im zweiten Fall ist $\tau$ surjektiv. Da $\tau$ auch injektiv ist, ist $\tau$ bijektiv, und das ist nicht möglich, da $\rho_1$, $\rho_2$ nicht äquivalent sind.

**(ii)** Für $\rho_1 = \rho_2$ ist $V_1 = V_2 = V$ und $\tau : V \to V$ hat mindestens einen Eigenwert $\lambda$ und Eigenvektor $x$ zu $\lambda$, also $\tau x = \lambda x$, $x \neq 0$. Sei $\tau' = \tau - \lambda$ und $W_1' = \tau'^{-1}(0)$. $W_1'$ ist invarianter Unterraum von $\rho$. Ist nämlich $v \in W_1'$, so ist $\tau'\rho(s)v = (\tau - \lambda)\rho(s)v = \rho(s)(\tau - \lambda)v = \rho(s)\tau' v = 0$. Also ist wieder entweder $W_1' = \{0\}$ oder $W_1' = V$. Das erste ist nicht möglich, weil $x \in W_1'$. Also muß $W_1' = V$ und damit $\tau v = \lambda v$ sein für alle $v \in B$. Also $\tau = \lambda$.

$\square$

**Satz 2.1.9** *Seien $\rho_1$, $\rho_2$ irreduzible Darstellungen von $G$ in $V_1$, $V_2$, und sei $\tau : V_1 \to V_2$ eine lineare Abbildung. Sei*

$$\tau' = \frac{1}{|G|} \sum_{t \in G} \rho_2(t^{-1})\tau\rho_1(t) .$$

*Dann gilt:*

*(i) Sind $\rho_1$, $\rho_2$ nicht äquivalent, so ist $\tau' = 0$.*

*(ii) Ist $\rho_1 = \rho_2$, so ist $\tau' = d^{-1}$ Spur $(\tau)$ mit dem Grad $d$ von $\rho_1$.*

**Beweis:** Für jedes $s \in G$ ist

$$\begin{aligned}
\rho_2(s)\tau' &= \frac{1}{|G|} \sum_{t \in G} \rho_2(s)\rho_2(t^{-1})\tau\rho_1(t) \\
&= \frac{1}{|G|} \sum_{t \in G} \rho_2(st^{-1})\tau\rho_1(t) \\
&= \frac{1}{|G|} \sum_{t \in G} \rho_2(t^{-1})\tau\rho_1(ts) \\
&= \frac{1}{|G|} \sum_{t \in G} \rho_2(t^{-1})\tau\rho_1(t)\rho_1(s) \\
&= \tau'\rho_1(s) \, .
\end{aligned}$$

Sind also $\rho_1$, $\rho_2$ nicht äquivalent, so ist nach dem Lemma von Schur $\tau' = 0$. Ist $\rho_1 = \rho_2 = \rho$, so folgt ebenfalls nach dem Lemma von Schur $\tau' = \lambda$. Also gilt

$$\lambda = \frac{1}{|G|} \sum_{t \in G} \rho(t^{-1})\tau\rho(t) \, .$$

Berechnen wir auf beiden Seiten die Spur, so folgt

$$\begin{aligned}
\lambda d &= \frac{1}{|G|} \sum_{t \in G} \text{Spur } (\rho(t^{-1})\tau\rho(t)) \\
&= \frac{1}{|G|} \sum_{t \in G} \text{Spur } ((\rho(t)^{-1}\tau\rho(t)) \\
&= \frac{1}{|G|} \sum_{t \in G} \text{Spur } (\tau) \\
&= \text{Spur } (\tau) \, .
\end{aligned}$$

**Satz 2.1.10** *(Orthogonalitätsrelationen) Seien $\rho_1$, $\rho_2$ irreduzible Darstellungen von $G$ in $V_1$, $V_2$, und seien $\rho_1$, $\rho_2$ bezüglich bestimmter Basen in $V_1$, $V_2$ durch die Matrizen $R^1$, $R^2$ beschrieben. Dann gilt:*

*(i) Sind $\rho_1$, $\rho_2$ nicht äquivalent, so ist für alle $i$, $j$, $\ell$, $k$*

$$\frac{1}{|G|}\sum_{t\in G} R^2_{i\ell}(t^{-1})R^1_{kj}(t) = 0$$

*(ii) Ist $\rho_1 = \rho_2$, so gilt mit $d = Grad\ (\rho_1)$*

$$\frac{1}{|G|}\sum_{t\in G} R^2_{i\ell}(t^{-1})R^1_{kj}(t) = \begin{cases} 1/d & \textit{falls } i=j \textit{ und } \ell = k\ , \\ 0 & , \textit{ sonst}\ . \end{cases}$$

**Beweis:** Sei $T$ die $(d_2, d_1)$-Matrix ($d_i =$ Grad $(\rho_i)$)

$$T_{mn} = \begin{cases} 1 & , \ m = \ell \text{ und } n = k\ , \\ 0 & , \ \text{sonst}\ . \end{cases}$$

Sei $\tau$ die lineare Abbildung von $V_1$, $V_2$, die bezüglich der gewählten Basen in $V_1$, $V_2$ die Matrix $T$ hat. Dann hat die lineare Abbildung $\tau'$ aus Satz 2.1.9 bezüglich dieser Basen die Matrix $T'$ mit

$$T'_{ij} = \frac{1}{|G|}\sum_{t\in G} R^2_{i\ell}(^{-1})R^1_{kj}(t)\ .$$

Sind $\rho_1$, $\rho_2$ nicht äquivalent, so ist nach Satz 2.1.9 $T' = 0$ und damit (i) bewiesen. Für $\rho_1 = \rho_2$ ist nach Satz 2.1.9 $T' = d^{-1}\delta_{\ell k}$, und daraus folgt (ii).

