Einfache Gruppen sind kompliziert

Die Klassifizierung der endlichen einfachen Gruppen

Stephan Wagner

27. November 2002

1 Einführung und Geschichte

Die Klassifizierung der endlichen einfachen Gruppen war ein mathematischer Kraftakt, der unzählige Gruppentheoretiker jahrzehntelang beschäftigte und erst in den Achzigerjahren fertiggestellt wurde. Der vollständige Beweis des Klassifizierungssatzes besteht aus rund 100 Einzelarbeiten, die in drei Jahrzehnten verfasst wurden und zusammen mehrere Tausend Seiten ausmachen. Wie viele mathematische Probleme ist auch dieses leicht zu formulieren, aber schwierig zu lösen.

Will man die Struktur endlicher Gruppen studieren, so muss man zunächst einen speziellen Typ betrachten, jenen der *einfachen Gruppen*. Dieser ist wie folgt definiert:

Definition 1 Eine Gruppe heißt *einfach*, wenn sie keinen nichttrivialen Normalteiler besitzt (also keinen außer $\{e\}$ und der Gruppe selbst).

Die einfachen endlichen Gruppen bilden quasi die Bausteine aller endlicher Gruppen. So zeigt sich, dass jede endliche Gruppe G eine endliche einfache Faktorgruppe ($\neq G/G \simeq \{e\}$) besitzen muss:

Beweis: Wenn eine endliche Gruppe G keinen nichttrivialen Normalteiler besitzt, ist $G/e \simeq G$ einfach. Ansonsten gibt es einen maximalen Normalteiler $N \trianglelefteq G$, $N \neq G$, also einen Normalteiler N, für den $(K \trianglelefteq G \wedge N \subseteq K) \Rightarrow (K = N \vee K = G)$ gilt. Nach dem 3. Isomorphiesatz ist dies genau dann der Fall, wenn G/N einfach ist.

□

Mit Hilfe dieser Feststellung definiert man sogenannte *Kompositionsreihen*:

Definition 2 Sei G eine Gruppe. Eine *Kompositionsreihe* ist eine Folge $G_0 = G, G_1, \ldots, G_n = \{e\}$ derart, dass $G_{i+1} \subsetneqq G_i$, $G_{i+1} \trianglelefteq G_i$ und G_i/G_{i+1} für alle i einfach ist (diese Faktorgruppen heißen *Kompositionsfaktoren*).

Der Satz von Jordan-Hölder besagt nun, dass je zwei Kompositionsreihen äquivalent sind, d.h. sie sind gleich lang, und die Kompositionsfaktoren sind bis auf Reihenfolge und Isomorphie dieselben.

Für die stukturelle Untersuchung von endlichen Gruppen sind Kompositionsreihen von entscheidender Bedeutung. So erklärt sich, weshalb man daran interessiert ist, alle endlichen einfachen Gruppen zu finden. Das Resultat liest sich folgendermaßen:

Satz 1 (Klassifizierung der endlichen einfachen Gruppen) *Eine endliche einfache Gruppe ist entweder*

- *eine zyklische Gruppe, deren Ordnung* 1 *oder eine Primzahl ist oder*
- *eine alternierende Gruppe* A_n *für* $n > 4$ *oder*
- *eine Gruppe vom Lie-Typ* (*Näheres dazu später*) *oder*
- *eine der 26 sporadischen Gruppen*

Besondere Schwierigkeiten bei der Klassifizierung bereiteten hierbei einige einfache Gruppen, die in keines der Muster passten und daher unter dem Begriff „sporadische Gruppen“ zusammengefasst wurden. Die letzte sporadische Gruppe, die entdeckt wurde, wird wegen ihrer ungeheuren Größe gar das „Monster“ genannt.

Einige Ergebnisse können mit erstaunlicher Leichtigkeit erzielt werden, andere benötigen großen Aufwand, wie etwa der Beweis von Thompson und Feit, dass jede nichtzyklische endliche einfache Gruppe gerade Ordnung hat, der eine ganze Ausgabe (250 Seiten) von *The Pacific Journal of Mathematics* umfasst (Band 13, S. 775-1029, 1963).

2 Die Klasse der zyklischen einfachen Gruppen

Proposition 2 Sei G eine endliche einfache Abelsche Gruppe. Dann ist G zyklisch, und $|G|$ ist 1 oder eine Primzahl.

