Darstellungstheorie endlicher Gruppen: Vortrag 1

Qi Zhu

15. Mai 2019

0 Wiederholung: Elementare Gruppentheorie

Das ist nur ein kurzer Refresher, deshalb wird alles in Stichpunkten geführt.

- Die Begriffe **Gruppe**, **Untergruppe**, **(Links-/Rechts-)Nebenklasse** und **Gruppenhomomorphismus** sollten bekannt sein.
- Sei G eine Gruppe. Eine Untergruppe $N \subseteq G$ heißt **Normalteiler**, wenn

  $$gNg^{-1} = N \quad \forall g \in G$$

  gilt. Schreibe $N \trianglelefteq G$.
- Die Motivation des Normalteilers war es die Quotientengruppe zu definieren. So ist $(G/N, \cdot)$ die **Faktorgruppe/Quotientengruppe** definiert durch

  $$G/N = \{gN \mid g \in G\}, \quad (gN)(hN) = (gh)N \quad \forall g, h \in G.$$

  Das ist wohldefiniert für $N \trianglelefteq G$.
- Seien G, H Gruppen. Auf $G \times H = \{(g,h) : g \in G \text{ and } h \in H\}$ definieren wir eine komponentenweise Operation

  $$(g,h)(g',h') = (gg', hh').$$

  Hiermit wird $G \times H$ zu einer Gruppe. Wir nennen sie das **direkte Produkt** von G und H. Das lässt sich verallgemeinern auf $G_1 \times \cdots \times G_r$ für $r \in \mathbb{N}$.
- Eine Gruppe $G \neq \{e\}$ heißt **einfach**, wenn die einzigen Normalteiler $\{e\}$ und G sind.
- Sei G eine Gruppe und $M \subseteq G$. Dann ist die kleinste Untergruppe $\langle M \rangle \subseteq G$, die M enthält, die **von M erzeugte Untergruppe**. Manchmal gibt man auch **Relationen** an, dann haben wir eine **Präsentation** einer Gruppe. Sei also R noch eine Menge von Relationen, dann schreiben wir $\langle M \mid R \rangle$. Grob ist das die größte von M erzeugte Gruppe, die alle Relationen aus R erfüllt.
- Ein wichtiges Beispiel ist die *Diedergruppe*

  $$D_{2n} = \left\langle a, b : a^n = b^2 = 1,\ b^{-1}ab = a^{-1} \right\rangle.$$

  Jedes Element von D_{2n} lässt sich eindeutig in der Form $a^i b^j$ darstellen mit $0 \leq i \leq n-1$ und $0 \leq j \leq 1$.

1 Gruppendarstellung

Sei G eine Gruppe und F entweder $\mathbb{R}$ oder $\mathbb{C}$.

Definition 1.1 (Darstellung einer Gruppe)**.** Eine **Darstellung** von G über F ist ein Homomorphismus $\rho : G \to \mathrm{GL}(n, F)$ für ein $n \in \mathbb{N}$. Der **Grad** von ρ ist n. Eine Darstellung heißt **treu**, wenn sie injektiv ist.

Bemerkung 1.2 (Motivation)**.** Der zentrale Begriff des Seminars bedarf ein wenig Motivation.

(1) Lineare Algebra ist leichter als (allgemeine) Algebra!

(2) Im 19. Jahrhundert gab es den Begriff der abstrakten Gruppe noch nicht. Trotzdem wurden Resultate bzgl. S_n oder $\mathrm{GL}(n, F)$ entwickelt.

Beispiel 1.3. Zum zentralen Begriff des Seminars wollen wir auch möglichst viele Beispiele geben!

(a) Die *triviale Darstellung* $\rho : G \to \mathrm{GL}(1, F)$ definiert durch $\rho(g) = (1)$ für alle $g \in G$.

(b) Definiere $\rho : G \to \mathrm{GL}(n, F)$ durch $\rho(g) = I_n$ für alle $g \in G$. Also hat jede Gruppe Darstellungen von beliebig großem Grad.

(c) Für $\rho : G \to \mathrm{GL}(n, F)$ ist $\det \circ \rho : G \to \mathrm{GL}(1, F)$ eine Darstellung.

(d) Betrachte $G \to S_n \to \mathrm{GL}(n, F)$ als Einbettung mit Cayleys Satz und Permutationsmatrizen. Das ist eine treue Darstellung.

(e) Eine Darstellung von $(\mathbb{C}^\times, \cdot)$ ist

$$\rho : \mathbb{C}^\times \to \mathrm{GL}(2, \mathbb{R}),\ a + ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Das ist eine alternative Möglichkeit, um $\mathbb{C}$ zu definieren. Entscheidend ist diese Darstellung z.B. auch in der Funktionentheorie im Bezug zu Cauchy-Riemann-Differentialgleichungen.

(f) Betrachte $D_8 = \langle a, b : a^4 = b^2 = 1,\ b^{-1}ab = a^{-1} \rangle$. Seien

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Dann ist

$$A^4 = B^2 = I,\ B^{-1}AB = A^{-1}.$$

Somit definiert

$$\rho : D_8 \to \mathrm{GL}(2, F),\ a^i b^j \mapsto A^i B^j$$

für $0 \le i \le 3,\ 0 \le j \le 1$ eine Darstellung von D_8 über F.

Sei nun $\rho : G \to \mathrm{GL}(n, F)$ eine Darstellung und $T \in \mathrm{GL}(n, F)$. Definiere

$$\sigma : G \to \mathrm{GL}(n, F),\ \sigma(g) = T\rho(g)T^{-1}.$$

Das ist eine weitere Darstellung von G, denn

$$\begin{aligned} \sigma(gh) &= T\rho(gh)T^{-1} \\ &= T\rho(g)\rho(h)T^{-1} \\ &= T\rho(g)T^{-1}T\rho(h)T^{-1} \\ &= \sigma(g)\sigma(h). \end{aligned}$$

Definition 1.4. Seien $\rho, \sigma : G \to \mathrm{GL}(n, F)$ Darstellungen von G über F. Dann ist ρ **äquivalent** zu σ, wenn es ein $T \in \mathrm{GL}(n, F)$ gibt, sodass für alle $g \in G$ gilt

$$\sigma(g) = T\rho(g)T^{-1}.$$

Äquivalenz von Darstellungen definiert eine Äquivalenzrelation.

