V4 Ü2.

§0 Einleitung, Erinnerung an Grundbegriffe

Eine Gruppe ist eine (nicht-leere) Menge G zusammen mit einer Verknüpfung $*: G \times G \to G$ mit folgenden Eigenschaften:

(1) $*$ assoziativ, also $a*(b*c) = (a*b)*c$ für alle $a, b, c \in G$.

(2) Es gibt ein neutrales Element $e \in G$ mit $a*e = e*a = a$ für alle $a \in G$.

(3) Zu jedem $a \in G$ gibt es ein inverses Element $a' \in G$ mit $a*a' = a'*a = e$.

(Hier sind e und a' jeweils eindeutig bestimmt)

$|G|$ = Mächtigkeit von G, werden sowohl endliche als auch unendliche Gruppen betrachten.

Beispiele, die Sie bereits aus der Linearen Algebra kennen:

- K Körper $A \in M_n(K)$, $A = (a_{ij})$ $n \times n$-Matrix

$$\det(A) = \sum_{\pi \in S_n} \underbrace{\operatorname{sgn}(\pi)}_{\text{Signum}} a_{1,\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)}$$

mit S_n = symmetrische Gruppe vom Grad n.

Als Menge: alle bijektiven Abbildungen

$\pi: \{1,\dots,n\} \to \{1,\dots,n\}$ Verknüpfung: "$\circ$"

$|S_n| = n!$ endl. Gruppe. (Hintereinanderausführung).

z.B. $n=3$

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{also} \quad \pi(1)=2,\ \pi(2)=1,\ \pi(3)=3$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \pi \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Beachte: Reihenfolge ist wichtig $\nabla_{\circ}$.

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq \pi \circ \sigma.$$

Definition: Eine Gruppe G heißt abelsch, wenn

$a * b = b * a$ für alle $a, b \in G$ gelt.

In diesem Fall wird oft Verknüpfung mit $+$ bezeichnet, neutrales Element mit 0 und inverses Element mit $-a$.

Standardbeispiel: $(\mathbb{Z}, +)$

Für $n \geq 3$ ist S_n nicht abelsch, s.o.

Weiteres Beispiel:

$$GL_n(K) = \{ A \in M_n(K) \mid A \text{ invertierbar (bzgl. Multiplikation)} \}$$

$$= \{ A \in M_n(K) \mid \det(A) \neq 0 \}$$

Gruppe bzgl. üblicher Matrixmultiplikation:

$|K| = \infty \iff GL_n(K)$ unendlich

Definition: Sei G eine Gruppe und $H \subseteq G$ Teilmenge. Dann heißt H eine Untergruppe (in Zeichen $H \leq G$), wenn gilt:

$e \in H$, $a * b \in H$ und $a^{-1} \in H$ für alle $a, b \in H$.
(insbesondere $H \neq \emptyset$)

$\Rightarrow$ H zusammen mit der Einschränkung der Verknüpfung aus G ist wieder eine Gruppe.

Beispiele: a) $G = GL_n(K)$ K Körper

$SL_n(K) = \{ A \in GL_n(K) \mid \det(A) = 1 \}$.

Untergruppe (benutze $\det(AB) = \det(A)\det(B)$)

$$H := \left\{ \begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{pmatrix} \mid \begin{array}{l} 0 \neq a_i \in K \\ * \in K \text{ bel.} \end{array} \right\} \subseteq G \text{ Untergruppe.}$$

(benutze: Produkte und Inverse von oberen Dreiecksmatrizen sind wieder obere Dreiecksmatrizen)

$$\begin{pmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{pmatrix}^{-1} = \begin{pmatrix} a_1^{-1} & & * \\ & \ddots & \\ 0 & & a_n^{-1} \end{pmatrix}.$$

b) $G = GL_n(K)$ K Körper

$O_n(K) = \{ A \in GL_n(K) \mid A \cdot A^{tr} = \underset{\uparrow}{I_n} \}$.

ist Untergruppe. Einheitsmatrix

(selbst nachrechnen),

GL_n = allgemeine lineare Gruppe

SL_n = spezielle — " —

O_n = orthogonale Gruppe.

c) $G = S_n$ symmetrische Gruppe

$A_n := \{ \pi \in S_n \mid \operatorname{sgn}(\pi) = 1 \}$ alternierende

Gruppe, sog Untergruppe (benutze $\operatorname{sgn}(\pi \circ \sigma) = \operatorname{sgn}(\pi) \cdot \operatorname{sgn}(\sigma)$)

$\pi \in A_n \Leftrightarrow \pi$ "gerade" Permutation.

Definition: Seien G, H Gruppen. Eine Abbildung $f: G \to H$ heißt Gruppen-Homomorphismus, wenn

$$f(a * b) = f(a) \cdot f(b) \quad \text{für alle } a, b \in G \text{ gelt}$$

($*$: Verknüpfung in G; $\cdot$: Verknüpfung in H.)

Es folgt dann automatisch $f(e_G) = e_H$ und

$$f(a') = f(a)'$$

(a': Inverse in G; $f(a)'$: Inverse in H.)

Ein Homomorphismus, der bijektiv ist, heißt Isomorphismus. Die beteiligten Gruppen heißen dann isomorph, in Zeichen $G \cong H$.

Sind zwei Gruppen G, H isomorph, so kann man in G genauso rechnen wie in H, die beiden Gruppen sind in diesem Sinne also "gleich".

Satz von Cayley: Sei G endliche Gruppe. Dann gibt es ein $n \in \mathbb{N}$, so daß G isomorph ist zu einer Untergruppe von S_n.

$\rightsquigarrow$ ein Thema dieser Vorlesung: Wie rechnet man effizient mit Untergruppen von S_n?

Definition. Sei G eine Gruppe und $S \subseteq G$ Teilmenge. Dann heißt

$$\langle S \rangle := \bigcap_{H \leq G \text{ mit } S \subseteq H} H \leq G$$

die von S erzeugte Untergruppe von G.

Bemerke: Ist $\{H_i\}_{i \in I}$ beliebige Familie von Untergruppen von G, so ist auch $\bigcap_{i \in I} H_i$ eine Untergruppe (Beweis selbst).

Also $\langle S \rangle$ tatsächlich Untergruppe.

Man sieht leicht: Für $S = \emptyset$, ist $\langle \emptyset \rangle = \{e\}$.

Für $S \neq \emptyset$ ist

$$\langle S \rangle = \{ x_1 * \dots * x_r \mid r \geq 1, x_i \in S \text{ oder } x_i^{-1} \in S \} \cup \{e\}.$$

Im besondere: Ist $S = \{g\}$ 1-elementig, so

$$\langle g \rangle := \langle \{g\} \rangle = \{ g^m \mid m \in \mathbb{Z} \} \text{ wobei}$$

$$g^m = \begin{cases} g * \dots * g \ (m\text{-mal}) & \text{falls } m > 0 \\ e & \text{falls } m = 0 \\ g^{-1} * \dots * g^{-1} \ (-m)\text{-mal} & \text{falls } m < 0. \end{cases}$$

Mit dieser Regel gelt: $g^m * g^n = g^{m+n}$ für alle $m, n \in \mathbb{Z}$.
(siehe Skript §5).

Definition Für $g \in G$ heißt

$$o(g) := |\langle g \rangle|$$ die Ordnung von g.

Man sieht leicht: Ist $o(g) < \infty$, so

gelt $o(g) = \min \{ m \geq 1 \mid g^m = 1 \}$

und $\langle g \rangle = \{ e, g, g^2, \dots, g^{o(g)-1} \}$. (Skript Beisp. 5.3)

Ist $G = \langle g \rangle$ für ein $g \in G$, so heißt G zyklisch. Insbesondere ist dann G abelsch.

Beispiel: Sei $G = S_3$ symmetrische Gruppe vom Grad 3.

$|G| = 3! = 6$.

$G = \{ id, \pi, \pi', \sigma_1, \sigma_2, \sigma_3 \}$ mit $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$\pi' = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.

$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

$H_i = \langle \sigma_i \rangle$ für $i = 1, 2, 3$ Untergruppe der Ordnung 2

denn $\sigma_i^2 = id$ für $i = 1, 2, 3$.

$o(\pi) = 3 \Rightarrow U = \langle \pi \rangle = \{ id, \pi, \pi' \}$

Untergruppe der Ordnung 3

zusammen mit $\{e\}$ und G komplette Liste aller Untergruppen von G.

(Man muß noch zeigen, daß es keine weiteren Untergruppen gibt; dazu braucht man am besten:)

Satz von Lagrange: Ist G eine endliche Gruppe und $H \leq G$ eine Untergruppe, so gilt $|H| \mid |G|$.

Insbesondere: $o(g) \mid |G|$ für alle $g \in G$.

Allgemeine Fragestellungen (1) Zu gegebener Gruppe G, finde Erzeugendensystem $S \subseteq G$ mit $G = \langle S \rangle$ und "guten" Eigenschaften, z.B. S so klein wie möglich.

(2) Umgekehrt: Ist $S \subseteq G$ gegeben, bestimme $\langle S \rangle$, z.B. $|\langle S \rangle|$ falls G endlich.

Beispiele:

$$M_{11} = \left\langle \underbrace{\begin{pmatrix} 1&2&3&4&5&6&7&8&9&10&11 \\ 2&3&4&5&6&7&8&9&10&11&1 \end{pmatrix}}_{=\pi}, \underbrace{\begin{pmatrix} 1&2&3&4&5&6&7&8&9&10&11 \\ 1&2&7&10&6&4&11&3&9&5&8 \end{pmatrix}}_{=\sigma} \right\rangle$$

"Mathieu-Gruppe" $\leq S_{11}$

Es gelt $o(\pi) = 11$ $\quad o(\sigma) = 4$

Was ist $|M_{11}| = ?$

$K = \mathbb{Z}/11\mathbb{Z}$ Körper mit 11 Elementen

$J_1 := \langle A, B \rangle \leq GL_7(K)$ wobei

$$A = \begin{bmatrix} 0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&1 \\ -1&0&0&0&0&0&0 \end{bmatrix}, \quad B = \begin{bmatrix} -3&2&-1&-1&-3&-1&-3 \\ -2&1&1&3&1&3&3 \\ -1&-1&-3&-1&-3&-3&2 \\ -1&-3&-1&-3&-3&2&-1 \\ -3&-1&-3&-3&2&-1&-1 \\ 1&3&3&-2&1&1&3 \\ 3&3&-2&1&1&3&1 \end{bmatrix}$$

Janko-Gruppe (~1966)

Es gelt $o(A) = 2$ und $o(B) = 7$

Was ist $|J_1| = ?$

} siehe "Klassifikation der endlichen einfachen Gruppen"

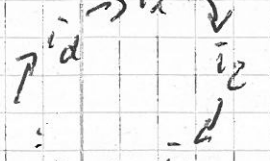
Noch einmal zu S_n: Vereinfachte Schreibweise

Gegeben seien $i_1, \dots, i_n \in \{1, \dots, n\}$ paarweise verschieden.

Dann erhalten wir eine Permutation $\sigma \in S_n$

durch: $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, ..., $\sigma(i_{d-1}) = i_d$

$\sigma(i_d) = i_1$ und $\sigma(i) = i$ für $i \notin \{i_1, \dots, i_d\}$



σ heißt d-Zyklus oder einfach Zyklus.

Schreibe einfach $\sigma = (i_1\ i_2\ \dots\ i_d)$.

Man kann in jeder Stelle im Kreis anfangen und erhält stets die gleiche Permutation, also $\sigma = (i_2\ i_3\ \dots\ i_d\ i_1)$ etc.

Potenzen von σ $\rightsquigarrow$ Drehe Kreis um 1, 2, etc Kanten weiter $\Rightarrow$ $\boxed{o(\sigma) = d}$ Ein d-Zyklus hat Ordnung d

z.B. $\sigma = (3\,5\,4) \in S_5$, d.h. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}$

$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix} = (3\,4\,5)$ $\quad \sigma^3 = id$.

Ein 2-Zyklus heißt Transposition $\tau = (i\ j)$ vertauscht genau 2 Ziffern und lässt alle anderen fest.

[1-Zyklus: = Identität].

$\boxed{\text{Jedes } \pi \in S_n \text{ lässt sich als Produkt von disjunkten Zyklen schreiben}}$

z.B. $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 5 & 1 & 8 & 7 & 2 \end{pmatrix} \in S_8$

$= (1\,3\,4\,5) \circ (2\,6\,8) \circ (\not{7})$ ← kann man weglassen.

↑ kleinste Ziffer

↑ kleinste Ziffer, die noch nicht in vorherigen Zyklen ist

Beachte: σ, τ disjunkte Zykel $\Rightarrow \sigma \circ \tau = \tau \circ \sigma$.
also Reihenfolge in Zykeldarstellung beliebig!

Beispiel: M_{11} $\quad \pi = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11)$
11-Zykel $\quad o(\pi) = 11$.

$\sigma = (3\ 7\ 11\ 8) \circ (4\ 10\ 5\ 6) \quad o(\sigma) = 4$.

> σ d-Zykel $(d \geq 2) \Rightarrow \sigma$ Produkt von $d-1$ Transpositionen.

denn sei $\sigma = (i_1\ i_2 \dots i_d)$ dann

$$\sigma = (i_1\ i_2) \circ (i_2\ i_3) \circ \dots \circ (i_{d-1}\ i_d)$$

(wende beide Seiten auf ein beliebiges i an $\rightarrow$ erhalte jeweils gleiches Ergebnis.)

Schließlich: $\tau = (i\ j)$ Transposition $\Rightarrow \operatorname{sgn}(\tau) = -1$
Also σ d-Zykel $\Rightarrow \operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{falls } d \text{ ungerade} \\ -1 & \text{falls } d \text{ gerade.} \end{cases}$

Satz: $S_n = \langle (i\ j) \mid 1 \leq i < j \leq n \rangle$
S_n wird von Transpositionen erzeugt.

denn: $\sigma \in S_n$ beliebig $\Rightarrow \sigma$ Produkt von disjunkten Zykeln, schreibe dann jeden Zykel als Produkt von Transpositionen.

Analog Übungsaufgabe:

$$A_n = \langle (i\ j) \circ (k\ l) \mid i, j, k, l \text{ paarweise verschieden} \rangle$$

für $n \geq 5$.

Definition: Eine Untergruppe $U \leq G$ heißt Normalteiler, wenn $g \cdot u \cdot g^{-1} \in U$ für alle $g \in G$ und $u \in U$ gilt

Bedeutung: Man kann Faktorgruppe bilden

$G/U = \{ gU \mid g \in G \}$ Menge der Nebenklassen.

$gU * hU := (gh)U$ für alle $g, h \in G$

"wohldefiniert" wegen Normalteilerbedingung

Im Beispiel: $U \trianglelefteq G$.

Elementare Bausteine der Gruppentheorie:

G heißt "einfach", wenn $G \neq \{1_G\}$ und $\{1_G\}, G$ die einzigen Normalteiler von G sind.

Satz Für $n \geq 5$ ist A_n einfach. (nicht abelsch)

Beachte: Für $n = 2, 3, 4$ ist A_n tatsächlich nicht einfach, oder abelsch. dann:

$n=2$ $|A_2| = 1$ $n=3$ $|A_3| = 3$ zyklisch

$n=4$ $V_4 = \{ id, (12)\circ(34), (13)\circ(24), (14)\circ(23) \} \trianglelefteq A_4$

"Kleinsche Vierergruppe" nachrechnen.

Beweis: Sei $N \trianglelefteq A_n$ mit $N \neq \{id\}$.

Reicht zu zeigen: $N = A_n$. Nach Übungsaufgabe genügt es zu zeigen: N enthält alle Elemente der Form $(ij)\circ(kl)$ mit i,j,k,l paarweise verschieden.

Idee: Sei $id \neq u \in N$. Dann versuche, aus u neue Elemente von N zu produzieren

Verfahren: Für $\sigma \in A_n$ ist $\sigma \circ u^{-1} \circ \sigma^{-1} \in N$

und dann auch $u \circ \sigma \circ u^{-1} \circ \sigma^{-1} \in N$.

Schreibe u als Produkt von disjunkten Zyklen.
Ist u Produkt von disjunkten 2-Zyklen,
so kommen mindestens 2 vor (wegen $u \in A_n$).
Sonst enthält u einen Zyklus der Länge ≥ 3.
4 Fälle:

(I) $u = (a,b) \circ (c,d) \circ \ldots$ (Produkt von disj. 2-Zyklen)

(II) $u = (a,b,c)$ (ein Dreierzyklus)

(III) $u = (a,b,c) \circ (d,e,\ldots) \circ \ldots$ (ein 3-Zyklus und mind. ein weiterer Zyklus)

(IV) $u = (a,b,c,d,\ldots) \circ \ldots$ (mind. 1 Zyklus der Länge ≥ 4)

Wähle in jedem Fall geeignetes $\sigma \in A_n$.

u	σ	$u \circ \sigma \circ u^{-1}$	σ^{-1}	$(u \circ \sigma \circ u^{-1}) \circ \sigma^{-1}$
(I)	(a,b,c)	(b,a,d)	$(a\ c\ b)$	$(a,c) \circ (b,d)$
(II)	(a,b,d)	(b,a,d)	$(a\ d\ b)$	$(a\ b) \circ (c,d)$
(III)	(a,b,d)	(b,c,e)	$(a\ d\ b)$	$(a\ d\ c\ e\ b)$
(IV)	(a,b,c)	(b,c,d)	$(a\ c\ b)$	$(a\ d\ b)$

Beachte: Ist $\sigma = (i_1\ i_2\ i_3)$ 3-Zyklus und $\pi \in S_n$ beliebig, so $\pi \circ \sigma \circ \pi^{-1} = (\pi(i_1)\ \pi(i_2)\ \pi(i_3))$
(einfaches Nachrechnen, analog auch für Zyklus beliebiger Länge.)

Fälle (I), (II) erhalte Element der Form $(i\,j) \circ (k\,l)$ mit gewünschtem.

Fall (IV): wende dann Fall (II) an $\rightsquigarrow$ gewünschtes Element.

Fall (III): Ergebnis mit Fall (IV), danach wieder Fall (II).

Also: es gibt paarweise verschiedene i,j,k,l mit $(ij)\circ(kl) \in N$.

Jetzt zeige: N enthält alle Elemente dieser Form.

Zuerst: $(12)\circ(34) \in N$.

Dann betrachte

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ i & j & k & l & 5 & \dots & n \end{pmatrix} \in S_n$$

$$\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \dots & n \\ j & i & k & l & 5 & \dots & n \end{pmatrix} = (ij)\circ\sigma \in S_n.$$

Dann gelt also $\sigma \in A_n$ oder $\sigma' \in A_n$.

In beiden Fällen $\sigma\circ(12)\circ(34)\circ\sigma^{-1} = \sigma'\circ(12)\circ(34)\circ\sigma'^{-1}$

$$= (ij)\circ(kl)$$

also [redacted] $(12)\circ(34) \in N$.

Sind nun a,b,c,d beliebig paarweise verschieden, so folgt mit völlig analoger Rechnung (nur umgelehrt) dass $(ab)\circ(cd) \in N$. □

Weiterer fundamentaler Begriff:

Operation von Gruppen auf Mengen.

Definition. Sei G Gruppe und X eine nicht-leere Menge. Wir sagen, dass G auf X operiert, oder dass X eine G-Menge ist, wenn es eine Abbildung $\mu: G\times X \to X$, $(g,x) \mapsto g\cdot x$ gibt mit folgenden Eigenschaften:

(a) $1_G \cdot x = x$ für alle $x \in X$.

(b) $(g*h)\cdot x = g\cdot(h\cdot x)$ für alle $g,h \in G$, $x \in X$.

Standardbeispiel:

$G = S_n$ operiert auf $X = \{1, \dots, n\}$ durch

$$G \times X \to X$$
$$(\pi, i) \mapsto \pi \circ i = \pi(i),$$

$(\sigma \circ \pi) \cdot i = (\sigma \circ \pi)(i) = \sigma(\pi(i)) = \sigma \cdot (\pi \cdot i)$, $id \cdot i = id(i) = i$ ✓.

Zusammenhang mit Permutationen:

Für festes $g \in G$ definiere

$$\pi_g : X \to X, \quad x \mapsto g \cdot x$$

Sei auch $h \in G$. Dann sind

$$\pi_h : X \to X, \quad \pi_{g*h} : X \to X, \quad \pi_{h \circ g} : X \to X$$

definiert.

$$\pi_{g*h}(x) = (g*h) \cdot x = g \cdot (h \cdot x) = \pi_g(\pi_h(x)) = (\pi_g \circ \pi_h)(x).$$

für alle $x \in X$, also

(*) $\pi_{g*h} = \pi_g \circ \pi_h$ für alle $g, h \in G$.

$\pi_{1_G}(x) = 1_G \cdot x = x$ für alle $x \in X$, also $\pi_{1_G} = id_X$.

Ist $h = g^{-1}$ (Inverses), so $\pi_g \circ \pi_{g^{-1}} = \pi_{g \cdot g^{-1}} = \pi_{1_G} = id_X$

und genauso $\pi_{g^{-1}} \circ \pi_g = id_X$.

D.h. $\pi_g : X \to X$ bijektiv mit $\pi_g^{-1} = \pi_{g^{-1}}$.

und damit $\pi_g \in S_X$ = symmetrische Gruppe auf X (mit $\circ$ als Verknüpfung)

Obige Formel (*) zeigt dann, daß

$$\pi : G \to S_X, \quad g \mapsto \pi_g$$

ein Gruppen-Homomorphismus ist.

D.h. zu jeder Operation von G auf X gehört ein Homomorphismus von G nach S_X.

Umgekehrt: Ist $\varphi: G \to S_X$ ein Gruppen-Homomorphismus (X bel. Menge $\neq \emptyset$), so operiert G auf X durch

$$G \times X \to X, \quad (g, x) \mapsto g.x = \varphi(x).$$

$$\mathrm{Kern}(\pi) = \{ g \in G \mid \pi_g = id_X \}$$
$$= \{ g \in G \mid g.x = x \text{ für alle } x \in X \}.$$

Definition: Die Operation von G auf X heißt "treu", wenn $\mathrm{Kern}(\pi) = \{1_G\}$ gilt.

In diesem Fall ist $\pi: G \to S_X$ injektiv, also G isomorph zu einer Untergruppe von S_X.

Beispiel: Sei K Körper und $G \leq GL_n(K)$.

Dann operiert G auf $V = K^n$ durch

$$G \times V \to V$$
$$(A, v) \mapsto Av = \text{Produkt Matrix} \cdot \text{Spaltenvektor}$$

Diese Operation ist treu: $Av = v$ für alle $v \in K^n$

$\Rightarrow A = I_n$ Einheitsmatrix.

Sei nun $X = \{ \langle v \rangle \mid 0 \neq v \in K^n \}$

Menge der 1-dimensionalen Teilräume von V "projektiver Raum".

Ist $A \in G$ und $0 \neq v \in K^n$, so ist auch $Av \neq 0$ und $A.(sv) = s.Av$ für alle $s \in K$.

Also operiert G auch auf X durch.

$G \times X \to X$

$(A, \langle v \rangle) \mapsto \langle Av \rangle$ (wohl-definiert).

Erhalte zugehörigen Homomorphismus $\pi: G \to S_X$

mit $\ker(\pi) = \{ A \in G \mid \pi_A = id_X \}$

$= \{ A \in G \mid \langle Av \rangle = \langle v \rangle$ für alle $0 \neq v \in K^n \}$.

$= \{ A \in G \mid Av = sv$ für ein $0 \neq s \in K$, für alle $0 \neq v \in K^n \}$?

$\overset{!}{=} \{ A \in G \mid A = sI_n$ für ein $0 \neq s \in K \}$?

"Skalarmatrizen in G".

denn: $A = sI \Rightarrow Av = sv$, also $\langle Av \rangle = \langle v \rangle$ für alle $0 \neq v \in K^n$ ✓.

Umgekehrt: $Av = sv$ für alle $0 \neq v \in K^n$

$\Rightarrow Ae_i = s_i e_i$ mit $0 \neq s_i \in K$, wobei

$e_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \leftarrow i$ Einheitsvektoren in K^n.

also $A = \begin{bmatrix} s_1 & & 0 \\ & s_2 & \\ & & \ddots \\ 0 & & s_n \end{bmatrix}$ diagonal.

Annahme: es gibt $i < j$ mit $s_i \neq s_j$.

Dann betrachte $v = e_i + e_j$

$Av = Ae_i + Ae_j = s_i e_i + s_j e_j$

aber dies soll auch $sv = se_i + se_j$ für ein $0 \neq s \in K$ sein,

also $s = s_i = s_j$ ↯. ✓

Bahnen und Stabilisatoren

Sei X eine G-Menge.

Für festes $x \in X$ heißt

$$\mathrm{Stab}_G(x) = G_x = \{ g \in G \mid g \cdot x = x \}.$$

der Stabilisator von x. Dies ist eine Untergruppe von G. Weiterhin heißt

$$\mathcal{O}_x := \{ g \cdot x \mid g \in G \}$$ die Bahn von x unter der Operation von G. Dies ist eine Teilmenge von X. Die folgende Abbildung ist wohl-definiert und bijektiv

$$\begin{aligned} \mu_x : \mathcal{O}_x &\to G/G_x \\ g \cdot x &\mapsto g G_x. \end{aligned}$$

Insbesondere: Ist $|G| < \infty$, so folgt $|\mathcal{O}_x| < \infty$ und $$|\mathcal{O}_x| = |G/G_x| = \frac{|G|}{|G_x|}.$$

Allgemein: Für $x, y \in X$ sind $\mathcal{O}_x, \mathcal{O}_y$ entweder gleich oder disjunkt.

$$\boxed{X \text{ ist disjunkte Vereinigung von Bahnen}}$$

(siehe Skript).

Definition: Sei X eine G-Menge. Die Operation von G auf X heißt transitiv, wenn es nur eine Bahn gibt, d.h. zu $x, y \in X$ gibt es stets ein $g \in G$ mit $g \cdot x = y$.

Beispiele: a) $G = S_n$ operiert auf $X = \{1, \dots, n\}$. Diese Operation ist transitiv, denn z.B. $X = \mathcal{O}_1$

Ist $i \geq 1$, so $(1\ i) \cdot 1 = i \quad \forall$.

b) K Körper $G = GL_n(K)$ operiert auf $V = K^n$

$\mathcal{O}_0 = \{A \cdot 0 \mid A \in G\} = \{0\}$ eine Bahn, die nur aus einem Element besteht.

↑ Null-Vektor

Sei $e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$. Behauptung: $\mathcal{O}_{e_1} = K^n \setminus \{0\}$.

denn: $\mathcal{O}_{e_1} = \{Ae_1 \mid A \in GL_n(K)\}$.

$= \{v \in K^n \mid v$ 1. Spalte einer Matrix $A \in GL_n(K)\}$.

aber jeder Spaltenvektor $\neq 0$ kann zu einer Basis von K^n ergänzt werden, also gibt es $A \in GL_n(K)$ mit $Ae_1 =$ geg. Spaltenvektor $\neq 0$.

Zerlegung in Bahnen: $K^n = \mathcal{O}_0 \dot\cup \mathcal{O}_{e_1}$.

Operation nicht transitiv.

Weitere nützliche Operationen

(1) G Gruppe. Dann operiert G auf $X = G$ durch Linksmultiplikation

$$G \times X \to X$$
$$(g, x) \mapsto g \cdot x = g * x.$$

Diese Operation ist transitiv ($\mathcal{O}_{1_G} = G$) und treu ($\ker(\pi) = \{g \in G \mid g * x = x$ für alle $x \in G\} = \{1_G\}$).

also G isomorph zu Untergruppe von S_X.

(Dies ist Idee des Beweises des Satzes von Cayley: Ist $n = |G| < \infty$, so G isomorph zu Un...

von $S_G \cong S_n$ wegen $|G| = n$).

(2) G operiert auf $X = G$ durch Konjugation

$$G \times X \to X$$
$$(g, x) \mapsto g * x * g^{-1}.$$

Es gilt $\Theta_{1_G} = \{ g * 1_G * g^{-1} \mid g \in G \} = \{1_G\}$

also ist dies niemals transitiv wenn $G \neq \{1_G\}$

$$\mathrm{Kern}(\pi) = \{ g \in G \mid g * x * g^{-1} = x \text{ für alle } x \in X \}.$$
$$= \{ g \in G \mid g * x = x * g \text{ für alle } x \in G \}$$
$$=: Z(G) \text{ wird auch als Zentrum von } G \text{ bezeichnet.}$$

(1) Bestimme $Z(S_n)$, $Z(A_n)$, $Z(GL_n(K))$.

(3) Sei $0 \neq f \in \mathbb{Q}[X]$ nicht-konstantes Polynom

Nach Fundamentalsatz der Algebra zerfällt dies in Linearfaktoren über $\mathbb{C}$, also

$$f = c(X - z_1) \cdots (X - z_n) \text{ mit } 0 \neq c \in \mathbb{Q}, \; z_i \in \mathbb{C}$$

wobei $n = \mathrm{Grad}(f) \geq 1$

Sei $L = \mathbb{Q}(z_1, \ldots, z_n) \subseteq \mathbb{C}$ Zerfällungskörper von f

und $G := \mathrm{Aut}(L, \mathbb{Q}) = \{ \varphi : L \to L \mid \varphi \text{ Körperautom.} \}$ (mit $\varphi|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$)

Galois-Gruppe von f.

Dann $|G| = |L : \mathbb{Q}| \leq n!$, also G endliche Gruppe. Diese operiert auf $X = \{z_1, \ldots, z_n\}$ durch

$$G \times X \to X \qquad \text{Operation ist treu:}$$
$$(\varphi, z_i) \mapsto \varphi(z_i). \qquad \varphi(z_i) = z_i \text{ für alle } i \Rightarrow \varphi = \mathrm{id}_L.$$

f irreduzibel $\Rightarrow$ Operation ist transitiv, $n = |X|$

und G isomorph zu Untergr. von S_n.

Schließlich noch Wiederholungen zu Vektorräumen mit Skalarprodukten.

Def. Sei K Körper, V K-Vektorraum. Eine Abbildung $\beta: V \times V \to K$ heißt Bilinearform, wenn β linear in jedem Argument ist, also

$$\beta(sv + tv', w) = s\beta(v, w) + t\beta(v', w)$$
$$\beta(v, sw + tw') = s\beta(v, w) + t\beta(v, w')$$

für alle $v, v', w, w' \in V$, $s, t \in K$.

Standardbeispiel: $V = K^n$

$$\beta\left(\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}\right) = \sum_{i=1}^{n} x_i y_i.$$

Ist $K = \mathbb{R}$, so gilt $\beta\left(\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}\right) = \sum_{i=1}^{n} x_i^2 \geq 0$

mit "$=0$" nur für $\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$.

Also β "positiv-definit", "Skalarprodukt".

Sei von nun an $n = \dim V < \infty$.

$B = \{v_1, \dots, v_n\}$ Basis von V

$$G := \left(\beta(v_i, v_j)\right)_{1 \leq i,j \leq n} \in M_n(K)$$

heißt Gram-Matrix von β (bzgl. B).

Ist $C = \{w_1, \dots, w_n\}$ ebenfalls Basis von V

so erhalte neue Gram-Matrix

$$G' := \left(\beta(w_i, w_j)\right)_{1 \leq i,j \leq n} \in M_n(K)$$

Sei $T = (t_{ij}) \in M_n(K)$ Basiswechselmatrix.

also $w_j = \sum_{i=1}^{n} t_{ij} v_i$ für $1 \le j \le n$.

Dann $\beta(w_i, w_j) = \sum_{k,l=1}^{n} t_{ki}\, t_{lj}\, \beta(v_k, v_l)$

$$= \underbrace{\sum_{k,l=1}^{n} t_{ki}\, \beta(v_k, v_l) \cdot t_{lj}}$$

$= (i,j)$-Eintrag von $T^{tr} \cdot G \cdot T$

also Formel $\boxed{G' = T^{tr} \cdot G \cdot T}$

wobei $\det(T) \neq 0$, weil Basiswechsel-

Insbesondere $\det(G') = \det(T)^2 \det(G) \neq 0$

$\Leftrightarrow \det(G) \neq 0$

<u>Definition</u>: β heißt nicht-ausgeartet, wenn $\det(G) \neq 0$, wobei G Gram-Matrix bzgl. einer Basis von V ist.

Betrachten meistens nur nicht-ausgeartete Bilinearformen.

<u>Definition</u>: Eine lineare Abbildung $\varphi: V \to V$ heißt "orthogonal" bzgl. $\beta: V \times V \to K$ wenn $\beta(\varphi(v), \varphi(w)) = \beta(v,w)$ für alle $v, w \in V$ gilt.

<u>Matrixversion</u>:

Sei $B = \{v_1, \dots, v_n\}$ Basis von V

$A = M_B(\varphi) \in M_n(K)$ Matrix von φ bzgl. B,

d.h. $A = (a_{ij})$ mit $\varphi(v_j) = \sum_{i=1}^{n} a_{ij} v_i$

$G = (g_{ij}) = (\beta(v_i, v_j))$ Gram-Matrix. Dann:

φ orthogonal $\iff$ $\beta(\varphi(v_i), \varphi(v_j)) = \beta(v_i, v_j)$

$\uparrow$ β bilinear für alle $1 \le i, j \le n$.

$$\iff g_{ij} = \sum_{k,l=1}^{n} a_{ki}\, a_{lj}\, \beta(v_k, v_l).$$

$$= \sum_{k,l=1}^{n} a_{ki}\, \underbrace{\beta(v_k, v_l)}_{=\beta_{kl}}\, a_{lj} \quad \leftarrow (i,j)\text{-Eintrag von } A^{tr} \cdot G \cdot A.$$

Also: $\boxed{\varphi \text{ orthogonal} \iff G = A^{tr} \cdot G \cdot A}$

Insbesondere sehen wir: β nicht-ausgeartet $\Rightarrow$

$\det(G) \neq 0 \Rightarrow 0 \neq \det(G) = \det(A)^2 \det(G)$

$\rightarrow \det(A) \neq 0 \Rightarrow \varphi$ invertierbar.