□

**Beispiel:** $G = C_n$. Seien $\omega_1$, $\omega_2$ $n$-te Einheitswurzeln. Dann sind $\rho_1(q^k) = \omega_1^k$, $\rho_2(q^k) = \omega_2^k$ irreduzible Darstellungen von $C_n = \{1, q, \ldots, q^{n-1}\}$, die für $\omega_1 \neq \omega_2$ nicht äquivalent sind. Nach Satz 2.1.10 (i), (ii) ist dann

$$\frac{1}{n}\sum_{r=0}^{n-1} \omega_2^{-r}\omega_1^r = \begin{cases} 0 & , \ \omega_1 \neq \omega_2\ , \\ 1 & , \ \omega_1 = \omega_2\ . \end{cases}$$

Dies sind die bekannten Orthogonalitätsrelationen der Exponentialfunktion.

## 2.2 Charaktere endlicher Gruppen

Darstellungen von Gruppen sind recht komplizierte Gebilde. Für viele Fragen genügt es, einfachere Gebilde, nämlich Charaktere zu betrachten.

**Definition 2.2.1** *Sei $\rho$ eine Darstellung von $G$ in $V$. Dann heißt die Abbildung $\chi : G \to \mathbf{C}$, welche durch*

$$\chi(s) = Spur(\rho(s))$$

*definiert ist, der Charakter von $\rho$ und ein Charakter von $G$. Charaktere von irreduziblen Darstellungen heißen irreduzible Charaktere.*

**Satz 2.2.2** *(Eigenschaften von Charakteren):*

1. *Äquivalente Darstellungen haben den gleichen Charakter.*
2. $\chi(1) = d = Grad(\rho)$.
3. $\chi(a^{-1}sa) = \chi(s)$.
4. *Sind $\chi_1, \ldots, \chi_r$ die Charaktere der Darstellungen $\rho_1, \ldots, \rho_r$, dann hat $\rho_1 + \ldots + \rho_r$ den Charakter $\chi_1 + \ldots + \chi_r$.*
5. $\overline{\chi}(s) = \chi(s^{-1})$.

**Beweis:**

1. Ist $\rho_1 = \tau\rho_2\tau^{-1}$, so gilt Spur $(\rho_1) =$ Spur $(\rho_2)$.
2. Spur ($d$-dimensionale Einheitsmatrix) $= d$.
3. Siehe 1.

4. Seien $\rho_1, \ldots, \rho_r$ bezüglich gewisser Basen beschrieben durch Matrizen $R_1, \ldots, R_r$. Dann hat $\rho_1 + \ldots + \rho_r$ die Matrix
$$\begin{pmatrix} R_1 & & \\ & \ddots & \\ & & R_r \end{pmatrix} ,$$
deren Spur gerade Spur $(R_1) + \ldots +$ Spur $(R_r)$ ist.

5. Bezüglich eines geeigneten Skalarproduktes ist die Darstellung $\rho$ unitär und damit
$$\begin{aligned} \chi(s^{-1}) &= \text{Spur } (\rho(s^{-1})) = \text{Spur } (\rho(s)^*) = \overline{\text{Spur}(\rho(s))} \\ &= \overline{\chi}(s) \ . \end{aligned}$$

□

In dem linearen Raum der komplexwertigen Funktionen auf $G$ führen wir nun das Skalarprodukt
$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum_{t \in G} \varphi(t) \overline{\psi}(t)$$
ein. Damit gilt

**Satz 2.2.3** *(Orthogonalität der Charaktere): Seien $\chi_1$, $\chi_2$ die Charaktere der irreduziblen Darstellungen $\rho_1$, $\rho_2$ von $G$. Dann gilt*
$$\langle \chi_1, \chi_2 \rangle = \begin{cases} 1 & , \ \rho_1, \rho_2 \ \textit{äquivalent} \\ 0 & , \ \textit{sonst} \ . \end{cases}$$

**Beweis:** Seien $\chi_1$, $\chi_2$ die Charaktere der Darstellungen $\rho_1$, $\rho_2$ von $G$, und seien $\rho_1$, $\rho_2$ bezüglich gewisser Basen beschrieben durch die Matrizen $R^1$, $R^2$. Dann ist
$$\begin{aligned} \langle \chi_1, \chi_2 \rangle &= \frac{1}{|G|} \sum_{t \in G} \chi_1(t) \overline{\chi}_2(t) = \frac{1}{|G|} \sum_{t \in G} \chi_1(t) \chi_2(t^{-1}) \\ &= \sum_{k,\ell} \frac{1}{|G|} \sum_{t \in G} R^1_{kk}(t) R^2_{\ell\ell}(t^{-1}) \ . \end{aligned}$$
Die Behauptung folgt aus Satz 2.1.10.

□

Für die direkte Summe von $c$ zu einer Darstellung $\rho$ äquivalenten Darstellungen schreiben wir in Zukunft einfach $c\rho$. Mit dieser Schreibweise haben wir

**Satz 2.2.4** *Jede Darstellung $\rho$ einer Gruppe $G$ läßt sich eindeutig (bis auf die Reihenfolge) als direkte Summe*

$$\rho = c_1\rho_1 + \ldots + c_m\rho_m$$

*irreduzibler und paarweise nicht äquivalenter Darstellungen $\rho_1, \ldots, \rho_m$ schreiben. Sind $\chi$, $\chi_i$ die Chraktere von $\rho$, $\rho_i$, so gilt*

$$c_i = \langle \chi, \rho_i \rangle \ .$$

**Beweis:** Nach Satz 2.1.6 gibt es irreduzible Darstellungen $\rho'_1, \ldots, \rho'_r$, so daß

$$\rho = \rho'_1 + \ldots + \rho'_r \ .$$

Sind $\chi'_1, \ldots, \chi'_r$ die Charaktere von $\rho'_1, \ldots, \rho'_r$, so ist

$$\langle \chi, \chi'_i \rangle = \sum_{k=1}^{r} \langle \chi'_i, \chi'_k \rangle \ .$$

Nach 2.1.3 ist dies genau die Anzahl der zu $\rho'_i$ äquivalenten Darstellungen unter den $\chi'_1, \ldots, \chi'_r$. Fassen wir jeweils äquivalente Darstellungen zusammen, so folgt die Behauptung.