Beweis: Es sei G nicht zyklisch. Dann muss $|G| > 2$ sein, und daher gibt es ein Element $g \in G$ mit $|G| > |g| > 1$. Damit ist jedoch $\langle g \rangle$ ein nichttrivialer Normalteiler (weil jede Untergruppe einer Abelschen Gruppe bereits Normalteiler ist).
Folglich muss G zyklisch sein. Ist $|G|$ weder Primzahl noch 1, gibt es einen Teiler d von $|G|$ mit $|G| > d > 1$ sowie eine Untergruppe von G mit der Ordnung d. Diese ist dann ein nichttrivialer Normalteiler.

□

Umgekehrt muss offensichtlich jede zyklische Gruppe von Primzahlordnung einfach sein, denn nach dem Satz von Lagrange muss die Ordnung eines potenziellen Normalteilers entweder 1 oder die Ordnung der ganzen Gruppe sein. Diese einfache Proposition beschränkt unsere Suche also auf nichtkommutative Gruppen.

3 Die alternierenden Gruppen

Satz 3 *Die alternierenden Gruppen A_n sind für $n > 4$ einfach.*

Beweis: Zunächst zeigt man, dass A_n von den 3-Zyklen erzeugt wird. Dies folgt aus der Tatsache, dass jedes Element von A_n als Produkt einer geraden Zahl von Transpositionen geschrieben werden kann und das Produkt zweier Transpositionen sich aus 3-Zyklen in der folgenden Weise ergibt:

$$(ab)(cd) = (abc)(bcd) \text{ und } (ab)(bc) = (abc)$$

Nun folgt der Nachweis der Tatsache, dass ein Normalteiler N von A_n, der einen 3-Zyklus $\sigma = (abc)$ enthält, bereits alle 3-Zyklen enthält. Es ist bekannt, dass je zwei 3-Zyklen in S_n konjugiert sind. Sei also π ein beliebiger 3-Zyklus. Es gibt dann eine Permutation $\rho \in S_n$, die $\pi = \rho\sigma\rho^{-1}$ erfüllt. Ist $\rho \in A_n$, ist bereits alles erledigt. Andernfalls ist $\sigma^{-1} = (cba) = (ab)(abc)(ab)$ auch sicher ein Element von N, und es gilt $\pi = \rho\tau\sigma^{-1}\tau^{-1}\rho^{-1}$ mit $\tau = (ab)$. Dabei ist $\rho\tau$ eine gerade Permutation, d.h. σ^{-1} und π sind in A_n konjugiert.
Nun unterscheiden wir die folgenden Fälle:

1. N enthält eine Permutation, die in der Zyklendarstellung einen Zyklus der Länge $r \geq 4$ enthält, d.h. $\sigma = (a_1 \dots a_r)\pi$, wobei $(a_1 \dots a_r)$ und π disjunkt sind. Dann ist $\rho = (a_1 a_2 a_3) \in A_n$, und $\sigma^{-1}(\rho\sigma\rho^{-1}) = (a_1 a_3 a_r) \in N$.

2. N enthält eine Permutation, die in der Zyklendarstellung zwei 3-Zyklen enthält, $\sigma = (a_1 a_2 a_3)(a_4 a_5 a_6)\pi$. Dann ist $\rho = (a_1 a_2 a_4) \in A_n$, und $\sigma^{-1}(\rho\sigma\rho^{-1}) = (a_1 a_4 a_2 a_6 a_3) \in N$, womit wir wieder bei Fall 1. sind.

3. N enthält eine Permutation, die in der Zyklendarstellung aus einem 3- sowie mehreren 2-Zyklen besteht, d.h. $\sigma = (a_1 a_2 a_3)\pi$, wobei π das Produkt disjunkter 2-Zyklen ist. Dann ist $\sigma^2 = (a_1 a_3 a_2) \in N$.

4. N besteht nur aus Elementen, die sich als Produkte disjunkter 2-Zyklen schreiben lassen. Sei $\sigma \in N$, $\sigma \neq e$. Da σ gerade ist, besteht die Zyklendarstellung aus zumindest zwei Zyklen, d.h. $\sigma = (a_1 a_2)(a_3 a_4)\pi$, wobei π Produkt disjunkter 2-Zyklen ist. Dann ist $\rho = (a_1 a_2 a_3) \in A_n$ und $\sigma^{-1}(\rho\sigma\rho^{-1}) = (a_1 a_3)(a_2 a_4) =: \delta \in N$. Da $n > 4$ ist, gibt es ein $b \in \underline{n} \setminus \{a_1, a_2, a_3, a_4\}$. Es ist $\tau = (a_1 a_3 b) \in A_n$ und damit $\delta(\tau\delta\tau^{-1}) = (a_1 a_3 b) \in N$.