Folgerung $\beta : V \times V \to K$ nicht-ausgeartet.

$\Rightarrow \Gamma(V, \beta) := \{ \varphi : V \to V \mid \varphi$ linear und orthogonal bzgl. $\beta \}$

ist eine Gruppe mit $\circ$ als Verknüpfung.

[nachrechnen: $\varphi, \psi \in \Gamma(V, \beta) \Rightarrow \varphi \circ \psi \in \Gamma(V, \beta)$

$id_V \in \Gamma(V, \beta)$

$\varphi \in \Gamma(V, \beta) \Rightarrow \varphi^{-1} \in \Gamma(V, \beta)$]

also $\Gamma(V, \beta)$ Untergruppe von

$GL(V) = \{ \varphi : V \to V \mid \varphi$ linear, bijektiv $\}$.

Matrixversion: G Gram-Matrix von β bzgl. Basis von V

$\Gamma_n(G) := \{ A \in M_n(K) \mid G = A^{tr} \cdot G \cdot A \}$.

Untergruppe von $GL_n(K)$.

Definition Sei $\beta: V \times V \to K$ Bilinearform.

β heißt reflexiv, wenn gilt:

$$\beta(v,w) = 0 \iff \beta(w,v) = 0 \quad \text{für alle } v,w \in V.$$

Gilt $\beta(v,w) = 0$, so heißen v, w orthogonal zueinander, in Zeichen $v \perp w$.

Lemma: Sei β reflexiv. Dann gilt

$$\beta(u,v)\,\beta(w,u) = \beta(v,w)\,\beta(u,w) \quad \text{für}$$

alle $u,v,w \in V$.

Beweis: Setze $x := \beta(u,v)\,w - \beta(u,w)\,v \in V$.

Dann $\beta(u,x) = \beta(u,v)\,\beta(u,w) - \beta(u,w)\,\beta(u,v) = 0$.

Wegen reflexiv also auch

$$0 = \beta(x,u) = \beta(u,v)\,\beta(w,u) - \beta(u,w)\,\beta(v,u) \qquad \square$$

Satz: Sei $\beta: V \times V \to K$ Bilinearform. Dann gilt

β reflexiv $\iff$ β symmetrisch oder alternierend.

wobei β symmetrisch, falls $\beta(u,v) = \beta(v,u)$ für alle $u,v \in V$

β alternierend, falls $\beta(v,v) = 0$ für alle $v \in V$.

Im zweiten Fall folgt

$$0 = \beta(u+v, u+v) = \underbrace{\beta(u,u)}_{=0} + \beta(u,v) + \beta(v,u) + \underbrace{\beta(v,v)}_{=0}$$

also $\beta(v,u) = -\beta(u,v)$ für alle $u,v \in V$.

Beweis: „$\Leftarrow$" β symmetrisch $\Rightarrow$ β reflexiv (klar).

β alternierend $\Rightarrow$ $\beta(u,v) = -\beta(u,v)$

also auch $\beta(u,v) = 0 \iff \beta(v,u) = 0$

"$\Rightarrow$" Sei nun β reflexiv. Setze $u = v$ in Lemma und erhalte

$$\beta(v,v)\,\beta(w,v) = \beta(v,v)\,\beta(v,w)$$

d.h. (*) $\beta(v,v)\,\big(\beta(w,v) - \beta(v,w)\big) = 0$ für alle $v,w \in V$

Wollen zeigen: Entweder $\beta(v,v) = 0$ für alle $v \in V$

oder $\beta(w,v) = \beta(v,w)$ für alle $v,w \in V$.

Annahme: Dies gilt nicht. Dann gibt es

$x,y,z \in V$ mit $\beta(y,y) \neq 0$ und $\beta(x,z) \neq \beta(z,x)$.

Mit (*) folgt:

(1) $\beta(x,x) = \beta(z,z) = 0$

(2) $\beta(x,y) = \beta(y,x)$

(3) $\beta(y,z) = \beta(z,y)$

Lemma mit $u = x$, $v = y$, $w = z$ $\Rightarrow$

$$\beta(x,y)\,\beta(z,x) = \beta(y,x)\,\beta(x,z) \overset{(2)}{=} \beta(x,y)\,\beta(x,z).$$

Wegen $\beta(x,z) \neq \beta(z,x)$ folgt also $\beta(x,y) = \beta(y,x) = 0$

Lemma mit $u = z$, $v = y$, $w = x$ $\Rightarrow$

$$\beta(z,y)\,\beta(x,z) = \beta(y,z)\,\beta(z,x) \overset{(3)}{=} \beta(z,y)\,\beta(z,x)$$

Wie vorher folgt $\beta(y,z) = \beta(z,y) = 0$.

Damit $\beta(x,y+z) = \beta(x,z) \neq \beta(z,x) = \beta(y+z,x)$

(*) $\beta(y+z,y+z)\,\big(\underbrace{\beta(x,y+z) - \beta(y+z,x)}_{\neq 0}\big) = 0$

$\Rightarrow 0 = \beta(y+z,y+z) = \beta(y,y) + \underbrace{\beta(y,z)}_{=0} + \underbrace{\beta(z,y)}_{=0} + \underbrace{\beta(z,z)}_{=0}$

$= \beta(y,y) \neq 0$ $\lightning$. $\square$

Definition: Sei $\beta: V \times V \to K$ nicht-ausgearteter und reflexiv.

Ist β symmetrisch, so heißt $\Gamma(V, \beta)$ auch "orthogonale Gruppe" und wird mit $O(V, \beta)$ bezeichnet.

Ist β alternierend, so heißt $\Gamma(V, \beta)$ auch "symplektische Gruppe" und wird mit $Sp(V, \beta)$ bezeichnet.

Frage: Wie ändert sich $\Gamma(V, \beta)$ in Abhängigkeit von β?

Definition: Sei $\beta: V \times V \to K$ und $\beta': V \times V \to K$ Bilinearformen. Dann heißen β, β' äquivalent, wenn es eine invertierbare lineare Abbildung $\varphi: V \to V$ gibt mit

$$\beta'(v, w) = \beta(\varphi(v), \varphi(w)) \text{ für alle } v, w \in V.$$

Matrizenform: $B = \{v_1, \dots, v_n\}$ Basis von V, $n = \dim V$.

G = Gram-Matrix von β bzgl. B.

G' = " " β' bzgl. B.

Rechnung wie am Anfang:

β, β' äquivalent $\Leftrightarrow$ es gibt eine invertierbare Matrix $T \in M_n(K)$ mit

$$G' = T^{tr} \cdot G \, T.$$

Problem: Ausgehend von G, finde T so daß G' möglichst einfach wird.

Beispiel: Sei $\beta: V \times V \to K$ nicht-ausgeartet und symmetrisch.

(1) Sei $\mathrm{char}(K) \neq 2$ (also $1+1 \neq 0$ in K!)
Dann gibt es Orthogonalbasis $\mathcal{B} = \{v_1, \dots, v_n\}$
d.h. $d_i = \beta(v_i, v_i) \neq 0$ für $1 \leq i \leq n$.
und $\beta(v_i, v_j) = 0$ für $i \neq j$.

Damit $G = \begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{bmatrix}$ einfache Gestalt.

(2) Sei nun außerdem $K = \mathbb{R}$. Dann kann man $d_i = \pm 1$ erreichen.

Also $G = \begin{bmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & 1 & & \\ & & & -1 & \\ & & & & \ddots \\ 0 & & & & -1 \end{bmatrix}$ } p mit $0 \leq p \leq n$.

β ist bis auf Äquivalenz eindeutig durch p bestimmt. "Trägheitssatz von Sylvester"

(3) Sei nun außerdem $K = \mathbb{C}$. Dann kann man $d_i = 1$ für $1 \leq i \leq n$ erreichen.

Also $G = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} = I_n$.

Bis auf Äquivalenz gibt es genau ein β.

Bemerkung Sei nun $\beta, \beta': V \times V \to K$ nicht-ausgeartet und reflexiv.
$\mathcal{B} = \{v_1, \dots, v_n\}$ Basis von V.

$G = G'$ Gram-Matrizen bzgl. B.

Annahme: B, B' äquivalent, also ex. $T \in M_n(K)$ invertierbar mit $G' = T^{tr} G \cdot T$.

Nun haben wir $O_n(G) = \{ A \in M_n(K) \mid G = A^{tr} G A \}$

$O_n(G') = \{ A \in M_n(K) \mid G' = A^{tr} G' A \}$.

Denn gilt für $A \in M_n(K)$:

$A^{\varphi} \in O_n(G') \iff G' = A^{tr} G' A$

$T^{tr} G T$ $= A^{tr} T^{tr} G T A$.

$\iff \underbrace{(T^{tr})^{-1} A^{tr} T^{tr}}_{= (TAT^{-1})^{tr}} G \; TAT^{-1} = G$.

$\iff TAT^{-1} \in O_n(G)$.

Betrachte Abbildung $\varphi: GL_n(K) \to GL_n(K)$

$A \mapsto TAT^{-1}$

Gruppenisomorphismus.

Es gilt also $\varphi(O_n(G')) = O_n(G)$

also $O_n(G')$, $O_n(G)$ isomorph

(sogar konjugiert in $GL_n(\mathbb{C})$).

Werden später zeigen:

Satz: K beliebiger Körper

Dann gibt es bis auf Äquivalenz genau eine nicht-ausgeartete alternierende Bilinearform auf V ($\dim V < \infty$).

Außerdem muß $\dim V$ gerade sein.

Problem: Gegeben $\pi_1, \dots, \pi_d \in S_n$; sei $G := \langle \pi_1, \dots, \pi_d \rangle$
Bestimme $|G| = ?$

1. Schritt: Der allgemeine Baum-Algorithmus.

G Gruppe, $G = \langle g_1, \dots, g_d \rangle$, $X \neq \emptyset$ Menge
Operation von G auf X. Für $x \in X$ bestimme
Baum $\mathcal{O}_x = \{ g \cdot x \mid g \in G \}$

Kleine gute Idee: Bestimme zuerst komplette Menge G. Wende alle $g \in G$ auf x an.

Extremfall: $G = S_n$ operiert auf $X = \{1, \dots, n\}$
($n!$ riesig; klein.)

Algorithmus A. Input: $G = \langle g_1, \dots, g_d \rangle$, $x \in X$
Output: $\mathcal{O}_x \subseteq X$.

Initialisieren: $\mathcal{O} := [x]$, $i := 1$;
Schleife:

```
while i ≤ |O| do
    for j in [1, ..., d] do
        y := g_j . O[i]
        if y ∉ O then
            Add(O, y)
        fi;
    od;
    i := i+1;
od;
return O
```

"Beweis" Nach Konstruktion gehören alle Elemente in $\mathcal{O}$ zum Baum $\mathcal{O}_x$

Umgekehrt: sei $y \in O$ und $j \in \{1, \dots, d\}$.
Wiederum nach Konstruktion ist $g_j \cdot y \in O$.
Also gilt: $g_j \cdot O \subseteq O$ für $j = 1, \dots, d$.
Wegen $G = \langle g_1, \dots, g_d \rangle$ folgt $g \cdot O \subseteq O$ für alle $g \in G$.
Also ist O Vereinigung von Bahnen. ∎
Schleife bricht ab, weil nach jeder Runde i erhöht wird und irgendwann $> |O|$ wird. □

In modernen Programmsprachen (wie GAP) kann man Code ein bißchen besser organisieren:

```
Initialisieren    O := [x]
Schleife          for y in O do
                      for j in [1, ..., d] do
                          y1 := g_j . y
                          if y1 ∉ O then
                              Add(O, y1)
                          fi;
                      od;
                  od;
                  return O.
```

[Man braucht nicht den extra-Index i und die Abfrage $i \leq |O|$, sondern die Schleife läuft direkt über O, welches im Verlauf der Rechnung größer wird. Man stelle sich O als Liste vor, die rechts weiter aufgefüllt wird, und y ist ein Index, der ganz links in Liste anfängt und dann Schritt für Schritt nach rechts geht.]

Wir benötigen noch eine Ergänzung zu Algorithmus A. Sei $O_x = \{x_1, x_2, \dots, x_m\}$ mit $x_1 = x$. Dann möchten wir auch noch Elemente $t_1, \dots, t_m \in G$ mit $t_i . x = x_i$ für $1 \le i \le m$ ($t_1 = 1_G$).

Algorithmus A^+ Input $G = \langle g_1, \dots, g_d \rangle$, $x \in X$

Output $[O, T]$ wobei

$O = O_x = \{x_1, \dots, x_m\}$ und $T = \{t_1, \dots, t_m\}$.
($x_1 = x$, $t_1 = 1_G$)

```
Initialisieren:   O := [x]; T := [1_G]; i := 1;
Schleife:         while i ≤ |O| do
                    for j in [1, ..., d] do
                      y := g_j . O[i];
                      if y ∉ O then
                        Add(O, y);
                        Add(T, g_j . T[i])
                      fi;
                    od;
                    i := i + 1;
                  od;
                  return [O, T];
```

einziger Unterschied! →

Bemerkung: Wie oben sei $x \in X$ und $O_x = \{x_1, \dots, x_m\}$ mit $x_1 = x$ Bahn von x. Sei außerdem $G_x = Stab_G(x)$ Stabilisator von x (Untergruppe von G).

Bahnensatz: $O_x \to G/G_x$, $g.x \mapsto g G_x$.

wohldefiniert und bijektiv.

Seien wie oben $t_1, \dots, t_m \in G$ mit $x_i = t_i \cdot x$ und $t_n = 1$.

Dann ist also $G/G_x = \{ \underbrace{t_i G_x}_{\text{paarweise verschieden}} \mid 1 \le i \le m \}$.

also $\{t_1, \dots, t_m\}$ ein Vertretersystem der Nebenklassen von G nach G_x.

D.h. wir haben folgende Situation.

Gegeben $G = \langle g_1, \dots, g_d \rangle$.

sowie $x \in X$ und wir kennen Nebenklassenvertreter der Untergruppe $G_x \le G$.

Frage: Können wir damit Erzeuger von G_x berechnen?

Sei allgemein G beliebige Gruppe, $S \subseteq G$ mit $G = \langle S \rangle$. Sei $U \le G$ beliebige Untergruppe und $T \subseteq G$ ein Nebenklassenvertretersystem von U in G, d.h.

$$G = \dot{\bigcup_{t \in T}} tU \quad , \text{ nehmen an } 1_G \in T$$

Dies definiert eine Abbildung, "Schnitt"

$$\tau : G \to T$$

für $g \in G$, sei $t = \tau(g)$ eindeutiges Element von T mit $g \in tU$.

also $\tau(g) U = gU$ für alle $g \in G$.

$1_G \in T \Rightarrow \tau(h) = 1_G$ für alle $h \in U$.

Satz (Schreier's Untergruppen-Lemma).

Mit obigen Bezeichnungen gelt

$$U = \langle \tau(st)^{-1} st \mid s \in S, t \in T \rangle$$

wobei wir annehmen, daß $S = S^{-1}$ gelt *)
(d.h. mit jedem $s \in S$ gelt auch $s^{-1} \in S$.)

Beweis: Sei $h \in U$ beliebig. Wegen $G = \langle S \rangle$ und $S = S^{-1}$ ist $h = s_1 \cdots s_k$ mit $s_i \in S$.

Für $0 \le i \le k$ setze $t_i := \tau(s_{i+1} \cdots s_k)$

also $t_k = \tau(1_G) = 1_G$ und $t_0 = \tau(s_1 \cdots s_k) = \tau(h) = 1_G$.

Damit erhalte:

$$(*)\quad h = (t_0^{-1} s_1 t_1)(t_1^{-1} s_2 t_2) \cdots (t_{k-1}^{-1} s_k t_k)$$

($t_0 = 1_G$; heben sich jeweils weg; $t_k = 1_G$)

Nun ist $(s_i t_i) U = s_i (t_i U) = s_i (\tau(s_{i+1} \cdots s_k) \cdot U)$

$$= s_i (s_{i+1} \cdots s_k U) = s_i s_{i+1} \cdots s_k U$$

$$= \tau(s_i s_{i+1} \cdots s_k) U = t_{k-1} U.$$

und damit $\tau(s_i t_i) = t_{i-1}$ für $1 \le i \le k$.

Damit können wir (*) umschreiben:

$$h = (\tau(s_1 t_1)^{-1} s_1 t_1)(\tau(s_2 t_2)^{-1} s_2 t_2) \cdots (\tau(s_k t_k)^{-1} s_k t_k)$$

jeweils Elemente der gewünschten Form,

müssen also nur noch zeigen, daß diese in U liegen

Dazu: $(\tau(st)^{-1} st) U = \tau(st)^{-1} (stU)$

$$= \tau(st)^{-1} (\tau(st) U) = 1_G U = U.$$

also $\tau(st)^{-1} st \in U$ für alle $s \in S, t \in T$. □

*) Man benötigt eigentlich nur: Jedes $g \in G$ ist Produkt von Elementen aus S. (z.B. ok für $|G| < \infty$)

Folgerung Ist G endlich erzeugt und $U \leq G$ mit $|G/U| < \infty$, so ist auch U endlich erzeugt.

denn: $G = \langle S \rangle$ mit $|S| < \infty$ können OBdA annehmen, daß $S = S^{-1}$. Schreier's Lemma: U wird von den endlich vielen Elementen $\{ r(st)^{-1} st \mid s \in S, t \in T \}$ erzeugt. □

Der Schreier - Sims - Algorithmus (~ 1970)

Input: $g_1, \dots, g_d \in S_n$

Output $|G|$ = Ordnung von $G = \langle g_1, \dots, g_d \rangle$.

1. Schritt. Finde $x \in \{1, \dots, n\}$ mit $g_i \cdot x \neq x$ für mind. ein $i \in \{1, \dots, d\}$.

(Ist $g_i \cdot x = x$ für alle i und alle $x \in \{1, \dots, n\}$, so $g_i = id$ für $1 \leq i \leq d$ und damit $G = \{id\}$.)

2. Schritt: Benutze Algorithmus A^+, um Bahn $O_x \subseteq \{1, \dots, n\}$ zu bestimmen sowie Elemente $t_1, \dots, t_m \in G$ mit $O_x = \{ t_i \cdot x \mid 1 \leq i \leq m \}$. $|O_x| = m$. wobei $t_1 = id$.

3. Schritt: (Erzeuger von $U = G_x = Stab_G(x)$).

Initialisieren: $R = [\,]$.

Schleife: for $i \in \{1, \dots, d\}$.

for $j \in \{1, \dots, m\}$.

$y := g_i t_j$. $x \in O_x$.

Dann $\tau(g_i t_j) = t_\ell$
denn $g_i t_j \cdot x = t_\ell \cdot x$
$\Rightarrow t_\ell^{-1} g_i t_j \in G_x$
$\rightarrow t_\ell G_x = g_i t_j G_x$.

{ finde $\ell \in \{1, \dots, m\}$ mit
$y = t_\ell \cdot x$
Add $(R, t_\ell^{-1} g_i t_j)$
od
od
return R.

4. Schritt: Falls fest mit Rekursion, wende analoges Verfahren auf Untergruppe $U = G_x \leq S_n$ an.

Formel: $|G| = |O_x| \cdot |G_x|$.
$\uparrow$
$\neq 1$ wegen $g_i \cdot x \neq x$ für ein i.

Beispiel 1 Mathieu-Gruppe $M_{11} \leq S_{11}$.

Finde $|M_{11}| = 7920$.

Beispiel 2 Janko-Gruppe $G = J_1 = \langle A, B \rangle \leq GL_7(\mathbb{F}_{11})$

Wandle G in eine Permutationsgruppe um!
G operiert auf $V = \mathbb{F}_{11}^7$ und dann auch auf $X = \{\langle v \rangle \mid 0 \neq v \in V\} = \mathbb{P}(V)$
projektiver Raum.

Aber X ist noch zu groß. Sei $0 \neq v_0 \in V$ fest und $O_0 \subseteq \mathbb{P}(V)$ Bahn von $\langle v_0 \rangle$.
Dann operiert G auch auf O_0 (klar).
Suche v_0 so dass $|O_0|$ möglichst klein wird.
z.B. bilde einige Produkte (*) von A, B bis man ein Element C findet, das

1 als Eigenwert hat; sei $0 \neq v_0 \in \mathbb{F}_{11}^7$ zug. Eigenvektor. Dann $C \in Stab_G(\langle v_0 \rangle)$

also $o(C) \mid |Stab_G(\langle v_0 \rangle)|$

und damit Chance, dass $|O_{v_0}|$ klein.

Berechne dann von A, B bewirkte Permutationen auf O_{v_0} und wende dann Schreier-Sims an.

Berichte: erhalte Homomorphismus

$\varphi: J_1 \to S_N$ wobei $N = |O_{v_0}|$.

$A, B \neq I_7$ also $\ker(\varphi) \subsetneq J_1$.

J_1 einfach $\Rightarrow$ $\ker(\varphi) = \{1\}$.

also φ injektiv und $|J_1| = |Bild(\varphi)|$

(*) Hier kann man z. B. nehmen:

$C = [redacted]$ BABAB.

$\Rightarrow$ C hat 1-dim. Eigenraum zum Eigenwert 1.

$o(C) = 11$ durch weil O_{v_0} enthält Basis von $\mathbb{F}_{11}^7$.

und $|O_{v_0}| = [redacted]1540$

Damit $\varphi: J_1 \to S_{[redacted]1540}$ injektiv.

Schreier-Sims: $|J_1| = 175560$

Werden später noch viele weitere Beispiele sehen.

[redacted] mit Schreier-Sims

Eine weitere Anwendung des obigen Algorithmus.

Membership-Test

Input: $g_1, \dots, g_d \in S_n$ sowie ein weiteres beliebiges Element $g \in S_n$.

Output: true oder false je nachdem ob $g \in G := \langle g_1, \dots, g_d \rangle$ oder nicht.

1. Schritt: Sei $x \in \{1, \dots, n\}$ wie im 1. Schritt von Schreier-Sims.

Falls $g \cdot x \notin O_{x_1}$ so ist $g \notin G_1$ fertig.
Sei nun $g \cdot x \in O_x$ und $j \in \{1, \dots, n\}$ so daß $g \cdot x = t_j \cdot x$.
Dann $t_j^{-1} g \cdot x = x_1$
also $g \in G \iff t_j^{-1} g \in G_x = \mathrm{Stab}_G(x)$.

2. Schritt: Wende Rekursion auf G_x an um $t_j^{-1} g \in G_x$ zu testen.

(Nach Schreier-Sims erhalten wir ein endliches Erzeugendensystem von G_x.)

Bemerkung: Das von Schreier-Sims produzierte Erzeugendensystem von U enthält viele überflüssige Elemente. Um einen optimalen Algorithmus zu erhalten, sollte man dieses Problem näher studieren, siehe dazu: §1.14 in

P. J. Cameron, Permutation Groups, London Math. Soc. Student Texts 45, Cambridge Univ. Press, 1999.

Beispiel: Sei $G = \langle (1\,2\,4), (2\,3) \rangle \leq S_4$.
 $\overset{\shortparallel}{g_1}$ $\overset{\shortparallel}{g_2}$

$x = 1 \quad g_1 . 1 = 2, \quad g_2 . 2 = 3, \quad g_1 . 2 = 4.$

Also $O_x = \{ 1, 2, 3, 4 \}$ mit

$t_1 = 1, \quad t_2 = g_1, \quad t_3 = g_2 g_1, \quad t_4 = g_1^2.$

Erhalten 8 Erzeuger für G_x: bilde $\tau(g_i t_j)^{-1} g_i t_j$
für $i = 1, 2$, $j = 1, 2, 3, 4$.

$\tau(g_1 t_1)^{-1} g_1 t_1 = \tau(g_1)^{-1} g_1 = t_2^{-1} g_1 = \quad id.$

$\tau(g_1 t_2)^{-1} g_1 t_2 = \tau(g_1^2)^{-1} g_1^2 = t_4^{-1} t_4 = \quad id.$

$\tau(g_1 t_4)^{-1} g_1 t_3 = \tau(g_1^3)^{-1} g_1^3 = \tau(id)^{-1} id = id.$

$\tau(g_1 t_3)^{-1} g_1 t_3 = \tau(g_1 g_2 g_1)^{-1} g_1 g_2 g_1.$

$g_1 g_2 g_1 = (1\,3\,4\,2)$ $\qquad$ $g_1 g_2 g_1 . 1 = 3 = \underbrace{g_2 g_1}_{= t_3} . 1$

also $\tau(g_1 g_2 g_1) = g_2 g_1$.

$\tau(g_1 g_2 g_1)^{-1} = g_1^2 g_2$.

$g_1^2 g_2 g_1 g_2 g_1 = (1)(2\,4\,3)$
$= (2\,4\,3).$

$\tau(g_2 t_1)^{-1} g_2 t_1 = \tau(g_2)^{-1} g_2 = g_2.$
$= (2\,3)$

$g_2 . 1 = 1 . = t_1 . 1$
also $g_2 \in G_x$, d.h.
$\tau(g_2) = id.$

$\tau(g_2 t_2)^{-1} g_2 t_2 = \tau(\underbrace{g_2 g_1}_{= t_3})^{-1} g_2 g_1 . = t_3^{-1} t_3 = id.$

$\tau(g_2 t_3)^{-1} g_2 t_3 = \tau(g_2^2 g_1)^{-1} g_2^2 g_1 = \tau(g_1)^{-1} g_1 . = t_1^{-1} t_1 = id.$ ($\tau(g_1) = t_1$)

$\tau(g_2 t_4)^{-1} g_2 t_4 = \tau(g_2 g_1^2)^{-1} g_2 g_1^2$
$= g_1^{-2} g_2 g_1^2 = (3\,4)$

$g_2 g_1^2 . 1 = 4 = t_4 . 1.$
$\tau(g_2 g_1^2) = t_4 = g_1^2$

Also: $G_x = \langle (2\,4\,3), (3\,4) \rangle$. Falne fort
$\uparrow = S_{\{2,3,4\}}$ also $|G_x| = 6$.

Damit $G = S_4$. !

§2 Freie Gruppen und Präsentationen

Ausser Permutationen und Matrizen gibt noch (mindestens) eine weitere allgemeine Methode, um Gruppen zu konstruieren

Definition Sei F eine Gruppe und $S \subseteq F$ mit $F = \langle S \rangle$. Dann heißt F freie Gruppe auf S, wenn es zu jeder Gruppe G und jeder Abbildung $f: S \to G$ stets einen Gruppenhomomorphismus $\varphi: F \to G$ gibt mit $\varphi|_S = f$.

[Wegen $F = \langle S \rangle$ ist dann φ eindeutig bestimmt.]

Beispiel (a) $F = \{1\}$ ist freie Gruppe auf $S = \emptyset$.

(b) Sei $F = (\mathbb{Z}, +)$ und $S = \{1\}$. Dann ist F frei auf S, denn $\mathbb{Z} = \langle 1 \rangle$ ✓.

Sei G bel. und $f: S \to G$ mit einem $1 \mapsto g$ festen $g \in G$.

Dann $\varphi: F \to G$, $m \mapsto g^m$ Homom. mit $\varphi|_1 = f$.

Hauptsatz: Sei S beliebige Menge. Dann gibt es eine Gruppe F mit $S \subseteq F$, so daß F frei auf S ist. F ist bis auf Isomorphie eindeutig bestimmt.

Beweis: Zuerst Eindeutigkeit. Sei auch $S \subseteq F'$ und F' frei auf S. Sei $f: S \to F'$ Inklusion.

Dann gibt es $\varphi: F \to F'$ Homomorphismus mit $\varphi|_S = f$. Sei $g: S \to F$ Inklusion.

Dann gibt es $\psi: F' \to F$ mit $\psi|_S = g$

$(\varphi \circ \psi)(s) = (\varphi \circ g)(s) = \varphi(s) = s$ für alle $s \in S$.

$F' = \langle S \rangle \Rightarrow \varphi \circ \psi = id_{F'}$

$(\psi \circ \varphi)(s) = (\psi \circ f)(s) = \psi(s) = s$ für alle $s \in S$.

$F = \langle S \rangle \Rightarrow \psi \circ \varphi = id_F$.

Also φ, ψ bijektiv und inverse zueinander, $F \cong F'$!

Jetzt Existenz: Ist $S = \emptyset$, so $F = \{1\}$ siehe oben.

Nehmen wir nun $S \neq \emptyset$ an.

Sei $\bar{S}$ Menge, die gleichmächtig zu S ist und, $S \cap \bar{S} = \emptyset$, und $S \to \bar{S}$, $s \mapsto \bar{s}$ Bijektion

Sei $A := S \cup \bar{S}$

Definiere auch $\bar{\bar{s}} = s$ für $s \in S$.

Sei $X_0 := \{()\}$ und $X_n := \{(x_1, \dots, x_n) \mid x_i \in A\}$ für $n \geq 1$.

Setze $W := \bigcup_{n \geq 0} X_n$ "alle Wörter endlicher Länge mit $A = S \cup \bar{S}$"

Sei $w = (w_1, \dots, w_n) \in W$. Wir sagen, dass w "reduziert" ist, wenn $w_{i+1} \neq \bar{w}_i$ für alle i gilt.

[Das leere Wort $()$ wird auch als reduziert bezeichnet.] Sei

$$W_{red} := \{w \in W \mid w \text{ reduziert}\}.$$

Wir identifizieren A mit $\{(x) \mid x \in X\}$ Σ Wörter mit 1 Buchstaben.

Dann $S \subseteq A \subseteq W_{red}$.

Multiplikation auf W_{red}: Seien $u = (u_1, \dots, u_n)$ und $v = (v_1, \dots, v_m) \in W_{red}$. Dann setze

$$u \cdot v := (u_1, \dots, u_{n-r}, v_{r+1}, \dots, v_m) \in W_{red}.$$

wobei $r \geq 0$ dadurch bestimmt ist, daß

$u_n = \overline{v_1}$, $u_{n-1} = \overline{v_2}$, ..., $u_{n-r+1} = \overline{v_r}$

und $u_{n-r} \neq \overline{v_{r+1}}$

Wir haben dann folgende Regel:

$$(u_1, \dots, u_n) \cdot (v_1, \dots, v_m) = (u_1, \dots, u_{n-1}) \cdot (v_2, \dots, v_m) \quad \text{falls } u_n = \overline{v_1} \qquad (*)$$

Beh: Damit wird $(W_{red}, \cdot)$ eine Gruppe.

$()$ ist offenbar neutrales Element.

Ist $w = (w_1, \dots, w_n) \in W_{red}$, so setze

$\overline{w} := (\overline{w_n}, \dots, \overline{w_1}) \in W_{red}$. Dann $w \cdot \overline{w} = \overline{w} \cdot w = ()$

also gibt es inverse Elemente. Bleibt noch zu zeigen: $\cdot$ assoziativ.

Seien also $u = (u_1, \dots, u_\ell) \in W_{red}$,

$v = (v_1, \dots, v_m) \in W_{red}$.

$w = (w_1, \dots, w_n) \in W_{red}$.

Müssen zeigen: $(u \cdot v) \cdot w = u \cdot (v \cdot w)$.

Vollständige Induktion nach m.

Anfang $m = 0$: $v = () \Rightarrow (u \cdot v) \cdot w = u \cdot w$
$= u \cdot (v \cdot w)$ ✓.

Sei nun $m = 1$, also $v = (x)$ mit einem $x \in X$.

Unterscheiden 4 Fälle:

1) $u_\ell \neq \overline{x}$ und $w_1 \neq \overline{x} \Rightarrow u \cdot v = (u_1, \dots, u_\ell, x) \in W_{red}$.

$v \cdot w = (x, w_1, \dots, w_n) \in W_{red}$.

$\Rightarrow (u \cdot v) \cdot w = (u_1, \dots, u_\ell, x) \cdot (w_1, \dots, w_n) = (u_1, \dots, u_\ell, x, w_1, \dots, w_n) \in W_{red}$.

und man erhält das gleiche Ergebnis für $u \cdot (v \cdot w)$.

2) $u_\ell \neq \bar{x}$ und $w_1 = \bar{x} \Rightarrow$

$u \cdot v = (u_{1|-1}\, u_\ell, x) \in W_{red}$, $v \cdot w = (w_{2|-1}\, w_m) \in W_{red}$.

Mit (*) folgt:

$(u \cdot v) \cdot w = (u_{1|-1}\, u_\ell, x) \cdot (w_{1|-1}\, w_m) \overset{(*)}{=} (u_{1|-1}\, u_\ell) \cdot (w_{2|-1}\, w_m)$

$= u \cdot (v \cdot w)$ ✓.

3) $u_\ell = \bar{x}$ und $w_1 \neq \bar{x} \Rightarrow$

$u \cdot v = (u_{1|-1}\, u_{\ell-1}) \in W_{red}$, $v \cdot w = (x, w_{1|-1}\, w_m) \in W_{red}$.

Mit (*) folgt:

$u \cdot (v \cdot w) = (u_{1|-1}\, u_\ell) \cdot (x, w_{1|-1}\, w_m) = (u_{1|-1}\, u_{\ell-1}) \cdot (w_{1|-1}\, w_m)$

$= (u \cdot v) \cdot w$ ✓.