2 FG-Moduln

Gruppendarstellungen liefern Matrizen. Entsprechend definieren sie Endomorphismen auf Vektorräumen, also eine Aktion auf Vektorräume.

Definition 2.1 (FG-Modul)**.** Sei V ein Vektorraum über F und G eine Gruppe. Dann ist V ein **FG-Modul**, wenn die Multiplikation gv für $g \in G,\ v \in V$ definiert ist und für alle $u, v \in V,\ \lambda \in F,\ g, h \in G$ die folgenden Bedingungen erfüllt sind

(1) $gv \in V$,

(2) $(gh)v = g(hv)$,

(3) $1v = v$,

(4) $g(\lambda v) = \lambda(gv)$,

(5) $g(u + v) = gu + gv$.

Mit (1), (4), (5) wird

$$\varphi : V \to V,\ v \mapsto gv$$

zu einem Endomorphismus in V.

Definition 2.2. Sei V ein FG-Modul und $\mathfrak{B}$ eine Basis von V. Für $g \in G$ bezeichnen wir mit $[g]_{\mathfrak{B}}$ die Darstellungsmatrix des Endomorphismus $v \mapsto gv$ bezüglich Basis $\mathfrak{B}$.

Satz 2.3. Sei G eine Gruppe und F ein Körper.

(1) Sei $\rho : G \to \mathrm{GL}(n, F)$ eine Darstellung von G über F und $V = F^n$. Dann wird V zu einem FG-Modul mit der Multiplikation

$$gv = \rho(g)v \quad \text{für } v \in V, g \in G.$$

Es gibt eine Basis $\mathfrak{B}$ von V mit

$$\rho(g) = [g]_{\mathfrak{B}} \quad \text{für alle } g \in G.$$

(2) Sei V ein FG-Modul und $\mathfrak{B}$ eine Basis von V. Dann ist die Funktion

$$g \mapsto [g]_{\mathfrak{B}} \quad \text{für } g \in G$$

eine Darstellung von G über F.

Beweis. Die Bedingungen sind alle leicht nachzurechnen. In i) funktioniert die Standardbasis $\mathfrak{B} = \{e_1, \ldots, e_n\}$. □

Beispiel 2.4. Betrachte Darstellung von D_8 durch

$$\rho(a) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ \rho(b) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Dann wird F^2 zu einem FG-Modul für $gv = \rho(g)v$. Mit Standardbasis e_1, e_2 erhalten wir

$$ae_1 = e_2,\ ae_2 = -e_1,\ be_1 = -e_1,\ be_2 = e_2.$$

Wie erwartet: Die Darstellung $g \mapsto [g]_{\{e_1,e_2\}}$ liefert ρ.

Wie so oft in der linearen Algebra determiniert eine Basis die komplette Struktur. Auch hier: Mit einer linearen Fortsetzung können wir FG-Moduln definieren.

Proposition 2.5. Sei $v_1, \ldots, v_n$ eine Basis des F-Vektorraum V. Für eine Multiplikation gv_i für alle $v \in V$ und $g \in G$ sei für alle $1 \leq i \leq n$ und alle $g, h \in G$ sowie alle $\lambda_1, \ldots, \lambda_n \in F$ die folgenden Bedingungen erfüllt:

(1) $gv_i \in V$,

(2) $(gh)v_i = g(hv_i)$,

(3) $1v_i = v_i$,

(4) $g(\lambda_1 v_1 + \cdots + \lambda_n v_n) = \lambda_1(gv_1) + \cdots + \lambda_n(gv_n)$.

Dann ist V ein FG-Modul.

Beweis. Die Bedingungen eines FG-Moduls sind leicht nachzuprüfen. □

Definition 2.6. Das ist die Übersetzung der besonderen Darstellungen in FG-Moduln.

i) Der **triviale** FG-Modul ist der 1-dimensionale F-Vektorraum mit $gv = v$ für alle $v \in V$, $g \in G$.

ii) Ein FG-Modul V ist **treu**, wenn

$$gv = v \quad \text{für alle } v \in V \implies g = 1.$$

Satz 2.7. Sei V ein FG-Modul mit Basis $\mathfrak{B}$ und ρ eine Darstellung von G über F definiert durch $\rho : g \mapsto [g]_{\mathfrak{B}}$ für $g \in G$.

(1) Sei $\mathfrak{B}'$ eine Basis von V, dann ist die Darstellung

$$\varphi : g \mapsto [g]_{\mathfrak{B}'}$$

von G äquivalent zu ρ.

(2) Sei σ eine Darstellung von G, die äquivalent zu ρ ist, dann gibt es eine Basis $\mathfrak{B}''$ von V, sodass $\sigma : g \mapsto [g]_{\mathfrak{B}''}$ für $g \in G$.

Beweis. Nicht so spannend.

(1) Klar.

(2) Sei $[g]_{\mathfrak{B}} = \rho(g) = T\sigma(g)T^{-1}$ für alle $g \in G$. Dann ist $\sigma(g) = T^{-1}[g]_{\mathfrak{B}}T$. Das ist ein Basiswechsel.

□

Definition 2.8. Sei V ein FG-Modul. Eine Teilmenge $W \subseteq V$ heißt dann **FG-Untermodul von V**, wenn W ein Unterraum ist und $gw \in W$ für alle $w \in W$ und $g \in G$ gilt.