Also besteht N nur aus dem neutralen Element oder enthält einen 3-Zyklus, woraus bereits $N = A_n$ folgt. Somit ist A_n einfach, falls $n > 4$.

□

Man bemerkt, dass auch A_2 und A_3 einfach sind, allerdings zyklisch. A_4 hat jedoch einen nichttrivialen Normalteiler, der zur Klein'schen Vierergruppe isomorph ist.

4 Gruppen vom Lie-Typ

Die Gruppen, von denen hier die Rede sein wird, bauen allesamt auf der Gruppe der linearen Abbildungen über einem Vektorraum auf, ihre Grundlage bilden die sogenannten *Lie-Algebren*. Sie werden ihrerseits wieder in Klassen unterteilt, wobei einige hier kurz vorgestellt werden:

4.1 Die projektiven Gruppen

Es sei zunächst K ein beliebiger Körper. Dann bildet die Menge aller regulären Automorphismen des Vektorraumes K^n eine Gruppe bezüglich $\circ$, genannt $GL(n, K)$. Sie ist isomorph zur Gruppe der regulären $n \times n$-Matrizen über K. Die Gruppe $SL(n, K)$ ergibt sich dann als Kern der Abbildung $\det : GL(n, K) \to (K^*, \cdot)$. Nun betrachtet man die Faktorgruppe von $SL(n, K)$ bezüglich des Zentrums Z von $GL(n, K)$, das aus allen Matrizen der Form aI mit $a \in K^*$ besteht. Es gilt $SL(n, K) \cap Z = \{aI \mid a^n = e\}$. Diese Faktorgruppe bezeichnet man als *projektive lineare Gruppe*, und sie ist definiert als

$$PSL(n, K) = SL(n, K)/(SL(n, K) \cap Z)$$

Sie entspricht der Menge aller linearen Abbildungen auf den Geraden von K^n, da Z gerade aus jenen Abbildungen besteht, die alle Geraden fixieren.

Es zeigt sich, dass diese Gruppe bis auf wenige Spezialfälle stets eine einfache Gruppe ist. Sind wir nur an den endlichen Gruppen interessiert, so müssen auch endliche Körper betrachtet werden. Wie im Zuge der Algebra-Vorlesung bewiesen wird, gibt es zu jeder Primzahlpotenz genau einen endlichen Körper und keine weiteren. Man schreibt daher auch $PSL(n, p^k)$ für die projektive lineare Gruppe über dem eindeutigen Körper der Ordnung $p^k = q$. Die Ordnung von $PSL(n, q)$ ergibt sich kombinatorisch folgendermaßen:

Proposition 4

$$|PSL(n, q)| = d^{-1} \cdot q^{n-1} \cdot (q^n - 1)(q^n - q) \dots (q^n - q^{n-2})$$

wobei $d = \text{ggT}(n, q - 1)$.

Beweis: Sei $v_1, \dots, v_n$ eine Basis des Vektorraums $V = K^n$, wobei $|K| = q$. Dann ist jede lineare Abbildung A von V auf sich durch die Bilder der Basisvektoren eindeutig bestimmt. Damit eine solche Abbildung regulär ist, müssen diese linear unabhängig sein, womit sich die Bedingungen

$$Av_1 \neq 0,\ Av_2 \notin \langle Av_1 \rangle, \dots,\ Av_n \notin \langle Av_1, \dots, Av_{n-1} \rangle$$

ergeben. Der Raum $\langle Av_1, \dots, Av_m \rangle$ hat die Dimension m, also Mächtigkeit q^m. Es ergibt sich

$$|GL(n, q)| = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1})$$

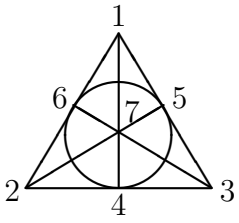
Aus der Tatsache, dass $GL(n, q)/SL(n, q) \simeq K^*$ gilt, folgt weiters

$$|GL(n, q)| = |SL(n, q)||K^*| = |SL(n, q)|(q - 1)$$

Die Gruppe $SL(n, K) \cap Z = \{aI \,|\, a^n = e\}$ hat soviele Elemente wie die multiplikative Gruppe von K Elemente der Ordnung n. Da die multiplikative Gruppe eines endlichen Körpers stets zyklisch ist, gibt es davon genau $d = \text{ggT}(n, q - 1)$, womit die Behauptung folgt.