□

**Definition 2.2.5** *Die Zahlen $c_i$ in Satz 2.2.4 heißen Vielfachheiten des Auftretens von $\rho_i$ in $\rho$.*

**Satz 2.2.6** *Darstellungen mit gleichem Charakter sind äquivalent.*

**Beweis:** Seien $\rho^1$, $\rho^2$ Darstellungen von $G$. Nach Satz 2.2.4 gibt es Zahlen $c_k^1$, $c_k^2$ mit

$$\rho^1 = \sum_{k=1}^{m} c_k^1 \rho_k \quad , \qquad \rho^2 = \sum_{k=1}^{m} c_k^2 \rho_k \; .$$

Dabei sind $\rho_1, \ldots, \rho_m$ irreduzible und paarweise nicht äquivalente Darstellungen von $G$ und $\chi_1, \ldots, \chi_m$ ihre Charaktere. Haben nun $\rho^1$, $\rho^2$ den gleichen Charakter $\chi$, so gilt nach Satz 2.2.3

$$c_k^1 = \langle \chi, \chi_k \rangle = c_k^2 \; .$$

Also sind $\rho^1$, $\rho^2$ äquivalent.

□

**Folgerung:** Infolge von Satz 2.2.6 lassen sich die Orthogonalitätsrelationen der Charaktere (Satz 2.2.3) einfacher formulieren: Seien $\chi_1$, $\chi_2$ irreduzible Charaktere einer Gruppe $G$. Dann gilt

$$\langle \chi_1, \chi_2 \rangle = \begin{cases} 1 & , \quad \chi_1 = \chi_2 \; , \\ 0 & , \quad \text{sonst} \; . \end{cases}$$

**Beispiel:** Die Diedergruppe $C_n$ besitzt für gerades $n$ folgende Charaktere:

| | $r^k$ | $sr^k$ | Bemerkungen |
|---|---|---|---|
| $\chi_1$ | $1$ | $1$ | |
| $\chi_2$ | $1$ | $-1$ | |
| $\chi_3$ | $(-1)^k$ | $(-1)^k$ | |
| $\chi_4$ | $(-1)^k$ | $(-1)^{k+1}$ | |
| $\chi_5$ | $2\cos(2\pi hk/n)$ | $0$ | $h = 1, \ldots, \frac{n}{2} - 1$ |

Neben einer Reihe trivialer Beziehungen erhält man aus Satz 2.2.6 auch die Orthogonalitätsrelationen

$$\sum_{k=0}^{n-1} \cos(2\pi h_1 k/n) \cos(2\pi h_2 k/n) = \begin{cases} \frac{n}{2} & , \quad h_1 = h_2 \; , \\ 0 & , \quad h_1 \neq h_2 \; , \end{cases}$$

mit $1 \leq h_1$, $h_2 < \frac{n}{2}$.

**Satz 2.2.7** *Zu einer Gruppe $G$ gibt es ein maximales endliches System irreduzibler paarweise inäquivalenter Darstellungen $\rho_1, \ldots, \rho_m$. Jedes $\rho_i$ ist in $\rho_{reg}$ genau so oft enthalten, wie es sein Grad $d_i$ angibt. Es ist*

$$|G| = \sum_{i=1}^{m} d_i^2 \ . \tag{2.2.1}$$

**Beweis:** Zunächst berechnen wir den regulären Charakter $\chi_{\text{reg}}$ der regulären Darstellung $\rho_{\text{reg}}(s)$. Ist $\{e_{t_1}, \ldots, e_{t_n}\}$ eine Basis von $V$, so wird $\rho_{\text{reg}}(s)$ beschrieben durch die Permutationsmatrix

$$P(s) = (e_{st_1}, \ldots, e_{st_n}) \ ,$$

wo $t_1, \ldots, t_n$ die Elemente der Gruppe sind. Für $s = 1$ ist $P(1) = I$ und damit $\chi_{\text{reg}}(1) = \text{Spur } (I) = |G|$. Für $s \neq 1$ hat $P(s)$ in der Diagonale nur Nullen. Also $\chi_{\text{reg}}(s) = \text{Spur } (P(s)) = 0$ für $s \neq 1$.

Sei nun $\rho_1, \ldots, \rho_m$ ein System irreduzibler paarweise inäquivalenter Darstellungen von $G$ und $\chi_1, \ldots, \chi_m$ die zugehörigen Charaktere. Dann ist

$$\begin{aligned}
\langle \chi\text{reg}, \chi_i \rangle &= \frac{1}{|G|} \sum_{t \in G} \chi\text{reg}(t) \overline{\chi}_i(t) \\
&= \frac{1}{|G|} \sum_{t \in G} \chi\text{reg}(t) \chi_i(t^{-1}) \\
&= \chi_i(1) = d_i \ .
\end{aligned}$$

Wir können nach Satz 2.2.4 die $\rho_i$ so wählen, daß

$$\rho\text{reg} = \sum_{i=1}^{m} d_i \rho_i \ .$$

Bilden wir hiervon die Spur, so erhalten wir

$$\begin{aligned}
|G| &= \chi_{\text{reg}}(1) = \text{Spur } (\rho_{\text{reg}}(1)) = \sum_{i=1}^{m} d_i \ \text{ Spur } \ (\rho_i(1)) \\
&= \sum_{i=1}^{m} d_i \chi_i(1) = \sum_{i=1}^{m} d_i^2 \ .
\end{aligned}$$

Wäre nun $\rho_{m+1}$ eine weitere irreduzible Darstellung von $G$, welche zu keinem der $\rho_1, \ldots, \rho_m$ äquivalent wäre, so wäre notwendig $d_{m+1} = 0$, $\rho_{m+1}$ also vom Grade 0. Ein solches $\rho_{m+1}$ kann es also nicht geben, d.h. $\rho_1, \ldots, \rho_m$ ist maximal.