Definition 2.9. Ein FG-Modul V heißt **irreduzibel**, wenn $V \neq \{0\}$ und es keine FG-Untermoduln außer $\{0\}$ und V hat. Sonst heißt es **reduzibel**.

Eine Darstellung $\rho : G \to \mathrm{GL}(n, F)$ heißt **irreduzibel**, wenn der dazugehörige FG-Modul F^n gegeben durch

$$gv = \rho(g)v \quad \text{für } v \in F^n, g \in G$$

irreduzibel ist. Sonst heißt es **reduzibel**.

Sei V ein reduzibler FG-Modul mit FG-Untermodul W mit $0 < \dim(W) < \dim(V)$. Wähle eine Basis $\mathfrak{B}_W$ von W und erweitere sie zu einer Basis $\mathfrak{B}$ von V. Dann ist für alle $g \in G$ die Darstellungsmatrix $[g]_{\mathfrak{B}}$ eine Blockmatrix von der Form

$$[g]_{\mathfrak{B}} = \begin{pmatrix} X_g & Y_g \\ 0 & Z_g \end{pmatrix}.$$

Hierbei sei X_g eine $\dim(W) \times \dim(W)$ Matrix. Umgekehrt ist ein FG-Modul genau dann reduzibel, wenn es in einer solchen Form dargestellt werden kann (‚sodass X_g eine $k \times k$ Matrix mit $0 < k < \dim(V)$ ist).

Beachte, dass $g \mapsto X_g$ und $g \mapsto Z_g$ weitere Darstellungen von G liefern.

Beispiel 2.10. Zwei Beispiele zum Schluss.

(a) Betrachte $C_3 = \{1, a, a^2\}$ und V ein FG-Modul mit Basis v_1, v_2, v_3 sowie

$$av_1 = v_2,\ av_2 = v_3,\ av_3 = v_1.$$

Offenbar ist $W = \mathrm{span}(v_1 + v_2 + v_3)$ ein FG-Untermodul. Sei $\mathfrak{B} = \{v_1 + v_2 + v_3, v_1, v_2\}$, so erhalten wir

$$[1]_{\mathfrak{B}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ [a]_{\mathfrak{B}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix},\ [a^2]_{\mathfrak{B}} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & -1 & 0 \end{pmatrix}.$$

Beachte die Blockmatrix-Struktur!

(b) Für D_8 und F^2 als FG-Modul mit

$$a\begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} -\mu \\ \lambda \end{pmatrix},\ b\begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} -\lambda \\ \mu \end{pmatrix}$$

wollen wir zeigen, dass F^2 ein irreduzibler FG-Modul ist. Sei U ein FG-Untermodul von Dimension ≤ 1, also $U = \mathrm{span}\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$. Doch die Aktionen a, b auf $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ zeigen, dass U genau dann ein Untermodul ist, wenn $U = \{0\}$.

Literatur

[1] G. James, M. Liebeck, *Representations and characters of groups. Second edition.*, Cambridge university Press, 2001.

[2] David S. Dummit, Richard M. Foote, *Abstract Algebra. Third edition.*, John Wiley & Sons, Inc., 2004.

Darstellungstheorie endlicher Gruppen: Vortrag 5

Qi Zhu

14. Juni 2019

1 Mehr zur Charakterisierung irreduzibler $\mathbb{F}G$-Moduln

Proposition 1.1. Sei U ein $\mathbb{F}G$-Modul. Dann gilt

$$\dim(\mathrm{Hom}_{\mathbb{F}G}(\mathbb{F}[G], U)) = \dim(U).$$

Beweis. Sei $d = \dim(U)$ und $u_1, \ldots, u_d$ eine Basis von U. Definiere die $\mathbb{F}G$-Homomorphismen (nachprüfen!)

$$\varphi_i : \mathbb{F}[G] \to U,\ \varphi_i(r) = ru_i \quad (1 \leq i \leq d).$$

Wir wollen beweisen, dass $B := \{\varphi_1, \ldots, \varphi_d\}$ eine Basis von $\mathrm{Hom}_{\mathbb{F}G}(\mathbb{F}[G], U)$ bildet.

- B ist ein Erzeugendensystem: Sei $\varphi \in \mathrm{Hom}_{\mathbb{F}G}(\mathbb{F}[G], U)$ beliebig. Dann können wir

  $$\varphi(1) = \lambda_1 u_1 + \cdots + \lambda_d u_d$$

  für $\lambda_1, \ldots, \lambda_d \in \mathbb{F}$ schreiben. Es folgt

  $$\begin{aligned} \varphi(r) &= r\varphi(1) \\ &= \lambda_1 r u_1 + \cdots + \lambda_d r u_d \\ &= (\lambda_1 \varphi_1 + \cdots + \lambda_d \varphi_d)(r). \end{aligned}$$

- B ist linear unabhängig: Nach Konstruktion sind $\varphi_1(1), \ldots, \varphi_d(1)$ linear unabhängig, also auch $\varphi_1, \ldots, \varphi_d$.

□

Bemerkung 1.2. Alternativ zeige man, dass $f \mapsto f(1)$ ein Vektorraumisomorphismus ist.

Satz 1.3. Sei $\mathbb{F}$ algebraisch abgeschlossen, $\mathrm{char}\,\mathbb{F} \nmid |G|$,[1] und

$$\mathbb{F}[G] = U_1 \oplus \cdots \oplus U_r.$$

eine direkte Summe irreduzibler Untermoduln. Sei U ein beliebiger irreduzibler $\mathbb{F}G$-Modul. Dann ist die Anzahl der $\mathbb{F}G$-Moduln U_i mit $U_i \cong U$ genau $\dim(U)$.

Beweis. In Vortrag 4 wurde gezeigt, dass $\dim(\mathrm{Hom}_{\mathbb{F}G}(\mathbb{F}[G], U))$ die Anzahl der U_i mit $U_i \cong U$ ist. Nach **Proposition 1.1** ist das genau $\dim(U)$. □

[1] Eigentlich brauchen wir nur, dass $\mathbb{F}[G]$ als direkte Summe irreduzibler Untermoduln unterteilt werden kann.