□

Die kleinste neue endliche einfache Gruppe dieser Art ist $PSL(3, 2)$. Sie besteht aus allen regulären 3×3-Matrizen modulo 2 (da in diesem Fall alle regulären Matrizen Determinante 1 haben und das Zentrum nur aus dem neutralen Element besteht) und hat die Ordnung 168. Diese Gruppe kann auch als Automorphismengruppe der kleinsten endlichen projektiven Ebene gesehen werden:



Sie besteht aus 7 Punkten und „Geraden“, die je 3 von ihnen verbinden (auch der Kreis zählt als Gerade). Die folgenden Bedingungen sind erfüllt:

- Je zwei Geraden schneiden einander in einem eindeutigen Punkt.
- Durch je zwei Punkte geht eine eindeutige Gerade.

Die Automorphismen auf dieser Menge sind dann genau jene bijektiven Abbildungen der Punkte auf sich, die Geraden in Geraden überführen. Damit folgt unmittelbar $PSL(3,2) \leq S_7$, und man erkennt auch, welche Untergruppen es geben muss: etwa die Stabilisatoren aller Punkte.

Wesentlich für uns ist nun der folgende Satz:

Satz 5 *Die Gruppe $PSL(n,q)$ ist für $n \geq 3$ sowie für $n = 2$ und $q > 3$ einfach.*

Beweis: Der Beweis verläuft in mehreren Schritten:

1. Sei $V = K^n$. Eine Abbildung $T : V \to V$ heißt *elementare Transformation*, falls sie bezüglich einer geeigneten Basis $\{v_1, \ldots, v_n\}$ die Darstellung $I + aE_{ij}$ hat (dabei ist I die Einheitsmatrix, E_{ij} die Matrix, die aus einer 1 an der Stelle (i,j) mit $i \neq j$ und ansonsten lauter Einträgen 0 besteht.
   Damit entspricht T einer elementaren Zeilenumformung bezüglich dieser Basis. Mit Hilfe eines etwas verfeinerten Gauß-Algorithmus (zunächst muss durch geeignetes Addieren einer anderen Zeile dafür gesorgt werden, dass als Pivot 1 entsteht, dann kann erst eliminiert werden; der letzte Pivot ergibt sich automatisch als 1) kann dann jede Matrix aus $SL(n,K)$ durch solche Umformungen in die Einheitsmatrix übergeführt werden. Also erzeugen die elementaren Transformationen bereits ganz $SL(n,K)$.

2. Für $n \geq 3$ sind je zwei elementare Transformationen in $SL(n,K)$ konjugiert:

Seien T_1, T_2 zwei elementare Transformationen. Dann haben beide bezüglich einer geeigneten Basis sogar die Form $I + E_{12}$. Die Transformation zwischen diesen beiden Basen lässt sich dann als Konjugation mit einer Matrix C schreiben. Weil $n \geq 3$ ist, kann man zuvor mit der Diagonalmatrix $M = diag(1, 1, d^{-1}, 1, \ldots)$ konjugieren, wobei $d = det(C)$ ist, ohne dabei T_1 zu verändern. CM hat dann die Determinante 1, liegt also in $SL(n, K)$, und es gilt $T_2 = (CM)T_1(CM)^{-1}$.