**Bemerkung:** (2.1) charakterisiert also maximale Systeme paarweise inäquivalenter irreduzibler Darstellungen.

**Satz 2.2.8** *Ein Charakter $\chi$ ist genau dann irreduzibel, wenn $\langle \chi, \chi \rangle = 1$.*

**Beweis:** Sei $\chi$ der Charakter von $\rho$ und $\rho$ irreduzible. Dann ist $\langle \chi, \chi \rangle = 1$ nach Satz 2.2.3. Sei umgekehrt $\langle \chi, \chi \rangle = 1$. Sei $\rho_1, \ldots, \rho_m$ ein maximales System irreduzibler paarweise inäquivalenter Darstellungen und seien $\chi_1, \ldots, \chi_m$ die zugehörigen Charaktere. Dann gibt es ganze Zahlen $c_1, \ldots, c_m$ mit $\chi = c_1\chi_1 + \ldots + c_m\chi_n$. Aus Satz 2.2.3 folgt

$$\langle \chi, \chi \rangle = \sum_{i=1}^{m} c_i^2 \langle \chi_i, \chi_i \rangle \ .$$

Nun ist $\langle \chi, \chi \rangle = 1$ und $\langle \chi_i, \chi_i \rangle = 1$, weil die $\chi_i$ irreduzibel sind. Also gilt

$$1 = \sum_{i=1}^{m} c_i^2 \ .$$

Da die $c_i$ alle ganz sind, ist genau eines der $c_i = 1$, und alle anderen $c_i$ sind Null. $\rho$ ist also äquivalent zu einem der $\rho_i$ und damit wie dieses irreduzibel. Also ist $\chi$ irreduzibel.

□

**Beispiel:** Wir wollen zeigen, daß das für $D_n$, $n$ gerade, angegebene System von Darstellungen ein maximales System paarweise inäquivalenter irreduzibler Darstellungen ist.

Die Darstellungen $\rho_1, \ldots, \rho_4$ sind trivialerweise irreduzibel und paarweise nicht äquivalent. Wir haben oben schon nachgerechnet, daß

$$\langle \chi_5^h, \chi_5^h \rangle = \frac{2}{n} \sum_{k=0}^{n-1} \cos^2(2\pi kh/n) = 1$$

ist für $h = 1, \ldots, \frac{n}{2} - 1$. Wir haben damit

$$d_1 = d_2 = d_3 = d_4 = 1 \; , \quad d_5^h = 2 \; , \quad h = 1, \ldots, \frac{n}{2} - 1$$

und damit

$$d_1^2 + d_2^2 + d_3^2 + d_4^2 = \sum_{h=1}^{\frac{n}{2}-1} (d_5^h)^2 = 2n = |G| \; .$$

Also haben wir ein maximales System.

**Definition 2.2.9** *$a$, $b \in G$ heißen äquivalent, falls es $s \in G$ gibt mit $a = s^{-1}bs$. Die zugehörigen Äquivalenzklassen seien $A_1, \ldots, A_k$, und es sei $s \in A_1$. Wir setzen $g_i = |A_i|$ und $g = |G|$, also $g = \sum_{i=1}^{k} g_i$. Eine Funktion $h : G \to \mathbb{C}$ heißt Klassenfunktion, falls $h$ auf jeder Äquivalenzklasse konstant ist.*

Offenbar ist jeder Charakter von $G$ eine Klassenfunktion. Der nächste Satz zeigt, daß dies im wesentlichen auch schon alle Klassenfunktionen sind.

**Satz 2.2.10** *Sei $\rho_1, \ldots, \rho_m$ ein maximales System irreduzibler und paarweise inäquivalenter Darstellungen von $G$ und $A_1, \ldots, A_k$ wie in Definition 2.2.9. Dann gilt:*

*(i)* $m = k$

*(ii) Jede Klassenfunktion ist Linearkombination von Charakteren von $G$.*

**Beweis:** Sei $\chi_j$ der Charakter von $\rho_j$. Dann können wir eine Funktion $\tilde{\chi}_j$ auf $\{A_1, \ldots A_k\}$ definieren durch

$$\tilde{\chi}_j(A_i) = \sqrt{\frac{g_i}{g}}\chi_j(s) \;, \quad s \in A_i \;.$$

Auf der Menge der Funktionen auf $\{A_1, \ldots, A_n\}$ definieren wir das Skalarprodukt

$$(u, v) = \sum_{i=1}^{k} u(A_i)\overline{v}(A_i) \;.$$

Wir zeigen, daß die $\tilde{\chi}_j$ bezüglich dieses Skalarproduktes ein Orthonormalsystem ist. Es ist mit $s_i \in A_i$

$$\begin{aligned}
\langle \tilde{\chi}_j, \tilde{\chi}_\ell \rangle &= \sum_{i=1}^{k} \sqrt{\frac{g_i}{g}}\chi_j(s_j)\sqrt{\frac{g_i}{g}}\overline{\chi}_\ell(s_j) \\
&= \frac{1}{g}\sum_{i=1}^{k} g_i \chi_j(s_i)\overline{\chi}_\ell(s_i) \\
&= \frac{1}{g}\sum_{i=1}^{k}\sum_{s\in A_i} \chi_j(s)\overline{\chi}_\ell(s) \\
&= \frac{1}{|G|}\sum_{s\in G} \chi_j(s)\overline{\chi}_\ell(s) \\
&= \delta_{j\ell}
\end{aligned}$$

nach Satz 2.2.3.

Eine unmittelbare Folgerung ist $m \leq k$. Denn $k$ ist die Dimension des Raumes der Klassenfunktionen, und in diesem Raum gibt es die $m$ linear unabhängigen Funktionen $\tilde{\chi}_1, \ldots, \tilde{\chi}_m$.