4) $u_\ell = \bar{x}$ und $w_1 = \bar{x} \Rightarrow u \cdot v = (u_{1|-1}\, u_{\ell-1}) \in W_{red}$.

und $v \cdot w = (w_{2|-1}\, w_m) \in W_{red}$. Dann

$(u \cdot v) \cdot w = (u_{1|-1}\, u_{\ell-1}) \cdot (w_{1|-1}\, w_m)$

$= (u_{1|-1}\, u_{\ell-1}) \cdot (\bar{x}, w_{2|-1}\, w_m)$

$= (u_{1|-1}\, u_{\ell-1}, \bar{x}, w_{2|-1}\, w_m) \in W_{red}$.

↑ beachte: $x \neq u_{\ell-1}$ da $u \in W_{red}$.

Man erhält das gleiche Ergebnis für $u \cdot (v \cdot w)$.

Sei schließlich $m > 1$. Schreibe

$$v = (v_{1|-1}\, v_m) = \underbrace{(v_{1|-1}\, v_{m-1})}_{=: v'} \cdot \underbrace{(v_m)}_{=: v''}$$

Dann:

$u \cdot (v \cdot w) = u \cdot ((v' \cdot v'') \cdot w)$

$= u \cdot (v' \cdot (v'' \cdot w))$ Fall $m = 1$.

$= (u \cdot v') \cdot (v'' \cdot w)$ (Induktion).

$= ((u \cdot v') \cdot v'') \cdot w$ (Fall $m = 1$)

$= (u \cdot (v' \cdot v'')) \cdot w$ (Induktion)

$= (u \cdot v) \cdot w$ ✓.

Zum Schluss: W_{red} frei auf S.

Sei G beliebige Gruppe und $f: S \to G$ Abbildung.

Können f auf $\bar{S}$ fortsetzen durch $f(\bar{s}) := f(s)^{-1}$ für alle $s \in S$.

Definiere dann

$\varphi: W_{red} \to G$ durch $\varphi(w) := f(w_1) \cdot \ldots \cdot f(w_m) \in G$

wobei $w = (w_1, \ldots, w_m) \in W_{red}$.

[$\varphi(()) = 1_G$.] Beh: φ ist Gruppen-Homom.

Seien $u = (u_1, \ldots, u_n) \in W_{red}$ und $v = (v_1, \ldots, v_m) \in W_{red}$.

$u \cdot v = (u_1, \ldots, u_{n-r}, v_{r+1}, \ldots, v_m) \in W_{red}$.

$r \geq 0$ wie oben.

d.h. $u_n = \bar{v}_1$, $u_{n-1} = \bar{v}_2, \ldots, u_{n-r+1} = \bar{v}_r$

Aber dann $f(u_n) = f(\bar{v}_1) = f(v_1)^{-1}$

$f(u_{n-1}) = f(v_2)^{-1}$

$\vdots$

$f(u_{n-r+1}) = f(v_r)^{-1}$

also $f(u_{n-r+1}) \cdots f(u_n) f(v_1) \cdots f(v_r) = 1_G$.

$\Rightarrow \varphi(u) \cdot \varphi(v) = f(u_1) \cdots f(u_{n-r}) f(u_{n-r+1}) \cdots f(u_n)$

$\cdot f(v_1) \cdots f(v_r) f(v_{r+1}) \cdots f(v_m)$

$= f(u_1) \cdots f(u_{n-r}) f(v_{r+1}) \cdots f(v_m)$

$= f(u_1, \ldots, u_{n-r}, v_{r+1}, \ldots, v_m) = \varphi(u \cdot v)$ □.

Folgerung Jede Gruppe ist isomorph zu einer Faktorgruppe einer freien Gruppe nach einem Normalteiler

denn sei G bel. Gruppe, $S \subseteq G$ mit $G = \langle S \rangle$.

F freie Gruppe auf S, $f: S \to G$ Inklusion.

es gibt genau $\varphi: F \to G$ mit $\varphi|_S = f$.

also $s = f(s) = \varphi(s) \in \text{Bild}(\varphi)$ für alle $s \in S$.

$\Rightarrow$ φ surjektiv, also $G = \text{Bild}(\varphi) \cong F/\text{Kern}(\varphi)$ ↯.

Homomorphiesatz.

Definition Sei G eine Gruppe und $S \subseteq G$ mit $G = \langle S \rangle$. Sei F freie Gruppe auf S und $\varphi: F \to G$ surjektiv wie oben, $N := \text{Kern}(\varphi) \trianglelefteq F$

Sei $R \subseteq F$ Teilmenge mit

$$\langle\langle R \rangle\rangle := \bigcap_{\substack{H \trianglelefteq F \\ \text{mit } R \subseteq H}} H = N.$$

↖ Normalteilererzeugnis von R

$=$ kleinster Normalteiler von F, der R enthält.

Mit diesen Bezeichnungen schreibt man dann

$$G = \langle S \mid R \rangle$$

und nennt diese eine "Präsentation" für G.

S: Erzeuger R: definierende Relationen.

Beachte: Für $r \in R$ ist $r \in N$ also

$\varphi(r) = 1_G$ in G.

"Wörter in R werden gleich 1_G in G"

Umgekehrt kann man diese Konstruktion auch dazu benutzen, um Gruppen zu konstruieren / definieren:
Sei S Menge, F freie Gruppe auf S und $R \subseteq F$ Teilmenge. Dann definiere

$$\langle S \mid R \rangle := F/N \quad \text{wobei } N := \langle\langle R \rangle\rangle$$

von R erzeugter Normalteiler ist

$$\left[\text{Ü 3: } \langle\langle R \rangle\rangle = \langle \{ grg^{-1} \mid r \in R,\ g \in F \} \rangle \trianglelefteq F. \right].$$

Damit zwei grundlegende Aufgabenstellungen:

1) Gegeben sei eine Gruppe G und $S \subseteq G$ mit $G = \langle S \rangle$. Sei F frei auf S und $\varphi: F \to G$ surjektiv wie oben (mit $\varphi|_S = id$). Finde "möglichst" kleine oder konstruiere gerade Teilmenge $R \subseteq F$ mit $\ker(\varphi) = \langle\langle R \rangle\rangle$.
Dann $G \cong \langle S \mid R \rangle$.

2) Gegeben sei Menge S, F = freie Gruppe auf S, und $R \subseteq F$. Sei $N := \langle\langle R \rangle\rangle$
Dann bestimme $G := F/N$, z.B. entscheide

$$|G| = \infty \quad \text{oder} \quad |G| < \infty.$$

zu 2): Satz von Novikov (1955), Boone (1958), Britton (1963)
Es gibt eine endliche Menge S und eine endliche Menge $R \subseteq F$ = freie Gruppe auf S, so daß das Wortproblem in $\langle S \mid R \rangle$ nicht entscheidbar ist, d.h. es gibt keinen Algorithmus der in endlich vielen Schritten entscheidet, ob ein gegebenes Wort in F gleich 1 wird in $\langle S \mid R \rangle$ oder nicht.

Literatur dazu: Chapter 12 in

J.J. Rotman, An introduction to the theory of groups, 4th edition, Springer Graduate Texts in Math. 148, Springer-Verlag 1995.

Bevor wir Beispiele behandeln, zuerst ein nützliches Hilfsmittel:

Relationen-Lemma: Sei G Gruppe, $S \subseteq G$ mit $G = \langle S \rangle$. Sei F freie Gruppe auf S und $\varphi: F \to G$ surjektiv wie oben ($\varphi|_S = id$). Sei $R \subseteq F$ Teilmenge mit $\varphi(r) = 1_G$ für alle $r \in R$. Dann ist G isomorph zu einer Faktorgruppe von $\langle S|R \rangle$; insbesondere also

$$|\langle S|R \rangle| \geq |G|.$$

Beweis: Sei $N := \ker(\varphi)$. Wegen $\varphi(r) = 1_G$ für alle $r \in R$ ist $R \subseteq N$ und damit auch $U := \langle\langle R \rangle\rangle \subseteq N$. Definiere

$$\psi: \begin{array}{ccc} F/U & \to & F/N \\ fU & \mapsto & fN \end{array}$$

Wegen $U \subseteq N$ ist dies wohldefiniert
[$fU = f'U \Rightarrow f^{-1}f' \in U \subseteq N \Rightarrow fN = f'N$].
und dann folgt auch sofort, daß ψ ein Gruppenhomomorphismus ist. Klar: ψ surjektiv.

Also $\langle S|R \rangle = \left(F/U\right)/\ker(\psi) \cong F/N = G$ Homomorphiesatz.

Also G isomorph zu Faktorgruppe von $\langle S|R \rangle$. □

Beispiel 1 Sei $n \geq 1$ und $G = \langle g \rangle$ zyklische Gruppe der Ordnung n. Also $o(g) = n$.
Sei F freie Gruppe auf $S = \{x\}$. Haben surjektiven Homom. $\varphi: F \to G$ wie oben, mit

$$\varphi(x) = g$$

(↑ ↑ verwende verschiedene Symbole, um nicht durcheinander zu kommen.)

Sei $R := \{x^n\}$. Dann $\varphi(x^n) = \varphi(x)^n = g^n = 1_G$
also Voraussetzungen von Relatoren-Lemma erfüllt.
Damit $G \cong$ Faktorgruppe von $\langle x \mid x^n \rangle$
$= F/\langle\langle x^n \rangle\rangle$.
Um zu zeigen, daß $G \cong \langle x \mid x^n \rangle$, müssen wir jetzt noch zeigen, daß $|\langle x \mid x^n \rangle| \leq n$ gelt.

Dazu: Sei $H := \langle x \mid x^n \rangle = F/\langle\langle x^n \rangle\rangle$.

$F = \langle x \rangle \Rightarrow H = \langle \bar{x} \rangle$ wobei $\bar{x} = x\langle\langle x^n \rangle\rangle$
(Nebenklasse in $F/\langle\langle x^n \rangle\rangle$).

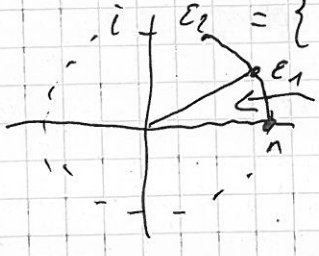
Wegen $x^n \in R$ ist $\bar{x}^n = 1$ in H
also $o(\bar{x}) \leq n$ und damit $|H| \leq n$, Rest ☐.

Damit: Für jedes $n \geq 1$ ist $\langle x \mid x^n \rangle$
zyklische Gruppe der Ordnung n.

Beispiel 2 (Diedergruppen) Sei $n \geq 3$ und
$\varepsilon_n := e^{2\pi i/n} = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right) \in \mathbb{C}$.

Dann $E_n := \{z \in \mathbb{C} \mid z^n = 1\}$ n-te Einheitswurzeln

$E_n = \{1, \varepsilon_n, \varepsilon_n^2, \ldots, \varepsilon_n^{n-1}\}$.



Teile Einheitskreis in n gleiche Stücke.

Definiere $\alpha: \mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$ komplexe Konjugation = Spiegelung an der reellen Achse.

und $\beta: \mathbb{C} \to \mathbb{C}$, $z \mapsto \varepsilon_n z$ = Drehung mit Uhrzeigersinn um $2\pi/n$.

Für $z \in E_n$ ist auch $\alpha(z) = \overline{z} \in E_n$

und $\beta(z) = \varepsilon_n z \in E_n$.

[illegible]

Insbesondere sind α, β bijektive Abbildungen.

Betrachte α, β nur als Abbildungen

$\alpha: E_n \to E_n$, $\beta: E_n \to E_n$.

Dann $\alpha, \beta \in \mathrm{Sym}_{E_n}$. Sei $G := \langle \alpha, \beta \rangle \leq \mathrm{Sym}_{E_n}$.

$\alpha^2 = id$, $\alpha \neq id \to o(\alpha) = 2$

β = Drehung um $2\pi/n \Rightarrow o(\beta) = n$.

Setze $\gamma := \alpha \circ \beta$. ($\Rightarrow \beta = \alpha^{-1} \circ \gamma = \alpha \circ \gamma$).

Dann ist auch $G = \langle \alpha, \beta \rangle = \langle \alpha, \gamma \rangle$.

Nun ist $\gamma(z) = (\alpha \circ \beta)(z) = \alpha(\varepsilon_n z)$

$= \overline{\varepsilon_n} \cdot \overline{z} = \varepsilon_n^{-1} \overline{z}$

Also $\gamma(1) = \varepsilon_n^{-1} \neq 1 \Rightarrow \gamma \neq id$.

$\gamma^2(z) = \gamma(\gamma(z)) = \gamma(\varepsilon_n^{-1} \overline{z}) = \varepsilon_n^{-1} \overline{\varepsilon_n^{-1} \overline{z}}$

$= \varepsilon_n^{-1} \varepsilon_n z = z$, also $\gamma^2 = id$.

d.h. $o(\gamma) = 2$ Schließlich: $o(\alpha \circ \gamma) = o(\beta) = n$.

$\Rightarrow$ ($\mathcal{O}$) G Diedergruppe der Ordnung $2n$.

$o(\alpha) = 2$, $o(\gamma) = 2$, $o(\alpha \circ \gamma) = n \geq 3$.

$\alpha \neq \gamma$.

Sei F freie Gruppe auf $S = \{s, t\}$ $(s \neq t)$.
Haben surjektiven Homom. $\varphi: F \to G$
$s \mapsto \alpha$
$t \mapsto \beta$

(benutze meist verschiedene Symbole, um nicht durcheinander zu kommen).

Sei $R := \{s^2, t^2, (st)^n\}$. Dann $\varphi(s^2) = \alpha^2 = id$.
$\varphi(t^2) = \beta^2 = id$
$\varphi((st)^n) = (\alpha\beta)^n = \beta^n = id$.

Also: Relatoren-Lemma:
$\Rightarrow$ $G \cong$ Faktorgruppe von $\langle s, t \mid s^2, t^2, (st)^n \rangle$.

Sei $H := F / \langle\langle s^2, t^2, (st)^n \rangle\rangle = \langle \bar{s}, \bar{t} \rangle$.
mit $\bar{s}$ = Bild von s in Faktorgruppe
$\bar{t}$ = " " " " " .

Wegen $s^2 \in \langle\langle R \rangle\rangle \Rightarrow \bar{s}^2 = 1$
Genauso $\bar{t}^2 = 1$ und $(\bar{s}\bar{t})^n = \underline{1}$.

analoge Rechnung wie in Ü 1 $\Rightarrow |H| \leq 2n$.

Damit: Für jedes $n \geq 3$ ist
$\langle s, t \mid s^2, t^2, (st)^n \rangle$ Diedergruppe der Ordnung $2n$.

<u>Beispiel 3</u> Seien $p, q, r \in \mathbb{N}$. Die Gruppe
$G = \langle x, y \mid x^p, y^q, (xy)^r \rangle$ heißt
"Dreiecks-Gruppe". Es gelte:

$1/p + 1/q + 1/r > 1 \Rightarrow |G| < \infty$
sonst $|G| = \infty$.

$1/p + 1/q + 1/r = 1$
$\Rightarrow |G| = \infty$ und $G' \subsetneq G$.

$1/p + 1/q + 1/r < 1 \Rightarrow |G| = \infty$ und $G' = G$
[G' = Kommutator-Untergruppe, siehe Ü 3].

Spezialfall: $p = 2, q = 3, r = 7$ (klassisches Beisp.

für 3. Fall) Eine endliche Gruppe heißt Hurwitz-Gruppe, wenn sie isomorph zu einer Faktorgruppe von $\langle x, y \mid x^2, y^3, (xy)^7 \rangle$ ist.

Verbindungen zur Geometrie, Riemann'schen Flächen siehe:

M. Conder, Hurwitz groups: A brief survey. Bull. Amer. Math. Soc. 23 (1990), 359–370.

Satz (Präsentation für die symmetrische Gruppe S_n).
Für alle $n \geq 2$ gilt

$$S_n \cong \langle x_1, \dots, x_{n-1} \mid x_i^2,\ (x_i x_{i+1})^3,\ (x_i x_j)^2 \text{ falls } |i-j| > 1 \rangle.$$

Also z.B.:

$S_3 \cong \langle x_1, x_2 \mid x_1^2,\ x_2^2,\ (x_1 x_2)^3 \rangle$ Diedergruppe der Ordnung 6.

$S_4 \cong \langle x_1, x_2, x_3 \mid x_1^2, x_2^2, x_3^2, (x_1 x_2)^3, (x_2 x_3)^3, (x_1 x_3)^2 \rangle$.

Beweis: 1. Schritt: Finde Erzeugendensystem für S_n, $n \geq 0$ das obige Relationen erfüllt sind.

Dann sei $s_i := (i\ i+1) \in S_n$ Transposition für $1 \leq i \leq n-1$.

Klar: $s_i^2 = id$ $\quad s_i \circ s_{i+1} = (i, i+1) \circ (i+1, i+2) = (i, i+1, i+2)$ 3-zykel

also $(s_i \circ s_{i+1})^3 = id$.

$|i-j| > 1 \Rightarrow s_i = (i, i+1)$ und $s_j = (j, j+1)$ disjunkt

also $s_i \circ s_j = s_j \circ s_i$ und damit $(s_i \circ s_j)^2 = id$.

Noch zu zeigen: $S_n = \langle s_1, \dots, s_{n-1} \rangle$.

Beweis mit Induktion nach n, Anfang $n = 2$

$S_2 = \{id, s_1\}$ v. Sei nun $n > 2$.
Sei $G := \langle s_1, \dots, s_{n-1} \rangle \leq S_n$ und $H := \langle s_1, \dots, s_{n-2} \rangle \leq G$.
Nach Induktion ist $H = S_{n-1}$, also $|H| = (n-1)!$
G operiert transitiv auf $\{1, \dots, n\}$, denn
$s_1 \cdot 1 = (1,2) \cdot 1 = 2$, $s_2 \cdot 2 = (2,3) \cdot 2 = 3$, $\dots$, $s_{n-1} \cdot (n-1) = n$.
Bahnensatz: $|G| = n \cdot |\mathrm{Stab}_G(n)|$.
aber $H \leq \mathrm{Stab}_G(n) \Rightarrow (n-1)! = |H| \leq |\mathrm{Stab}_G(n)|$!
$\Rightarrow |G| \geq n \cdot (n-1)! = n!$ $\Rightarrow$ $G = S_n$ v.

2. Schritt. Betrachte nun freie Gruppe F auf $S = \{x_1, \dots, x_{n-1}\}$. Haben surj. Homom. $\varphi: F \to S_n$ mit $\varphi(x_i) = s_i$ für $1 \leq i \leq n-1$. Sei
$R = \{ x_i^2, (x_i x_{i+1})^3, (x_i x_j)^2 \text{ für } |i-j| > 1 \}$.
Dann $\varphi(r) = id$ für alle $r \in R$. Können also Relationen-Lemma anwenden. Es genügt damit zu zeigen $|F / \langle\langle R \rangle\rangle| \leq n!$.
Sei $H = F / \langle\langle R \rangle\rangle = \langle \bar{x}_1, \dots, \bar{x}_{n-1} \rangle$.
In H gilt $\bar{x}_i^2 = 1$, $(\bar{x}_i \bar{x}_{i+1})^3 = 1$, $(\bar{x}_i \bar{x}_j)^2 = 1$ für $|i-j| > 1$.
$1 = (\bar{x}_i \bar{x}_j)^2 = \bar{x}_i \bar{x}_j \bar{x}_i \bar{x}_j$ und $\bar{x}_i^{-1} = \bar{x}_i$, $\bar{x}_j^{-1} = \bar{x}_j$ $\Rightarrow$ $\bar{x}_i \bar{x}_j = \bar{x}_j \bar{x}_i$ für $|i-j| > 1$

$1 = (\bar{x}_i \bar{x}_{i+1})^3 = \bar{x}_i \bar{x}_{i+1} \bar{x}_i \bar{x}_{i+1} \bar{x}_i \bar{x}_{i+1} \Rightarrow \bar{x}_i \bar{x}_{i+1} \bar{x}_i = \bar{x}_{i+1} \bar{x}_i \bar{x}_{i+1}$

Müssen also noch zeigen: Sei G beliebige Gruppe mit $G = \langle g_1, \dots, g_{n-1} \rangle$ wobei gilt:
$g_i^2 = 1$, $g_i g_j = g_j g_i$ für $|i-j| > 1$ und
$g_i g_{i+1} g_i = g_{i+1} g_i g_{i+1}$.
Dann $|G| \leq n!$

Sei $U := \langle g_2, \dots, g_{n-1} \rangle \leq G$. Nach Induktion ist $|U| \leq (n-1)!$ $\quad \left(n=2 \Rightarrow G = \langle g_1 \rangle \text{ mit } g_1^2 = 1 \right)$.

Müssen also noch zeigen: $|G/U| \leq n$.

Definiere dazu:

$t_0 = 1$

$t_1 = g_1$

$t_2 = g_2 g_1$

$t_3 = g_3 g_2 g_1$

$\vdots$

$t_{n-1} = g_{n-1} g_{n-2} \cdots g_1$

Behauptung: $G = \bigcup_{i=0}^{n-1} t_i U$.

$\Downarrow$

fertig.

Dazu sei $X := \bigcup_{i=0}^{n-1} t_i U$. Müssen dann nur zeigen (*) $g_j t_i \in X$ für alle j, i:

denn sei $g \in G$ bel. $\Rightarrow g = g_{i_1} \cdots g_{i_k}$.

$\Rightarrow g = g \cdot 1 = g \cdot t_1 = g_{i_1} \cdots g_{i_{k-1}} (g_{i_k} t_1)$

$(*) = t_{i_k} u_k$

$= g_{i_1} \cdots g_{i_{k-1}} (g_{i_{k-1}} t_{i_k} u_k)$

$(-) = t_{i_{k-1}} u_{k-1}$

$= \text{usw.} = t_{i_1} \cdots u_1 - u_k \in X$ Also $G = X$ ✓.

Jetzt zu (*): Unterscheiden mehrere Fälle:

(I) $i=0, j>1$: $g_j t_0 = g_j \in U$ wegen $j>1$
$= t_0 U \subseteq X$. ✓

(II) $i=0, j=1$: $g_1 t_0 = g_1 = t_1 \in t_1 U \subseteq X$ ✓.

(III) $i>0, j>i+1$ $\quad g_j t_i = g_j g_i g_{i-1} \cdots g_1$

Wegen $j > i+1$ vertauscht g_j mit allen Faktoren in t_i,
also $g_j \cdot t_i = t_i \cdot g_j \in t_i U \subseteq X \quad \checkmark$.
$(j > 1)$.

(IV) $i > 0$, $j = i+1$: $g_j t_i = g_{i+1} g_i g_{i-1} \cdots g_1 = t_{i+1} \in X$ ✓.

(V) $i > 0$, $j = i$: $g_j t_i = \underbrace{g_i g_i}_{=1} g_{i-1} \cdots g_1 = g_{i-1} \cdots g_1 = t_{i-1} \in X_V$.

(VI) $i > 0$, $j = i-1$: $g_j t_i = \underbrace{g_{i-1} g_i g_{i-1}}_{= g_i g_{i-1} g_i \text{ vertauschen!}} g_{i-2} \cdots g_1$
≥ 1
d.h. $i \geq 2$.

$= \underbrace{g_i g_{i-1} g_{i-2} \cdots g_1}_{= t_i} \underbrace{g_1}_{\in U} \in t_i U \subseteq X_V$.

(VII) $i > 0$, $j < i-1$. $g_j t_i = g_j \underbrace{g_i \cdots g_{j+1}}_{\text{vertauschen}} g_j g_{j-1} \cdots g_1$

$= g_i g_{i-1} \cdots \underbrace{g_j g_{j+1} g_j}_{= g_{j+1} g_j g_{j+1} \text{ vertauschen}} g_{j-1} \cdots g_1$

$= g_i g_{i-1} \cdots g_{j+1} g_j g_{j-1} \cdots g_1 g_{j+1}. = t_i g_{j+1}$
$\in t_i U \subseteq X_V$.

Damit alle Fälle abgehandelt, also (*) ok
Damit Satz vollständig bewiesen $\square$.

Beispiel 4 (Unendliches Beispiel).

Sei $G = \bigoplus_{\mathbb{N}} (\mathbb{Q}, +)$ Für $n \in \mathbb{N}$ setze
$s_n = \frac{1}{n!}$ Dann gelt
$G = \langle \{ s_n \mid n \in \mathbb{N} \} \rangle$, denn für $a/b \in \mathbb{Q}$
mit $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ ist
$a/b = a(b-1) \cdot x_b$ (additive Schreibweise)
Es gelt die Relation $n s_n = s_{n-1}$ für alle $n \geq 2$.

oder $s_n^m = s_{n-1}$ in multiplikativer Schreibweise.

Relationen-Lemma $\Rightarrow$ $(\mathbb{Q}, +)$ isomorph zu einer Faktorgruppe von $\langle \{x_n, n \geq 1\} \mid x_n^n = x_{n-1}$ für alle $n \geq 2 \rangle$.

Man kann zeigen, daß $(\mathbb{Q}, +)$ sogar isomorph zu dieser Gruppe ist. Weitere Literatur:

D.L. Johnson, Presentations of groups, London Math. Soc. Student Texts 15, Cambridge University Press, 1990.

Beispiel 5 Sei

$$G = \langle a, b, c, d, e \mid \begin{array}{ll} ac = ca & ad = da \\ bc = cb & bd = db \\ ce = eca & de = edb \\ cca = ccae & \end{array} \rangle.$$

Dann ist das Wortproblem in G unlösbar; d.h. es gibt keinen Algorithmus, der in endl. vielen Schritten entscheidet, ob ein gegebenes Wort in a, b, c, d, e in G gleich 1 wird oder nicht. Dies ist vermutlich das einfachste denkbare Beispiel!, Siehe

D.J. Collins, A simple presentation of a group with unsolvable word problem. Illinois J. Math., 30 (1986), 230–234.

In den Übungen werden noch einige weitere Beispiele behandelt.

§3 Quasi-Einfachheit von Matrix-Gruppen

Definition Sei G eine nicht-abelsche Gruppe. Dann heißt G quasi-einfach, wenn jeder echte Normalteiler von G mit Zentrum $Z(G)$ enthalten ist.

Klar: G einfach $\Rightarrow$ G quasi-einfach.

Bemerkung: Sei G quasi-einfach. Dann gilt

(a) $G/Z(G)$ ist einfach.

(b) $G = G'$ = Kommutator-Untergruppe (siehe Ü3)

Beweis: (a). Sei $\varphi: G \to \bar{G} := G/Z(G)$ kanonischer Homomorphismus. Sei $N \leq \bar{G}$ Normalteiler mit $N \neq \bar{G}$. Dann ist $\pi^{-1}(N) \neq G$ Normalteiler also $\pi^{-1}(N) \leq Z(G)$ nach Voraussetzung und damit $N = \pi(\pi^{-1}(N)) = \{1_{\bar{G}}\}$.

(b) Annahme $G' \neq G$. Da G' Normalteiler, folgt also $G' \leq Z(G)$. Ü3: $G/Z(G)$ abelsch. Aber $G/Z(G)$ einfach nach (a); also $G/Z(G)$ zyklisch (jede Untergruppe ist Normalteiler, wegen $G/Z(G)$ abelsch). Denksportaufgabe:

H bel. Gruppe mit $H/Z(H)$ zyklisch
$\Rightarrow$ H abelsch.

Also G abelsch, Widerspruch zur Voraussetzung ↯

Sei nun K Körper und V K-Vektorraum mit dim $V < \infty$. Sei

$GL(V) := \{\varphi: V \to V \mid \varphi$ linear, bijektiv$\}$

$SL(V) := \{\varphi \in GL(V) \mid \det(\varphi) = 1\}$

Matrixversion: Ist $n = \dim V$ und $\mathcal{B} = \{v_1, \dots, v_n\}$ Basis von $V \Rightarrow$

$$GL(V) \cong GL_n(K), \quad \varphi \mapsto M_{\mathcal{B}}(\varphi) = \text{Matrix von } \varphi \text{ bzgl. } \mathcal{B}.$$

$$SL(V) \cong SL_n(K), \quad \varphi \mapsto M_{\mathcal{B}}(\varphi).$$

Satz Für $n=2$ sei $|K| > 3$; ansonsten K beliebig für $n \geq 3$. Dann ist $SL(V)$ quasi-einfach.

Der Beweis ist ein Proto-Typ für Beweise, die auch für andere Matrixgruppen, wie symplektische und orthogonale Gruppen (siehe §1) funktionieren. Grundlage ist folgendes allgemeines Kriterium:

Iwasawa's Lemma (1941, Spezialfall) Sei G eine Gruppe und X eine G-Menge. Folgende Voraussetzungen seien erfüllt:

(a) G operiert 2-fach transitiv und $\{g \in G \mid g.x = x \text{ für alle } x \in X\} \subseteq Z(G)$.

(b) $G = G' \neq \{1_G\}$.

(c) Für $x \in X$ gibt es einen abelschen Normalteiler $U \leq \mathrm{Stab}_G(x)$ mit $G = \langle gug^{-1} \mid u \in U, g \in G \rangle$.

Dann ist G quasi-einfach.

Beweis: Sei $N \leq G$ Normalteiler mit $N \not\subseteq Z(G)$.
zu zeigen: $N = G$.

Beh. 1 N operiert transitiv auf X.
denn: Wegen $N \not\subseteq Z(G)$ gibt es ein $h \in N$ mit $h \notin Z(G)$. Dann auch $h \notin \{g \in G \mid g.x = x \text{ für alle } x \in X\}$
also gibt es ein $x_0 \in X$ mit $x_1 := h.x_0 \neq x_0$.
Sei nun $y \in X$ beliebig, $y \neq x$. Da G 2-fach transitiv operiert, gibt es ein $g \in G$ mit
$g.x_0 = x_0$ und $g.x_1 = y$. Dann
(also $g : (x_0, x_1) \rightsquigarrow (x_0, y)$.)

$$y = g.x_1 = g.(h.x_0) = gh.x_0 = ghg^{-1}g.x_0 = ghg^{-1}(g.x_0)$$
$$= \underbrace{ghg^{-1}}_{\in N}.x_0 \quad \checkmark.$$

Beh. 2 Für $x \in X$ ist $N \not\subseteq G_x = \mathrm{Stab}_G(x)$.
denn wäre $N \subseteq G_x$, so $u.x = x$ für alle $u \in N$,
d.h. $\{x\}$ ist eine Bahn der Operation von N auf X.
Beh. 1 $\Rightarrow$ $X = \{x\}$. Aber dann $g.x = x$ für alle $g \in G$ also $G = Z(G)$ nach Voraussetzung.
Also G abelsch $\Rightarrow$ $G' = \{1_G\}$, Widerspruch zu 6).

Beh. 3 Für $x \in X$ ist G_x eine maximale Untergruppe von G.
Sei also $U \leq G$ Untergruppe mit $G_x \subseteq U \subseteq G$.
zu zeigen $U = G_x$ oder $U = G$. Annahme: $G_x \subsetneq U$.
Sei $u \in U \setminus G_x$, also $u.x \neq x$.
Sei nun $g \in G$ beliebig. Ist $g.x = x$, so $g \in G_x \subseteq U$. Sei nun $g.x \neq x$.
Da G 2-fach transitiv, gibt es ein $g' \in G$ mit

$g' \cdot x = x$ und $g' \cdot (g \cdot x) = u \cdot x$

[also $g' : (x, \underbrace{g \cdot x}_{\neq}) \rightsquigarrow (x, \underbrace{u \cdot x}_{\neq})$].

Dann $g' \in G_x \subseteq U$, also $g \cdot x = \underbrace{g^{-1} u}_{=: u' \in U} \cdot x = u' \cdot x$

Dann $u^{-1} g' \in G_x \subseteq U \Rightarrow g' \in U$.

Also $g \in U$ für alle $g \in G$, d.h. $G = U$ ✓.

Beh. 4 Wegen N Normalteiler ist $UN \leq G$ Untergruppe. Es gilt sogar UN Normalteiler.

denn: N Normalteiler $\Rightarrow G_x N \leq G$ Untergruppe mit $G_x \subseteq G_x N$. Annahme: $G_x = G_x \cdot N$

$\Rightarrow N \subseteq G_x$ Widerspruch zu Beh. 2.

Nach Beh. 3 ist G_x maximale Untergruppe, also $G_x N = G$. Weil $U \trianglelefteq G_x$ Normalteiler, sieht man sofort, daß $UN \leq G_x N$ Normalteiler [beachte: für $u \in U$ und $h \in N$ ist

$h u h^{-1} = u \underbrace{u^{-1} h u}_{\in N} \underbrace{h^{-1}}_{\in N} \in UN$].

Also UN Normalteiler in G.

Beh. 5 $UN = G$.

denn: für $u \in U$ und $g \in G$ ist

$g u g^{-1} \in g U N g^{-1} = UN$ nach Beh. 4.

Mit (c) folgt $G = \langle g u g^{-1} \mid g \in G, u \in U \rangle \subseteq UN$

also $G = UN$.

Schließlich $G/N = UN/N \overset{\uparrow}{\cong} U/U \cap N$

1. Isomorphiesatz.

U abelsch $\Rightarrow N \supseteq G' = G$ (Vor. (b))

also $N = G$. □

Wollen nun versuchen, Voraussetzungen von Iwasawa's Lemma nachzuweisen für $G = SL(V)$.

Wissen bereits ($\mathcal{V}_1$): $Z(G) = \{ a\,id_V \mid a^n = 1 \}$

Sei $\mathbb{P}(V) = \{ \langle v \rangle \mid 0 \neq v \in V \}$ wie bereits in §1 diskutiert, operiert G auf $\mathbb{P}(V)$ durch

$$G \times \mathbb{P}(V) \to \mathbb{P}(V)$$
$$(\varphi, \langle v \rangle) \mapsto \langle \varphi(v) \rangle.$$

Lemma 1 Diese Operation ist 2-fach transitiv.