Beispiel 1.4. Vergleiche mit D_6 aus Vortrag 4.[2] Hier war

$$\mathbb{C}[D_6] = U_1 \oplus U_2 \oplus U_3 \oplus U_4$$

Dabei ist

- $\dim(U_1) = \dim(U_2) = 1$ und $U_1 \ncong U_2$,
- $\dim(U_3) = \dim(U_4) = 2$ und $U_3 \cong U_4$.

Definition 1.5. Irreduzible $\mathbb{F}G$-Moduln $V_1, \dots, V_k$ bilden eine **vollständige Menge nicht-isomorpher irreduzibler $\mathbb{F}G$-Moduln**, wenn jeder irreduzibler $\mathbb{F}G$-Modul isomorph zu einem der V_i ist und keine zwei der $V_1, \dots, V_k$ isomorph sind.

Satz 1.6. Sei $\mathbb{F}$ algebraisch abgeschlossen und $\operatorname{char}\mathbb{F} \nmid |G|$. Seien $V_1, \dots, V_k$ eine vollständige Menge nicht-isomorpher irreduzibler $\mathbb{F}G$-Moduln. Dann gilt

$$\sum_{i=1}^{k} (\dim V_i)^2 = |G|.$$

Beweis. Sei $\mathbb{F}[G] = U_1 \oplus \cdots \oplus U_r$. Dann gilt

$$\begin{aligned} \dim(\mathbb{F}[G]) &= \dim(U_1) + \cdots + \dim(U_r) \\ &= \sum_{i=1}^{k} (\dim V_i)(\dim V_i), \end{aligned}$$

da Untermoduln isomorph zu V_i nach **Satz 1.3** genau $\dim V_i$ oft vorkommen. □

Später werden wir noch sehen, dass $\dim V_i \mid |G|$ gilt. Diese zwei Reduktionen werden oft dabei helfen, die irreduziblen Moduln zu bestimmen.

Beispiel 1.7. Sei $|G| = 6$ und seien $d_1, \dots, d_k$ die Dimensionen aller irreduziblen $\mathbb{C}G$-Moduln. Nach **Satz 1.6** gilt

$$\sum_{i=1}^{k} d_i^2 = 6.$$

Es gibt hierfür nur zwei Möglichkeiten. Beide kommen tatsächlich vor.

- $(d_1, d_2, d_3, d_4, d_5, d_6) = (1, 1, 1, 1, 1, 1)$: Wähle G abelsch.
- $(d_1, d_2, d_3) = (1, 1, 2)$: Wähle $G = D_6$.

Hier hätte man das auch schneller einsehen können, da $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ und $D_6 \cong S_3$ (bis auf Isomorphie) die einzigen Gruppen mit Ordnung 6 sind. (Übung: Analysiere $|G| = 8$.)

[2] **Beispiel 10.8**(2) in James, Liebeck.

2 Konjugationsklassen

Im Anhang werden elementare Eigenschaften von Konjugationsklassen skizziert. Wieso Konjugationsklassen? Unter anderem werden wir im Laufe des Seminars noch sehen

$$\#\{\text{Irreduzible Charaktere von } G\} = \#\{\text{Konjugationsklassen von } G\}.$$

2.1 Zentrum der Gruppenalgebra

Kurze Erinnerung: Das **Zentrum einer Gruppenalgebra** $\mathbb{F}[G]$ ist

$$Z(\mathbb{F}[G]) = \{z \in \mathbb{F}[G] : rz = zr \text{ für alle } r \in \mathbb{F}[G]\}.$$

Definition 2.1. Seien $C_1, \dots, C_\ell$ die verschiedenen Konjugationsklassen einer endlichen Gruppe G. Die Elemente

$$\overline{C}_i = \sum_{g \in C_i} g \in \mathbb{F}[G] \quad (1 \le i \le \ell)$$

heißen **Klassensummen**.

Proposition 2.2. Die Klassensummen $\overline{C}_1, \dots, \overline{C}_\ell$ bilden eine Basis von $Z(\mathbb{F}[G])$.

Beweis. Der Beweis besteht aus drei Schritten. Sei $B = \{\overline{C}_1, \dots, \overline{C}_\ell\}$.

- $\overline{C}_i \in Z(\mathbb{F}[G])$: Konjugation permutiert bloß innerhalb der Konjugationsklassen.
- B ist linear unabhängig: Klar. (Beachte, dass $C_1, \dots, C_\ell$ disjunkt sind.)
- B ist ein Erzeugendensystem: Sei $r = \sum_{g \in G} \lambda_g g \in Z(\mathbb{F}[G])$. Für $h \in G$ gilt dann

$$\sum_{g \in G} \lambda_g g = h \left(\sum_{g \in G} \lambda_g g \right) h^{-1} = \sum_{g \in G} \lambda_g hgh^{-1}.$$

  Koeffizientenvergleich der linear unabhängigen g's liefert $\lambda_g = \lambda_{hgh^{-1}}$. Insbesondere ist also die Funktion $g \mapsto \lambda_g$ konstant auf den Konjugationsklassen von G. Seien $\lambda_1, \dots, \lambda_\ell$ die Koeffizienten der zugehörigen Konjugationsklassen. Dann folgt

$$r = \sum_{i=1}^{\ell} \sum_{g \in C_i} \lambda_g g = \sum_{i=1}^{\ell} \lambda_i \sum_{g \in C_i} g = \sum_{i=1}^{\ell} \lambda_i \overline{C}_i.$$

□

2.2 Konjugationsklassen der A_n

Natürlich gilt $\sigma^{A_n} \subseteq \sigma^{S_n}$ für alle $\sigma \in A_n$. Gleichheit muss aber nicht unbedingt gelten.