Es bleibt zu zeigen, daß $m \geq k$. Hierzu zeigen wir zunächst einmal: Ist $\rho$ eine irreduzible Darstellung von $G$ des Grades $d$ und $\chi$ ihr Charakter, so gilt

$$\frac{1}{d}\chi(a) = \chi(b) = \frac{1}{|G|}\sum_{t\in G} \chi(bt^{-1}at) \;. \qquad (2.2.2)$$

Aus Satz 2.1.9 mit $\tau = \rho(a)$ und $\rho_1 = \rho_2 = \rho$ folgt nämlich

$$\tau' = \frac{1}{|G|}\sum_{t\in G}\rho(t^{-1})\rho(a)\rho(t) = \frac{1}{d}\ \text{Spur}\ (\tau) = \frac{\chi(a)}{d}\,.$$

Linksmultiplikation mit $\rho(b)$ ergibt

$$\frac{1}{|G|}\sum_{t\in G}\rho(bt^{-1}at) = \frac{\chi(a)}{d}\rho(b)\ .$$

Gehen wir zum Charakter über, so folgt (2.2).

Wir wenden (2.2) an auf $\chi = \chi_\ell$, $a = s_i \in A_i$, $b^{-1} = s_j \in A_j$, und summieren über $\ell$. Es ergibt sich nach Satz 2.2.7

$$\begin{aligned}\sum_{\ell=1}^{m}\chi_\ell(s_i)\chi_\ell(s_j^{-1}) &= \frac{1}{|G|}\sum_{\ell=1}^{n} d_\ell\sum_{t\in G}\chi_\ell(s_j^{-1}t^{-1}s_it)\\ &= \frac{1}{|G|}\sum_{t\in G}\sum_{\ell=1}^{n} d_\ell\chi_\ell(s^{-1}t^{-1}s_it)\\ &= \frac{1}{|G|}\sum_{t\in G}\chi\text{reg}(s_j^{-1}t^{-1}s_it)\ .\end{aligned}$$

Da für $i \neq j$ die Elemente $s_i$, $s_j$ aus verschiedenen Äquivalenzklassen sind, ist für $i \neq j$ stets $s_j^{-1}t^{-1}s_i\ \ t \neq 1$. Also

$$\chi\text{reg}(s_j^{-1}t^{-1}s_it) = 0$$

für $i \neq j$ und damit

$$\sum_{\ell=1}^{m}\chi_\ell(s_i)\overline{\chi}_\ell(s_j) = 0 \tag{2.2.3}$$

für $i \neq j$. Wäre dies auch für $i = j$ richtig, so wäre

$$\sum_{\ell=1}^{m}|\chi_\ell(s_i)|^2 = 0 \tag{2.2.4}$$

und damit $\chi_\ell = 0$ auf $A_i$ für $\ell = 1, \ldots, m$. Da $\rho_1, \ldots, \rho_m$ maximal sind, verschwände jeder Charakter auf $A_i$. Dies ist z.B. für den Einheitscharakter sicher nicht der Fall. Also kann (2.4) nicht richtig sein.

Zusammen mit (2.3) folgt dann, daß die $k$-Spalten der $(m, k)$-Matrix

$$\begin{pmatrix} \chi_1(s_1) & , & \dots & , & \chi_1(s_k) \\ \vdots & & & & \\ \chi_m(s_1) & , & \dots & , & \chi_m(s_k) \end{pmatrix} \tag{2.2.5}$$

linear unabhängig sind. Diese Matrix muß also mindestens $k$ Zeilen haben. Damit ist $m \geq k$ gezeigt.

Daß jede Klassenfunktion sich als Linearkombination von Charakteren schreiben läßt, folgt nun unmittelbar aus der Tatsache, daß der Rang der Matrix (2.5) $m = k$ ist.

$\square$

## 2.3 Der Chinesische Restsatz

Sei $R$ ein Ring mit Einselement, z.B. der Ring $\mathbb{Z}$ der ganzen Zahlen oder der Polynomring $F[z]$ über einem Körper $F$. Ein Ring heißt kommutativ, wenn seine Multiplikation kommutativ ist. Ist $R$ kommutativ, so sagen wir, $a$ teilt $b$ $(a \mid b)$, falls es ein $r$ gibt mit $b = ar$. Wir sagen $a \equiv b \mod p$, falls $p \mid a - b$. Die Äquivalenzklassen dieser Äquivalenzrelation nennen wir Restklassen mod $p$. Diese bilden den Restklassenring $R/p$. Ein Ring heißt nullteilerfrei, wenn $ab = 0$ zur Folge hat, daß $a = 0$ oder $b = 0$.

**Beispiele:**

1) $\mathbb{Z}_p = \mathbb{Z}/p = \{0, 1, \ldots, p-1\}$. In $\mathbb{Z}_6$ ist z.B. $2+5 = 1$, $3 \cdot 4 = 0$. Also ist $\mathbb{Z}_6$ nicht nullteilerfrei. Aber $\mathbb{Z}_p$ ist nullteilerfrei für Primzahlen $p$.

2) Für den Ring $F[z]$ und $p = z^n + a_1 z^{n-1} + \ldots + a_0$ ist $F[z]/p$ der Ring der Polynome vom Grade $< n$. Für $p = z^2 - 1$ ist z.B. $z(z+1) = z^2 + z \equiv 1 + z \mod p$.

3) Der Ring $M_n[F]$ der $(n,n)$-Matrizen über $F$ ist nicht nullteilerfrei:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} .$$

**Definition 2.3.1** *Ein kommutativer nullteilerfreier Ring $R$ heißt euklidisch, wenn es für jedes $a \in R$, $a \neq 0$, eine ganze Zahl $g(a) \geq 0$ gibt mit*

*(i)* $g(ab) \geq g(b)$

*(ii)* *Zu $a$, $b \in R$, $a \neq 0$ gibt es $q$, $r \in R$*

$$b = qa + r ,$$

*wobei entweder $r = 0$ oder $g(r) < g(a)$ ist.*

*Man nennt $g$ den Grad.*

**Beispiele:**

1) $\mathbb{Z}$ mit $g(a) = |a|$ ist ein euklidischer Ring.