Beweis: Seien $\langle u_1 \rangle, \langle u_2 \rangle, \langle v_1 \rangle, \langle v_2 \rangle \in \mathbb{P}(V)$ mit $\langle u_1 \rangle \neq \langle u_2 \rangle$ und $\langle v_1 \rangle \neq \langle v_2 \rangle$.

Dann sind $\{u_1, u_2\}$ und $\{v_1, v_2\}$ jeweils linear unabhängig. Sei $n = \dim V \geq 2$. Ergänze zu Basen von V:

$$\mathcal{B} := \{u_1, u_2, \dots, u_n\} \text{ und } \mathcal{B}' = \{v_1, v_2, \dots, v_n\}.$$

Definiere lineare Abbildung $\varphi: V \to V$ durch

$$\varphi(u_j) = v_j \quad \text{für } 1 \leq j \leq n.$$

Schreibe $v_j = \sum_{i=1}^{n} a_{ij} u_i$ mit $a_{ij} \in K$.

Dann $A = [a_{ij}] \in M_n(K)$ Matrix von φ bzgl. $\mathcal{B}$.

Da $\mathcal{B}, \mathcal{B}'$ Basen sind, ist $\det(A) \neq 0$

also $\det(\varphi) = \det(A) \neq 0$, $\varphi \in GL(V)$.

Problem: Es könnte sein, daß $\det(\varphi) \neq 1$ ist.

Sei $0 \neq a \in K$ und definiere lineare Abbildung $\varphi_a: V \to V$ durch

$$\varphi_a(u_1) = a v_1$$
$$\varphi_a(u_j) = v_j \quad \text{für } 2 \leq j \leq n.$$

Matrix von φ_a bzgl. $\mathcal{B}$ entsteht aus A, indem 1. Spalte von A mit a multipliziert wird. Also

$$\det(\varphi_a) = a \det(\varphi)$$

Wähle a so, daß $\det(\varphi_a) = 1$ Dann $\varphi_a \in SL(V)$ und es gilt $\varphi_a \cdot \langle u_1 \rangle = \langle a v_1 \rangle = \langle v_1 \rangle$

$\varphi_a \cdot \langle u_2 \rangle = \langle v_2 \rangle$ □

Als nächstes benötigen wir ein geeignetes Erzeugendensystem für $G = SL(V)$.

Definition: Sei $V^* = \mathrm{Hom}(V, \mathbb{K})$ Dualraum von V. Sei $\lambda \in V^*$ und $u \in V$, Dann definiere

$\varphi_{\lambda,u} : V \to V$ durch $\varphi_{\lambda,u}(v) := v + \lambda(v)\, u$.

Klar: $\varphi_{\lambda,u} : V \to V$ linear

Ist $\lambda(u) = 0$, so heißt $\varphi_{\lambda,u}$ Transvektion.

Beachte: Ist $\lambda = \underline{0}$ oder $u = 0$, so $\varphi_{\lambda,u} = \mathrm{id}_V$.

Ist $\lambda \neq \underline{0}$, so $H := \mathrm{Ker}(\lambda) \subsetneq V$ Teilraum der Dimension $\dim V - 1$ "Hyperebene".

Es gilt $\varphi_{\lambda,u}(v) = v + \varphi(v)\, u = v$ für alle $v \in H$

Sei $n = \dim V$ und $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ Basis von V, wobei $\{v_1, \dots, v_{n-1}\}$ Basis von H.

Dann $\varphi_{\lambda,u}(v_1) = v_1, \dots, \varphi_{\lambda,u}(v_{n-1}) = v_{n-1}$

und $\varphi_{\lambda,u}(v_n) = v_n + \lambda(v_n)\, u$.

Ist $\lambda(u) = 0$, so $u \in \mathrm{Ker}(\lambda) = H$, also

u Linearkombination von $v_1, \dots, v_{n-1}$,

$$u = \sum_{i=1}^{n-1} a_i v_i.$$ Dann

Matrix von $\varphi_{\lambda,u}$ bzgl. Basis $\mathcal{B}$:

$$\left[\begin{array}{ccc|c} 1 & & 0 & a_1 \\ & \ddots & & \vdots \\ 0 & & 1 & a_{n-1} \\ \hline 0 & \cdots & 0 & 1 \end{array}\right] \Rightarrow \det(\varphi_{\lambda,u}) = 1.$$

also $\varphi_{\lambda,u} \in SL(V)$

falls $\lambda(u) = 0$, also $\varphi_{\lambda,u}$ Transvektion.

Lemma 2 Es gelten folgende Regeln für Transvektionen:

(i) $\varphi_{\lambda, cu} = \varphi_{c\lambda, u}$ $(0 \neq c \in K)$.

(ii) $\varphi_{\lambda_1+\lambda_2, u} = \varphi_{\lambda_1, u} \circ \varphi_{\lambda_2, u}$

(iii) $\varphi_{\lambda, u_1+u_2} = \varphi_{\lambda, u_1} \circ \varphi_{\lambda, u_2}$

(iv) $\varphi^{-1} \circ \varphi_{\lambda,u} \circ \varphi = \varphi_{\lambda \circ \varphi, \varphi^{-1}(u)}$ für $\varphi \in GL(V)$

Beweis (i) $\varphi_{\lambda, cu}(v) = v + \lambda(v)cu = v + c\lambda(v)u$

$= \varphi_{c\lambda, u}(v)$ ✓

(ii) $\varphi_{\lambda_1+\lambda_2, u}(v) = v + (\lambda_1+\lambda_2)(v)u = v + \lambda_1(v)u + \lambda_2(v)u.$

Andererseits:

$(\varphi_{\lambda_1,u} \circ \varphi_{\lambda_2,u})(v) = \varphi_{\lambda_1,u}(v + \lambda_2(v)u)$

$= \varphi_{\lambda_1,u}(v) + \lambda_2(v)\varphi_{\lambda_1,u}(u)$

$= v + \lambda_1(v)u + \lambda_2(v)[u + \underbrace{\lambda_1(u)u}_{=0}]$

$= v + \lambda_1(v)u + \lambda_2(v)u.$ ✓

(iii) analog zu (ii)

(iv) $(\varphi_{\lambda,u} \circ \varphi)(v) = \varphi_{\lambda,u}(\varphi(v)) = \varphi(v) + \lambda(\varphi(v))u$

$= \varphi(v) + (\lambda \circ \varphi)(v)u$ und andererseits

$(\varphi \circ \varphi_{\lambda\circ\varphi, \varphi^{-1}(u)})(v) = \varphi(\varphi_{\lambda\circ\varphi, \varphi^{-1}(u)}(v))$

$= \varphi(v + (\lambda\circ\varphi)(v)\varphi^{-1}(u)) = \varphi(v) + (\lambda\circ\varphi)(v)u$ ✓ □

Lemma 3 Sei $0 \neq u \in V$ und $x := \langle u \rangle \in \mathbb{P}(V)$.

Sei $X_u := \{ \varphi_{\lambda, cu} \mid \lambda \in V^* \text{ mit } \lambda(u) = 0,\ 0 \neq c \in K \}$.

Dann ist X_u ein abelscher Normalteiler von

$G_x = \mathrm{Stab}_G(x)$.

Beweis: ~~[illegible]~~

$\varphi_{\lambda, cu}(u) = u + \underbrace{\lambda(u)}_{=0} cu = u$, also $\varphi_{\lambda, cu} \in G_x$.

Seien $\lambda_1, \lambda_2 \in V^*$ mit $\lambda_1(u) = \lambda_2(u) = 0$

$0 \neq c_1, c_2 \in K$. Dann:

$$\varphi_{\lambda_1, c_1 u} \circ \varphi_{\lambda_2, c_2 u} \overset{\text{Lemma 2(a)}}{=} \varphi_{c_1 \lambda_1, u} \circ \varphi_{c_2 \lambda_2, u}$$

$$\overset{\text{Lemma 2(b)}}{=} \varphi_{\underbrace{c_1\lambda_1 + c_2\lambda_2}_{=0 \text{ on } u!}, u} = \ldots = \varphi_{\lambda_2, c_2 u} \circ \varphi_{\lambda_1, c_1 u}$$

$\varphi_{0, cu} = \mathrm{id}$, also X_u abelsche Untergruppe.

$\varphi_{\lambda, cu}^{-1} = \varphi_{-\lambda, cu}$ nach obiger Rechnung.

Schließlich sei $\varphi \in G_x$ beliebig, also $\varphi(u) = au$ mit $0 \neq a \in K$.

Dann mit Lemma 2(iv):

$$\varphi^{-1} \circ \varphi_{\lambda, cu} \circ \varphi = \varphi_{\lambda \circ \varphi,\ \varphi^{-1}(cu)}$$

$$= \varphi_{\lambda \circ \varphi,\ ca^{-1}u} \in X_u, \text{ denn}$$

$$(\lambda \circ \varphi)(u) = \lambda(\varphi(u)) = a\lambda(u) = 0 \quad \checkmark \quad \square$$

Beispiel Sei $n = \dim V = 2$ und K Körper mit $|K| > 3$. Welche Voraussetzungen in Iwasawa's Lemma haben wir bereits?

(a) G operiert 2-fach transitiv auf $X = \mathbb{P}(V)$ $\checkmark$

Außerdem: Kern der Operation auf $Z(G)$ (§1)

$Z(G) = \{\pm \mathrm{id}\}$.

Betrachte nun $V = K^2$ $\quad SL(V) = SL_2(K)$

(b) $G = G' = \left\langle \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ t & 1 \end{bmatrix} \mid s,t \in K \right\rangle$ siehe Ü1 und Ü3.

zu (c): Sei $e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ und $x = \langle e_1 \rangle$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G_x \iff \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \alpha \\ 0 \end{bmatrix}.$$

$$\begin{bmatrix} a \\ c \end{bmatrix} \qquad \text{also} \quad c = 0$$

$$\text{damit} \quad d = a^{-1}$$

und $\quad G_x = \left\{ \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} \mid 0 \neq a \in K,\ b \in K \right\}$.

Sei $U = \left\{ \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} \mid s \in K \right\}$ Untergruppe von G_x.

U abelsch $\quad \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & s' \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & s+s' \\ 0 & 1 \end{bmatrix}$ ✓.

$$\begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix}^{-1} = \begin{bmatrix} a^{-1} & -b \\ 0 & a \end{bmatrix}$$ Damit

$$\begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a^{-1} & -b \\ 0 & a \end{bmatrix} = \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$$

Also $U \trianglelefteq G_x$ Normalteiler. [$U = X_{e_1}$ wie in Lemma 3]

Fehlt also nur noch:

(*) $\quad G = \langle g u g^{-1} \mid u \in U,\ g \in G \rangle$.

Sei $g = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \in G \quad \Rightarrow \quad g^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, also $g^{-1} = g$.

$$g \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} g^{-1} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & -s \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ -s & 1 \end{bmatrix} \quad \text{für alle } s \in K.$$

Also $\quad \{ g u g^{-1} \mid u \in U,\ g \in G \} \supseteq \left\{ \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ t & 0 \end{bmatrix} \mid s,t \in K \right\}$.

Also (*) OK

Damit: G quasi-einfach.

Sei nun $n =$ dim $V > 2$ und K beliebig.

(a) G operiert weiterhin 2-fach transitiv auf $X = \mathbb{P}(V)$.
Kern der Operation ist $Z(G) = \{a \cdot \mathrm{id}_V \mid a^n = 1\}$. ✓

(b) $G = G'$ noch offen.

(c) Sei wieder $V = K^n$, $G = SL_n(K)$.

$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ und $x = \langle e_1 \rangle \in X$. Wie oben

$$G_x = \left\{ \left[\begin{array}{c|ccc} a & a_2 & \cdots & a_n \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right] \;\middle|\; a_i \in K,\ A' \in GL_{n-1}(K),\ a \det(A') = 1 \right\}.$$

Sei $U := \left\{ \left[\begin{array}{c|ccc} 1 & a_2 & \cdots & a_n \\ \hline 0 & & & \\ \vdots & & I_{n-1} & \\ 0 & & & \end{array}\right] \;\middle|\; a_i \in K \right\}$

$$= \left[\begin{array}{c|c} 1 & v \\ \hline 0 & I_{n-1} \end{array}\right] \quad v \in K^{n-1}$$

$U = Xe_1$ wie in Lemma 3. Zeilenvektor.

$$\left[\begin{array}{c|c} 1 & v \\ \hline 0 & I_{n-1} \end{array}\right] \left[\begin{array}{c|c} 1 & v' \\ \hline 0 & I_{n-1} \end{array}\right] = \left[\begin{array}{c|c} 1 & v+v' \\ \hline 0 & I_{n-1} \end{array}\right]$$

also U Untergruppe und abelsch.

Nachrechnen: $\underbrace{\left[\begin{array}{c|c} a & w \\ \hline 0 & A' \end{array}\right]^{-1}}_{\in G_x} = \left[\begin{array}{c|c} a^{-1} & -wA'^{-1} \\ \hline 0 & A'^{-1} \end{array}\right]$

$$\rightarrow \left[\begin{array}{c|c} a & w \\ \hline 0 & A' \end{array}\right] \left[\begin{array}{c|c} 1 & v \\ \hline 0 & I_{n-1} \end{array}\right] \left[\begin{array}{c|c} a & w \\ \hline 0 & A' \end{array}\right]^{-1} = \left[\begin{array}{c|c} 1 & * \\ \hline 0 & I_{n-1} \end{array}\right]$$

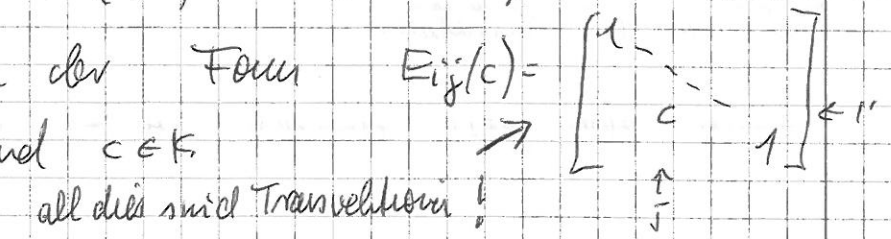
also $U \trianglelefteq G_x$ Normalteiler. Beachte nun:
Nach Ü4 sind alle Elemente von U Transvektionen.

Ebenfalls $\subseteq$: Transvektionen bilden komplette Konjugiertenklasse von G. $\Rightarrow$

$$\{gug^{-1} \mid g \in G,\ u \in U\} \supseteq \{\text{alle Transvektionen in } G\}$$

Also bleibt insgesamt noch zu zeigen:

(*) $G = G'$ und dies wird von Transvektionen erzeugt.

Lemma 4 $G = SL_n(K)$ wird erzeugt von den Elementarmatrizen der Form $E_{ij}(c) =$  mit $i \neq j$ und $c \in K$.

alle diese sind Transvektionen!

Beweis Klar da $E_{ij}(c) = 1$, also in $SL_n(K)$.

Lineare Algebra: Multiplikation einer Matrix von links oder rechts entspricht elementaren Zeilen- oder Spaltenoperationen:

(⊗) Addition Vielfaches einer Zeile/Spalte zu einer anderen.

Müssen also zeigen: Für Matrizen in $SL_n(K)$ funktioniert Gauß-Algorithmus allein mit Operationen der Form (⊗).

1. Schritt: Sei $A \in SL_n(K)$ $(n \geq 2)$. Dann können wir durch Operationen (⊗) erreichen, daß A in eine Matrix überführt wird mit Eintrag 1 an der Stelle $(1,1)$.

Dann: Erste Spalte von A ist nicht Null-Vektor (weil $\det(A) \neq 0$). Gibt es ein $i > 1$ mit $a_{i1} \neq 0$, so addiere das $c^{-1}(1 - a_{11})$-Fache

der i-ten Zeile zur 1. Zeile, Ergebnis:
in der neuen Matrix steht an der Position $(1,1)$
genau $a_{11} + a_{11}^{-1}(1-a_{11})\,a_{i1} = 1$ OK ✓

Wenn es ein solches i nicht gibt, so ist also
$a_{11} \neq 0$ und $a_{i1} = 0$ für alle $i \geq 2$.
Ist $a_{11} = 1$, OK. Wenn nicht, addieren
1. Zeile zur 2. Zeile, danach können wir
wie zuvor verfahren.

Haben also jetzt erreicht $A \to \left[\begin{array}{c|c} 1 & * \\ \hline * & \\ \vdots & * \\ * & \end{array}\right]$.

2. Schritt: Durch Operationen der Form $(\star)$
können wir ausschließlich alle Einträge in der
1. Spalte und 1. Zeile (außer $a_{11}=1$)
ausräumen, Erreichen also:

$$A \to \left[\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right]$$

mit $\det(A') = 1$.
und $A' \in SL_{n-1}(K)$

3. Schritt: Falls mit Induktion nach n
folgt, A' da kann man Operationen
der Form $(\star)$ auf I_{n-1} gebracht werden. □.

Lemma 5 Für $n > 2$ enthält $SL_n(K)$
eine Transvektion: $+ I_n$.

Beweis:

Betrachte $A = \begin{bmatrix} 1 & 0 & 0 & \\ 1 & 1 & 0 & \\ 0 & 0 & 1 & \\ \hline & & & \\ 0 & & & I_{n-3} \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 0 & 1 & 1 & \\ \hline & & & \\ & & & I_{n-3} \end{bmatrix}$

$A, B \in SL_n(K)$ und hier benutzen wir $n \geq 3$.

$A^{-1} = \begin{bmatrix} 1 & 0 & 0 & \\ -1 & 1 & 0 & \\ 0 & 0 & 1 & \\ \hline & & & \ddots \end{bmatrix}$ $\quad B^{-1} = \begin{bmatrix} 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 0 & -1 & 1 & \\ \hline & & & \ddots \end{bmatrix}$

Einfache Rechnung:

$AB = \begin{bmatrix} 1 & 0 & 0 & \\ 1 & 1 & 0 & \\ 0 & 1 & 1 & \\ \hline & & & \ddots \end{bmatrix}$ $\quad A^{-1}B^{-1} = \begin{bmatrix} 1 & 0 & 0 & \\ -1 & 1 & 0 & \\ 0 & -1 & 1 & \\ \hline & & & \ddots \end{bmatrix}$

$\Rightarrow [A, B] = ABA^{-1}B^{-1} = \begin{bmatrix} 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ -1 & 0 & 1 & \\ \hline & & & \\ & 0 & & I_{n-3} \end{bmatrix}$

Transvektion + Kommutator ✓ ∎.

Folgerung 6 Auch für dim $V \geq 3$ (und keine weiteren Voraussetzungen an K) sind alle Bedingungen in Iwasawa's Lemma für $G = SL(V)$ erfüllt und damit $SL(V)$ quasi-einfach.

denn: Fehlt nur noch $G = G'$

Nach Lemma 5 enthält G' eine Transvektion $\neq id$.

Nach $G' \trianglelefteq G$ Normalteiler, enthält G' die Konjugiertenklasse dieser Transvektion. Nach Ü4 sind alle Transvektionen konjugiert. Nach Lemma 4 wird G von Transvektionen erzeugt.

Also $G = G'$ ∎.

Folgerung 7 Sei K endlicher Körper mit q Elementen (also $q = p^f$ mit Primzahl p und $f \geq 1$).

Sei $PSL(n,q) := SL_n(K) / Z(SL_n(K))$.

Ist $(n,q) \notin \{(2,2),(2,3)\}$, so ist $PSL(n,q)$ eine endliche einfache Gruppe mit

$$|PSL(n,q)| = \frac{1}{ggT(n,q-1)} q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1).$$

Beweis: Nach allem, was wir bisher gezeigt haben, müssen wir nur noch $|PSL(n,q)|$ bestimmen.

Zunächst:
$$|GL_n(K)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$$
$$= q^{1+2+\cdots+(n-1)}(q^n-1)(q^{n-1}-1)\cdots(q-1).$$
$$n(n-1)/2.$$

$\det: GL_n(K) \to K^\times$ Homomorphismus

mit $SL_n(K) = SL_n(K)$

$\det$ surjektiv $\det \begin{bmatrix} \alpha & & \\ & \ddots & \\ & & 1 \end{bmatrix} = \alpha$ für alle $0 \neq \alpha \in K$.

Also $GL_n(K)/SL_n(K) \cong K^\times \Rightarrow$

$$|SL_n(K)| = \frac{|GL_n(K)|}{|K^\times|} \Rightarrow$$

$$|SL_n(K)| = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\cdots(q^2-1).$$

Bleibt noch $Z(GL_n(K)) = \{a \cdot I_n \mid a^n = 1, a \in K^\times\}$.

$K^\times$ zyklische Gruppe der Ordnung $q-1$.

$K^\times = \langle \alpha \rangle = \{\alpha^i \mid 1 \leq i \leq q-1\}$ $\quad 1 = \alpha^n = \alpha^{in}$

mit $o(\alpha) = q-1$ $\quad$ Sei $d = ggT(q-1,n)$

$\alpha^{i\cdot n} = 1 \Rightarrow q-1 = o(\alpha) \mid i\cdot n.$

$\Rightarrow \frac{q-1}{d} \mid i\cdot\frac{n}{d} \Rightarrow \frac{q-1}{d} \mid i.$

($\frac{n}{d}$ teilerfremd) Umgekehrt: Ist $\frac{q-1}{d} \mid i$

so $\alpha^{i\cdot n} = 1$. Damit

$$Z(SL(n,q)) = \left\{ \alpha^i I_n \;\middle|\; \begin{array}{l} 1 \le i \le q-1 \text{ und} \\ i \text{ Vielfaches von } \frac{q-1}{d} \end{array} \right\}.$$

$\Rightarrow |Z(SL(n,q))| = d$ □.

Mit Hilfe von Iwasawa's Lemma kann man auch die Quasi-Einfachheit von symplektischen und orthogonalen Gruppen (wie in §1) zeigen. Wollen hier zumindest für symplektische Gruppen andeuten, wie dies funktioniert.

Sei also $V \neq \{0\}$ K-Vektorraum mit $\dim V < \infty$ und $\beta : V \times V \to K$ nicht-ausgeartete alternierende Bilinearform auf, insbesondere also $\beta(v,v) = 0$ und $\beta(v,w) = -\beta(w,v)$ für alle $v, w \in V$.

Satz: Es gibt $\dim V = 2n$ mit $n \geq 1$. Es gibt eine Basis $\{v_1, w_1, v_2, w_2, \dots, v_n, w_n\}$ von V so daß zugehörige Gram-Matrix bzgl. dieser Basis folgende Gestalt hat:

$$\begin{bmatrix} \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} & & & 0 \\ & \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} & & 0 \\ & & \ddots & \vdots \\ 0 & 0 & \cdots & \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \end{bmatrix}$$

Beweis Induktion nach $\dim V$.

Ist $\dim V = 1$, so $\{v\}$ mit $0 \neq v \in V$ Basis von V.

$\beta(v,v) = 0 \Rightarrow$ Gram-Matrix $[0]$ widerspricht der Voraussetzung, dass β nicht-ausgeartet.

Sei nun $\dim V = 2$ und $0 \neq v_1 \in V$ beliebig.

Wäre $\beta(w, v_1) = 0$ für alle $w \in V$, so $v_1 \in V^\perp$ Widerspruch zu β nicht-ausgeartet.

Also gibt es $w_1 \in V$ mit $c := \beta(v_1, w_1) \neq 0$.

Ersetze w_1 durch $c^{-1} w \Rightarrow$ Es gilt

$$\beta(v_1, w_1) = 1 \qquad \beta(v_1, v_1) = 0$$

Damit auch $\beta(w_1, v_1) = -1$, $\beta(w_1, w_1) = 0$

[$w_1 \notin \langle v_1 \rangle$, sonst $\beta(v_1, w_1) = 0$ gelt nemero.]

Also $\{v_1, w_1\}$ gewünschte Basis.

Schließlich $\dim V > 2$. Genau wie im Fall $\dim V = 2$ finden wir $v_1, w_1 \in V$ mit

$\beta(v_1, w_1) = 1$, $\beta(w_1, v_1) = -1$ $\beta(v_1, v_1) = \beta(w_1, w_1) = 0$.

Wegen $w_1 \notin \langle v_1 \rangle$ ist $\{v_1, w_1\}$ linear unabhängig.

Sei $U := \langle v_1, w_1 \rangle$. Einschränkung von β auf $U \times U$ hat Gram-Matrix $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, ist also nicht-ausgeartet. Nach Ü4 gilt damit $V = U \oplus U^\perp$. $\dim U^\perp = \dim V - 2$.

Sei $B' = \{u_1, \dots, u_{m-2}\}$ Basis von $U^\perp$ $m = \dim V$.

Gram-Matrix von β bzgl. Basis $\{v_1, w_1, u_1, \dots, u_{m-2}\}$ ist

$$\left[\begin{array}{cc|c} 0 & 1 & \\ -1 & 0 & 0 \\ \hline & & \\ 0 & & A' \\ & & \end{array}\right]$$

$A' =$ Gram-Matrix von $\beta|_{U^\perp \times U^\perp} : U^\perp \times U^\perp \to K$ bzgl. B'

β nicht-ausgeartet $\Rightarrow \det(A') \neq 0$. Also Einschränkung von β auf $U^\perp$ nicht-ausgeartet und natürlich wieder alternierend. Nach Induktion ist dann $U^\perp$ gerade und es gibt Basis $\{v_2, w_2, \dots, v_n, w_n\}$ von $U^\perp$ mit Gram-Matrix

$$A' = \begin{bmatrix} \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} & & 0 \\ & \ddots & \\ 0 & & \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \end{bmatrix},$$ wie gewünscht. □

Folgerung Seien β, β' nicht-ausgeartete alternierende Bilinearformen auf V. Dann sind die zugehörigen symplektischen Gruppen $Sp(V, \beta)$ und $Sp(V, \beta')$ isomorph.

(siehe §1). Wählen wir Basis von V wie in obigem Satz, so berechne:

$$Sp_{2n}(K) = \{ A \in GL_{2n}(K) \mid A^{tr} \cdot G \cdot A = G \}$$

ab die symplektische Gruppe über K

wobei also $G = \begin{bmatrix} \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} & & 0 \\ & \ddots & \\ 0 & & \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \end{bmatrix}$

Folgerung Ist K endlicher Körper mit $|K| = q$, so gilt $|Sp_{2n}(K)| = q^{n^2}(q^{2n}-1)(q^{2(n-1)}-1)\cdots(q^2-1)$.

Beweis: Sei X die Menge aller Basen von $V = K^{2n}$ wie in obigem Satz, also $(v_1, w_1, \dots, v_n, w_n)$ mit Gram-Matrix

$$\begin{bmatrix} \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} & & \\ & \ddots & \\ & & \begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \end{bmatrix}$$

(bzgl. geg. $\beta: V \times V \to K$)

Dann operiert $G = Sp_{2n}(K)$ auf X.

Ist $A \in Sp_{2n}(K)$ und $(v_1, w_1, \dots, v_n, w_n) \in X$,

so $(Av_1, Aw_1, \dots, Av_n, Aw_n) \in X$.

weil $\beta(Av, Aw) = \beta(v, w)$ für alle $v, w \in V$.

Operation ist transitiv, denn sind

$(v_1, w_1, \dots, v_n, w_n) \in X$ und $(v_1', w_1', \dots, v_n', w_n') \in X$,

so gibt es invertierbare Matrix $A \in GL_{2n}(K)$ mit

$v_1' = Av_1$, $w_1' = Aw_1$, $\dots$, $v_n' = Av_n$, $w_n' = Aw_n$.

Denn

$\beta(Av, Aw) = \beta(v, w)$

für alle $v, w \in V$

(weil Gleichheit für alle Basisvektoren gilt)

also $A \in Sp_{2n}(K)$

Schließlich: Ist $(v_1, w_1, \dots, v_n, w_n) \in X$

so ist Stabilisator dieser Basis nur $\{I_{2n}\}$.

Damit $|Sp_{2n}(K)| = |X|$.

Müssen also alle Basen in X zählen.

Induktion nach n. Anfang $n = 1$

Basen (v_1, w_1) mit $\beta(v_1, w_1) = 1$.

$q^2 - 1$ Möglichkeiten für v_1.

Nun dim $\langle v_1 \rangle^\perp$ = dim V − dim $\langle v_1 \rangle$ = 1.

also $|\langle v_1 \rangle^\perp| = q$. Damit $q^2 - q$

Vektoren nicht senkrecht zu v_1.

Sei $w_1 \in V \setminus \langle v_1 \rangle^\perp$. Dann $\beta(v_1, cw_1) = c\beta(v_1, w_1)$ für $0 \neq c \in K$.

Also: unter den q^2-q Vektoren haben $\frac{q^2-q}{q-1}$ Skalarprodukt 1 mit v_1.

$$\Rightarrow \quad |X| = q^2-1 \cdot \frac{q^2-q}{q-1} = q(q^2-1) \quad \checkmark$$

Sei nun $n > 1$. Zähle alle $(v_1, w_1, v_2, w_2, \dots, v_n, w_n)$.

Zuerst $q^{2n}-1$ Möglichkeiten für v_1.

$\dim \langle v_1 \rangle^\perp = \dim V - \dim \langle v_1 \rangle = 2n-1$.

also $q^{2n} - q^{2n-1}$ Vektoren nicht senkrecht zu v_1.

wie oben $\Rightarrow$ $\frac{q^{2n}-q^{2n-1}}{q-1} = q^{2n-1}$ Möglichkeiten für w_1.

Sei nun $U = \langle v_1, w_1 \rangle$ für eine Wahl von (v_1, w_1).

$\beta|_{U \times U}$ nicht-ausgeartet $\Rightarrow V = U \oplus U^\perp$.

und $\beta|_{U^\perp \times U^\perp}$ nicht-ausgeartet (wie im obigen Beweis). Also nach Induktion:

$$\left| \begin{array}{c} \text{Anzahl Basen} \\ \text{in } U^\perp \end{array} \right| = |Sp_{2n-2}(K)|$$

$$= q^{(n-1)^2}(q^{2(n-1)}-1) \cdots (q^2-1).$$

Damit insgesamt

$$\underbrace{q^{2n-1}\, q^{(n-1)^2}}_{= q^{n^2}} (q^{2n}-1) \cdots (q^2-1)$$

□.

Beispiel: Sei $n=1$. $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(K)$.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Sp_2(K) \iff \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$= \begin{bmatrix} -c & a \\ -d & b \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -ca+ca & -cb+ad \\ -da+bc & -db+bd \end{bmatrix}$$

$$= \begin{bmatrix} 0 & ad-bc \\ -ad+bc & 0 \end{bmatrix}$$

$\Leftrightarrow$ $ad - bc = 1$ $\Leftrightarrow$ $\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} = 1 \Leftrightarrow \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(K)$

Also in diesem Fall: $Sp_2(K) = SL_2(K)$.

$|K| = q < \infty \Rightarrow$ beide haben Ordnung $q(q^2-1)$.

"4: Transvektionen in $Sp(V, \beta)$:

Für $0 \neq w \in V$ und $0 \neq c \in K$ definiere $\varphi : V \to V$

durch $\varphi(v) := v + c \cdot \beta(w, v) w$ für alle $v \in V$

Dann $\varphi \in Sp(V, \beta)$ und φ Transvektion.

Satz $Sp(V, \beta)$ wird erzeugt von Transvektionen wie oben.

Beweis: Sei $T \leq Sp(V, \beta)$ die von den Transvektionen erzeugte Untergruppe.

Bild-1 Zu $0 \neq v_1, v_2 \in V$ gibt es ein $\varphi \in T$ mit $\varphi(v_1) = v_2$, d.h. T operiert transitiv auf $V \setminus \{0\}$.

Ist $\beta(v_1, v_2) \neq 0$ (also $v_1 \neq v_2$), so setze $c := -\beta(v_1, v_2)^{-1} \in K$.
und $w := v_1 - v_2$.

Sei $\varphi : V \to V$ zugehörige Transvektion. Dann.

$$\varphi(v_2) = v_1 + c\,\beta(w, v_1)\, w = v_1 + c \underbrace{\beta(v_1 - v_2, v_1)}_{= \beta(v_1, v_1) - \beta(v_2, v_1)} (v_1 - v_2)$$

$$= v_1 - c\,\beta(v_2, v_1)(v_1 - v_2) = v_1 + c\,\beta(v_1, v_2)(v_1 - v_2)$$

$$= v_1 - (v_1 - v_2) = v_2 \quad \checkmark.$$

Sei nun $\beta(v_1, v_2) = 0$. Behauptung: Es gibt ein $w \in V$ mit $\beta(v_1, w) \neq 0$ und $\beta(v_2, w) \neq 0$

Ist $\langle v_1 \rangle = \langle v_2 \rangle$, so wähle irgendein $w \in V \setminus \langle v_1 \rangle^{\perp}$.

Beachte: dim $V \geq 2$, also $V \setminus \langle v_1 \rangle^\perp \neq \emptyset$

Seien nun (v_1, v_2) linear unabhängig. Annahme:

$$\underbrace{\{w \in V \mid \beta(v_1, w) = 0 \text{ oder } \beta(v_2, w) = 0\}}_{} = V.$$

$$= \{w \in V \mid \beta(v_1, w) = 0\} \cup \{w \in V \mid \beta(v_2, w) = 0\}$$

$$= \langle v_1 \rangle^\perp \cup \langle v_2 \rangle^\perp$$

echte Teilräume wegen $v_1 \neq 0$, $v_2 \neq 0$.