Beispiel 2.3. Betrachte $(1\ 2\ 3) \in A_3$. Es gilt

$$(1\ 2\ 3)^{A_3} = \{(1\ 2\ 3)\} \quad \text{und} \quad (1\ 2\ 3)^{S_3} = \{(1\ 2\ 3),\ (1\ 3\ 2)\}.$$

Glücklicherweise sind die Konjugationsklassen der A_n trotzdem gut charakterisiert.

Satz 2.4. Sei $\sigma \in A_n$ mit $n > 1$.

(a) Wenn σ mit einer ungeraden Permutation in S_n permutiert, dann folgt $\sigma^{S_n} = \sigma^{A_n}$.

(b) Wenn σ mit keiner ungeraden Permutation in S_n permutiert, dann wird σ^{S_n} in zwei gleich große Konjugationsklassen von A_n aufgeteilt

$$\sigma^{S_n} = \sigma^{A_n} \uplus ((1\ 2)\sigma(1\ 2)^{-1})^{A_n}.$$

Fall (b) trifft genau dann ein, wenn σ aus Zyklen paarweise verschiedener, ungerader Längen besteht.[3]

Beweis. Wie man erwarten könnte, ist der erste Teil ein wenig leichter.

(a) Sei ρ ungerade und $\rho\sigma\rho^{-1} = \sigma$. Sei $g = \tau\sigma\tau^{-1} \in \sigma^{S_n}$. Für $\tau \in A_n$ folgt $g \in \sigma^{A_n}$. Für $\tau \notin A_n$ folgt

$$g = \tau\sigma\tau^{-1} = (\tau\rho)\sigma(\tau\rho)^{-1} \in \sigma^{A_n}.$$

(b) Nach Annahme ist $C_{S_n}(\sigma) = C_{A_n}(\sigma)$. Also ist

$$|\sigma^{A_n}| = [A_n : C_{A_n}(\sigma)] = \frac{1}{2}[S_n : C_{S_n}(\sigma)] = \frac{1}{2}|\sigma^{S_n}|.$$

Weiter gilt

$$\{\rho\sigma\rho^{-1} : \rho \text{ ist ungerade}\} = ((1\ 2)\sigma(1\ 2)^{-1})^{A_n},$$

denn beliebige ungerade Permutationen können durch $\tau(1\ 2)$ für ein $\tau \in A_n$ dargestellt werden (Überprüfe das!). Somit

$$\begin{aligned}\sigma^{S_n} &= \{\rho\sigma\rho^{-1} : \rho \text{ ist gerade}\} \cup \{\rho\sigma\rho^{-1} : \rho \text{ ist ungerade}\} \\ &= \sigma^{A_n} \cup ((1\ 2)\sigma(1\ 2)^{-1})^{A_n}.\end{aligned}$$

Wegen $|\sigma^{A_n}| = \frac{1}{2}|\sigma^{S_n}|$ folgt $|((1\ 2)\sigma(1\ 2)^{-1})^{A_n}| = \frac{1}{2}|\sigma^{S_n}|$ und Disjunktheit der Konjugationsklassen.

□

Beispiel 2.5. Konjugationsklassen der A_5.

Repräsentant	id	$(1\ 2\ 3)$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3\ 4\ 5)$	$(1\ 3\ 4\ 5\ 2)$
Klassenordnung	1	20	15	12	12
Zentralisatorordnung	60	3	4	5	5

Tabelle 1: Konjugationsklassen der A_5

Lemma 2.6. Sei H eine Untergruppe von G. Dann gilt

$$H \trianglelefteq G \iff H = \bigcup_{h \in H} h^G.$$

[3] Siehe die Antwort von martini auf `https://math.stackexchange.com/questions/404656/`.

Beweis. Zwei Richtungen.

- $\Longrightarrow$: Mit $H \trianglelefteq G$ folgt $h^G \subseteq H$.
- $\Longleftarrow$: Für $h \in H,\ g \in G$ folgt $ghg^{-1} \in H$.

□

Korollar 2.7. A_5 ist eine einfache Gruppe.

Beweis. Sei $N \trianglelefteq G$. Nach Lagrange und **Lemma 2.6** gibt es nur die Möglichkeiten

$$|N| = 1,\ 1 + 12 + 12 + 15 + 20 = 60.$$

□

2.3 Konjugationsklassen der D_{2n}

Satz 2.8. Sei $G = D_{2n}$.

(a) Für ungerades n hat D_{2n} genau $\frac{n+3}{2}$ Konjugationsklassen:

$$D_{2n} = \{1\} \uplus \{a, a^{-1}\} \uplus \cdots \uplus \{a^{\frac{n-1}{2}}, a^{-\frac{n-1}{2}}\} \uplus \{b, ab, \ldots, a^{n-1}b\}.$$

(b) Für gerades n hat D_{2n} genau $\frac{1}{2}n + 3$ Konjugationsklassen:

$$\begin{aligned} D_{2n} = \{1\} \uplus \{a^{n/2}\} \uplus \{a, a^{-1}\} \uplus \cdots \uplus \{a^{m-1}, a^{-m+1}\} \\ \uplus \{a^{2j}b : 0 \leq j \leq n/2 - 1\} \uplus \{a^{2j+1}b : 0 \leq j \leq n/2 - 1\}. \end{aligned}$$

2.4 Konjugationsklassen der Quaternionengruppe Q_8

Sei $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ mit $i^2 = j^2 = k^2 = ijk = -1$ die Quaternionengruppe.

Satz 2.9. Die Konjugationsklassen von Q_8 sind

$$Q_8 = \{1\} \uplus \{-1\} \uplus \{i, -i\} \uplus \{j, -j\} \uplus \{k, -k\}.$$

A Appendix: Basics zu Konjugationsklassen

Konjugationsklassen kommen überall in der Mathematik vor, ein prominentes Beispiel wären die Klassen der ähnlichen Matrizen.