3. Jeder Normalteiler $\mathcal{N}$ von $SL(n, K)$, der $Z(SL(n, K)) \subsetneq \mathcal{N}$ erfüllt, enthält eine elementare Transformation, falls $n \geq 3$:
   Da $\mathcal{N}$ nicht nur aus Elementen des Zentrums besteht, gibt es ein $G \in \mathcal{N}$, das mit einer bestimmten elementaren Transformation T nicht kommutiert (würde G mit allen elementaren Transformationen kommutieren, dann auch mit allen übrigen, da diese von den elementaren Transformationen erzeugt werden).
   Damit ist $A = GTG^{-1}T^{-1} \in \mathcal{N}$, und da G und T nicht kommutieren, ist $A \neq I$. GTG^{-1} und T^{-1} sind elementare Transformationen, und es gilt
   $$\mathrm{Fix}(GTG^{-1}) \cap \mathrm{Fix}(T^{-1}) \subseteq \mathrm{Fix}(A)$$
   Da für eine elementare Transformation T stets
   $$\dim(\mathrm{Fix}(T)) = \dim(\mathrm{Ker}(T - I)) = n - 1$$
   gilt, folgt $\dim(\mathrm{Fix}(A)) \in n - 1, n - 2$. Im ersten Fall ist A eine elementare Transformation, womit folgt, dass alle elementare Transformationen in $\mathcal{N}$ liegen. Damit ist weiter $\mathcal{N} = SL(n, K)$.
   Sei daher $\dim(\mathrm{Fix}(A)) = n - 2$. Dann hat $\mathrm{Im}(A - I)$ die Dimension 2, und wegen $n \geq 3$ liegt damit $\mathrm{Im}(A - I)$ in einem Teilraum $U \subseteq V$ mit $\dim U = n - 1$. Wähle $u \neq 0$ aus U und v aus $V \setminus U$. Es gibt eine elementare Transformation $E \in SL(n, K)$ mit $\mathrm{Fix}(E) = U$ und $Ev = v + u$. Für diese gilt dann $\mathrm{Im}(E - I) = \langle u \rangle$.
   Weiters gilt für alle $x \in U$ $A^{-1}EAx = x$, da wegen $Ax = (A-I)x+x \in \mathrm{Im}(A - I) + U \subseteq U$ $EA(x) = Ax$ ist. Damit folgt $U \subseteq \mathrm{Fix}(A^{-1}EA) \cap \mathrm{Fix}(E^{-1}) \subseteq \mathrm{Fix}(A^{-1}EAE^{-1})$, also $\dim(\mathrm{Fix}(A^{-1}EAE^{-1}) \geq n - 1$, d.h. $B = A^{-1}EAE^{-1} \in \mathcal{N}$ ist eine elementare Transformation oder $B = I$.
   Wir unterscheiden zwei Fälle: ist $\mathrm{Fix}(A) \subseteq U$, dann folgt $\mathrm{Fix}(A^{-1}) \subsetneq U$. Also gibt es ein $u \in U$, sodass $A^{-1}u$ und u linear unabhängig sind, und damit
   $$A^{-1}EA(A^{-1}v) = A^{-1}Ev = A^{-1}v + A^{-1}u$$
   $C = A^{-1}EA$ ist somit eine elementare Transformation mit $\mathrm{Im}(C-I) = \langle A^{-1}u \rangle$, und es folgt $C \neq E$, also $B \neq I$.

Andernfalls kann man $v \in \mathrm{Fix}(A) \setminus U$ und $u \in U \setminus \mathrm{Fix}(A)$ wählen (da $\dim(\mathrm{Fix}(A)) < \dim(U)$). Es folgt

$$A^{-1}EAv = A^{-1}Ev = A^{-1}(v+u) = v + A^{-1}u \neq v + u = E(v)$$

und damit wieder $B \neq I$, d.h. $B \in \mathcal{N}$ ist eine elementare Transformation, und es folgt wiederum, dass $\mathcal{N} = SL(n, K)$.

4. Übrig bleibt der Fall $n = 2$, $|K| > 3$. Wir wählen eine feste Basis v, w und definieren mit $\mathcal{K}$ die Menge aller Abbildungen, die bezüglich dieser die Form $\pm(I+aE_{12})$ haben. Dann ist diese wegen $(I+aE_{12})(I+bE_{12}) = I + (a+b)E_{12}$ eine Abelsche Gruppe, die isomorph zu $(K, +)$ ist.
Definiere weiters mit $\mathcal{S}$ die Menge aller Abbildungen, die $\langle v \rangle$ fixieren. Es gilt dann für $T \in \mathcal{K}$ und $S \in \mathcal{S}$:

$$S^{-1}TSv = S^{-1}T(cv) = S^{-1}(cv) = v$$

Somit $S^{-1}TS \in \mathcal{K}$, d.h. $\mathcal{K} \trianglelefteq \mathcal{S}$.
Zuletzt definiere ich