Aber: Vereinigung von 2 Teilräumen ist nur dann ein Teilraum, wenn einer in anderen enthalten ist, also etwa $\langle v_1 \rangle^\perp \subseteq \langle v_2 \rangle^\perp \Rightarrow = V$ ↯.

Also Annahme falsch, d.h. es gibt $w \in V$ mit $\beta(v_1, w) \neq 0$ und $\beta(v_2, w) \neq 0$

Nach vorherigem Fall gibt es Transvektionen $\varphi_1 : V \to V$ und $\varphi_2 : V \to V$ mit $\varphi_1(v_1) = w$ und $\varphi_2(w) = v_2$.

Dann $\varphi_2 \circ \varphi_1(v_1) = \varphi_2(w) = v_2$ ✓.

Beh. 2 Seien (v_1, w_1) und (v_2, w_2) Paare von Vektoren mit $\beta(v_1, w_1) = 1$ und $\beta(v_2, w_2) = 1$.

Dann gibt es ein $\varphi : V \to V$ mit $\varphi(v_1) = v_2$, $\varphi(w_1) = \varphi(w_2)$, $\varphi \in T$.

Nach Beh. 1 gibt es ein $\varphi \in T$: $\varphi : V \to V$ mit $\varphi(v_1) = v_2$. Setze $v_1' := v_2$, $w_2' = \varphi(w_1)$.

Dann $\varphi(v_1) = v_1' = v_2$ und $\varphi(w_1) = w_2'$.

Also (v_2, w_2') neues Paar mit $\beta(v_2, w_2') = \beta(v_1, w_1) = 1$.

das man mit φ aus (v_1, w_1) erhält.

Können also o.Bd.A. $v := v_1 = v_2$ annehmen.

Müssen noch ~~[illegible]~~ $\varphi \in T$ finden mit

$$\varphi(v) = \varphi v \text{ und } \varphi(w_1) = w_2.$$

Dann: Ist $\beta(w_1, w_2) \neq 0$ so sei wie oben $c = -\beta(w_1, w_2)^{-1}$ und $w := w_1 - w_2$, und $\varphi \in Sp(V, \beta)$ zug.

Transvektion: Dann wie in Beh. 1:

$$\varphi(w_1) = w_2$$

aber wir haben auch. $\varphi(v) = v + c\beta(w, v)w$

$$= v + c\underbrace{\beta(w_1 - w_2, v)}_{= \beta(w_1, v) - \beta(w_2, v) = 1 - 1 = 0} w \quad = v \text{ , also ok.}$$

Sei nun $\beta(w_1, w_2) = 0$ Dann betrachte die 3 Paare:

(v, w_1), $(v, w_1 + v)$ und (v, w_2)

$\beta(v, w_1) = 1$ ✓ $\beta(v, w_1 + v) = \beta(v, w_1) = 1$ ✓ $\beta(v, w_2) = 1$ ✓

Hier $\beta(w_1, w_1 + v) = \beta(w_1, v) = -1$.

$\beta(w_1 + v, w_2) = \beta(v, w_2) = 1$.

also können wir vorherigen Fall anwenden: Es gibt ~~[illegible]~~ $\varphi_1 : V \to V$ und $\varphi_2 : V \to V$ mit $\varphi_1, \varphi_2 \in T$.

$\varphi_1(v) = v$ $\varphi_1(w_1) = w_1 + v$ und

$\varphi_2(v) = v$ $\varphi_2(w_1 + v) = w_2$.

Dann $\varphi_2 \circ \varphi_1(v) = v$ und $\varphi_2 \circ \varphi_1(w_1) = w_2$.

Beh. 3 Es gilt $T = Sp(V, \beta)$.

Beweis mit Induktion nach dim V.

Anfang dim $V = 2 \Rightarrow$ $Sp(V, \beta) \cong SL(V)$

(siehe obiges Beispiel) Aussage bereits bekannt.

Sei nun dim $V > 2$ und Behauptung bereits bewiesen für symplektische Gruppen kleinerer Dimension.

Seien $v_1, w_1 \in V$ mit (v_1, w_1) l.u., $\beta(v_1, w_1) = 1$.
wie oben. $\beta(w_1, v_1) = -1$

Sei $U = \langle v_1, w_1 \rangle$. Wie bereits früher gesehen, ist $\beta|_{U \times U}$ nicht-ausgeartet, also $V = U \oplus U^\perp$; außerdem $\beta|_{U^\perp \times U^\perp}$ wieder nicht-ausgeartet. Können also Induktion auf $U^\perp$ anwenden. Sei nun $\varphi \in Sp(V, \beta)$ beliebig. Dann setze $v_1' = \varphi(v_1)$ $w_1' = \varphi(w_1)$.
$\Rightarrow$ auch (v_1', w_1') erfüllen Bedingung $\beta(v_1', w_1') = 1$
$\beta(w_1', v_1') = -1$
Nach Beh. 2 gibt es also $\varphi_1 \in T$ (!)
ein $\varphi_1 \in Sp(V, \beta)$ mit
$\varphi_1(v_1) = v_1'$ und $\varphi_1(v_1') = w_1'$.
Setze nun $\varphi' := \varphi_1^{-1} \circ \varphi \in Sp(V, \beta)$.
Dann ist $\varphi'(v_1) = v_1$, $\varphi'(w_1) = w_1$ also
$\varphi'|_U = id_U$ Nach Ü5 ist dann auch
$\varphi'(U^\perp) \subseteq U^\perp$, also $\varphi'|_{U^\perp} \in Sp(U^\perp, \beta|_{U^\perp \times U^\perp})$.
Nach Induktion ist $\varphi'|_{U^\perp} = \psi_1 \circ \dots \circ \psi_r$
mit Transvektionen $\psi_i \in Sp(U^\perp, \beta|_{U^\perp \times U^\perp})$

Beh.: Jedes ψ_i läßt sich zu einer Transvektion $\tilde{\psi}_i \in Sp(V, \beta)$ fortsetzen mit
$\tilde{\psi}_i|_U = id_U$.

Dann: ψ_i Transvektion heißt (Ü4):

Es gibt $0 \neq c_i \in K$ und $0 \neq u_i \in U^\perp$ mit

$$\varphi_i(v) = v + c\,\beta(u_i, v)\,u_i \quad \text{für alle } v \in U^\perp$$

Definiere einfach $\tilde{\varphi}_i : V \to V$ durch die gleiche Formel! Dann $\tilde{\varphi}_i$ Transvektion in $Sp(V, \beta)$ und für $u \in U$ gilt $\beta(u_i, u) = 0$, also

$$\tilde{\varphi}_i(u) = u \quad \text{für alle } u \in U.$$

Damit folgt nun $\varphi_1^{-1} \circ \varphi = \varphi' = \tilde{\varphi}_1 \circ \dots \circ \tilde{\varphi}_r$

stimmen überein auf U und auf $U^\perp$, also auf V!

$\Rightarrow$ $\varphi = \varphi_1 \circ \tilde{\varphi}_1 \circ \dots \circ \tilde{\varphi}_r$ Produkt von Transvektionen □.

Folgerung: $\beta : V \times V \to K$ nicht-ausgeartet, alternierend. Dann gilt $Sp(V, \beta) \subseteq SL(V)$.

denn: Jedes $\varphi \in Sp(V, \beta)$ ist Produkt von Transvektionen; jede Transvektion hat $\det = 1$ also auch $\det(\varphi) = 1$ □.

Man kann nun die weiteren Bedingungen in Iwasawa's Lemma nachweisen und erhält am Ende.

Satz: Sei $\beta : V \times V \to K$ nicht-ausgeartet, alternierend $\Rightarrow$ $Sp(V, \beta)$ quasi-einfach außer: dim $V = 2$, $|K| = 2$ oder 3
dim $V = 4$, $|K| = 2$ (siehe Ü5).

Beweis: siehe Buch von Taylor, Theorem 8.8 □.

§4 Ausblick: Algebraische Gruppen und Gruppen mit BN-Paar

Haben bisher gesehen: Gruppen $GL_n(K)$, $SL_n(K)$, $P_n(Q,K)$, jeweils Untergruppen von $GL_n(K)$.

Erinnerung GAGA A:

Eine Teilmenge $V \subseteq K^n$ heißt algebraische Menge wenn es eine Teilmenge $P \subseteq \underbrace{K[X_1, \dots, X_n]}_{\text{Polynomring in } X_1, \dots, X_n}$ gibt mit

$$V = \left\{ v = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \in K^n \;\middle|\; \begin{array}{l} f(v) := \\ f(v_1, \dots, v_n) = 0 \text{ für} \\ \text{alle } f \in P \end{array} \right\}.$$

Damit wird K^n ein topologischer Raum

$$\left\{ \begin{array}{l} \text{abgeschlossene} \\ \text{Mengen in } K^n \end{array} \right\} = \left\{ \begin{array}{l} \text{algebraische Mengen} \\ \text{wie gerade definiert} \end{array} \right\}$$

"Zariski-Topologie".

Sei $n \geq 1$ und $r = n^2 + 1$. Definiere

$D \in \underbrace{K[X_0, X_{ij} \; (1 \leq i,j \leq n)]}_{\text{Polynomring in } r \text{ Variablen}}$ durch

$$D := 1 - X_0 \det(X_{ij}) \quad \text{mit}$$

$$\det(X_{ij}) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) X_{1\sigma(1)} \cdots X_{n\sigma(n)}$$

Setze $\tilde{GL}_n(K) = \{ v \in K^r \mid D(v) = 0 \}$.

Beachte: Können $GL_n(K)$ mit $\tilde{GL}_n(K)$ identifizieren durch

$$\begin{array}{ccc} GL_n(K) & \to & \tilde{GL}_n(K) \\ A & \mapsto & (\det(A), A^{-1}) \end{array}$$

Definition: Eine Gruppe G heißt Matrix-algebraische Gruppe wenn es ein $n \geq 1$ gibt und einen algebraisch abgeschlossenen Körper K mit (a) $G \leq GL_n(K)$ Untergruppe

(b) $G \subseteq GL_n(K) \equiv \tilde{G}L_n(K)$ algebraische Menge.

K algebraisch abgeschlossen.

Beispiele a) $G = GL_n(K)$ selbst ist Matrix-algebraisch.

b) $SL_n(K) \leq GL_n(K)$ Untergruppe und Matrix-algebraisch $SL_n(K) = \{ v \in K^r \mid D_n(v) = 0 \}$.

wobei $D_n = 1 - \det(X_{ij})$

c) Sei $Q \in M_n(K)$ mit $\det(Q) \neq 0$.

Entweder $Q = Q^{tr}$ oder $Q = -Q^{tr}$ und $q_{ii} = 0$ für $1 \leq i \leq 4$

$Q = Q^{tr}$ ↙ symmetrisch

$q_{ii} = 0$ ↓ alternierend.

$\Gamma_n(Q, K) = \{ A \in M_n(K) \mid A^{tr} Q A = Q \} \leq GL_n(K)$ Untergruppe.

$A = [a_{ij}] \in \Gamma_n(Q, K)$ $\Leftrightarrow$

$A^{tr} Q A = Q \Leftrightarrow \sum_{i,j=1}^{n} a_{ki} q_{kl} a_{lj} = q_{ij}$ für $1 \leq k, l \leq n$.

$D(v) = 0$ und

Also $\Gamma_n(Q, K) = \{ v \in K^r \mid D_{kl}(v) = 0$ für $1 \leq k, l \leq n \}$

wobei $D_{kl} = \sum_{i,j=1}^{n} q_{kl} X_{ki} X_{lj} - q_{kl}$.

$\rightsquigarrow$ Theorie der algebraischen Gruppen.

Als algebraische Menge hat eine Matrix-algebraische Gruppe (1) irreduzible Komponenten (GAGA: Prop. 16.1) und (2) eine Dimension (GAGA: Thm. 1.40).

zu (1) $X \subseteq K^n$ algebraische Menge:

X heißt irreduzibel, wenn X nicht Vereinigung von 2 echten abgeschlossenen Teilmengen ist.

Im Allgemeinen: $X = X_1 \cup \dots \cup X_s$

mit X_i abgeschlossen + irreduzibel. $X_i \not\subseteq X_j$ für $i \neq j$

zu (2) $\dim X = \max(\dim X_i \mid 1 \leq i \leq s)$
falls X nicht irreduzibel.
mit Hilfe von Hilbert-Polynom.

Für G Matrix-algebraische Gruppe gilt:
Sei G^0 = irreduzible Komponente von $1_G \in G$.
Dann ist G^0 abgeschlossener Normalteiler von G und die weiteren irreduziblen Komponenten sind genau die Nebenklassen von G^0, insbesondere $[G : G^0] < \infty$.

$GL_n(K)$, $SL_n(K)$ und $Sp_{2n}(K)$ sind irreduzibel und

$\dim GL_n(K) = n^2$
$\dim SL_n(K) = n^2 - 1$
$\dim Sp_{2n}(K) =$

Satz 1.3.13 und Cor. 1.5.14 in

M. Geck, An introduction to algebraic geometry and algebraic groups, Oxford Univ. Press, 2005.

Chevalley's Klassifikationssatz (1957/58):

Jede einfache algebraische Matrixgruppe G über K ist entweder isomorph zu $PSL_n(K)$, zu einer der Gruppen $PT(Q, K)$ (und noch gewissen Varianten dazu, siehe §5) oder zu einer von 5 Ausnahme-Gruppen, die mit $G_2(K)$, $F_4(K)$, $E_6(K)$, $E_7(K)$, $E_8(K)$ dim 14, 52, 78, 133, 248. bezeichnet werden.

Elementare Theorie dazu:

Jacques Tits, Abel-Preis 2008.

Definition (Tits 1962). Sei G eine beliebige Gruppe und seien $B, N \leq G$ Untergruppen. Dann bilden diese ein "BN-Paar" (oder auch "Tits-System" genannt), wenn folgende Bedingungen gelten:

(BN1) $G = \langle B, N \rangle$ (G wird von B und N erzeugt)

(BN2) $H := B \cap N$ ist ein Normalteiler von N und $W := N/H$ wird von einer Menge S erzeugt mit $s^2 = 1$ für alle $s \in S$.

Sei $\pi : N \to W$ kanonischer Epimorphismus. Für $w \in W$ sei $n_w \in N$ Element mit $\pi(n_w) = w$.

[Ist auch $n_{w'} \in N$ mit $\pi(n_{w'}) = w$, so $n_{w'} = h n_w$ mit einem $h \in H$ und $n_{w'} B = n_w B$]

(BN3) Es gilt $n_s B n_s \notin B$ für alle $s \in S$.

(BN4) $n_s B n \subseteq B n_s n B \cup B n B$ für alle $s \in S$ und $n \in N$.

Die Gruppe W heißt Weyl-Gruppe des BN-Paares. Gilt außerdem:

(BN5) $\bigcap_{n \in N} nBn^{-1} = H$

so heißt das BN-Paar gesättigt.

Beachte: $H \subset B$ und $H \trianglelefteq N$ Normalteiler,
d.h. $H = nHn^{-1} \subseteq nBn^{-1}$ für alle $n \in N$,
also $H \subseteq \bigcap_{n \in N} nBn^{-1}$ gilt immer

Bemerkung Sei G beliebige Gruppe, $U, V \leq G$ Untergruppen. Dann heißt für festes $g \in G$ die Menge

$UgV := \{ugv \mid u \in U, v \in V\}$ Doppelnebenklasse von G bzgl. U, V.

G ist disjunkte Vereinigung von Doppelnebenklassen,
denn: Betrachte die Gruppe $H := U \times V$ (direktes Produkt).
Diese operiert auf der Menge $X = G$ durch

$H \times X \to H$ (einfaches Nachrechnen)
$((u,v), g) \mapsto ugv^{-1}$

Bahn von g $= \{ugv^{-1} \mid u \in U, v \in V\}$
$= \{ugv \mid u \in U, v \in V\} = UgV$.

Bahnensatz $\Rightarrow$ G disjunkte Vereinigung von Bahnen = Doppelnebenklassen.

Dies zeigt auch: Ist $A \subseteq G$ beliebige Teilmenge mit $UA \subseteq A$ und $AV \subseteq V$, so ist A Vereinigung von Doppelnebenklassen.

Beispiel Sei G Gruppe und X nicht-leere Menge, so G 2-fach transitiv operiert und $|X| \geq 3$ gelt. Sei $e \in X$ fest und $B := \mathrm{Stab}_G(e)$.

Sei auch $e' \in X$, $e' \neq e$. Da G 2-fach transitiv, gibt es ein $n \in G$ mit $n.e = e'$ und $n.e' = e$.

Sei $N := \langle n \rangle$. Dann bilden B, N ein BN-Paar mit $|W| = 2$.

Dazu:

(BN1) Sei $g \in G$ beliebig. Zu zeigen $g \in \langle B, N \rangle$

Sei $\tilde{e} := g.e$ 1. Fall: $\tilde{e} = e \Rightarrow g \in \mathrm{Stab}_G(e) = B$ ✓.

2. Fall: $\tilde{e} \neq e$ Wegen 2-fach transitiv gibt es ein $h \in G$ mit $h : (e, e') \mapsto (e, \tilde{e})$, also $h.e = e$ und $h.e' = \tilde{e}$ Dann $h \in \mathrm{Stab}_G(e) = B$ und $g.e = \tilde{e} = h.e' = h.(ne) = hn.e$

also $(hn)^{-1} g \in \mathrm{Stab}_G(e) = B \Rightarrow g \in hnB \subseteq \langle B, N \rangle$ ✓.

(BN2) Sei $H := B \cap N \subseteq N$. Da N zyklisch, ist N abelsch, also $H \trianglelefteq N$ Normalteiler

Nun ist $n^2.e = n.(n.e) = n.e' = e$, also $n^2 \in B \cap N = H$.

Wegen $n.e = e' \neq e$ ist $n \notin B$, also $n \notin H$.

Damit $|N/H| = 2$ und $W = N/H$ wird erzeugt von $s = nH \in N/H$.

Beweis von (BN1) zeigt sogar: $G = B \dot{\cup} BnB$ (wegen $n \notin B$)

also genau 2 Doppelnebenklassen mit Repräsentanten $\{1, n_s = n\}$.

(BN3) Annahme $nBn \subseteq B \Rightarrow Bn \subseteq n^{-1}B$

$\Rightarrow BnB \subseteq n^{-1}B$ also $G = B \cup n^{-1}B$

und damit $[G : B] = 2$.

über $B = \mathrm{Stab}_G(e)$ und G transitiv auf X

$\Rightarrow |X| = [G : \mathrm{stab}_G(e)] = [G : B] \geq 2$ Widerspruch zur Voraussetzung

(BN4) $nBn' \subseteq Bnn'B \cup Bn'B$ für alle $n' \in N$.

Nun $N = \langle n \rangle$ also $n' = n^i$ für ein i.

Ist i gerade, so $n' = n^i \in \langle n^2 \rangle \subseteq H$

und damit $nBn' = nB$ $\quad Bnn'B = BnB$

$Bn'B = B$ ✓.

Ist i ungerade, so $n' = nn^{i-1} \in nH$

$= Hn$

also $nBn' = nBHn = nBn$.

$Bnn'B = BnnHB = Bn^2B = B$ (wegen $n^2 \in H \subseteq B$)

$Bn'B = BnHB = BnB$.

also noch zu zeigen $nBn \subseteq B \cup BnB = G$

also o.k. □

Satz Sei K beliebiger Körper. Dann besitzt $G = GL_n(K)$ ein BN-Paar, so daß zugehörige Weyl-Gruppe isomorph zu S_n ist; BN gestaltet.

Beweis: Sei $B := \left\{ \begin{bmatrix} * & \cdots & * \\ & \ddots & \vdots \\ 0 & & * \end{bmatrix} \right\} \subseteq G$

Untergruppe der oberen Dreiecksmatrizen in G.

Dann ist $B = U \cdot H$ mit

$U = \left\{ \begin{bmatrix} 1 & \cdots & * \\ & \ddots & \vdots \\ 0 & & 1 \end{bmatrix} \right\} \subseteq G$ und $H = \left\{ \begin{bmatrix} t_1 & & 0 \\ & \ddots & \\ 0 & & t_n \end{bmatrix} \mid 0 \neq t_i \in K \right\}$.

$U \cap H = \{I_n\}$ und U ist Normalteiler von B.

Für $\sigma \in S_n$ definiere zugehörige Permutationsmatrix $P^\sigma \in G$ durch $P^\sigma := (p_{ij}^\sigma)$ mit $p_{ij}^\sigma = \begin{cases} 1 & \text{falls } i = \sigma(j) \\ 0 & \text{sonst.} \end{cases}$

Einfaches Nachrechnen: $P^\sigma \cdot P^\tau = P^{\sigma\circ\tau}$
für alle $\sigma, \tau \in S_n$.

Außerdem
$P^\sigma e_j$ = j-te Spalte von P^σ = $e_{\sigma(j)}$

wobei $\{e_1, \dots, e_n\}$ Standardbasis von K^n.

Sei $D = \begin{bmatrix} t_1 & & 0 \\ & \ddots & \\ 0 & & t_n \end{bmatrix} \in H$ Dann gilt

$$(P^\sigma)^{-1} D P^\sigma = \begin{bmatrix} t_{\sigma(1)} & & 0 \\ & \ddots & \\ 0 & & t_{\sigma(n)} \end{bmatrix}$$

denn: $(P^\sigma)^{-1} D P^\sigma e_i = (P^\sigma)^{-1} D e_{\sigma(i)} = t_{\sigma(i)} (P^\sigma)^{-1} e_{\sigma(i)} = t_{\sigma(i)} e_i$
für $1 \le i \le n$.

Sei $N := \{$ monomiale Matrizen in $G\}$
$\uparrow$ in jeder Zeile und Spalte genau ein Eintrag $\neq 0$.

Dies ist eine Untergruppe, $N = \{ DP^\sigma \mid D \in H, \sigma \in S_n \}$
Wegen obiger Transformationsregel ist $H \trianglelefteq N$
Normalteiler in N, $N = D\tilde{W}$ und
$\tilde{W} = \{ P^\sigma \mid \sigma \in S_n \}$ Untergruppe von G isomorph
und $W = N/H \cong \tilde{W}$ zu S_n.

Schließlich: $B \cap N = \{$ Dreiecksmatrix und monomial$\}$
$= \{$ Diagonalmatrizen $\} = H$.

Damit haben wir Ingredienzien, um BN-Paar-Axiome nachzuweisen.

Zu (BN1) Gauß-Algorithmus: Jede invertierbare Matrix läßt sich durch elementare Zeilen/Spalten-Umformungen auf die Einheitsmatrix bringen.
Elementare Umformungen entsprechen Multiplikation mit Elementarmatrizen der folgenden Form

von links oder rechts:

(i) $\begin{bmatrix} 1 & & & \\ & \ddots & t & \\ & & \ddots & \\ & & & 1 \end{bmatrix} \in i$ mit $t \neq 0$

(ii) $\begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ & & 0 & 1 & \\ & & 1 & 0 & \\ & & & & \ddots \end{bmatrix}$ vertauscht 2 Zeilen oder Spalten

(iii) $\begin{bmatrix} 1 & & t & \\ & \ddots & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}$ mit $t \in K$

(iv) $\begin{bmatrix} 1 & & & 0 \\ & \ddots & & \\ & & \ddots & \\ t & & & 1 \end{bmatrix}$ mit $t \in K$.

Matrix der Form (i): $\in H \subseteq B$.

— " — (ii): Permutationsmatrix in N.

— " — (iii) oder Dreiecksmatrix $\in B$

(iv) unter Dreiecksmatrix $\in B' = \left\{ \begin{bmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{bmatrix} \right\}$.

Also folgt bereits: $G = \langle B, N, B' \rangle$.

Müssen nur noch zeigen $B' \subseteq \langle B, N \rangle$.

Dann sei $n_0 = \begin{bmatrix} 0 & & & 1 \\ & \ddots & \iddots & \\ & \iddots & \ddots & \\ 1 & & & 0 \end{bmatrix} \in N$.

(entspricht Permutation $\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ n & n-1 & & \cdots & 1 \end{pmatrix} \in S_n$)

$$n_0 \begin{bmatrix} * & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & * \end{bmatrix} n_0 = \begin{bmatrix} 0 & \cdots & * \\ \vdots & \iddots & \vdots \\ * & \cdots & * \end{bmatrix} n_0 = \begin{bmatrix} * & \cdots & 0 \\ \vdots & \iddots & \vdots \\ * & \cdots & * \end{bmatrix}$$

also $n_0 B n_0 = B' \subseteq \langle B, N \rangle$ ✓.

zu (BN2) $H = B \cap N \trianglelefteq N$ und $W = N/H \cong S_n$ bereits gesehen. Außerdem:

$S_n = \langle \tau_1, \ldots, \tau_{n-1} \rangle$ mit $\tau_i = (i, i+1)$ für $1 \leq i \leq n-1$

$\tau_i^2 = \mathrm{id}$.

Sei $S = \{ s_1, \ldots, s_{n-1} \} \subseteq W$ mit $s_i \mapsto \tau_i$.

Dann $W = \langle S \rangle$ mit $s_i^2 = 1$ für $1 \leq i \leq n-1$

zu (BN3) und (BN4): Sei $s_i \in S$ und $n \in \mathbb{N}$. Wegen $N = H \cdot \{ P^\sigma \mid \sigma \in S_n \}$ und $H \subseteq B$ können wir annehmen, daß

$$n_i = n_{s_i} = P^{\sigma_i} \quad \text{und} \quad n = P^\sigma \text{ gilt.}$$

Für $1 \le i, j \le n$ sei $E_{ij} \in M_n(K)$ Elementarmatrix mit 1 an Position (i,j) und 0 sonst. Für $i \neq j$ setze $X_{ij} = \{ I_n + t E_{ij} \mid t \in K \} \subseteq G$ Untergruppe.

$$= \left\{ \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & t & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \leftarrow i \;\middle|\; t \in K \right\}$$

$\uparrow$ j

Setze $X_i = X_{i,i+1}$.

$X_{-i} = X_{i+1,i}$

und $Y_i = \{ [a_{ij}] \in U \mid a_{i,i+1} = 0 \}$.

$$= \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ & \ddots & \ddots & \vdots \\ & & 0 & * \\ & & & 1 \end{pmatrix} \leftarrow i \right\} \subseteq U.$$

$\uparrow$ $i+1$

ebenfalls Untergruppe.

Es gilt:

(a) $U = X_i Y_i = Y_i X_i$ und $X_i \cap Y_i = \{ I_n \}$.

(b) $n_i X_i n_i^{-1} = X_{-i}$ und $n_i Y_i n_i^{-1} = Y_i$.

(c) $n^{-1} X_i n = X_{\sigma^{-1}(i), \sigma^{-1}(i+1)}$ wobei $N \to S_n$, $n \mapsto \sigma$.

Einfaches Nachrechnen, z.B. (c)

$$n^{-1} (I_n + t E_{i,i+1}) n = I_n + t n^{-1} E_{i,i+1} n.$$

$$= I_n + t \underbrace{(P^\sigma)^{-1} E_{i,i+1} P^\sigma}$$

mal dem Elementarmatrix, müssen also nur herausfinden, wo die 1 steht.

$(P^\sigma)^{-1} E_{i,i+1} P^\sigma e_{\sigma^{-1}(i+1)} = (P^\sigma)^{-1} E_{i,i+1} e_{i+1}$

$= (P^\sigma)^{-1} e_i = e_{\sigma^{-1}(i)}$ also steht d_i^{-1} an der Stelle $(\sigma^{-1}(i), \sigma^{-1}(i+1))$

Jetzt zu (BN3): Brauche $n_i^- = n_i^{-1}$

$n_i B n_i \not\subseteq B$, denn $X_i \subseteq B$ aber

$n_i X_i n_i = X_{-i} \not\subseteq B$

$n_i B n_i^- = n_i H n_i^{-1} n_i U n_i^{-1} = H \underbrace{n_i X_i n_i^{-1}}_{= X_{-i}} \underbrace{n_i Y_i n_i^{-1}}_{= Y_i}$

$= H Y_i X_{-i}$

Wäre dies in B enthalten, so auch X_{-i}, Widerspruch.

Jetzt zu (BN4): $n_i B n = n_i H U n = n_i H n_i^{-1} n_i U n$

$\subseteq H n_i U n = H n_i Y_i n_i^{-1} n_i X_i n = \underbrace{H Y_i}_{\subseteq B} n_i X_i n$

$\subseteq B n_i X_i n = B n_i n n^{-1} X_i n.$

$= B n_i n X_{\sigma^{-1}(i), \sigma^{-1}(i+1)}$ wobei wieder $n \mapsto \sigma$.

1. Fall $\sigma^{-1}(i) < \sigma^{-1}(i+1)$.

Dann $X_{\sigma^{-1}(i), \sigma^{-1}(i+1)} \subseteq B$, also $n_i B n \subseteq B n_i n B$ ✓.

2 Fall: $\sigma^{-1}(i) > \sigma^{-1}(i+1)$ Dann setze $n' := n_i n$.

$n' \mapsto \sigma' = s_i \sigma$ $\sigma'^{-1}(i) = \sigma^{-1} s_i(i) = \sigma^{-1}(i+1)$

$< \sigma^{-1}(i) = \sigma^{-1} s_i(i+1) = \sigma'^{-1}(i+1)$

also sind wir im 1. Fall und damit

$n_i B n' \subseteq B n_i n B = B n B$

Damit $n_i B n \subseteq B n_i X_i n = B n_i X_i n_i^{-1} n'$

$= B X_{-i} n'$ so.

Jetzt brauche folgende Aussage in $SL_2(K)$:

$$\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} = \begin{pmatrix} 1 & t^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & -t^{-1} \end{pmatrix}$$

Bette $SL_2(K)$ an die entsprechende für $0 \neq t \in K$
Position $\begin{matrix} i & i+1 \\ i+1 & i \end{matrix}$ in $GL_n(K)$ ein.

Dann folgt:

$$X_{-i} = \left\{ \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & \boxed{\begin{matrix} 1 & 0 \\ t & 1 \end{matrix}} & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} \;\middle|\; t \in K \right\}$$

(0 oben rechts; 0 unten links; i, $i+1$ markiert)

$$\subseteq \{I_n\} \cup X_i n_i X_i H \subseteq B \cup B n_i B.$$

Also $BX_{-i} n' \subseteq B (B \cup B n_i B) n'$

$$\subseteq Bn' \cup \underbrace{B n_i B n'}_{\text{1. Fall}} \subseteq Bn' \cup B n_i n' B$$

$$= Bn' \cup BnB$$

$$\subseteq B n_i n B \cup BnB \quad \checkmark.$$

Fehlt noch: (BN5) Sättigung

$B = UH \Rightarrow nBn^{-1} = nUn^{-1}H \supseteq H.$

$n = n_0$ wie oben $\Rightarrow n_0 B n_0^{-1} = B'$

$B \cap B' = H \Rightarrow H = \bigcap_{n \in N} nBn^{-1}$ □.

Bemerkung Betrachte $SL_n(K) \leq GL_n(K)$

Sei $B' = B \cap SL_n(K)$, $N' = N \cap SL_n(K)$

Dann sind (B', N') ein BN-Paar in $SL_n(K)$ und es gelt wieder $W' \cong W = S_n$.

($\rightsquigarrow$ ☺).

Definition Sei G eine Gruppe mit einem BN-Paar $B, N \leq G$ und Weyl-Gruppe W.

(a) Für $w \in W$ sei $C(w) := BnwB$ wobei $n_w \in N$ mit $\pi(n_w) = w$ $\pi: N \to W$ hom. Epim.

Bemerke: $C(w)$ hängt nicht ab von der Wahl von n_w, denn ist auch $n' \in N$ mit $\pi(n') = w$ so $n' = h n_w$ mit $h \in H = \ker(\pi)$ und damit $Bn'B = BhnwB = BnwB$.

(b) $W = \langle S \rangle$ mit $s^2 = 1$ für alle $s \in S$.

Wegen (BN3) ist $s \neq 1$ für alle $s \in S$.

Also $o(s) = 2$, $s = s^{-1}$ $\Rightarrow$ Jedes $w \in W$ läßt sich schreiben als $w = s_1 \cdots s_m$ mit $s_i \in S$.

Ein solcher Ausdruck heißt reduziert, wenn m minimal ist, in diesem Fall heißt $\ell(w) = m$ die Länge von w.

$$\ell(1) = 0 \qquad \ell(s) = 1 \text{ für alle } s \in S$$

Bemerke: Ist $1 \neq w \in W$, so gibt es stets ein $s \in S$ mit $\ell(sw) = \ell(w) - 1 \leq \ell(w)$.

denn sei $w = s_1 \cdots s_m$ mit $s_i \in S$ und $m = \ell(w)$

Setze $s = s_1 \Rightarrow sw = s_1 s_1 s_2 \cdots s_m = \underbrace{s_2 \cdots s_m}$ reduziert

also $\ell(sw) = \ell(w) - 1$

↑ denn sonst wäre auch ursprünglicher Ausdruck nicht reduziert.

Werden dies häufig in Induktionsargumenten verwendet.

Es gelte einer $\ell(w) - 1 \leq \ell(sw) \leq \ell(w) + 1$.

$\ell(w^{-1}) = \ell(w)$.

Satz Sei $J \subseteq S$ und $W_J = \langle J \rangle \subseteq W$ Untergruppe. Sei $N_J = \pi^{-1}(W_J) \leq N$.
Dann ist $P_J := BNB \leq G$ Untergruppe von G.
Insbesondere gilt $G = BNB = \bigcup_{n \in N} BnB$.
$\swarrow$ $= \langle B, N \rangle$ weil Ugr.