Definition A.1. Seien $x, y \in G$. Dann ist x **konjugiert zu** y **in** G, falls gilt

$$y = gxg^{-1} \quad \text{für ein } g \in G.$$

Die Menge

$$x^G = \left\{gxg^{-1} : g \in G\right\}$$

heißt **Konjugationsklasse** von x in G.

Lemma A.2. Konjugation induziert eine Äquivalenzrelation.

Beweis. Konjugation induziert eine Gruppenwirkung. Diese induziert eine Äquivalenzrelation. □

Korollar A.3. Seien $x, y \in G$.

(a) Entweder $x^G = y^G$ oder $x^G \cap y^G = \emptyset$.

(b) Konjugationsklassen sind disjunkt. Jede Gruppe ist eine Vereinigung von Konjugationsklassen.

Definition A.4. Sei $G = x_1^G \cup \cdots \cup x_\ell^G$, sodass die Konjugationsklasse $x_1^G, \ldots, x_\ell^G$ unterschiedlich sind. Dann heißen $x_1, \ldots, x_\ell$ **Repräsentanten** der Konjugationsklassen von G.

Proposition A.5. Seien $x, y \in G$. Dann gilt

$$x^G = y^G \implies (x^n)^G = (y^n)^G \quad \text{für alle } n \in \mathbb{Z}.$$

Weiter gilt $\operatorname{ord}(x) = \operatorname{ord}(y)$.

Beweis. Die Abbildung $\operatorname{int}_g : G \to G,\ x \mapsto gxg^{-1}$ ist für alle $g \in G$ ein Automorphismus[4]. □

Definition A.6. Sei $x \in G$. Der **Zentralisator von** x **in** G ist die Untergruppe[5]

$$C_G(x) := Z(x) := \{g \in G : gx = xg\} = \{g \in G : gxg^{-1} = x\}.$$

Satz A.7 (Bahnformel und Klassengleichung)**.** Sei G eine endliche Gruppe.

(a) Sei $x \in G$. Dann gilt

$$|x^G| = [G : C_G(x)] = \frac{|G|}{|C_G(x)|}.$$

Insbesondere $|x^G| \mid |G|$.

(b) Seien $x_1, \ldots, x_\ell$ Repräsentanten der Konjugationsklassen von G. Dann gilt

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |x_i^G| \overset{(a)}{=} |Z(G)| + \sum_{x_i \notin Z(G)} [G : C_G(x_i)].$$

[4] Die sogenannten *inneren Automorphismen*.
[5] Übung!

Beweis. Siehe Algebra 1. Dabei gilt (a) allgemeiner für Gruppenwirkungen. □

Zum Abschluss soll noch an die Konjugationsklassen der S_n erinnert werden. Die wichtigste Eigenschaft ist

Lemma A.8. Sei $\sigma = (a_1\ a_2\ \dots\ a_k) \in S_n$ ein k-Zykel und $\rho \in S_n$. Dann gilt

$$\rho \circ \sigma \circ \rho^{-1} = (\rho(a_1)\ \rho(a_2)\ \dots\ \rho(a_k)).$$

Beweis. Nachrechnen. □

Nicht schwer folgt hieraus die Klassifikation der Konjugationsklassen der S_n.

Satz A.9. Für $\sigma \in S_n$ gilt

$$\sigma^{S_n} = \{\rho \in S_n : \rho \text{ hat den gleichen Permutationstyp wie } \sigma\}.$$

Literatur

[1] G. James, M. Liebeck, *Representations and characters of groups. Second edition.*, Cambridge university Press, 2001.

[2] Siegfried Bosch, *Algebra, 8. Auflage*, Springer, 2013.

Darstellungstheorie endlicher Gruppen: Vortrag 9

Qi Zhu

10. Juli 2019

1 Liften von Charakteren

Proposition 1.1. Sei $N \trianglelefteq G$ und $\tilde{\chi}$ ein Charakter von G/N. Sei

$$\chi : G \to \mathbb{C},\ \chi(g) = \tilde{\chi}(gN) \quad (g \in G).$$

Dann ist χ ein Charakter von G und $\deg \chi = \deg \tilde{\chi}$. Sie heißt **Lift von $\tilde{\chi}$ nach G**.

Beweis. Sei $\tilde{\rho} : G/N \to \mathrm{GL}_n(\mathbb{C})$ eine Darstellung mit Charakter $\tilde{\chi}$. Dann ist

$$\rho : G \to \mathrm{GL}_n(\mathbb{C}),\ \rho = \tilde{\rho} \circ \pi$$

eine Darstellung und sie hat Charakter

$$\chi(g) = \operatorname{tr} \rho(g) = \operatorname{tr} \tilde{\rho}(gN) = \tilde{\chi}(gN).$$

Insbesondere folgt auch

$$\deg \chi = \chi(1) = \chi(\tilde{N}) = \deg \tilde{\chi}.$$

□

Satz 1.2 (Korrespondenz von Charakteren)**.** Sei $N \trianglelefteq G$. Dann ist

$$\begin{aligned} \{\tilde{\chi} : \tilde{\chi} \text{ Charakter von } G/N\} &\xrightarrow{\sim} \{\chi : \chi \text{ Charakter von } G,\ N \subseteq \ker \chi\} \\ \tilde{\chi} &\longmapsto \chi = \tilde{\chi} \circ \pi \end{aligned}$$

eine Bijektion. Genauso korrespondieren irreduzible Charaktere:

$$\begin{aligned} \{\tilde{\chi} : \tilde{\chi} \text{ irreduzibler Charakter von } G/N\} &\xrightarrow{\sim} \{\chi : \chi \text{ irreduzibler Charakter von } G,\ N \subseteq \ker \chi\} \\ \tilde{\chi} &\longmapsto \chi = \tilde{\chi} \circ \pi \end{aligned}$$

Beweis. Offenbar ist $N \subseteq \ker \chi$. Also ist die Abbildung wohldefiniert.