2) $F[z]$ mit dem Polynomgrad als Grad ist ebenfalls euklidisch. Z.B. ist
$$z^3 + 2z^2 + z + 1 = (z + 2)(z^2 - 1) + 2z + 3$$

3) Der Ring $\mathbb{Z} + \sqrt{-3}\mathbb{Z}$ ist nicht euklidisch.

Ein Element $e \in R$ heißt Einheit, falls ein $e' \in R$ existiert mit $ee' = e'e = 1$. Wir nennen $e'$ das Inverse zu $e$ und schreiben $e' = e^{-1}$.

**Beispiele:**

1) $\mathbb{Z}$ hat die Einheiten $+1$, $-1$.

2) $F[z]$ hat die Einheiten $F$ mit Ausnahme der Null.

3) $M_n[F]$ hat als Einheiten die invertierbaren Matrizen.

Ein Element $p \in R$ heißt prim, falls $p = p_1 p_2$ nur möglich ist, wenn $p_1$ oder $p_2$ Einheit ist.

**Beispiele:**

1) In $\mathbb{Z}$ sind genau die Elemente prim, für welche der Betrag eine Primzahl ist.

2) In $F[z]$ nennt man die Primelemente irreduzibel über $F$. Z.B. ist

$$\begin{array}{lcl}
z^2 - 1 & = & (z+1)(z-1) \quad \text{nicht prim für beliebiges } F \\
z^2 + 1 & & \text{prim für } F = \mathbb{R}, \text{ nicht prim für } F = \mathbb{C} \\
z^2 - 2 & & \text{prim für } F = \Gamma = \text{Körper der rationalen Zahlen,} \\
 & & \text{aber nicht prim für } F = R \ .
\end{array}$$

Folgende Sätze findet man in jedem Lehrbuch der Algebra.

**Satz 2.3.2** *In einem euklidischen Ring gibt es zu jedem Paar $a$, $b \neq 0$ einen größten (im Sinne des Grades) gemeinsamen Teiler $ggt(a, b)$. Es gibt $p$, $q \in R$ mit $ggt(a, b) = ap + bq$.*

**Satz 2.3.3** *In einem euklidischen Ring ist jedes Element eindeutig (bis auf Reihenfolge und Einheiten) als Produkt von Primelementen darstellbar.*

**Beispiele:** In dem Ring $\mathbb{Z} + \sqrt{-3}\mathbb{Z}$ gilt $4 = 2 \cdot 2 = (1 - \sqrt{-3})(1 + \sqrt{-3})$. Dieser Ring ist also nicht euklidisch.

Wir suchen nun Lösungen von simultanen Kongruenzen modulo $p_1, \ldots, p_m$. Seien also $a_1, \ldots, a_m$ gegeben. Gesucht ist ein $a$ mit

$$a \equiv a_i \mod p_i \,, \qquad i = 1, \ldots, m \,. \tag{2.3.1}$$

Der Chinesische Restsatz gibt ein Kriterium für Existenz und Eindeutigkeit von (3.1).

**Satz 2.3.4** *Sei $R$ ein euklidischer Ring, und seien $p_1, \ldots, p_n \in R$ paarweise teilerfremd. Dann ist (3.1) für jede Wahl der $a_1, \ldots, a_m \in R$ lösbar. Die Lösung ist mod $p_1 \ldots p_m$ eindeutig bestimmt.*

**Beweis:** Wir zeigen zunächst: Die Gleichung $ax \equiv b \mod p$ ist genau dann lösbar, wenn $ggt(a, p)|b$. Ist diese Kongruenz nämlich lösbar, so gibt es $y$ mit $ax + py = b$, und es folgt $ggt(a, p)|b$. Sei umgekehrt diese Bedingung erfüllt. Nach Satz 2.3.2 gibt es $u$, $v$ mit $ggt(a, p) = au + vp$. Multiplikation mit $q = b/ggt(a, p)$ ergibt $b = aqu + qvp$. Damit ist $x = qu$ Lösung der Kongruenz.

Sei $p = p_1 \ldots p_m$. Dann ist $ggt(\frac{p}{p_i}, p_i) = 1$, und es gibt nach obigem ein $x_i$ mit $\frac{p}{p_i} x_i \equiv 1 \mod p_i$. Wir behaupten, daß

$$a = \sum_{i=1}^{n} \frac{p}{p_i} a_i x_i$$

Lösung von (3.1) ist. Wir schreiben für ein $j$

$$\begin{aligned} a &= \sum_{i \neq j} \frac{p}{p_i} a_i x_i + \frac{p}{p_j} a_j x_j \\ &= p_j \sum_{i \neq j} \frac{p}{p_i p_j} a_i x_i + a_j \left( \frac{p}{p_j} x_j \right) \end{aligned}$$

und dies ist kongruent $a_j$ mod $p_j$ nach Konstruktion von $x_j$.

Sind $a$, $a'$ Lösungen von (3.1), so ist $a - a' \equiv 0 \bmod p_i$ für $i = 1, \ldots, m$ und damit $a \equiv a' \bmod p$.

□

**Beispiel:** $R = R[z]$, $p_i = z - z_i$, $z_i$ paarweise verschieden. Wir suchen ein $a \in R$ mit $a \equiv a_i \bmod p_i$, d.h.

$$a(z_i) = d_i \,, \qquad i = 1, \ldots, m \,.$$

Nach Satz 2.3.4 ist $a$ modulo $p = p_1 \ldots p_m$ eindeutig bestimmt. $a$ ist also das Polynom vom Grad $n-1$, das an den Stellen $z_i$ die Werte $a_i$ annimmt. $a$ ergibt sich als

$$a = \sum_{i=1}^{m} \frac{p}{p_i} a_i x_i \,, \quad \frac{p}{p_i} x_i \equiv 1 \quad \text{mode } p_i \,.$$

Mit

$$\omega_i(z) = \frac{p}{p_i} = \prod_{j \neq i} (z - z_j)$$

haben wir $x_i = \frac{1}{\omega_i(z_i)}$ und damit

$$a = \sum_{i=1}^{m} \frac{\omega_i(z)}{\omega_i(z_i)} a_i \,.$$

Dies ist die Lagrange'sche Interpolationsformel.