Beweis: Müssen zeigen, daß P_J abgeschlossen unter Inversen und Multiplikation ist.
Sei $p \in P_J$ beliebig, $p = bnb'$ mit $b, b' \in B$, $n \in N_J$.
$\Rightarrow p^{-1} = b'^{-1} n^{-1} b^{-1} \in BN_JB = P_J$ ✓.

Beh.: $N_J P_J \subseteq P_J$.
Dazu sei $n \in N$, $\pi(n) = w \in W$.
$w = s_1 \cdots s_m$ mit $s_i \in S$, $n_i \in N$ Urbild von s_i.
$\Rightarrow n = h n_1 \cdots n_m$ mit $h \in H$.
$n_i P_J = n_i BN_J B \subseteq Bn_i N_J B \cup BN_J B$
(BN4) $\nearrow$ $\subseteq BN_JB \cup BN_JB = P_J$
für alle i, also auch $nP_J \subseteq P_J$.

Damit $P_J P_J = BN_J P_J \subseteq BP_J \subseteq P_J$ □.

Hauptsatz (Bruhat-Zerlegung) Es gelt
$G = \dot{\bigcup}_{w \in W} C(w)$ (disjunkte Vereinigung)
Für $s \in S$ und $w \in W$ gelt $\ell(sw) = \ell(w) \pm 1$ und

$$C(s) \cdot C(w) = \begin{cases} C(sw) & \text{falls } \ell(sw) = \ell(w) + 1 \\ C(sw) \cup C(w) & \text{falls } \ell(sw) = \ell(w) - 1 \end{cases}$$

Beweis: Wissen bereits $G = BNB = \bigcup_{n \in N} BnB$.

Müssen also noch zeigen, daß Vereinigung disjunkt ist, wenn Doppelnebenklassen nur über n_w, $w \in W$, laufen.

Seien $y, w \in W$ mit $C(y) = C(w)$ und $\ell(y) \leq \ell(w)$.

Beh: $y = w$.

Dann: Induktion nach $\ell(y)$

Anfang $\ell(y) = 0$, d.h. $y = 1 \Rightarrow C(y) = B = B n_w B$

wobei $n_w \in N$ mit $\pi(n_w) = w$.

$\Rightarrow n_w \in B \cap N = H$ also $w = 1$ OK ✓

Sei nun $\ell(y) > 0$. Dann $y = sx$ mit $s \in S$, $x \in W$

und $\ell(y) = \ell(x) + 1$.

$n_s n_x B \subseteq B n_s n_x B = B n_y B = B n_w B$

$\Rightarrow n_x B \subseteq n_s^{-1} B n_w B = n_s B n_w B$

$\subseteq$ (BN4) $B n_s n_w B \cup B n_w B$.

also $B n_x B \subseteq B n_s n_w B \cup B n_w B$.

aber Doppelnebenklassen sind entweder gleich oder disjunkt. $\Rightarrow B n_x B = B n_s n_w B$ oder $B n_x B = B n_w B$.

Nach Induktion: $x = sw$ oder $x = w$.

2. Fall ist unmöglich wegen $\ell(x) = \ell(y) - 1 < \ell(w)$

also $x = sw$ und damit $y = sx = s(sw) = w$ ✓.

Jetzt zur Multiplikationsregel. $s \in S$ und $w \in W$

Klar $\ell(w) - 1 \leq \ell(sw) \leq \ell(w) + 1$. (s.o.).

Beh.: $\ell(sw) > \ell(w) \Rightarrow C(s) C(w) = C(sw)$.

Bew mit Induktion nach $\ell(w)$

Anfang $\ell(w) = 0$, d.h. $w = 1 \Rightarrow C(1) = B$

$C(s) C(1) = B n_s B B = B n_s B = C(s)$ OK ✓

Sei nun $\ell(w) > 0$, schreibe $w = yt$ mit $y \in W$

$t \in S$ und $\ell(w) = \ell(y) + 1$.

Annahme: $C(s)\,C(w) \cap C(w) \neq \emptyset$

$\Rightarrow$ $B\, u_s B\, u_w B \cap B u_w B \neq \emptyset$.

$\Rightarrow$ $u_s B u_w \cap B u_w B \neq \emptyset$

Dann $u_s B u_y \cap B u_w B u_t = (u_s B u_w \cap B u_w B) u_t \neq \emptyset$

wegen $w = yt$ ~~geht~~ $sw = syt$

$\ell(sw) > \ell(w)$ wäre $\ell(sy) < \ell(y)$, so

$\ell(syt) < \ell(y) + 1 = \ell(w)$, Widerspruch. Also $\ell(sy) > \ell(y)$

Nach Induktion $u_s B u_y \subseteq B u_{sy} B$

$\Rightarrow$ $B u_{sy} B \cap B u_w B u_t \neq \emptyset$.

"Zwischen BW4" $\rightarrow$ $B u_w B u_t \subseteq B u_w u_t B \cup B u_w B$.

$\Rightarrow$ $B u_{sy} B \cap B u_w u_t B \neq \emptyset$

oder $B u_{sy} B \cap B u_w B \neq \emptyset$. (Nachtr.: $\ell(y) < \ell(w)$)

1. Teil des Beweises: $\Rightarrow$ (i) $sy = wt$ oder (ii) $sy = w$

Aber $w = yt$ also $wt = y t^2 = y$

Wäre (i), so $sy = y \Rightarrow s = 1$ Widerspruch zu (BW3)

Also gelt (ii): ~~gelt~~ $sy = w$.

und damit $\ell(sw) = \ell(ssy) = \ell(y) < \ell(w)$ Widerspruch.

Also war Annahme $C(s)\,C(w) \cap C(w) \neq \emptyset$ falsch.

Wegen $C(s)\,C(w) \subseteq C(sw) \cup C(w)$ (BW4)

folgt also $C(s)\,C(w) \subseteq C(w)$, d.h.

$C(s)\,C(w) = C(w)$ wie behauptet (falls $\ell(sw) > \ell(w)$)

Sei nun $\ell(sw) < \ell(w)$. (BW4) $\Rightarrow$

$u_s B u_s \subseteq B \cup B u_s B$.

(BN3) $\Rightarrow$ $n_s B n_s \cap B n_s B \neq \emptyset$.

$\Rightarrow$ $n_s B \cap B n_s B n_s \neq \emptyset$ $\Rightarrow$

$n_s B n_w \cap B n_s B n_s n_w \neq \emptyset$. Nun gilt

$l(s(sw)) = l(w) > l(sw)$, also nach vorherigem Fall:

$B n_s B n_s n_w \subseteq B n_s^2 n_w B = B n_w B$

$\Rightarrow$ $n_s B n_w \cap B n_w B \neq \emptyset \Rightarrow C(w) \subseteq C(s) C(w)$

andererseits $n_s n_w \in B n_s B n_w B = C(s) C(w)$

also auch $C(sw) \subseteq C(s) C(w)$

(BN4) $\Rightarrow$ $C(s) C(w) \subseteq C(sw) \cup C(w)$

also gilt Gleichheit andernfalls folgt $l(sw) = l(w)$ □

Folgerung: (Austausch-Lemma) Sei $w \in W$ und $w = s_1 \cdots s_m$ mit $s_i \in S$ reduziert, also $l(w) = m$. Sei $s \in S$ beliebig mit $l(sw) < l(w)$. Dann gibt es ein $i \in \{1, \dots, m\}$ mit

$$sw = s_1 \cdots s_{i-1} s_{i+1} \cdots s_m.$$

Beweis: Wegen $l(sw) < l(w)$ ist $C(s) C(w) = C(sw) \cup C(w)$ nach Bruhat-Zerlegung, also

$B n_s B n_w B \cap B n_w B \neq \emptyset$ und damit auch $n_s B n_w \cap B n_w B \neq \emptyset$.

ex. $b_1, b_2, b_3 \in B$ mit $n_s b_1 n_w = b_2 n_w b_3$

also $n_s = b_2 n_w b_3 n_w^{-1} b_1 \in B n_w B n_w^{-1} B$.

$= C(w) C(w^{-1})$.

Mit (BN4) folgt sofort mit Induktion nach $m = l(w)$:

$$C(w)C(y) \subseteq \bigcup_{1 \le i_1 < \dots < i_\ell \le m} C(s_{i_1} \cdots s_{i_\ell} y) \quad \text{für alle } y \in W.$$
mit $0 \le \ell \le m$.

Induktionsanfang $m = 0$, d.h. $w = 1$ $\quad C(w) = C(1) = B$

also $\quad C(w)C(y) = C(y)$ ✓.

$m > 0$: $\quad C(w) = C(s_1)\, C(s_2 \cdots s_m)$ nach Zerlegung

also $\quad C(w)C(y) \subseteq C(s_1)\, \underbrace{C(s_2 \cdots s_m)\, C(y)}_{\text{Induktion}}$

$$\subseteq \bigcup_{2 \le i_2 < \dots < i_\ell \le m} \underbrace{C(s_1)\, C(s_{i_2} \cdots s_{i_\ell} y)}_{\text{wende noch einmal (BW4) an.}}$$

$$\subseteq C(s_1 s_{i_2} \cdots s_{i_\ell} y) \cup C(s_{i_2} \cdots s_{i_\ell} y), \quad \checkmark$$

also folgt (wende obiges Induktion an mit $y = w^{-1}$):

$ns \in C(w)C(w^{-1})$ also $s = x w^{-1}$ und

$$x = s_{i_1} \cdots s_{i_\ell}$$

$$\Rightarrow \ell(x) \le \ell \le m = \ell(w)$$

sei $x = t_1 \cdots t_p$ mit $s_i \in S$ reduziert

$$\ell(x) = p \le \ell.$$

$$1 = \ell(s) = \ell(x w^{-1}) = \ell(t_1 \cdots t_p w^{-1}) \ge \ell(w) - \ell(x) \ge m - p \ge m - \ell$$

$$\Rightarrow m = \ell(w) \le \ell + 1 \quad \text{also} \quad \ell \ge \ell(w) - 1.$$

$\ell(w)$ ≥

Falls $\ell = \ell(w)$, dann $x = w$ also $s = 1$, Widerspruch

also $\ell = \ell(w) - 1$, d.h. $x = s_1 \cdots s_{i-1} s_{i+1} \cdots s_m$ ✓

□.

Werden nun sehen, daß das obige, zunächst so harmlos aussehende Austausch-Lemma einige sehr starke Konsequenzen für W nach sich zieht.

§5 Coxeter-Gruppen

Erinnerung §2: S Menge F = freie Gruppe auf S; sei $R \subseteq F$ Teilmenge und $N = \langle\langle R \rangle\rangle \subset F$ der von R erzeugte Normalteiler von F $\rightsquigarrow$ $\langle S \mid R \rangle := F/N$

"Präsentation" mit $S :=$ Erzeuger, $R :=$ definierende Relationen.

Relationen-Lemma: Jede andere Gruppe, in der die durch R gegebenen "Relationen" gelten (für ein Erzeugendensystem von G), ist isomorph zu einer Faktorgruppe von $\langle S \mid R \rangle$.

Definition: Sei S endliche Menge und $M = (m_{st})_{s,t \in S}$ Matrix mit $m_{st} = m_{ts} \geq 2$ für alle $s,t \in S$, $s \neq t$ und $m_{ss} = 1$.

Sei F = freie Gruppe auf S und

$$R := \{ (st)^{m_{st}} \mid s,t \in S \}.$$

Insbesondere: $s = t \Rightarrow m_{st} = 1 \Rightarrow s^2 \in R$ für alle $s \in S$.

Dann heißt

$$W(S,M) := F/\langle\langle R \rangle\rangle$$ Coxeter-Gruppe zur Matrix M. Bezeichnen wir Bilder der $s \in S$ in $W(S,M)$ mit $\bar{s}$, so gilt also:

$$\bar{s}^2 = 1 \text{ und } (\bar{s}\bar{t})^{m_{st}} = 1 \text{ für alle } s,t \in S.$$

Beispiel (§2) S_n, $n \geq 2$, ist eine Coxeter-Gruppe mit $S = \{ s_1, \dots, s_{n-1} \}$ und Relationen: s_i^2 für alle i,

$(s_i s_j)^2$ für $|i-j|>1$, $(s_i s_{i+1})^3$

d.h. zugehörige Matrix M hat Größe $(n-1)\times(n-1)$

und $M = \begin{bmatrix} 1 & 3 & & & & \\ 3 & 1 & 3 & & & \\ & 3 & 1 & \ddots & 2 & \\ & & \ddots & \ddots & \ddots & \\ & & & & & 3 \\ & 2 & & & 3 & 1 \end{bmatrix}$

Ziel dieses Abschnittes ist es folgenden Satz zu zeigen:

Haupt-Satz Sei G eine Gruppe, $B, N \leq G$ Untergruppen, die ein BN-Paar bilden. Sei W zugehörige Weyl-Gruppe mit Erzeugen S.

Annahme: $|W| < \infty$ Für $s,t \in S$ sei m_{st} = Ordnung von $st \in W$.

(also $m_{ss} = 1$ für $s = t$ und $m_{st} = m_{ts}$ für alle $s \neq t$).

Dann ist W Coxeter-Gruppe $\cong W(S, M)$ mit $M = (m_{st})_{s,t \in S}$.

Angewandt auf $G = GL_n(K)$ erhalten wir also als Spezialfall, daß $S_n \cong W$ eine Coxeter-Gruppe ist (neuer Beweis für obige Präsentation).

Außerdem werden wir sehen, wie man alle endlichen Coxeter-Gruppen klassifizieren kann.

Sei zunächst W beliebige Gruppe und $S \subseteq W$ Teilmenge mit $W = \langle S \rangle$ und $o(s) = 2$ für alle $s \in S$.

Wegen $s = s^{-1}$ für $s \in S$ ist dann wieder jedes $w \in W$ darstellbar als $w = s_1 \cdots s_m$ mit $s_i \in S$. Ist m minimal, so heißt der Ausdruck wieder reduziert und $\ell(w) = m$ Länge von w.

Wie zuvor: $\ell(1) = 0$ $\quad \ell(s) = 1$ für $s \in S$

$$\ell(w) - 1 \leq \ell(sw) \leq \ell(w) + 1 \quad \text{für } s \in S,\ w \in W$$

$$\ell(w) = \ell(w^{-1}) \quad \text{für alle } w \in W.$$

Wir nehmen jetzt an, daß die Aussage des Austauschs-Lemmas gilt, d.h.:

(A) $\begin{cases} \text{sei} & w = s_1 \cdots s_p \text{ mit } s_i \in S \text{ reduziert,} \\ \text{also} & \ell(w) = p, \text{ und } s \in S \text{ mit } \ell(sw) \leq \ell(w) \end{cases}$

Dann gibt es ein i mit $sw = s_1 \cdots s_{i-1} s_{i+1} \cdots s_p$.

Lemma 1 Sei $w \in W$ und $w = s_1 \cdots s_m$ mit $s_i \in S$ beliebiger Ausdruck, nicht notwendig reduziert. Dann gibt es $1 \leq i_1 < \cdots < i_p \leq m$ mit

$$w = s_{i_1} \cdots s_{i_p} \quad \text{und} \quad \ell(w) = p$$

Beweis: Induktion nach m. Anfang $m = 0$, d.h. $w = 1$ Aussage o.k.

$m = 1$: $w = s \in S$ reduziert, ebenfalls o.k.

Sei nun $m > 1$. Ist $w = s_1 \cdots s_m$ bereits reduziert, so ist nichts zu zeigen ($p = m$). Sei also nun $\ell(w) < m$. Dann gibt es ein i, so daß $s_{i+1} \cdots s_m$ reduziert, aber $s_i s_{i+1} \cdots s_m$ nicht reduziert ist. (A) $\Rightarrow$ ex. j mit

$$s_i s_{i+1} \cdots s_m = s_{i+1} \cdots s_{j-1} s_{j+1} \cdots s_m$$

$$\Rightarrow w = s_1 \cdots s_{i-1} s_i s_{i+1} \cdots s_m = s_1 \cdots s_{i-1} s_{i+1} \cdots s_{j-1} s_{j+1} \cdots s_m$$

Ausdruck mit $m-2$ Faktoren, also folgt Beh. mit Induktion. ∎

Bemerkung 2 Seien $s, t \in S$, $s \neq t$, und $\infty > m_{st} \geq 2$ Ordnung von st. Ü1 $\Rightarrow$

$W_{st} := \langle s, t \rangle \leq W$ Diedergruppe der Ordnung $2m_{st}$

Die $2m$ Elemente von W_{st} sind wie folgt gegeben:

$1, \; s, \; st, \; sts, \ldots, \underbrace{sts\ldots}_{m_{st}-1}$ Faktoren.

$t, \; ts, \; tst, \ldots, \underbrace{tst\ldots}_{m_{st}-1}$ Faktoren.

$\Delta_{st} := \underbrace{ststs\ldots}_{m_{st}} = \underbrace{tsts\ldots}_{m_{st}}$ Faktoren.

Beachte: $1 = (st)^{m_{st}} = \underbrace{stst\ldots}_{\text{insgesamt } 2m_{st} \text{ Faktoren.}}$

Bringt eine Hälfte auf die andere Seite $\Rightarrow$ die beiden Ausdrücke für Δ_{st}.

Alle obigen Ausdrücke sind reduziert !

Siehe noch einmal die Rechnungen in Ü1.

Satz 3 (Matsumoto, Tits) Sei M ein Monoid d.h. eine Menge zusammen mit einer assoziativen Verknüpfung $*$ so daß neutrales Element $e \in M$ existiert. Sei $f: S \to M$ eine Abbildung mit

$$\underbrace{f(s) * f(t) * f(s) * \ldots}_{m_{st}} = \underbrace{f(t) * f(s) * f(t) * \ldots}_{m_{st}}$$

für alle $s, t \in S$ mit $s \neq t$ und $m_{st} < \infty$.

Dann läßt sich f fortsetzen zu einer Abbildung $\tilde{f}: W \to M$ mit

$$\tilde{f}(w) = f(s_1) * \ldots * f(s_p)$$

falls $w = s_1 \ldots s_p$ mit $s_i \in S$ reduziert.

Beweis: Setze $f(1) = e$ und $f(s) = f(s)$ für $s \in S$.

Sei nun $w \in W$ beliebig mit $p = \ell(w) \geq 1$.

Gegeben zwei reduzierte Ausdrücke

$$w = s_1 \cdots s_p = t_1 \cdots t_p \quad \text{mit } s_i, t_j \in S.$$

Müssen zeigen: $f(s_1) * \ldots * f(s_p) = f(t_1) * \cdots * f(t_p)$.

Induktion nach p. Anfang $p = 1$, $w \in S$ o.k.

Sei nun $p \geq 2$, und Aussage bereits bewiesen für Elemente kleinerer Länge. Annahme: Aussage für w ist falsch, also $w = s_1 \cdots s_p = t_1 \cdots t_p$ aber

$$f(s_1) * \cdots * f(s_p) \neq f(t_1) * \cdots * f(t_p).$$

Nun ist $t_1 w = t_1 s_1 \cdots s_p = t_2 \cdots t_p$

also $\ell(t_1 w) \leq p - 1 < \ell(w)$. Wegen (A) angewandt auf $w = s_1 \cdots s_p$, gibt es ein i mit

$$t_1 w = s_1 \cdots s_{i-1} s_{i+1} \cdots s_p.$$

$$\Rightarrow \quad w = t_1 s_1 \cdots s_{i-1} s_{i+1} \cdots s_p \quad (p \text{ Faktoren!})$$

neuer reduzierter Ausdruck für w

Annahme: $i \neq p$ Dann

$$w s_p = t_1 s_1 \cdots s_{i-1} s_{i+1} \cdots s_{p-1}$$

$$= s_1 \cdots s_{p-1}$$

$\geq$ reduzierte Ausdrücke für $w s_p$.

also nach Induktion:

$$f(t_1) * f(s_1) * \cdots * f(s_{i-1}) * f(s_{i+1}) * \cdots * f(s_{p-1})$$

$$= f(s_1) * \cdots * f(s_{p-1}) \quad \text{und dann}$$

$$f(t_1) * f(s_1) * \cdots * f(s_{i-1}) * f(s_{i+1}) * \cdots * f(s_{p-1}) * f(s_p)$$

$$= f(s_1) * \cdots * f(s_p)$$

andererseits $t_1 w = s_1 \cdots s_{i-1} s_{i+1} \cdots s_p$

$$= t_2 \cdots t_p \quad \geq \text{reduzierte}$$

Ausdrücke für $t_1 w$. Also nach Induktion:

$$f(s_1) \ast \dots \ast f(s_{i-1}) \ast f(s_{i+1}) \ast \dots \ast f(s_p)$$
$$= f(t_2) \ast \dots \ast f(t_p) \text{ und damit}$$

$$f(t_1) \ast f(s_1) \ast \dots \ast f(s_{i-1}) \ast f(s_{i+1}) \ast \dots \ast f(s_p)$$
$$= f(t_1) \ast \dots \ast f(t_p).$$

Vergleiche die beiden obigen Ausdrücke $\Rightarrow$

$$f(s_1) \ast \dots \ast f(s_p) = f(t_1) \ast \dots \ast f(t_p)$$

Widerspruch zur Annahme.

Also gilt $i = p$, d.h.

$w = t_1 s_1 \dots s_{p-1}$ neuer reduzierter Ausdruck für w.

Es gibt $f(t_1) \ast f(s_1) \ast \dots \ast f(s_{p-1}) \neq f(s_1) \ast \dots \ast f(s_p)$

denn: $t_1 w = s_1 \dots s_{p-1} = t_2 \dots t_p$ zwei reduzierte Ausdrücke.

Induktion

$$f(s_1) \ast \dots \ast f(s_{p-1}) = f(t_2) \ast \dots \ast f(t_p).$$

$\Rightarrow$

$$f(t_1) \ast f(s_1) \ast \dots \ast f(s_{p-1}) = f(t_1) \ast \dots \ast f(t_p)$$
$$\neq f(s_1) \ast \dots \ast f(s_p)$$

↑ Annahme.

Fahre nun fort mit den beiden reduzierten Ausdrücken

$$w = \overbrace{t_1 s_1 \dots s_{p-1}}^{\text{neu}} \quad \text{und} \quad = \overbrace{s_1 \dots s_{p-1} s_p}^{\text{alt.}}$$

Dann $\ell(s_1 t_1 s_1 \dots s_{p-1}) = \ell(s_2 \dots s_p) < p$

also nach (A) gibt es ein i mit.

$s_1 t_1 s_1 \dots s_{p-1} =$ lasse einen Faktor in $t_1 s_1 \dots s_{p-1}$ weg.

Nach gleichem Argument wie oben muß dies wieder

der letzte Faktor sei also 0

$s_2 t_2 s_2 \cdots s_{p-1} = t_2 s_2 \cdots s_{p-2}$ und damit

$w = t_2 s_2 \cdots s_{p-1} = s_2 t_2 s_2 \cdots s_{p-2}$ neue reduzierte, dieselbe für w

Wiederum wie oben:

$$f(t_2) \cdot f(s_2) \cdot \cdots \cdot f(s_{p-1}) \neq f(s_2) \cdot f(t_2) \cdot f(s_2) \cdots \cdot f(s_{p-2}).$$

Falsche Form mit

$$w = \underbrace{t_2 s_2 \cdots s_{p-1}}_{\text{alt}} \quad \text{und} \quad = \underbrace{s_2 t_2 s_2 \cdots s_{p-2}}_{\text{neu}}.$$

Dann $\ell(t_2 s_2 t_2 s_2 \cdots s_{p-2}) = \ell(s_2 \cdots s_{p-1}) < p$, also gibt es wieder ein i mit

$t_2 s_2 t_2 s_2 \cdots s_{p-2} =$ kann einen Faktor in $s_2 t s_2 \cdots s_{p-2}$ weg.

Dies muß wieder der letzte sein, also:

$$t_2 s_2 t_2 s_2 \cdots s_{p-2} = s_2 t s_2 \cdots s_{p-3}$$

und damit:

$$w = \underbrace{s_2 t_2 s_2 \cdots s_{p-2}}_{\text{alt}} = \underbrace{t_2 s_2 t_2 s_2 \cdots s_{p-3}}_{\text{neu}}.$$

und zwischen Bildern unter f nicht gleich.

Nach endlich vielen Schritten werden alle Faktoren $s_2, \ldots, s_p$ verschwinden, also bleibt am Ende

$$\underbrace{s_2 t s_2 \cdots e}_{p} = \underbrace{t_2 s_2 t_2 \cdots}_{p} \text{ Faktoren.}$$

und $f(s_2) \cdot f(t_2) \cdot f(s_2) \cdots \neq f(t_2) \cdot f(s_2) \cdots$

Nun sind die Ausdrücke reduziert, also o.B.d.A. muß $p \leq m_{s_1 t_1}$ gelten (siehe Bemerkung 2).

Wäre $p < m_{s_1 t_1}$, dann $(s_1 t_1)^p = 1$ Widerspruch zu $m_{s_1 t_1}$ = Ordnung von $s_1 t_1$.

Also $p = m_{s_1 t_1}$, aber dann Widerspruch zur Voraussetzung an f. □

Folgerung 4 Sei F = freie Gruppe auf S.

$R = \{ s^2, (st)^{m_{st}}$ falls $s \neq t, m_{st} < \infty \}$.

Dann ist $\langle S | R \rangle \cong W$.

Beweis: Sei $\bar{F} := F / \langle\langle R \rangle\rangle$. Nach Relationen-Lemma in §2 gibt es zugehörige Homomorphismen $\varphi: \bar{F} \to W$ mit $\varphi(\bar{s}) = s$ für alle $s \in S$ ($W \cong$ Faktorgruppe von $\bar{F}$). Nun ist $\bar{F}$ insbesondere ein Monoid, wegen $s^2 \in R$ gilt $\bar{s}^2 = 1$ in $\bar{F}$. Wegen $(st)^{m_{st}} \in R$ gilt $(\bar{s}\bar{t})^{m_{st}} = 1$ und damit

$$\underbrace{\bar{s}\bar{t}\bar{s}\cdots}_{m_{st}} = \underbrace{\bar{t}\bar{s}\bar{t}\cdots}_{m_{st}}$$ Faktoren falls $m_{st} < \infty$.

Können also $f: S \to \bar{F}$, $s \mapsto \bar{s}$, betrachten und diese Abbildung erfüllt Voraussetzung von Matsumoto-Tits. Also gibt es Fortsetzung $\hat{f}: W \to \bar{F}$ mit $\hat{f}(w) = \bar{s}_1 \cdots \bar{s}_m$ wenn $w = s_1 \cdots s_m$ mit $s_i \in S$ reduziert

Behauptung: $\hat{f}$ ist ein Gruppen-Homomorphismus.

Dazu: Müssen zeigen $\hat{f}(yw) = \hat{f}(y)\hat{f}(w)$ für alle $y, w \in W$.

Eine einfache Induktion nach $\ell(y)$ zeigt, daß es genügt, dies für $\ell(y)=1$, also $y=s\in S$ zu testen. Müssen also zeigen

$$\hat{f}(sw)= f(s)\,f(w) = \bar{s}\,f(w) \quad \text{für alle } w\in W \text{ und } s\in S.$$

1. Fall: $\ell(sw)>\ell(w)$ Sei $w=s_1\cdots s_m$ mit $s_i\in S$ reduziert.

$\Rightarrow$ $ss_1\cdots s_m$ ebenfalls reduziert, also

$$\hat{f}(ss_1\cdots s_m) = f(s)f(s_1)\cdots f(s_m) = \bar{s}\,\hat{f}(s_1\cdots s_m)$$
$$= \bar{s}\,\hat{f}(w) \quad \checkmark$$

2. Fall: $\ell(sw)\leq \ell(w)$ Setze $w'=sw \Rightarrow w=sw'$

(A) $\Rightarrow \ell(sw)<\ell(w)$ also $\ell(w')<\ell(w)=\ell(sw')$.

Nach 1. Fall ist $\hat{f}(w) = \hat{f}(sw') = \bar{s}\,\hat{f}(w') = \bar{s}\,\hat{f}(sw)$

wegen $\bar{s}=\bar{s}^{-1}$ also auch $\hat{f}(sw)=\bar{s}\,\hat{f}(w)$ $\checkmark$

Damit φ und $\hat{f}$ jeweils Homom. mit

$(\varphi\circ\hat{f})(\bar{s})=\bar{s}$ und $(\hat{f}\circ\varphi)(\bar{s})=\bar{s}$ für alle $s\in S$

$\Rightarrow$ $\varphi\circ\hat{f}=\mathrm{id}_W$ und $\hat{f}\circ\varphi=\mathrm{id}_{\bar{W}}$

also $\varphi,\hat{f}$ Isomorphismen. □

Da Weyl-Gruppe einer Gruppe mit BN-Paar die Bedingung (A) erfüllt, folgt nun der Hauptsatz P_0. Nun zur Klassifikation

Nehmen stets an: $W=\langle S\rangle$ mit

$s^2=1$ für $s\in S$ und es gilt (A).

$s\neq 1$

Außerdem ab jetzt: $|W|<\infty$.

Manchmal auch $|S|<\infty$ und $m_{st}=o(st)<\infty$ für alle $s,t\in S$.

Sei $|S| = d$ und $S = \{s_1, \dots, s_d\}$

$m_{ij} := m_{s_i s_j}$ für $1 \le i, j \le d$.

Sei V ein $\mathbb{R}$-Vektorraum mit Basis $\{e_1, \dots, e_d\}$

Für $1 \le i \le d$ definiere lineare Abbildung $\rho_i : V \to V$

durch $\rho_i(e_j) = e_j + 2\cos\left(\frac{\pi}{m_{ij}}\right) e_i$

Lemma 1 $\rho_i(e_i) = -e_i$ $\quad$ Spur $(e_i) = d-2$

$\rho_i^2 = id_V$ $\quad$ ρ_i ist diagonalisierbar mit genau einem Eigenwert -1 und $d-1$ Eigenwerten 1.

Beweis: Gleiche Rechnung wie in Ü6.

Lemma 2 Seien $i \neq j$ und $U := \langle e_i, e_j \rangle_{\mathbb{R}} \subseteq V$ Teilraum. Dann gilt $\rho_i(U) \subseteq U$, $\rho_j(U) \subseteq U$.

und es gibt Teilraum $U' \subseteq V$ mit $V = U \oplus U'$

und $\rho_i(u') = u'$, $\rho_j(u') = u'$ für alle $u' \in U'$!

Beweis: $\rho_i(e_i) = -e_i \in U$ $\quad$ $\rho_i(e_j) = e_j + 2\cos\left(\frac{\pi}{m_{ij}}\right) e_i \in U$

genauso $\rho_j(e_i), \rho_j(e_j) \in U$. Komplement von U:

Für $l \neq i, j$ betrachte Gleichungen:

$$x_l - \cos\left(\frac{\pi}{m_{ij}}\right) y_l = \cos\left(\frac{\pi}{m_{il}}\right)$$

$$-2\cos\left(\frac{\pi}{m_{ij}}\right) x_l + y_l = \cos\left(\frac{\pi}{m_{jl}}\right)$$

mit Unbekannten x_l, y_l.

$$\det \begin{bmatrix} 1 & -\cos\left(\frac{\pi}{m_{ij}}\right) \\ -\cos\left(\frac{\pi}{m_{ij}}\right) & 1 \end{bmatrix} = 1 - \underbrace{\cos^2\left(\frac{\pi}{m_{ij}}\right)}_{< 1 \text{ wegen } i \neq j \text{ und } m_{ij} < \infty.} > 0$$

Also jeweils genau eine Lösung $\begin{bmatrix} x_l \\ y_l \end{bmatrix}$.

Setze $U' := \langle e_\ell' = e_\ell + x_\ell e_i + y_\ell e_j \mid \ell \neq i,j \rangle_{\mathbb{R}} \subseteq V$.

Klar: $U \oplus U' = V$. ($U \cap U' = \{0\}$ und $\dim U' = d-2$).

$$\rho_i(e_\ell') = \rho_i(e_\ell) + x_\ell \rho_i(e_i) + y_\ell \rho_i(e_j)$$

$$= e_\ell + 2\cos\left(\tfrac{\pi}{m_{i\ell}}\right) e_i - x_\ell e_i + y_\ell e_j + 2\cos\left(\tfrac{\pi}{m_{ij}}\right) e_i$$

$$= e_\ell + 2\underbrace{\left[\cos\left(\tfrac{\pi}{m_{i\ell}}\right) + \cos\left(\tfrac{\pi}{m_{ij}}\right)\right]}_{= x_\ell} e_i - x_\ell e_i + y_\ell e_j$$

$$= e_\ell + x_\ell e_i + y_\ell e_j = e_\ell' \quad \checkmark$$

Genauso $\rho_j(e_\ell') = e_\ell'$ ✓.

<u>Folgerung 3</u> Es gibt einen Gruppen-Homomorphismus $\rho: W \to GL(V)$ mit $\rho(s_i) = \rho_i$ für $1 \leq i \leq d$.

<u>Beweis:</u> Nach Lemma 1 ist $\rho_i^2 = id_V$ für alle i.

Nach Relationen-Lemma und wegen $W \cong \langle S \mid R \rangle$ müssen wir nur noch zeigen, daß $(\rho_i \rho_j)^{m_{ij}} = id$ gelt für alle $i \neq j$.

Seien also $i \neq j$ fest und betrachte $V = U \oplus U'$ wie in Lemma 2. Neue Basis

$B = \{e_i, e_j, e_\ell' \mid \ell \neq i,j\}$ von V.