$$\mathcal{T} = \langle \{A\mathcal{K}A^{-1} \mid A \in SL(n, K)\} \rangle$$

$\mathcal{K}$ enthält gerade alle jene elementaren Transformationen, die v fixieren. $A\mathcal{K}A^{-1}$ enthält jene elementaren Transformationen, die Av fixieren. Klarerweise lässt sich jeder Vektor $\neq 0$ in V als Av darstellen, d.h. $\mathcal{T}$ enthält alle elementaren Transformationen, und es gilt $\mathcal{T} = SL(n, K)$. Sei nun $\mathcal{N}$ ein Normalteiler von $SL(n, K)$, der $Z(SL(n, K)) \subsetneq \mathcal{N}$ erfüllt. Gilt $\mathcal{N} \subseteq \mathcal{S}$, so wähle $N \in \mathcal{N}$ und $u \in V$ derart, dass $N(u) \notin \langle u \rangle$ (existiert, weil $\mathcal{N}$ nicht nur aus dem Zentrum besteht). Zudem wählen wir ein $G \in SL(n, K)$ mit $G(u) = v$. Dann gilt:

$$NG^{-1}v = Nu \notin \langle u \rangle = G^{-1}(\langle v \rangle)$$

Also $GNG^{-1} \notin \mathcal{S}$, aber $GNG^{-1} \in \mathcal{N}$, ein Widerspruch.
Also besteht $\mathcal{NS}$ aus mehr als einer Nebenklasse von $\mathcal{S}$. Alle Nebenklassen von $\mathcal{S}$ haben die Form

$$\mathcal{S}_u := \{A \in SL(n, K) \mid A(\langle v \rangle) = \langle u \rangle\}$$

für einen Vektor $u \neq 0$.
Angenommen nun, $\mathcal{NS} \neq SL(n, K)$. Es gibt dann $u \in \mathcal{N}(v)$, wobei $u \notin \langle v \rangle$, und $x \in V$, sodass $\langle x \rangle \cap \mathcal{N}(v) = \{0\}$. Wir können $G \in SL(n, K)$ derart wählen, dass $Gv = v$ und $Gu \in \langle x \rangle$. Damit folgt für ein $N \in \mathcal{N}$ mit $Nv = u$:

$$GNG^{-1}v = GNv = Gu \in \langle x \rangle$$

Damit würde jedoch der Widerspruch $\langle x\rangle \cap \mathcal{N}(v) \neq \{0\}$ folgen. Also gilt $\mathcal{NS} = SL(n,K)$.
$SL(n,K)$ wird von den Konjugiertenklassen von $\mathcal{K}$ erzeugt. Jede solche lässt sich wegen $\mathcal{NS} = SL(n,K)$ in der Form $NS\mathcal{K}S^{-1}N^{-1}$ mit $N \in \mathcal{N}$ und $S \in \mathcal{S}$ schreiben. Wegen $\mathcal{K} \trianglelefteq \mathcal{S}$ ist dies jedoch gleich $\mathcal{NKN} = \mathcal{NK}$, weswegen $\mathcal{NK} = SL(n,K)$ folgt.
Sei nun schließlich T eine beliebige elementare Transformation. Wegen $|K| > 3$ gibt es ein Element $d \neq 0, \pm 1$ in K, und für dieses gilt $d^2 - 1 \neq 0$. Daher hat T bezüglich einer geeigneten Basis die Form $I + (d^2-1)E_{12}$. Wegen

$$\begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d^2-1 \\ 0 & 1 \end{pmatrix}$$

lässt sich T in der Form $ABA^{-1}B^{-1}$ für gewisse $A, B \in SL(n,K)$ schreiben. Wegen $\mathcal{NK} = SL(n,K)$ kann man $A = N_1K_1$ und $B = N_2K_2$ mit $N_i \in \mathcal{N}$ und $K_i \in \mathcal{K}$ setzen, und es folgt:

$$T = N_1K_1N_2K_2K_1^{-1}N_1^{-1}K_2^{-1}N_2^{-1}$$

Da $\mathcal{N}$ Normalteiler ist, gilt $\mathcal{N}K_i = K_i\mathcal{N}$. Somit kann man T auch in der Form

$$T = \tilde{N}K_1K_2K_1^{-1}K_2^{-1}$$

mit $\tilde{N} \in \mathcal{N}$ schreiben. Da $\mathcal{K}$ Abelsch ist, folgt damit $T = \tilde{N} \in \mathcal{N}$. Also enthält $\mathcal{N}$ alle elementaren Transformationen, woraus $\mathcal{N} = SL(n,K)$ folgt.

□

Es sei bemerkt, dass $PSL(2,2) \simeq S_3$ und $PSL(2,3) \simeq A_4$ nicht einfach sind.