Sei nun χ ein Charakter von G mit $N \subseteq \ker \chi$ und Darstellung $\rho : G \to \mathrm{GL}_n(\mathbb{C})$. Nach Homomorphiesatz gibt es eine eindeutige Darstellung

$$\tilde{\rho} : G/N \to \mathrm{GL}_n(\mathbb{C}),\ \rho = \tilde{\rho} \circ \pi.$$

Sei $\tilde{\chi}$ der Charakter zu $\tilde{\rho}$. Dann ist $\chi \mapsto \tilde{\chi}$ eine Umkehrabbildung.

Bleibt zu zeigen, dass irreduzible Charaktere korrespondieren. Sei U ein Unterraum von $\mathbb{C}^n$. Dann gilt

$$\rho(g)u \in U \quad \forall u \in U \iff \tilde{\rho}(gN)u \in U \quad \forall u \in U.$$

Also ist U genau dann ein $\mathbb{C}G$-Untermodul von $\mathbb{C}^n$, wenn U ein $\mathbb{C}(G/N)$-Untermodul von $\mathbb{C}^n$ ist. Hieraus folgt die Korrespondenz von Irreduzibilität. □

Mit der nächsten Proposition können wir alle Normalteiler von einer Charaktertafel herauslesen!

Proposition 1.3. Es gilt $N \trianglelefteq G$ genau dann, wenn es irreduzible Charaktere $\chi_1, \ldots, \chi_s$ von G gibt mit

$$N = \bigcap_{i=1}^{s} \ker \chi_i.$$

Beweis. Die Rückrichtung folgt daraus, dass der Schnitt von Normalteiler wieder ein Normalteiler ist.

Zur Hinrichtung. Wenn g in jedem Kern irreduzibler Charaktere von G ist, dann folgt $\chi(g) = \chi(1)$ für alle Charaktere χ, also $g = 1$ nach Vortrag 9.[1] Also

$$\bigcap_{\chi \text{ irreduzibel}} \ker \chi = \{1\}.$$

Seien nun $\tilde{\chi}_1, \ldots, \tilde{\chi}_s$ die irreduziblen Charaktere von G/N. Nach obiger Beobachtung folgt

$$\bigcap_{i=1}^{s} \ker \tilde{\chi}_i = \{N\}.$$

Für $1 \leq i \leq s$ sei χ_i der Lift von $\tilde{\chi}_i$ nach G. Offenbar gilt

$$g \in \ker \chi_i \iff gN \in \ker \tilde{\chi}_i.$$

Somit

$$g \in \bigcap_{i=1}^{s} \ker \chi_i \iff gN \in \bigcap_{i=1}^{s} \ker \tilde{\chi}_i = \{N\} \iff g \in N$$

Folglich

$$N = \bigcap_{i=1}^{s} \ker \chi_i.$$

□

Korollar 1.4. Die Gruppe G ist genau dann nicht einfach, wenn

$$\chi(g) = \chi(1)$$

für einen nicht-trivialen irreduziblen Charakter χ von G und ein $1 \neq g \in G$ gilt.

Beweis. Zwei Richtungen.

- $\Longrightarrow$: Dann gibt es einen Normalteiler $\{1\} \subsetneq N \subsetneq G$. Nach **Proposition 1.3** gibt es einen irreduziblen Charakter χ mit $\{1\} \subsetneq \ker \chi \subsetneq G$. Damit ist χ nicht-trivial und für ein $1 \neq g \in \ker \chi$ gilt $\chi(g) = \chi(1)$.
- $\Longleftarrow$: Dann ist $\ker \chi$ ein nicht-trivialer Normalteiler.

□

Somit ist es einfach aus der Charaktertafel zu erkennen, ob eine Gruppe einfach ist!

[1] **Proposition 15.5** in James, Liebeck

Lemma 1.5. Sei χ ein linearer Charakter von G. Dann $G' \subseteq \ker \chi$.

Beweis. Lineare Charaktere sind Homomorphismen. □

Satz 1.6. Die linearen Charaktere von G sind genau die Lifts der irreduziblen Charaktere von der Abelianisierung $G^{\mathrm{ab}} = G/G'$.

Insbesondere gibt es $[G : G'] \mid G$ lineare Charaktere.

Beweis. Sei $m := [G : G']$. Da G/G' abelsch ist, hat G/G' nach Vortrag 3[2] genau m irreduzible Charaktere $\tilde{\chi}_1, \ldots, \tilde{\chi}_m$, alle vom Grad 1.

Die Lifts $\chi_1, \ldots, \chi_m$ haben also auch Grad 1 und sind genau die irreduziblen Charaktere von G mit $G' \subseteq \ker \chi$. Nach **Proposition 1.5** sind das alle linearen Charaktere. □

Proposition 1.7. Sei χ ein Charakter von G und λ ein linearer Charakter von G. Dann ist das Produkt

$$\lambda\chi : G \to \mathbb{C},\ \lambda\chi(g) = \lambda(g)\chi(g)$$

ein Charakter von G. Dabei ist χ genau dann irreduzibel, wenn $\lambda\chi$ irreduzibel ist.

Beweis. Es gibt zwei Teile.

- $\lambda\chi$ ist ein Charakter: Sei $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ eine Darstellung mit Charakter χ. Definiere die Darstellung
$$\lambda\rho : G \to \mathrm{GL}_n(\mathbb{C}),\ (\lambda\rho)(g) = \lambda(g)\rho(g).$$
Nun ist
$$\operatorname{tr}(\lambda\rho)(g) = \lambda(g)\operatorname{tr}\rho(g),$$
also hat $\lambda\rho$ Charakter $\lambda\chi$.
- Da $\lambda : G \to \mathbb{C}^\times$ ein Homomorphismus ist, folgt $\lambda(g)\overline{\lambda(g)} = 1$. Also
$$\langle\lambda\chi, \lambda\chi\rangle = \frac{1}{|G|}\sum_{g\in G}\chi(g)\lambda(g)\overline{\chi(g)\lambda(g)} = \frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\chi(g)} = \langle\chi,\chi\rangle.$$
Nach Vortrag 7[3] ist also $\lambda\chi$ genau dann irreduzibel, wenn χ irreduzibel ist.