M_i = Matrix von ρ_i bzgl B =

$$\begin{bmatrix} -1 & 2\cos(\pi/m_{ij}) & & 0 \\ 0 & 1 & & \\ & & 1 & \\ & & & \ddots \\ 0 & & & 1 \end{bmatrix}$$

M_j = Matrix von ρ_j bzgl. B =

$$\begin{bmatrix} 1 & 0 & & & 0 \\ 2\cos(\pi/m_{ij}) & -1 & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{bmatrix}$$

also Matrix von $\rho_i \rho_j$ ist gleich $\begin{bmatrix} A & & \\ & 1 & 0 \\ & 0 & \ddots \end{bmatrix}$

mit

$$A = \begin{bmatrix} -1 & 2\cos(\pi/m_{ij}) \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 2\cos(\pi/m_{ij}) & -1 \end{bmatrix}$$

$\overset{\text{Ü6}}{\Rightarrow}$ Diese Matrix hat Ordnung m_{ij},

also ist auch $o(\rho_i \rho_j) = m_{ij}$ □

Lemma 4 Definiere eine symmetrische Bilinearform $\beta: V \times V \to \mathbb{R}$ durch

$$\beta(e_i, e_j) = -\cos(\pi/m_{ij}) \quad \text{für } 1 \le i,j \le d$$

Dann ist β positiv-definit (Vor: $|W| < \infty$).

Beweis: Betrachte Homomorphismus $\varphi: W \to GL(V)$

Sei $G := \text{Bild}(\varphi) = \langle \rho_i \mid 1 \le i \le d \rangle \le GL(V)$

$|W| < \infty \Rightarrow |G| < \infty$. Sei $\langle , \rangle: V \times V \to \mathbb{R}$

Standard-Skalarprodukt, also

$$\langle e_i, e_j \rangle = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases}$$

symmetrisch, pos.-definit

Dann def. $\Phi: V \times V \to \mathbb{R}$ durch

$$\Phi(v, v') := \sum_{g \in G} \langle g(v), g(v') \rangle$$

Klar: Φ ebenfalls symmetrische Bilinearform

Sei $v \in V$. Dann $\Phi(v, v) = \sum_{g \in G} \underbrace{\langle g(v), g(v) \rangle}_{\ge 0} \ge 0$

Ist $\Phi(v, v) = 0$ so $\langle g(v), g(v) \rangle = 0$ für alle $g \in G$

$g = 1 \Rightarrow \langle v, v \rangle = 0 \Rightarrow v = 0$.

Also auch Φ positiv-definit.

Schließlich: Φ ist G-invariant, d.h.

$$\Phi(g(v), g(v')) = \sum_{h \in G} \langle h(g(v)), h(g(v')) \rangle$$

$$= \sum_{h \in G} \langle hg(v), hg(v') \rangle = \sum_{h \in G} \langle h(v), h(v') \rangle$$

↑ mit h durchläuft auch gh alle Elemente von G

$$= \Phi(v, v')$$

für alle $v, v' \in V$ und alle $g \in G$.

Damit folgt jetzt:

$$\Phi(e_i, e_j) = \Phi(\rho_i(e_i), \rho_i(e_j))$$

$$= \Phi(-e_i, e_j + 2\cos(\pi/m_{ij})\, e_i)$$

$$= -\Phi(e_i, e_j) + -2\cos(\pi/m_{ij})\, \Phi(e_i, e_i).$$

$$\Rightarrow (*) \quad \Phi(e_i, e_j) = -\cos(\pi/m_{ij})\, d_i \quad \text{wobei}$$

$$d_i := \Phi(e_i, e_i) > 0.$$

Können auch ρ_j anstelle von ρ_i benutzen.

Analoge Rechnung $\Rightarrow \Phi(e_i, e_j) = -\cos(\pi/m_{ij})\, d_j$

Also: Ist $\Phi(e_i, e_j) \neq 0$, so folgt $d_i = d_j$

Sei nun $v \in V$ beliebig; $v = \sum_{i=1}^{d} x_i e_i$ mit $x_i \in \mathbb{R}$.

Setze $v' := \sum_{i=1}^{n} \sqrt{d_i}^{-1} x_i e_i \in V$.

Dann

$$\beta(v, v) = \beta\left(\sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} x_j e_j\right) = \sum_{i,j=1}^{n} x_i x_j \beta(e_i, e_j)$$

$$= \sum_{i,j=1}^{n} x_i x_j \left(-\cos\left(\pi/m_{ij}\right)\right) \overset{(*)}{=} \sum_{i,j=1}^{n} x_i x_j\, d_i^{-1}\, \Phi(e_i, e_j)$$

$$= \sum_{i,j=1}^{n} x_i x_j\, d_i^{-1}\, \Phi(e_i, e_j) =$$

mit $\Phi(e_i, e_j) \neq 0$ ↖

$$= \sqrt{d_i}^{-1} \sqrt{d_j}^{-1}$$

wegen $d_i = d_j$

$$= \sum_{i,j=1}^{n} \left(\sqrt{d_i}^{-1} x_i\right)\left(\sqrt{d_j}^{-1} x_j\right) \Phi(e_i, e_j)$$

mit $\Phi(e_i, e_j) \neq 0$

$$= \sum_{i,j=1}^{n} \left(\sqrt{d_i}^{-1} x_i\right)\left(\sqrt{d_j}^{-1} x_j\right) \Phi(e_i, e_j)$$

$$= \Phi\left(\sum_{i=1}^{n} \sqrt{d_i}^{-1} x_i e_i, \sum_{j=1}^{n} \sqrt{d_j}^{-1} x_j e_j\right)$$

$$= \Phi(v', v') \geq 0$$

Falls "$=0$", so $v'=0$ und dann auch $v=0$

Also β positiv-definit □

Bemerkung 5 V $\mathbb{R}$-Vektorraum, $\dim V = d$ mit Basis $\{e_1, \dots, e_d\}$, $\alpha: V \times V \to \mathbb{R}$ positiv-definite symmetrische Bilinearform.

$\Rightarrow$ ex. Orthonormalbasis $\{b_1, \dots, b_d\}$ von V

(z.B. mit Gram-Schmidt-Verfahren)

Sei T Basiswechselmatrix

$A = (\alpha(e_i, e_j))_{1 \leq i,j \leq d}$ Gram-Matrix von α bzgl. $\{e_1, \dots, e_d\}$

$B = (\alpha(b_i, b_j))_{1 \leq i,j \leq d} = I_d$ wegen Orthonormalbasis.

Basiswechselformel (§1)

$\Rightarrow$ $A = T^{tr} B T = T^{tr} T$ und damit

$\det(A) = \det(T^{tr} T) = \det(T^{tr}) \det(T)$

$= \det(T)^2 > 0.$

Sei $I \subseteq \{1, \dots, d\}$ Teilmenge und

$U = \langle e_i \mid i \in I \rangle_{\mathbb{R}} \leq V$ Teilraum.

$A_I = \left(\alpha(e_i, e_j)\right)_{i,j \in I}$ Gram-Matrix von

$\alpha|_{U \times U} : U \times U \to \mathbb{R}$

Nun ist $\alpha|_{U \times U}$ immer noch positiv-definit

also mit vorherigem Argument $\det(A_I) > 0$

Mit den Bezeichnungen aus Lemma 4 gilt also:

$$|W| < \infty \Rightarrow \det\left(-\cos\left(\tfrac{\pi}{m_{ij}}\right)\right)_{i,j \in I} > 0$$

für alle Teilmengen $I \subseteq \{1, \dots, d\}$?

<u>Bemerkung 6</u> Kodiere die Matrix $M = (m_{ij})_{1 \le i,j \le d}$

in einem Graphen $\Gamma = \Gamma(W, S)$

wie folgt:

Knoten in Bijektion zu $S = \{s_1, \dots, s_d\}$.

Seien $i \neq j$. Verbinde s_i, s_j mit

einer Kante falls $m_{ij} > 2$.

Ist $m_{ij} > 3$, so schreibe diese Kante mit m_{ij}.

Beachte: $m_{ij} = 2 \Leftrightarrow (s_i s_j)^2 = 1 \Leftrightarrow s_i s_j = s_j s_i$,

d.h. s_i, s_j vertauschen.

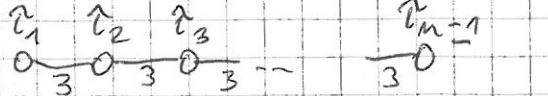
z.B.: $W = S_n$ $S = \{\tau_1, \dots, \tau_{n-1}\}$ mit $\tau_i = (i, i+1)$

$\tau_i \tau_j = \tau_j \tau_i$ falls $|i - j| > 1$.

Ausserdem $(\tau_i \tau_{i+1})^3 = 1$, also $m_{i,i+1} = 3$.

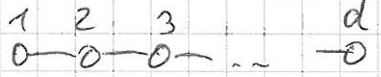
Damit $M = \begin{bmatrix} 1 & 3 & & & 2 \\ 3 & \ddots & \ddots & & \\ & \ddots & \ddots & \ddots & \\ & & \ddots & \ddots & 3 \\ 2 & & & 3 & 1 \end{bmatrix}$ $\Big\}$ $n-1$ und

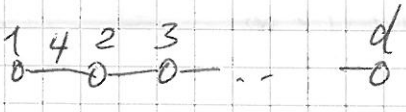
$\Gamma(S_n, S)$:

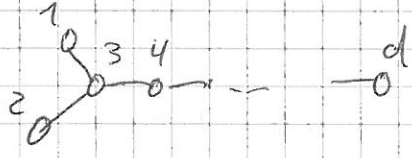


Hauptsatz Sei W endliche Gruppe mit $W = \langle S \rangle$, $s^2 = 1$ für $s \in S$, $(s \neq 1)$, so daß Bedingung (A) aus dem Austausch-Lemma gilt.

Sei $m_{ij} :=$ Ordnung von $s_i s_j$ für $1 \leq i, j \leq d$, wobei $S = \{s_1, \dots, s_d\}$. Bilde zugehörigen Graphen $\Gamma = \Gamma(W, S)$. Dann ist Γ eine Vereinigung von Graphen der folgenden Typen:

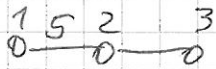
A_d 

B_d 

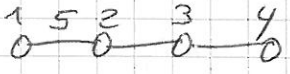
D_d 

$I_2(m)$: 

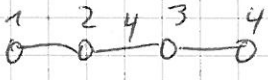
$(d = 2)$

H_3 

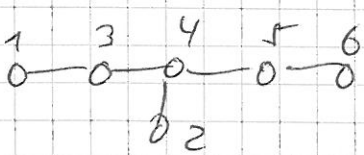
$(d = 3)$

H_4 

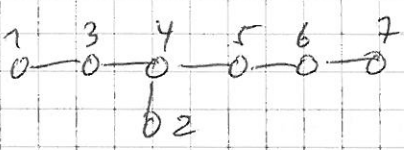
$(d = 4)$

F_4 

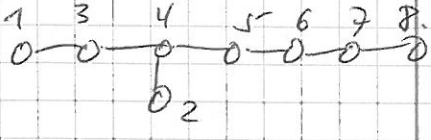
$(d = 4)$

E_6 

$(d = 6)$

E_7 

$(d = 7)$

E_8 

$(d = 8)$

Beweis: (Skizze, Details in den Übungen)

Sei $M = (m_{ij})_{1 \leq i,j \leq d}$ beliebige Matrix mit $m_{ii} = 1$ und $m_{ij} = m_{ji} \in \{2, 3, 4, \dots\}$ für $i \neq j$.

Bilde dann Graph $\Gamma = \Gamma(M)$ nach obigem Schema.

Sei V $\mathbb{R}$-Vektorraum mit Basis $\{e_1, \dots, e_d\}$ und definiere symmetrische Bilinearform $\beta : V \times V \to \mathbb{R}$ durch $\beta(e_i, e_j) = -\cos(\pi / m_{ij})$ für alle i, j.

Wollen alle M finden mit β positiv-definit.

Sei $I \subseteq \{1, \dots, d\}$ und $M' = (m'_{ij})_{i,j \in I}$ Matrix mit gleichen Bedingungen wie oben.

Wir sagen, daß M' eine Untermatrix von M ist, wenn

$m'_{ij} \leq m_{ij}$ für alle $i,j \in I$ gilt

und $\Gamma' = \Gamma(M')$ aus Γ durch Weglassen von einigen Knoten und Verringerung der Indizes an den Kanten entsteht (mehrfaches Weglassen einer Kante). Sei $V' := \langle e_i \mid i \in I \rangle_{\mathbb{R}} \leq V$ und $\beta' : V' \times V' \to \mathbb{R}$ durch M' definierte symmetrische Bilinearform.

Beh.: β positiv-definit $\Rightarrow$ β' positiv-definit

denn: indirekt: β' nicht-positiv definit

Dann existiert $0 \neq v' \in V'$ mit $\beta'(v', v') \leq 0$

Schreibe $v' = \sum_{i \in I} x_i e_i$ mit $x_i \in \mathbb{R}$ (nicht alle $= 0$),

Setze $y_i := \begin{cases} |x_i| & \text{falls } i \in I \\ 0 & \text{sonst.} \end{cases}$

und $v := \sum_{i=1}^{d} y_i e_i$ Dann ist $v \neq 0$.

und $\beta(v,v) = \sum_{i,j=1}^{d} y_i x_j \beta(e_i, e_j) = \sum_{i,j \in I} |x_i||x_j| \beta(e_i, e_j)$

$= \sum_{i \in I} |x_i|^2 - \sum_{\substack{i,j \in I \\ i \neq j}} |x_i||x_j| \cos\left(\pi / m_{ij}\right)$

$(\beta(e_i, e_i) = 1)$

Nun $i \neq j$, $i,j \in I$, $2 \leq m'_{ij} \leq m_{ij}$

$\Rightarrow \cos\left(\pi / m_{ij}\right) \geq \cos\left(\pi / m'_{ij}\right)$

Damit $\beta(v,v) \leq \sum_{i \in I} |x_i|^2 - \sum_{i,j \in I, i \neq j} |x_i||x_j| \underbrace{\cos\left(\pi / m'_{ij}\right)}_{\geq 0}$.

$$\leq \sum_{i \in I} x_i^2 - \sum_{\substack{i,j \in I \\ i \neq j}} x_i x_j \cos\left(\pi / m_{ij}\right)$$

$$= \sum_{i,j \in I} x_i x_j \beta'(e_i, e_j) = \beta'(v', v') \leq 0$$

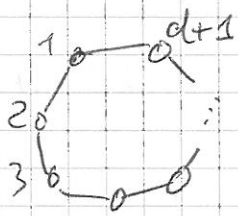
$\Rightarrow$ zu β pos. definit $\lightning$.

Jetzt gehe wie folgt vor:

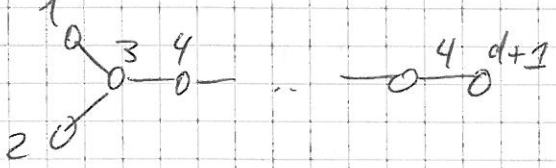
(1) Zeige, daß Gram-Matrix zu Graphen in der obigen Liste alle positive Determinante haben $\rightarrow$ (i)

(2) Zeige, daß folgende Graphen eine Gram-Matrix mit Determinante ≤ 0 haben $\rightarrow$ (ii).

$\tilde{A}_d$

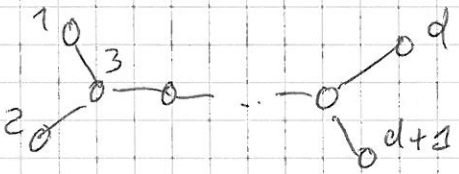


$\tilde{B}_d$

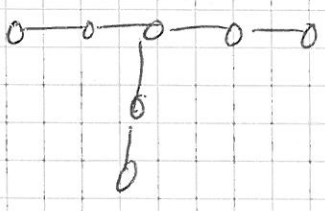


$\tilde{C}_d$

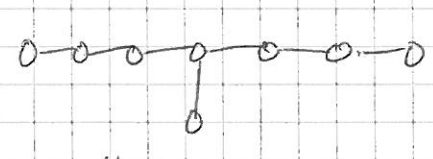
$\tilde{D}_d$



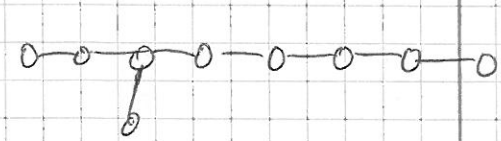
$\tilde{E}_6$



$\tilde{E}_7$

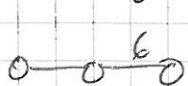


$\tilde{E}_8$

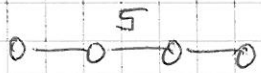


$\tilde{F}_4$

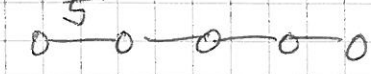
$\tilde{G}_2$



$\tilde{H}_3$



$\tilde{H}_4$



Hat Γ pos. def. zugehörige Bilinearform, so kann kein Teilgraph in der neuen Liste vorkommen.

$\rightsquigarrow$ Gehe alle möglichen Fälle durch $\rightsquigarrow$

Es bleibt nur Liste im Hauptsatz übrig $\square$

Beispielhaft einige Argumente:

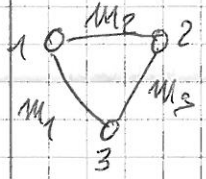
Sei zuerst $d=2$, also Graph mit genau 2 Ecken.

$\rightarrow$ OK, Vereinigung von 2 Graphen vom Typ A_1.

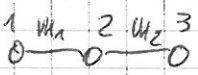
mit $m \geq 3$, möglich und erlaubt.

Sei nun $d=3$, also Graph mit genau 3 Ecken.

Können annehmen, daß Graph zusammenhängend

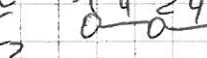


mit $m_i \geq 3$ nicht möglich, weil sonst $\tilde{A}_2$ Teilgraph.

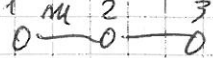
Also 

mit $m_1, m_2 \geq 3$.

Es können nicht beide $m_1, m_2 \geq 4$ sein, sonst

$\tilde{C}_2$ 

Teilgraph, also $m_1 = 3$ oder $m_2 = 3$.

Wähle Notation so daß 

mit $m \geq 3$.

Falls $m=3 \rightsquigarrow$ Graph A_3 OK

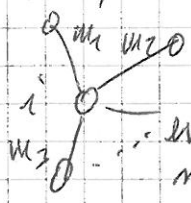
Falls $m=4 \rightsquigarrow$ Graph B_3 OK.

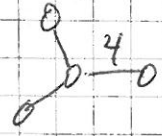
Falls $m=5 \rightsquigarrow$ Graph H_3 OK.

Falls $m \geq 6$, so $\tilde{G}_2$ Teilgraph, Widerspruch, also alle Möglichkeiten gefunden.

Schließlich $d \geq 4$.

1. Fall: Es gibt einen Verzweigungspunkt, also eine Ecke, von der mindestens 3 Kanten abgehen.



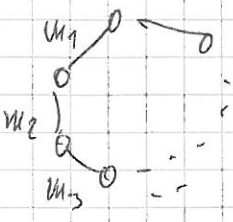
Dann müssen alle m_1, m_2, m_3 bei drei Ecke gleich 3 sein, sonst wäre $\tilde{B}_3$ 

Teilgraph.

Gehe alle Fälle durch

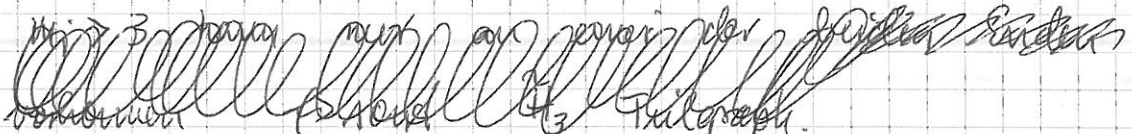
$\rightsquigarrow$ es bleiben nur D_{n+1}, E_6, E_7, E_8.

2. Fall: Es gibt keine Verzweigungspunkte.

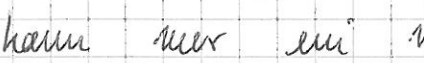
also entweder  oder 

unmöglich weil sonst $\tilde{A}_{l-1}$ Teilgraph.

Also muß Graph  sein.



Es kann nur ein $m_i > 3$ sein, denn sonst

$\tilde{C}_m$  Teilgraph.

Also nun alle m_i bis auf eines gleich 3.

Gehe Fälle durch $\rightsquigarrow$ es bleiben nur

A_l, B_l, F_4, H_4 übrig $\square$.

Zusammenfassung: Sei G Gruppe mit einem BN-Paar, $W = \langle S \rangle$ Weyl-Gruppe von G. Sei $|W| < \infty$.

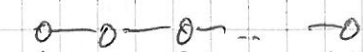
Haben gesehen: W, S erfüllt Vertauschungs-Bedingung,

also $W \cong \langle S \mid R \rangle$ mit $S = \{s_1, \dots, s_l\}$,

$R = \{ s_i^2 = 1, \ (s_i s_j)^{m_{ij}} = 1 \ (i \neq j) \}$ wobei

m_{ij} = Ordnung von $s_i s_j$ in W.

Matrix $M = (m_{ij})$ definiert Graph Γ. Dieser muß Vereinigung von Graphen in obigem Hauptsatz sein. Kennen bisher nur ein echtes Beispiel: $G = GL_n(K)$ mit $W \cong S_n$

Graph A_{n-1} 

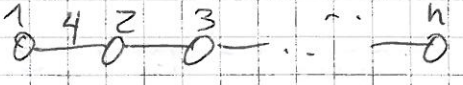
Man kann zeigen: Sei $G = Sp_{2n}(K)$ bzgl. Gram-Matrix

$$G = \begin{pmatrix} 0 & & & 1 \\ & \ddots & \iddots & \\ & -1 & & \\ -1 & & & 0 \end{pmatrix} \in M_{2n}(K)$$

Sei $B := \{$ obere Dreiecksmatrizen in $G \}$.

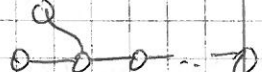
$N := \{$ monomiale Matrizen in $G \}$.

Dann bilden B, N ein BN-Paar in G mit Weyl-Gruppe, so daß zugehöriger Graph vom Typ B_n



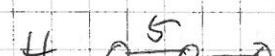
Analog Gruppen $\Omega(V, Q)$ wie in Ü 6:

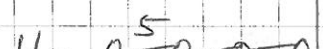
$\rightsquigarrow$ BN-Paar mit Graph D_n



oder wieder B_n.

Was ist mit den anderen Graphen:

* Es gibt keine Gruppe mit BN-Paar und Graph $I_2(m)$  , H_3 

mit $m = 5$ ~~[illegible]~~ $m = 7$ oder $m \geq 9$. H_4 

* Es gibt Gruppen mit BN-Paar zu den Graphen $I_2(6)$  , F_4, E_6, E_7, E_8.

Allgemeine Konstruktion: C. Chevalley 1955 benutzt Theorie der Lie-Algebren.

(Im diesem Zusammenhang erhält man auch die Gruppen zu Graphen A_n, B_n, D_n aufgrund einer allgemeinen Konstruktion).

Bemerkung: Sei Γ einer der Graphen im obigen Hauptsatz $\rightsquigarrow$ Bilde zugehörige Matrix $M = (m_{ij})_{1 \le i,j \le d}$. Sei V $\mathbb{R}$-Vektorraum mit Basis $\{e_1, \dots, e_d\}$. Bilde symmetrische Bilinearform $\beta: V \times V \to \mathbb{R}$ mit $\beta(e_i, e_j) = -\cos(\pi/m_{ij})$.

Man kann nun ungefähr zeigen, daß β einer positiv-definit ist, also "echtes" Skalarprodukt.

Definiere $\rho_i: V \to V$ wie zuvor:

also $\rho_i(e_j) = e_j + 2\cos\left(\frac{\pi}{m_{ij}}\right) e_i$.

Wie in Ü6 sieht man, daß dies eine "echte" Spiegelung ist

$$\begin{cases} \rho_i = w_{e_i} \\ \rho_i(e_i) = -e_i \\ \rho_i(v) = v \text{ für } v \perp e_i \end{cases}$$

$G := \langle \rho_i \mid 1 \le i \le d \rangle \le GL(V)$ Untergruppe, die von Spiegelungen erzeugt wird.

Frage: Ist stets $|G| < \infty$ (wenn man mit einem Graphen Γ wie oben startet)

Wenn ja, was genau sind die Ordnungen $|G|$ und welche Gruppen erhält man auf diese Weise?

$\rightsquigarrow$ siehe Buch von Benson-Grove.

Γ	$\lvert G \rvert$
A_n	$(n+1)!$
B_n	$2^n n!$
D_n	$2^{n-1} n!$
$I_2(m)$	$2m$

Γ	$\lvert G \rvert$
F_4	1152
E_6	51840
E_7	2903040
E_8	696729600
H_3	120
H_4	14400

Um die Fälle $F_{4(-1)}$ H_4 zu behandeln, benutzt man zweckmäßigerweise Computer-Algebra.

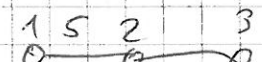
* Gegeben Graph Γ, bilde Matrix $M = (m_{ij})_{1 \le i,j \le d}$
  $\rightsquigarrow$ M ist geeigneter Input für Computer.

* Bilde $A = \left(-\cos\left(\pi/m_{ij}\right)\right)_{1 \le i,j \le d}$. Brauche:

m_{ij}	1	2	3	4	5
$\cos(\pi/m_{ij})$	-1	0	$1/2$	$\sqrt{2}/2$	$\frac{1}{4}(\sqrt{5}+1)$

"Goldener Schnitt": $\frac{\sqrt{5}+1}{2} \approx 1{,}618033\ldots$

* Betrachte $V = \mathbb{R}^d$ und stelle Matrix A_i von ρ_i bzgl. Standardbasis von $\mathbb{R}^d$ auf.

z.B. $\Gamma = H_3$ 

$d = 3$.

$$A_1 = \begin{bmatrix} -1 & \times & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} \times & 0 & 0 \\ \times & -1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -1 \end{bmatrix}$$

$\rho_1(e_1) = -e_1$
$\rho_1(e_2) = e_2 + 2\cos(\pi/m_{12})\, e_1$
$= e_2 + \underbrace{\frac{1}{2}(\sqrt{5}+1)}_{=:\alpha}\, e_1$.
$\rho_1(e_3) = e_3$

$\rho_2(e_2) = -e_2$
$\rho_2(e_1) = e_1 + 2\cos(\pi/5)\, e_2$
$\rho_2(e_3) = e_3 + \underbrace{2\cos(\pi/3)}_{=1}\, e_2$.

$\rightsquigarrow$ erhalten also explizit eine Matrixgruppe
$$G = \langle A_1, A_2, A_3 \rangle \le GL_3(\mathbb{R}).$$

* Wandle $G = \langle A_i \mid 1 \le i \le d \rangle \le GL_d(\mathbb{R})$ in eine Permutationsgruppe um, so daß wir Methoden in §1 (Schreier-Sims) anwenden können.

Sei $\underline{\Phi} := \{ g(e_i) \mid g \in G, 1 \le i \le d \} \subseteq \mathbb{R}^d$.

d.h. bilde Bahnen der Standardbasisvektoren unter G.

Dann ist $g(\underline{\Phi}) \subseteq \underline{\Phi}$ für alle $g \in G$

also operiert G auf $\underline{\Phi}$.

Weil $\underline{\Phi}$ eine Basis von $\mathbb{R}^d$ enthält, ist diese Operation treu. erhalte also injektiven Homom. $\pi : G \hookrightarrow S_{\underline{\Phi}}$.

Führe diese Zählung explizit aus:

Γ	$\lvert\underline{\Phi}\rvert$
F_4	48
E_6	72
E_7	126
E_8	240
H_3	30
H_4	120

erhalte also jeweils $|\underline{\Phi}| < \infty$ (ist a priori nicht klar!) und damit auch $|G| < \infty$!

* Bestimme dann explizit die durch jede Matrix A_i bewirkte Permutation σ_i von $\underline{\Phi}$

$\Rightarrow$ erhalte $\tilde{G} := \langle \sigma_i \mid 1 \le i \le d \rangle \le S_{\underline{\Phi}}$

bestimme Ordnung $|\tilde{G}|$ mit Schreier-Sims-Algorithmus.

Alles realisiert in CHEVIE-Projekt

siehe www.math.rwth-aachen.de/~CHEVIE

"Chevalley + Lie" seit ≈ 1990.

$\Rightarrow$ Vorführung am Computer.

§6 Darstellungen und Charaktere endlicher Gruppen

Skript: siehe Bonus-Kapitel in

M. Geck, Algebra: Gruppen, Ringe, Körper, Edition Delkhofen 2019

(5 Doppelstunden)
2½ Wochen

Zusammenfassung:

- Definition, Beispiele von Gruppen, insbesondere Permutationsdarstellung zu Operation einer Gruppe auf einer Menge.
- Äquivalenz von Darstellung, die 2 Sprechweisen: Matrixdarstellungen ↔ G-Moduln
  Direkte Summen und Produkte von G-Moduln
- Charaktere von Darstellungen, Raum der Klassenfunktionen auf einer endlichen Gruppe, Summe und Produkte von Charakteren sind wieder Charaktere.
- Irreduzible Darstellungen, Transformation auf Blockdreiecksgestalt, Lemma von Schur und Anwendungen, Schur-Relationen
- Charaktere endlicher Gruppen über $\mathbb{C}$, Frobenius-Orthogonalität von irreduziblen Charakteren, Zerlegung des regulären Charakters
- Klassen-Orthogonalität, $|\mathrm{Irr}(G)|$ = Anzahl Konjugiertenklassen von G, Charaktertafel von G, erste Beispiele ($\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, S_3)

- Klassenmultiplikationskoeffizienten, Verfahren zum Berechnen der Charaktertafel (durch Radizieren auf ein Eigenwertproblem), Beispiel A_5., Charakterformel für Klassenmultiplikationskoeffizienten.

Bemerkung: Es werden die Abschnitte 20, 21, 22, 23 des obigen Skriptes behandelt, aber ohne Satz 23.3 (ganz algebraische Zahlen)

Generell: Gruppen-Algebra, allgemeine Theorie von Moduln über Algebren, Tensorprodukte, Halbeinfachheit von Moduln über $\mathbb{C}$ werden nicht benötigt.

In den Übungen:

- symmetrische und antisymmetrische Potenz von Charakteren
- Charaktertafeln von S_4, Q_8, D_8, A_4.
- Charaktertafel eines direkten Produkts von Gruppen
- Determinante der Charaktertafel.
- Charaktertrennung von A_5 durch Zentralisator einer Involution (Spezialfall Brauer-Fowler)
- Zeilensummen in Charaktertafeln

§7 Polynomiale Invarianten endlicher Gruppen

Sei G endliche Gruppe und $\rho: G \to GL_n(\mathbb{C})$ Matrixdarstellung. Sei $R := \mathbb{C}[X_1, \dots, X_n]$ Polynomring in n Unbestimmten $X_1, \dots, X_n$. Definiere folgende Operation

$$G \times R \to R, \quad (g, f) \mapsto g \cdot f.$$

Sei $g \in G$ und $A = \rho(g) = (a_{ij})_{1 \le i,j \le n}$

Dann setze

$$g \cdot f := f\left(\sum_{i=1}^n a_{i1} X_i, \dots, \sum_{i=1}^n a_{in} X_i\right)$$

d.h. ersetze in f die Variable X_j durch

$$\sum_{i=1}^n a_{ij} X_i.$$

Dies ist eine Operation, denn: $g = 1 \Rightarrow A = I_n$.

ersetze also X_j durch X_j ✓.

Sei nun auch $h \in G$ und $B = \rho(h) = (b_{kl})_{1 \le k,l \le n}$

Dann $h \cdot f = f\left(\sum_{i=1}^n b_{i1} X_i, \dots, \sum_{i=1}^n b_{in} X_i\right)$.

und danach $g \cdot (h \cdot f)$ = ersetze jedes X_i durch $\sum_{k=1}^n a_{ki} X_k$

$$= f\left(\sum_{i=1}^n b_{i1}\left(\sum_{k=1}^n a_{ki} X_k\right), \dots, \sum_{i=1}^n b_{in}\left(\sum_{k=1}^n a_{ki} X_k\right)\right)$$

$$= f\left(\sum_{k=1}^n \underbrace{\left(\sum_{i=1}^n a_{ki} b_{i1}\right)}_{= (k,1)\text{-Koeff. von } AB} X_k, \dots, \sum_{k=1}^n \underbrace{\left(\sum_{i=1}^n a_{ki} b_{in}\right)}_{= (k,n)\text{-Koeff. von } AB} X_k\right)$$

$= \rho(gh)$ $= \rho(gh)$

$= (gh) \cdot f$ ✓. Also Operation von G auf R

Außerdem ist für festes $g \in G$ die Abbildung

$$R \to R, \quad f \mapsto g \cdot f, \quad \text{linear.}$$

Also: R G-Modul wie Sonst von §6.

Aber hier natürlich dim $R = \infty$.

Beispiel: $G = S_n$ $\quad \rho: S_n \to GL_n(\mathbb{C})$

$$\pi \mapsto A^\pi$$

wobei A^π Permutationsmatrix zu π ist, also

$$(i,j)\text{-Eintrag von } A^\pi = \begin{cases} 1 & \text{wenn } i = \pi(j) \\ 0 & \text{sonst.} \end{cases}$$

Damit:

$$\pi \cdot f = f\Big(\underbrace{\sum_{i=1}^n (A^\pi)_{i1}}_{=1 \Leftrightarrow i = \pi(1)} X_i, \dots, \underbrace{\sum_{i=1}^n (A^\pi)_{in}}_{=1 \Leftrightarrow i = \pi(n)} X_i \Big).$$

$$= f(X_{\pi(1)}, \dots, X_{\pi(n)}).$$

f heißt symmetrisches Polynom, wenn $\pi \cdot f = f$ für alle $\pi \in S_n$ gelt.