Seien $R_1$, $R_2$ Ringe. Wir definieren dann einen weiteren Ring $R_1 \otimes R_2$ folgendermaßen. $R_1 \otimes R_2$ besteht aus den Paaren $(a_1, a_2)$ mit $a_i \in R_i$.

Addition und Multiplikation in $R_1 \otimes R_2$ sind komponentenweise erklärt, also

$$\begin{aligned}(a_1, a_2) + (b_1, b_2) &= (a_1 + b_1, a_2 + b_2) \\ (a_1, a_2)(b_1, b_2) &= (a_1 a_2, b_1 b_2) \ .\end{aligned}$$

$R_1 \otimes R_2$ heißt direktes Produkt von $R_1$ und $R_2$.

**Satz 2.3.5** *Sei $R$ ein euklidischer Ring und seien $p_1, \ldots, p_m$ paarweise teilerfremd. Sei $p = p_1 \ldots p_m$. Dann gilt*

$$R/p = R/p_1 \otimes \ldots \otimes R/p_m \ .$$

**Beweis:** Wir definieren eine Abbildung $\varphi : R/p_1 \otimes \ldots R/p_m \to R/p$ mit Hilfe des Satzes 2.3.4. Für $(a_1, \ldots, a_m) \in R/p_1 \otimes \ldots \otimes R/p_m$ sei $a$ die Lösung aus (3.1). Diese ist in $R/p$ wohlbestimmt. Ist $(b_1, \ldots, b_m) \in R/p_1 \otimes \ldots \otimes R/p_m$ und $b$ die zugehörige Lösung von (3.1), so ist

$$\begin{aligned}a + b &\equiv a_i + b_i \mod p_i \\ ab &\equiv a_i b_i \qquad \mod p_i \ .\end{aligned}$$

$\varphi$ ist also ein Ring-Homomorphismus. Ist $a \in R$ und $a_i$ ein Repräsentant von $a$ mod $p_i$, so ist $a = \varphi(a_1, \ldots, a_m)$. Also ist $\varphi$ surjektiv. Nach der Eindeutigkeitsaussage von Satz 2.3.4 ist $\varphi$ injektiv. Also ist $\varphi$ sogar ein Ring-Isomorphismus.

□

## 2.4 Gruppentheorie

Sei $G$ eine endliche Gruppe und $H$ eine Untergruppe von $G$. Dann können wir in $G$ die Äquivalenzrelation

$$s \sim t \quad \Longleftrightarrow \quad t^{-1}s \in H$$

erklären. Sei $s_1, \ldots, s_r$ ein Repräsentantensystem dieser Äquivalenzrelation, also $s_1H, \ldots, s_rH$ die Äquivalenzklassen. Diese heißen (Links-) Nebenklassen von $H$. Es ist $G = s_1H \cup \ldots \cup s_rH$ und $r|H| = |G|$.

$H$ heißt Normalteiler in $G$, falls $tH = Ht$ für $t \in G$, d.h. falls die Linksnebenklassen gleich den Rechtsnebenklassen sind. Ist $H$ Normalteiler von $G$, dann bilden die Nebenklassen wieder eine Gruppe, die Faktorgruppe $G/H$.

Sei $a \in G$. Die Ordnung $m$ ist die kleinste natürliche Zahl $m \geq 1$, für welche $a^m = 1$. Es bildet dann $C_m = \{1, a, a^2, \ldots, a^{n-1}\}$ eine Untergruppe von $G$ der Ordnung $m$. $C_m$ heißt zyklische Gruppe der Ordnung $m$. Sie ist isomorph der additiven Gruppe $\mathbb{Z}$ mod $m$.

**Satz 2.4.1** *Sei $G$ abelsch, und haben $a_1, \ldots, a_r \in G$ die Ordnung $m_1, \ldots, m_r$. Sei $ggt(m_i, m_j) = 1$ für $i \neq j$. Dann hat $a = a_1 \ldots a_r$ die Ordnung $m = m_1 \cdot \ldots \cdot m_r$.*

**Beweis:** Sicher ist $a^m = 1$. Gäbe es ein $n$ mit $a^n = 1$ und $n < m$, so könnten wir unter diesen $n$'s das kleinste wählen. Die $n$ Elemente $1, \ldots, a^{n-1}$ würden dann eine Untergruppe von $C_m$ bilden, also $n|m$. Da die $m_i$ paarweise teilerfremd sind, wäre sogar $n|m_i$ für mindestens ein $i$, etwa $i = 1$. Dann wäre

$$a^n = a_1^n a_2^n \ldots a_r^n = a_2^n \ldots a_r^n = 1 \ .$$

Hätten wir die Behauptung für $r-1$ Faktoren schon bewiesen, so würde sie für $r$ Faktoren folgen. Da $r = 1$ trivial ist, ist der Satz nach dem Prinzip der vollständigen Induktion bewiesen.

□

Ähnlich wie das direkte Produkt von Ringen ist das direkte Produkt von Gruppen definiert. Seien $A$, $B$ Gruppen. Ihr direktes Produkt $A \otimes B$ besteht aus den Paaren $(a, b) \in A \times B$ mit kompetenterweiser Multiplikation: $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)$. Die Elemente $(a, 1)$ bilden eine Untergruppe von $A \otimes B$, die isomorph zu $A$ ist. Wir schreiben $A$ für diese Untergruppe, identifizieren also $(a, 1)$ mit $a$. $A$ wird so zu einer Untergruppe von $A \otimes B$, und dasselbe gilt für $B$. Offenbar sind $A$, $B$ sogar Normalteiler in $A \otimes B$. Wegen $(a, b) = (a, 1)(1, b) = (1, b)(a, 1)$ können wir $ab$ oder $ba$ für $(a, b)$ schreiben. Damit haben wir folgende äquivalente Definition des direkten Produkts: Eine Gruppe $G$ ist direktes Produkt seiner Untergruppen $A$, $B$ genau dann, wenn

(i) Jedes $g \in G$ sich eindeutig als $g = ab$ mit $a \in A$, $b \in B$ schreiben läßt.