□

Allgemeinere Produkte werden wir in Vortrag 10 sehen.

[2] **Satz 9.8** in James, Liebeck.
[3] **Satz 14.20** in James, Liebeck.

2 Einige Charaktertafeln

2.1 Symmetrische Gruppe S_4

Zuerst wollen wir lineare Charaktere der Abelianisierung hochliften. Es ist

$$S_n/S_n' \cong S_n/A_n = \{A_n,\ (1\ 2)A_n\} \cong C_2.$$

Also hat S_n/S_n' genau die zwei linearen Charaktere

$$\tilde{\chi}_1((1\ 2)A_n) = 1, \quad \tilde{\chi}_2((1\ 2)A_n) = -1.$$

Nach **Satz 1.6** hat S_n genau die linearen Charaktere $\chi_1,\ \chi_2$ gegeben durch

$$\chi_1 \equiv 1, \quad \chi_2(g) = \begin{cases} 1 & g \in A_n \\ -1 & g \notin A_n \end{cases}.$$

Als Nächstes sei χ_3 der Charakter

$$\chi_3(g) = |\operatorname{fix}(g)| - 1 \quad (g \in S_4)$$

gegeben in Vortrag 6.[4] Nach **Proposition 1.7** ist $\chi_4 := \chi_2\chi_3$ auch ein Charakter von S_4.

g_i	id	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3\ 4)$
$\lvert C_G(g_i)\rvert$	24	4	3	8	4
χ_2	1	-1	1	1	-1
χ_3	3	1	0	-1	-1
$\chi_2\chi_3$	3	-1	0	-1	1

Da

$$\langle \chi_3, \chi_3 \rangle = \frac{9}{24} + \frac{1}{4} + \frac{0}{3} + \frac{1}{8} + \frac{1}{4} = 1$$

gilt, ist χ_3 irreduzibel und somit auch $\chi_2\chi_3$.

Da S_4 genau 5 Konjugationsklassen hat, hat sie 5 irreduzible Charaktere. Wir kennen vier, also bekommen wir den letzten Charakter gratis durch Orthogonalitätsrelationen oder durch χ_{reg}.

g_i	id	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3\ 4)$
$\lvert C_G(g_i)\rvert$	24	4	3	8	4
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	3	1	0	-1	-1
χ_4	3	-1	0	-1	1
χ_5	2	0	-1	2	0

Tabelle 1: Charaktertafel der S_4

Man beachte, dass die Charaktertafel nur ganzzahlige Werte hat. Das ist ein allgemeines Phänomen der S_n. Siehe **13.1** in Serre.

[4] **Proposition 13.12** in James, Liebeck.

2.2 Alternierende Gruppe A_4

Es gilt $A_4' = V_4 = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. Hiermit ist

$$A_4 / A_4' \cong C_3.$$

Man erhält also die Charaktertafel (mit $\omega = e^{\frac{2\pi i}{3}}$)

$g_i G'$	G'	$(1\ 2\ 3)G'$	$(1\ 3\ 2)G'$
$\tilde{\chi}_1$	1	1	1
$\tilde{\chi}_2$	1	ω	ω^2
$\tilde{\chi}_3$	1	ω^2	ω

Wieder kann man auch nachrechnen, dass $\chi_4(\cdot) = |\mathrm{fix}(\cdot)| - 1$ einen irreduziblen Charakter von A_4 definiert. Mit den Lifts erhalten wir also die gesamte Charaktertafel

g_i	id	$(1\ 2)(3\ 4)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$\lvert C_G(g_i)\rvert$	12	4	3	3
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	3	-1	0	0

Tabelle 2: Charaktertafel der A_4

2.3 D_8 und Q_8

Man kann die Charaktertafel der D_8 und Q_8 mit den bisherigen Methoden finden.

$g_i^{Q_8} / g_i^{D_8}$	1	$-1/a^2$	i/b	j/a	k/ab
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

Tabelle 3: Charaktertafel der D_8 und der Q_8

Aufgabe 2.1. Verifiziere das.

Die Charaktertafeln von Q_8 und D_8 sind identisch. Aber es gilt $Q_8 \ncong D_8$. Charaktere bestimmen also bloß $\mathbb{C}G$-Moduln bis auf Isomorphie (bzw. Darstellungen bis auf Äquivalenz). Im Allgemeinen bestimmen sie keine Gruppen bis auf Isomorphie!

A Appendix: Kommutatorgruppen

Wir wollen kurz an Kommutatorgruppen erinnern.

Definition A.1. Sei G eine Gruppe.

(a) Der **Kommutator** für $x, y \in G$ ist

$$[x, y] := xyx^{-1}y^{-1}.$$

(b) Die **Kommutatorgruppe** von G ist

$$G' := K(G) := [G, G] := \langle [x, y] : x, y \in G \rangle.$$

Proposition A.2. Sei $N \trianglelefteq G$.

(a) $G' \trianglelefteq G$.

(b) $G' \subseteq N \iff G/N$ abelsch. Insbesondere ist G/G' abelsch.

Die Gruppe $G^{\text{ab}} := G/G'$ heißt **Abelianisierung** von G.

Beispiel A.3. Eine wichtige Kommutatorgruppe ist $S_n' = A_n$.

Literatur

[1] G. James, M. Liebeck, *Representations and characters of groups. Second edition.*, Cambridge university Press, 2001.

[2] Siegfried Bosch, *Algebra, 8. Auflage*, Springer, 2013.

[3] Jean-Pierre Serre, *Linear Representations of Finite Groups*, Springer, 1977.