Beispiele sind die elementar-symmetrischen Polynome

$$s_1 = X_1 + \dots + X_n$$

$$s_2 = \sum_{1 \le i < j \le n} X_i X_j$$

$$\vdots$$

$$s_r = \sum_{1 \le i_1 < \dots < i_r \le n} X_{i_1} X_{i_2} \cdots X_{i_r}$$

$$\vdots$$

$$s_n = X_1 X_2 \cdots X_n.$$

Satz (Newton, Gauß 1816) Jedes symmetrische Polynom läßt sich auf eindeutige Weise als Polynom in $s_1, \dots, s_n$ schreiben.

z.B. $f = X_1^2 + X_2^2 + X_3^2 \in \mathbb{C}[X_1, X_2, X_3]$ offenbar symmetrisch.

$S_1^2 = \underbrace{X_1^2 + X_2^2 + X_3^2}_{=f} \underbrace{- 2X_1X_2 - 2X_1X_3 - 2X_2X_3}_{=-2S_2}$ also $f = S_1^2 + 2S_2$

Mehr dazu siehe Algebra-Skript Wise 2016, Satz 13.11 S. 105.

Benötigen später eine Variante davon:

Für $d \geq 1$ heißt $p_d := \sum_{i=1}^{n} X_i^d \in \mathbb{C}[X_1, \dots, X_n]$

Newton-Potenzsumme, offenbar sehr diese alle symmetrisch.

Satz (Newton 1680) Jedes symmetrische Polynom in $\mathbb{C}[X_1, \dots, X_n]$ läßt sich schreiben als Polynom in $p_1, \dots, p_n$.

Beweis: Nach vorherigem Satz müssen wir nur noch zeigen: Für $1 \leq d \leq n$ läßt sich das elementar-symmetrische Polynom S_d als Polynom in $p_1, \dots, p_n$ schreiben. Dazu benutzt man die Newton-Identitäten

$$(*) \quad p_j - S_1 p_{j-1} + \dots + (-1)^{j-1} S_{j-1} p_1 + (-1)^j j S_j = 0$$

für $1 \leq j \leq n$.

(siehe Webseite für Beweis)

und eine Rekursion; z.B.

$j=1$ $S_1 = X_1 + \dots + X_n = p_1$

$j=2$ $p_2 - S_1 p_1 + 2S_2 = 0 \Rightarrow S_2 = \frac{1}{2}(S_1 p_1 - p_2)$

$= \frac{1}{2}(p_1^2 - p_2)$

$j=3$ $p_3 - S_1 p_2 + S_2 p_1 - 3S_3 = 0$

$\Rightarrow S_3 = \frac{1}{3}[S_2 p_1 - S_1 p_2 + p_3]$

$= \frac{1}{3}[\frac{1}{2}(p_1^2 - p_2) p_1 - p_1 p_2 + p_3] = \frac{1}{6}(p_1^3 - 3p_1 p_2 + 2p_3)$

usw.

Beweis von (*) hat lange Geschichte, siehe Wikipedia Artikel zu "Newton-Identitäten".

Einfacher Induktionsbeweis:

Z. Reichstein: An inductive proof of Newton's identities.
https://www.math.ubc.ca/~reichst/nfind.html.

Zurück zum allgemeinen Fall:

Definition: Sei $\rho: G \to GL_n(\mathbb{C})$ mit zugehöriger Operation auf $R = \mathbb{C}[X_1, \dots, X_n]$ wie oben. Dann heißt $f \in R$ invariant unter G, wenn $g \cdot f = f \ \forall g \in G$ gilt.
Sei $R^G := \{f \in R \mid f \text{ invariant unter } G\}$.
Offenbar Teilraum von R; außerdem: $f, f' \in R^G \Rightarrow f \cdot f' \in R^G$ (weil Elemente in Polynome ein Homomorphismus ist).

Bemerkung: Sei $0 \neq f \in R \Rightarrow f$ = endliche Summe von Termen $a_{(i_1, \dots, i_n)} X_1^{i_1} \cdots X_n^{i_n}$ mit $i_1, \dots, i_n \geq 0$, $a_{(i_1, \dots, i_n)} \neq 0$.
$i_1 + \dots + i_n$ heißt Grad des Termes.
Dann können wir eindeutig schreiben
$f = f_0 + f_1 + \dots + f_d$ mit $d = \max\{i_1 + \dots + i_n \mid a_{(i_1, \dots, i_n)} \neq 0\}$
und f_j = Summe aller Terme vom Grad j
(oder $f_j = 0$ wenn es keine Terme vom Grad j in f gibt). Die f_j heißen "homogene Komponenten" von f. Sei $R_d := \{f \in \mathbb{C}[X_1, \dots, X_n] \mid f = 0$ oder $f \neq 0$ Summe von Termen vom Grad $d\}$.
R_d Teilraum von R für $d = 0, 1, 2, \dots$
Eindeutige Darstellung $\Rightarrow R = R_0 \oplus R_1 \oplus R_2 \oplus \dots$
Beachte: $f \in R_d$ und $g \in R_e$ mit $d, e \geq 0$

$\Rightarrow \quad f \cdot g \in R_{d+e}$.

[denn f = Summe von Termen $a_{(i_1,\dots,i_n)} X_1^{i_1} \cdots X_n^{i_n}$

mit $i_1 + \dots + i_n = d$

g = Summe von Termen $b_{(j_1,\dots,j_n)} X_1^{j_1} \cdots X_n^{j_n}$

mit $j_1 + \dots + j_n = e$.

$\Rightarrow$ $f \cdot g$ = Summe von allen möglichen Produkten obiger Terme, also $a_{(\dots)} b_{(\dots)} X_1^{i_1+j_1} \cdots X_n^{i_n+j_n}$;
diese habe alle Grad $d+e$.

Außerdem: dim $R_d < \infty$ für alle $d \geq 0$.

Genauer: dim R_d = Anzahl aller $(i_1, \dots, i_n)$
mit $i_1, \dots, i_n \geq 0$ und $i_1 + \dots + i_n = d$.

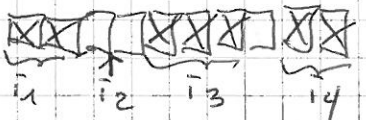
$= \binom{n+d-1}{d}$.

Beweisidee: Betrachte $n+d-1$ Boxen

[□□□ ··· □□]

Wähle d Boxen aus und kreuze sie an
$\rightsquigarrow$ dies definiert $i_1, \dots, i_n$

z.B. $d=7$, $n=4$



10 Boxen.

$i_1 = 2, i_2 = 0, i_3 = 3, i_4 = 2$

Auf diese Weise erhalte Bijektion zwischen angewandten Listen von Boxen und Vektoren $(i_1, \dots, i_n)$ wie gewünscht, also $\binom{n+d-1}{n}$ Möglichkeiten].

Lemma: Für jedes $d \geq 0$ setze $R_d^G := R_d \cap R^G$.
Dann ist R_d^G Teilraum von R^G und es gilt $R^G = R_0^G \oplus R_1^G \oplus R_2^G \oplus \dots$

Beweis: Weil Summe $R = R_0 \oplus R_1 \oplus R_2 \oplus \dots$ direkt, müssen wir nur noch zeigen:

$$R^G = R_0^G + R_1^G + R_2^G + \dots$$

"$\supseteq$" klar nach Definition von R_d^G.

"$\subseteq$" Sei $0 \neq f \in R^G$ und schreibe $f = f_0 + f_1 + \dots + f_d$ mit homogenen Komponenten $f_0, \dots, f_d$.

Sei $g \in G$ und $A = \rho(g) = (a_{ij})$.

$$g \cdot X_{i_1} \cdots X_{i_n} = \underbrace{\Big(\underbrace{\sum_{i=1}^{n} a_{i i_1} X_i}_{\text{homogen vom Grad 1}}\Big) \cdots \Big(\underbrace{\sum_{i=1}^{n} a_{i i_n} X_i}_{\text{homogen vom Grad 1}}\Big)}_{\text{homogen vom Grad } i_1 + \dots + i_n}$$

$$\underbrace{\qquad\qquad}_{\text{homogen vom Grad } i_1} \qquad \underbrace{\qquad\qquad}_{\text{homogen vom Grad } i_n}$$

Also folgt: $g \cdot f_j \in R_j$ für $0 \leq j \leq d$.

Also $f = g \cdot f = \underbrace{g \cdot f_0}_{\in R_0} + \underbrace{g \cdot f_1}_{\in R_1} + \dots + \underbrace{g \cdot f_d}_{\in R_d}$.

Eindeutigkeit der Darstellung $\Rightarrow g \cdot f_j = f_j$

also $f_j \in R_j^G$ für $0 \leq j \leq d$.

und damit $R^G \subseteq R_0^G + R_1^G + \dots$ □

Wenn man also invariante Polynome unter G bestimmen möchte, genügt es homogene Polynome zu betrachten.

Wie kann man systematisch invariante Polynome finden?

Definition: Sei $\rho: G \to GL_n(\mathbb{C})$ mit zug. Operation auf $R = \mathbb{C}[X_1, \dots, X_n]$ wie oben.

Dann definiere Abbildung $*: R \to R$, $f \mapsto f^*$

durch $f^* := \frac{1}{|G|} \sum_{g \in G} g \cdot f$ "Reynolds-Operator"

Weil R ein G-Modul ist, ist $*$ linear

Außerdem:

- $f^* \in R^G$, denn sei $x \in G$. Dann

$$x \cdot f^* = \frac{1}{|G|} \sum_{g \in G} x \cdot (g \cdot f) = \frac{1}{|G|} \sum_{g \in G} (xg) \cdot f$$

$$= \frac{1}{|G|} \sum_{y \in G} y \cdot f = f^*.$$

↑ mit g durchläuft auch xg alle Elemente von G genau einmal

- Ist $f \in R^G$, so $f^* = f$, denn

$$f^* = \frac{1}{|G|} \sum_{g \in G} \underbrace{g \cdot f}_{= f} = \frac{1}{|G|} \sum_{g \in G} f = f \quad \checkmark$$

Beispiel: $G = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle \leq GL_2(\mathbb{C})$.

[also Darst. gegeben durch Inklusion $G \hookrightarrow GL_2(\mathbb{C})$]

Sei $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \Rightarrow A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ und $A^4 = I_2$.

also G zyklisch Ordnung 4.

Um zu testen, ob $f \in R = \mathbb{C}[X, Y]$ invariant unter ganz G ist, genügt es zu testen ob

$A \cdot f = f$ gilt.

[oder allgemeiner: Es genügt, Erzeugendensystem von G zu betrachten.]

$$\Rightarrow f^* = \frac{1}{4}\left(f + f(Y, -X) + f(-X, -Y) + f(-Y, X) \right)$$

z.B. $X^* = \frac{1}{4}(X + Y + (-X) + (-Y)) = 0$.

ebenso $Y^* = 0$.

$(X^2)^* = \frac{1}{4}[X^2 + Y^2 + (-X)^2 + (-Y)^2] = \frac{1}{2}(X^2+Y^2)$

$(XY)^* = \frac{1}{4}[XY + Y(-X) + (-X)(-Y) + (-Y)X] = 0$

$(X^3Y)^* = \dots = \frac{1}{2}(X^3Y - XY^3)$

$(X^2Y^2)^* = \dots = X^2Y^2$ usw.

haben also hier gefunden:

(X^2+Y^2), $(X^3Y - XY^3)$, $X^2Y^2 \in \mathbb{C}[X,Y]^G$.

Wie viel weiter müssen wir noch gehen? Der folgende Satz zeigt, daß wir bereits im Wesentlichen alle Invarianten gefunden haben ▽.

Satz (E. Noether 1915) Jedes $f \in R^G$ läßt sich schreiben als Polynom in den endlich vielen Invarianten $(X_1^{i_1} \cdots X_n^{i_n})^*$ mit $i_1, \dots, i_n \geq 0$ und $i_1 + \dots + i_n \leq |G|$.

"Endliche Erzeugbarkeit der Invarianten unter G"

Beweis: Sei o.B.d.A. $f \in \mathbb{C}[X_1, \dots, X_n]^G$. Schreibe

$f = \sum_{\text{endl.}} a_{(i_1,\dots,i_n)} X_1^{i_1} \cdots X_n^{i_n}$. Dann folgt mit Reynolds-Operator

$f = f^* = \sum_{\text{endl.}} a_{(i_1,\dots,i_n)} (X_1^{i_1} \cdots X_n^{i_n})^*$.

Also ist f bereits Linearkombination von Termen der Form $(X_1^{j_1} \cdots X_n^{j_n})^*$ aber mit $j_1, \dots, j_n \geq 0$ beliebig. Müssen also noch zeigen, daß wir diese als Polynom in $(X_1^{i_1} \cdots X_n^{i_n})^*$ mit $i_1 + \dots + i_n \leq |G|$ schreiben können.

Vereinfachte Notation: $\mathbb{N}_0^n = \{\alpha = (i_1, \dots, i_n) \mid i_1, \dots, i_n \in \mathbb{N}_0\}$

Für $\alpha = (i_1, \dots, i_n) \in \mathbb{N}_0^n$ schreibe

$X^\alpha := X_1^{i_1} \cdots X_n^{i_n}$ und $|\alpha| := i_1 + \dots + i_n$.

Sei nun $d \geq 0$ fest und betrachte alle $(X^\beta)^*$ mit $\beta = (j_1, \dots, j_n) \in \mathbb{N}_0^n$ und $|\beta| = d$.

Zur Erinnerung:

$$(X^\beta)^* = \frac{1}{|G|} \sum_{g \in G} g \cdot X^\beta \overset{\text{Def. der Operation}}{=} \frac{1}{|G|} \sum_{g \in G} (g \cdot X_1)^{j_1} \cdots (g \cdot X_n)^{j_n}$$

Def. der Operation

$$g \cdot X_j = \sum_{i=1}^n q_{ij} X_i \quad \text{wobei} \quad \rho(g) = (q_{ij}).$$

Vergrößern nun R mit n neuen Variablen $Y_1, \dots, Y_n$, also jetzt $R = \mathbb{C}[X_1, \dots, X_n] \subseteq \mathbb{C}[X_1, \dots, X_n, Y_1, \dots, Y_n]$.

Setze $S_d := \frac{1}{|G|} \sum_{g \in G} \left(Y_1 \cdot (g \cdot X_1) + \dots + Y_n \cdot (g \cdot X_n) \right)^d$

Dann werden wir S_d auf 2 Weisen ausrechnen.

zuerst $S_d = \frac{1}{|G|} \sum_{g \in G} \sum_{\substack{j_1, \dots, j_n \geq 0 \\ j_1 + \dots + j_n = d}} \frac{d!}{j_1! j_2! \cdots j_n!} (Y_1 (g \cdot X_1))^{j_1} \cdots (Y_n (g \cdot X_n))^{j_n}$

Multinomialformel

$$= \frac{1}{|G|} \sum_{g \in G} \sum_{j_1 + \dots + j_n = d} \frac{d!}{j_1! \cdots j_n!} \underbrace{(g \cdot X_1)^{j_1} \cdots (g \cdot X_n)^{j_n}}_{= g \cdot (X_1^{j_1} \cdots X_n^{j_n}) = g \cdot X^\beta \text{ mit } \beta = (j_1, \dots, j_n)} Y_1^{j_1} \cdots Y_n^{j_n}$$

Setze auch

$\beta! := j_1! \cdots j_n!$

$Y^\beta = Y_1^{j_1} \cdots Y_n^{j_n}$

$$= \frac{1}{|G|} \sum_{g \in G} \sum_{\beta \in \mathbb{N}_0^n} \frac{d!}{\beta!} (g \cdot X^\beta) \cdot Y^\beta$$

$$= \sum_{\substack{\beta \in \mathbb{N}_0^n \\ |\beta| = d}} \frac{d!}{\beta!} \left(\frac{1}{|G|} \sum_{g \in G} g \cdot X^\beta \right) \cdot Y^\beta$$

$$= \sum_{\substack{\beta \in \mathbb{N}_0^n \\ |\beta| = d}} \underbrace{\frac{d!}{\beta!}}_{\neq 0} (X^\beta)^* \cdot Y^\beta$$

Erhalten also $(Y^\beta)^*$ als Koeffizient von Y^β, wenn wir S_d wie oben ausmultiplizieren.

Andererseits setze $u_g := Y_1 \cdot (g \cdot X_1) + \dots + Y_n \cdot (g \cdot X_n)$

für alle $g \in G$.

Dann $S_d = \frac{1}{|G|} \sum_{g \in G} u_g^d$

Betrachte jetzt auch noch Polynomring

$$\mathbb{C}[u_g \mid g \in G]$$

↑ Unbestimmte indiziert durch Elemente von G.

Dann $S_d = \frac{1}{|G|} \pi_d\left((u_g)_{g \in G}\right)$ wobei

$$\pi_d = \sum_{g \in G} u_g^d \in \mathbb{C}[u_g \mid g \in G]$$

Newton-Potenzsumme.

Haben oben gesehen: Jedes symmetrische Polynom in $\mathbb{C}[u_g \mid g \in G]$ lässt sich als Polynom in den Potenzsummen $\pi_1, \dots, \pi_{|G|} \in \mathbb{C}[u_g \mid g \in G]$ schreiben. Also

π_d ~~d~~ $= F(\pi_1, \dots, \pi_{|G|})$ mit einem Polynom F in $|G|$ Unbestimmten.

Einsetzen der u_g $(g \in G)$ ergibt

$$S_d = \frac{1}{|G|} \pi_d\left((u_g)_{g \in G}\right) = F\left(\pi_1((u_g)_{g \in G}), \dots, \pi_{|G|}((u_g)_{g \in G})\right)$$

Haben aber oben gesehen: Für beliebiges $k \geq 1$

sind S_k eine Linearkombination von
$(X^\alpha)^* Y^\alpha$ mit $\alpha \in \mathbb{N}_0^n$ und $|\alpha| = k$.

Also folgt nun:

S_d = Linearkombination von Summen und Produkten (Polynom $\neq 1$) von Termen der Form
$(X^\alpha)^* Y^\alpha$ mit $|\alpha| = k$, $1 \leq k \leq |G|$

Vergleiche Koeffizienten von Y^β, $|\beta| = d$
$\Rightarrow (X^\beta)^*$ = Polynom in $(X^\alpha)^*$ mit $\alpha \in \mathbb{N}_0^n$
und $1 \leq |\alpha| \leq |G|$. □.

Fortsetzung des obigen Beispiels mit
$G = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle \leq Gl_2(\mathbb{C})$ zyklisch Ordnung 4.

Nach obigem Satz müssen wir "nur"
$(X^i Y^j)^*$ bestimmen für $i+j \leq 4$, um
Erzeuger für ganz $\mathbb{C}[X,Y]^G$ zu finden.

X^iY^j	$(X^iY^j)^*$
X	0
Y	0
X^2	$\frac{1}{2}(X^2+Y^2)$ (s.o.)
XY	0 (s.o.)
Y^2	$\frac{1}{2}(X^2+Y^2)$
X^3	0
X^2Y	0

X^iY^j	$(X^iY^j)^*$
XY^2	0
Y^3	0
X^4	$\frac{1}{2}(X^4+Y^4)$
X^3Y	$\frac{1}{2}(X^3Y - XY^3)$ (s.o.)
X^2Y^2	X^2Y^2 (s.o.)
XY^3	$-\frac{1}{2}(X^3Y - XY^3)$
Y^4	$\frac{1}{2}(X^4+Y^4)$

$\Rightarrow \mathbb{C}[X,Y]^G$ erzeugt von X^2+Y^2, X^4+Y^4, $X^3Y - XY^3$
und X^2Y^2. Aber X^4+Y^4 brauchen wir nicht,
weil $X^4+Y^4 = (X^2+Y^2)^2 - 2X^2Y^2$.

also erhalten wir $\mathbb{C}[X,Y]^G = \mathbb{C}[X^2+Y^2,\ X^3Y-XY^3,\ X^2Y^2]$.

Weiteres Beispiel: $G = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \leq GL_2(\mathbb{C})$

jeweils Ordnung 2

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$\Rightarrow$ Produkt hat Ordnung 4, also G Diedergruppe der Ordnung 8.

Gruppe des vorherigen Beispiel ist Untergruppe von G, also $\mathbb{C}[X,Y]^G \subset \mathbb{C}[X^2+Y^2,\ X^3Y-XY^3,\ X^2Y^2]$.

↑ nicht invariant unter $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Zeigen Sie, daß $\mathbb{C}[X,Y]^G = \mathbb{C}[X^2+Y^2,\ X^2Y^2]$ gilt.

Definition: Sei $\rho: G \to GL_n(\mathbb{C})$ mit zugehöriger Operation auf $R = \mathbb{C}[X_1, \dots, X_n]$ wie oben.

Seien $f_1, \dots, f_m \in R$ so daß

$$R^G = \mathbb{C}[f_1, \dots, f_m] \text{ gilt}$$
$$= \{h(f_1, \dots, f_m) \mid h \in \mathbb{C}[Y_1, \dots, Y_m]\}$$

Sei $F := (f_1, \dots, f_m)$ und definiere

$$I_F := \{h \in \mathbb{C}[Y_1, \dots, Y_m] \mid h(f_1, \dots, f_m) = 0\}.$$

Dies ist ein Ideal in $\mathbb{C}[Y_1, \dots, Y_m]$ und heißt "Ideal der Relationen für F" oder Syzygien-Ideal

Beispiele (a) $G = S_n$ und $\rho: S_n \to GL_n(\mathbb{C})$ Permutationsdarstellung $\Rightarrow$

$R^{S_n} = \mathbb{C}[s_1, \dots, s_n]$ wobei $s_1, \dots, s_n$ die elementar-symmetrischen Polynome sind

Eindeutigkeit mit Hauptsatz über symmetrische Polynome $\Rightarrow$ $I_F = \{0\}$ für $F = (s_1, \dots, s_n)$.

(denn wäre $0 \neq h \in I_F$, so hätte das Polynom $0 \in \mathbb{C}[s_1, \dots, s_n]^{S_n}$ zwei Darstellungen als Polynom in $s_1, \dots, s_n$, nämlich einmal mit dem 0-Polynom und einmal mit $h \neq 0$).

(b) Sei $G = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle \leq GL_2(\mathbb{C})$ zyklisch Ordnung 4

mit $\mathbb{C}[x,y]^G = \mathbb{C}[\underbrace{x^2+y^2}_{=:f_1}, \underbrace{x^3y - xy^3}_{=:f_2}, \underbrace{x^2y^2}_{=:f_3}]$

Probieren ... $\Rightarrow$

$$\underbrace{(x^2+y^2)}_{=f_1}{}^2 \underbrace{x^2y^2}_{=f_3} = \underbrace{(x^3y - xy^3)}_{=f_2}{}^2 + 4\underbrace{(x^2y^2)}_{=f_3}{}^2$$

also $f_1^2 f_3 = f_2^2 + 4 f_3$

$$f_1^2 f_3 - f_2^2 - 4 f_3 = 0$$

d.h. $h := u^2 w - v^2 - 4w \in I_F \subseteq \mathbb{C}[u,v,w]$.

Wie kann man I_F allgemein bestimmen?

(c) Sei $G = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle \leq GL_2(\mathbb{C})$

Diedergruppe der Ordnung 8.

$\mathbb{C}[x,y]^G = \mathbb{C}[\underbrace{x^2+y^2}_{=:f_1}, \underbrace{x^2y^2}_{=:f_2}]$ Hier kann man auch zeigen $I_{(f_1,f_2)} = \{0\}$.

Satz (Verfahren zur Bestimmung von I_F).

Sei $F = (f_1, \dots, f_m)$ wie oben, also

$$\mathbb{C}[x_1, \dots, x_n]^G = \mathbb{C}[f_1, \dots, f_m]$$

Betrachte Polynomring $\mathbb{C}[X_1, \dots, X_n, Y_1, \dots, Y_m]$ und darin das Ideal

$$J_F := \langle f_1 - Y_1, \dots, f_m - Y_m \rangle \trianglelefteq \mathbb{C}[X_1, \dots, X_n, Y_1, \dots, Y_m]$$

Dann gelt $I_F = J_F \cap \mathbb{C}[Y_1, \dots, Y_m]$

und einen solchen Durchschnitt kann man mit Hilfe von Groebner-Basen explizit berechnen (also Eliminieren bestimmen), siehe GAGA A

§1. The Elimination Theorem.

Beweis: Zuerst zeigen wir, sei $g \in \mathbb{C}[X_1, \dots, X_n, Y_1, \dots, Y_m]$ beliebig. Dann gelt:

$$(*) \quad g \in J_F \iff g(X_1, \dots, X_n, f_1, \dots, f_m) = 0$$

in $\mathbb{C}[X_1, \dots, X_n]$

setze $f_1, \dots, f_m$ für $Y_1, \dots, Y_m$ ein.

Dann: "$\Rightarrow$" sei $g \in J_F \Rightarrow$

$g = g_1 (f_1 - Y_1) + \dots + g_m (f_m - Y_m)$ mit

$g_i \in \mathbb{C}[X_1, \dots, X_n, Y_1, \dots, Y_m]$

Ersetze $Y_j \to f_j$ für $1 \le j \le m$.

$\Rightarrow g(X_1, \dots, X_n, f_1, \dots, f_m) = g_1(\dots) \underbrace{(f_1 - f_1)}_{=0} + \dots + g_m(\dots) \underbrace{(f_m - f_m)}_{=0}$

$= 0$ ✓

"$\Leftarrow$" Schreibe jedes Y_j in g als $Y_j - (f_j - Y_j)$ und multipliziere aus $\overset{(S.u.)}{\Longrightarrow}$

$$g = g(X_1, \dots, X_n, f_1, \dots, f_m) + B_1 (f_1 - Y_1) + \dots + B_m (f_m - Y_m)$$

mit $B_1, \dots, B_m \in \mathbb{C}[X_1, \dots, X_n, Y_1, \dots, Y_m]$

Ist also $g(X_1, \dots, X_n, f_1, \dots, f_m) = 0$, so folgt

$g = B_1 (f_1 - Y_1) + \dots + B_m \cdot (f_m - Y_m) \in J_F$. ✓

Sei nun $h \in \mathbb{C}[Y_1, \dots, Y_m]$.
Ist $h \in I_F$, so $h(f_1, \dots, f_m) = 0$, also
h erfüllt mehr Spalte von $(*)$, $\Rightarrow h \in J_F \cap \mathbb{C}[Y_1, \dots, Y_m]$.
Ist $h \in J_F \cap \mathbb{C}[Y_1, \dots, Y_m]$, so erfüllt h mehr Spalte von $(*)$, $\Rightarrow h(X_1, \dots, X_n, f_1, \dots, f_m) = 0 \Rightarrow h \in I_F$
$h(f_1, \dots, f_m)$ ″ □.

[Beachte: $Y_1^{i_1} \cdots Y_m^{i_m} = \underbrace{(f_1 - (f_1 - Y_1))^{i_1}}_{\sum_{j_1=0}^{i_1} \binom{i_1}{j_1} f_1^{j_1} (f_1 - Y_1)^{i_1 - j_1}} \cdots (f_m - (f_m - Y_m))^{i_m}$

$= f_1^{i_1} + \sum_{j_1=0}^{i_1-1} \binom{i_1}{j_1} f_1^{j_1} (f_1 - Y_1)^{\underbrace{i_1 - j_1}_{>0}}$

$= f_1^{i_1} + h_1 (f_1 - Y_1)$ mit

analog für die $h_1 \in \mathbb{C}[X_1, \dots, X_n, Y_1, \dots, Y_m]$.
anderen Terme im obigen Produkt, also.

$Y_1^{i_1} \cdots Y_m^{i_m} = (f_1^{i_1} + h_1 (f_1 - Y_1)) \cdots (f_m^{i_m} + h_m (f_m - Y_m))$.

$= f_1^{i_1} \cdots f_m^{i_m} + r_1 (f_1 - Y_1) + \cdots + r_m (f_m - Y_m)$

mit $r_j \in \mathbb{C}[X_1, \dots, X_n, Y_1, \dots, Y_m]$

$\Rightarrow$ Beh. □]

Definition Sei $\mathbb{C}[X_1, \dots, X_n]^G = \mathbb{C}[f_1, \dots, f_m]$
und $I_F \trianglelefteq \mathbb{C}[Y_1, \dots, Y_m]$ zugehöriges Syzygienideal.
Dann definiert

$$V_F := \left\{ \begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix} \in \mathbb{C}^m \;\middle|\; h(v_1, \dots, v_m) = 0 \text{ für alle } h \in I_F \right\}$$

affine algebraische Teilmenge im $\mathbb{C}^m$.

Beachte: $\varphi : \mathbb{C}[Y_1, \dots, Y_m] \longrightarrow \mathbb{C}[X_1, \dots, X_n]^G$
$h \longmapsto h(f_1, \dots, f_m)$

surjektiver Algebra-Homomorphismus mit
$\ker(\varphi) = I_F$ (nach Definition).
Also $\mathbb{C}[Y_1, \dots, Y_m]/I_F \cong \mathbb{C}[X_1, \dots, X_n]^G$
(Homomorphiesatz).

$\mathbb{C}[X_1, \dots, X_n]^G \subseteq \mathbb{C}[X_1, \dots, X_n]$ ← Integritätsring
also $\mathbb{C}[X_1, \dots, X_n]^G$ Integritätsring und
damit $I_F \trianglelefteq \mathbb{C}[Y_1, \dots, Y_m]$ Primideal.

[illegible]: $\Rightarrow$ $I_F = \sqrt{I_F}$ Radikalideal
(GAGA A 146. Definition)

Daraus folgt (GAGA A, 155. Proposition):
$V_F \subseteq \mathbb{C}^m$ ist eine irreduzible affine Varietät.

Bemerkung (ohne Beweis, siehe dazu das Buch von Cox, Little, O'Shea, Chap. 7, §4).
G operiert auf $\mathbb{C}^n$ durch $G \times \mathbb{C}^n \to \mathbb{C}^n$
$(g, v) \mapsto \rho(g)\, v$ ($\rho(g)$: Matrix × Spaltenvektor)
Sei $\mathbb{C}^n/G$ die Menge der Bahnen unter dieser Operation:
Betrachte die Abbildung $F: \mathbb{C}^n \to \mathbb{C}^m$,
$\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} \mapsto \begin{pmatrix} f_1(v_1, \dots, v_n) \\ \vdots \\ f_m(v_1, \dots, v_n) \end{pmatrix}$
Mit $I_F = J_F \cap \mathbb{C}[Y_1, \dots, Y_m]$ sieht man leicht:
$F(\mathbb{C}^n) \subseteq V_F$ und dann kann man zeigen,
daß sogar "$=$" gilt. Außerdem F konstant auf Bahnen von G $\Rightarrow$ induzierte Abbildung
$\tilde{F}: \mathbb{C}^n/G \to V_F$ die bijektiv ist.

Haben also Menge der Bahnen als irreduzible affine Varietät realisiert.

Schließlich: Was passiert im Extremfall, wo $I_F = \{0\}$ ist? Haben 2 Beispiele gesehen:

$G = S_n$ mit Permutationsdarstellung $\rho: G \to GL_n(\mathbb{C})$

G = Diedergruppe der Ordnung $8 \leq GL_2(\mathbb{C})$

Definition Eine Matrix $A \in GL_n(\mathbb{C})$ heißt Pseudo-Spiegelung, wenn A ähnlich ist zu einer Diagonalmatrix der Form

$$\begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \\ & & & \lambda \end{bmatrix}$$

wobei $0 \neq \lambda \in \mathbb{C}$ eine Einheitswurzel $\neq 1$ ist

Spiegelung = Pseudo-Spiegelung mit $\lambda = -1$

Sei $\rho: G \to GL_n(\mathbb{C})$ mit zugehöriger Operation auf $R = \mathbb{C}[X_1, \dots, X_n]$. Nehmen an, daß ρ injektiv ist, d.h. wir können auch gleich $G \leq GL_n(\mathbb{C})$ annehmen. Dann heißt G eine Pseudo-Spiegelungsgruppe, wenn G von Pseudo-Spiegelungen erzeugt wird (und $|G| < \infty$ wie üblich).

Beispiel: Die Gruppen W, die als endliche Weyl-Gruppen von Gruppen mit einem BN-Paar vorkommen, sind von Spiegelungen in $GL_n(\mathbb{R}) \leq GL_n(\mathbb{C})$ erzeugt (siehe §5) und damit insbesondere auch Pseudo-Spiegelungsgruppen.

Hauptsatz (Shephard-Todd-Chevalley 1954/55)

Sei $\mathbb{C}[X_1, \dots, X_n]^G = \mathbb{C}[f_1, \dots, f_n]$ und $F = (f_1, \dots, f_n)$. Dann gilt:

$I_F = \{0\} \iff$ G endliche Pseudo-Spiegelungsgruppe.

Insbesondere gilt also $I_F = \{0\}$ für alle $G = W_i$, die als Weyl-Gruppe einer Gruppe mit einem BN-Paar vorkommen.

Beweis: Siehe §2.4 im Buch von Sturmfels.

Nächstes Semester: Master-Vorlesung "Lie algebras and Chevalley groups"

Insbesondere: zu jedem Diagramm in Klassifikation der endlichen Coxetergruppen (außer H_3, H_4, $I_2(m)$ mit $m = 5$, $m \geq 7$) wird explizit zugehörige Gruppe und BN-Paar konstruiert, z.B. $E_8(K)$ für beliebigen Körper K.