(ii) $ab = ba$ für $a \in A$, $b \in B$.

**Satz 2.4.2** *Seien $n_1$, $n_2$ teilerfremd und $n = n_1 n_2$. Dann ist*

$$C_n = C_{n_1} \otimes C_{n_2} .$$

**Beweis:** Wir identifizieren $C_n$ mit der Gruppe $\mathbb{Z}$ mit Addition mod $n$. Dann können wir die Abbildung $\varphi : C_{n_1} \otimes C_{n_2} \to C_n$ erklären durch $\varphi(m_1, m_2) = m$, wobei $m$ die simultanen Kongruenzen $m \equiv m_i$ mod $n_i$, $i = 1, 2$ löst. Da $m$ mod $n$ eindeutig bestimmt ist, ist $\varphi$ injektiv. Da $n_1$, $n_2$ teilerfremd sind, gibt es Zahlen $q_1$, $q_2$ mit $q_1 n_1 + q_2 n_2 = 1$. Also ist $(q_1 m) n_1 + (q_2 m) n_2 = m$ und damit $m = \varphi(q_2 m n_2, q_1 m n_1)$ für jedes $m \in C_n$. Also ist $\varphi$ surjektiv. Daß $\varphi$ ein Homomorphismus ist, ist klar.

□

An Hand des Beispiels $n_1 = n_2 = 2$ macht sich leicht klar, daß die Voraussetzung $n_1$, $n_2$ teilerfremd nicht gestrichen werden kann.

Sei $M_n = \{m \in \mathbb{Z} : 1 \leq m < n,\ ggt(m,n) = 1\}$. Mit der Multiplikation mod $n$ wird $M_n$ zur Gruppe. Es ist nämlich $1 \in M_n$. Zu jedem $m \in M_n$ kann man die Kongruenz $x\ m \equiv 1 \bmod n$ lösen, und es ist $ggt(x,n) = 1$. Also ist $x \in M_n$ und $x = m^{-1}$. Und schließlich ist offenbar $m_1 m_2 \in M_n$, falls $m_1, m_2 \in M_n$.

Die Ordnung $\varphi(n) = |M_n|$ heißt Euler'sche $\varphi$-Funktion, also

| $n$ | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| $\varphi(n)$ | 1 | 2 | 2 | 4 | 3 |

Offenbar ist $\varphi(p) = p - 1$ für Primzahlen $p$, und $\varphi(p^r) = p^r - p^{r-1} = (p-1)p^{r-1}$.

**Satz 2.4.3** *Sei p prim. Dann gilt*

$$M_{p^r} = \begin{cases} C_{p^{n-1}(p-1)} & , \quad p > 2\ ,\ r \geq 1 \\ C_2 \otimes C_{2^{r-2}} & , \quad p = 2\ ,\ r \geq 2 \end{cases}$$

**Beweis:** Siehe z.B. Hasse, Number Theory, Chapt. 4.5.

Für $p > 2$ ist $M_{p^r}$ also zyklisch, d.h. es gibt $a$ mit $M_{p^r} = \{1, a, \ldots, a^{\varphi(p^r)-1}\}$. Für $r = 1$ ist $a$ die primitive Wurzel mod $p$. Diese finden sich für $p < 10000$ in Abramowitz/Stegun, Handbook of Mathematical Functions, pp. 864-869. Ein kleiner Auszug ist

| $p$ | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 |
|---|---|---|---|---|---|---|---|---|
| $a$ | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 5 |

**Beispiele:**

**1)** $M_5 = \{1,2,3,4\}$. Die Gruppentafel ist

| | 1234 |
|---|---|
| 1 | 1234 |
| 2 | 2413 |
| 3 | 3142 |
| 4 | 4321 |

Nach Satz 2.4.3 ist $M_5 = C_4 = \{0, 1, 2, 3\}$ mit Addition mod 4. Die Gruppentafel von $C_4$ ist

| | 0123 |
|---|---|
| 0 | 0123 |
| 1 | 1230 |
| 2 | 2301 |
| 3 | 3012 |

Die $(i+1)$-te Zeile entsteht aus der $i$-ten durch Links-Ring-Schift.

Nach Satz 2.4.3 sind $M_5$ und $C_4$ isomorph. Die Isomoraphie wird hergestellt durch ein erzeugendes Element, etwa 2 aus der obigen Tabelle. Danach ist $M_5 = \{1, 2, 3, 2^2, 2^3\} = \{1, 2, 4, 3\}$. Dadurch ergibt sich für $M_5$ auch die Gruppentafel

| | 1243 |
|---|---|
| 1 | 1243 |
| 2 | 2431 |
| 4 | 4312 |
| 5 | 3124 |

Diese Tafel ist in der Tat identisch zu der obigen Tafel von $C_4$: Die $(i+1)$-te Zeile ergibt sich durch Links-Ring-Schift aus der $i$-ten Zeile.

**2)** $M_9 = \{1, 2, 4, 5, 7, 8\}$ hat als erzeugendes Element die Zahl 5, also $M_9 = C_6 = \{1, 5, 5^2, 5^3, 5^4, 5^5\} = \{1, 5, 7, 8, 4, 2\}$. Die Gruppentafel von $M_9$ ist

| | 157842 |
|---|---|
| 1 | 157842 |
| 5 | 578421 |
| 7 | 784215 |
| 8 | 842157 |
| 4 | 421578 |
| 2 | 215784 |