4.2 Die symplektische Gruppe

Es sei wieder K ein beliebiger Körper und V ein Vektorraum über K. Im Gegendatz zum vorhergegangenen Kapitel betrachten wir nun ein Skalarprodukt $(.,.)$ auf diesem Raum, das folgende Eigenschaften haben soll:

- $(.,.)$ ist bilinear, d.h.

  $(a_1v_1+a_2v_2, w) = a_1(v_1,w)+a_2(v_2,w)$ und $(w, a_1v_1+a_2v_2) = a_1(w,v_1)+a_2(w,v_2)$

- $(v,v) = 0$ für alle $v \in V$

Ein Raum, der ein solches Skalarprodukt besitzt, heißt *symplektischer Raum*. Es sei hier nur erwähnt, dass es zu jeder geraden Zahl $2n$ und jedem Körper K genau einen nicht ausgearteten (d.h. es gibt keinen Vektor $v \neq 0$, der $(v, w) = 0\ \forall w \in V$ erfüllt) symplektischen Raum der Dimension $2n$ über K und keine weiteren gibt. Mit der Abbildung $(\binom{a}{b}, \binom{c}{d}) = ad - bc$ bildet etwa K^2 für jeden Körper K einen symplektischen Raum.

Eine bijektive lineare Abbildung $T : V \to V$, die $(Tv_1, Tv_2) = (v_1, v_2)$ für beliebige Vektoren v_1, v_2 erfüllt, heißt dann *Isometrie*. Die Gruppe aller Isometrien über dem symplektischen Raum der Dimension $2n$ über K heißt *symplektische Gruppe* $Sp(2n, K)$. Analog zur Definition von $PSL(n, K)$ definieren wir auch

$$PSp(2n, K) = Sp(2n, K)/Z$$

wobei Z das Zentrum von $Sp(2n, K)$ ist. Ist K ein endlicher Körper der Ordnung qk, schreiben wir wieder $PSp(2n, q)$ anstelle von $PSp(2n, K)$. Es zeigt sich, dass diese sogenannte *projektive symplektische Gruppe* stets einfach ist, ausgenommen die Fälle $PSp(2, 2)$, $PSp(2, 3)$ und $PSp(4, 2)$ (wird im Folgenden aber nicht bewiesen). Mit denselben Methoden wie in Proposition 4 kann man zeigen, dass für die Ordnung folgendes gilt:

Proposition 6

$$|PSp(2n, q)| = d^{-1} \cdot q^{n^2}(q^2 - 1)(q^4 - 1) \dots (q^{2n} - 1)$$

wobei $d = \mathrm{ggT}(2, q - 1)$.

4.3 Orthogonale und Unitäre Gruppen

Wiederum betrachten wir einen Vektorraum V über K und ein Skalarprodukt auf diesem. Sei dazu A ein Automorphismus auf K mit $A^2 = id_K$. Auf V sei ein Skalarprodukt $(.,.)$ definiert, das folgende Eigenschaften hat:

- $(v_1 + v_2, w) = (v_1, w) + (v_2, w)$ und $(w, v_1 + v_2) = (w, v_1) + (w, v_2)$
- $(av, w) = a(v, w)$
- $(v, w) = A(w, v)$

Ist $A = id_K$, so heißt V ein *orthogonaler Raum*, ansonsten *hermitescher Raum*. In diesem Sinne sind $\mathbb{R}^n$ bzw. $\mathbb{C}^n$ mit dem bekannten Skalarprodukt orthogonale bzw. hermitesche Räume (mit der Konjugation als Automorphismus von $\mathbb{C}$).

Ist V ein nicht ausgearteter orthogonaler Raum, so definieren wir in Analogie zur symplektischen Gruppe die *orthogonale Gruppe* $O(V)$ aller bijektiven linearen Abbildungen $T : V \to V$, die $(Tv_1, Tv_2) = (v_1, v_2)$ für beliebige Vektoren v_1, v_2 erfüllen. Ebenso definieren wir auch die *unitäre Gruppe* $U(V)$ auf einem hermiteschen Raum. Analog zu den Gruppen $SL(V)$ und $PSL(V)$ sind dann auch $SO(V)$, $SU(V)$, $PSO(V)$ und $PSU(V)$ definiert.

Es zeigt sich wiederum, dass solche Räume für gegebene Dimensionen über endlichen Körpern eindeutig bestimmt sind. Hierbei gibt es nur über Körpern quadratischer Ordnung (d.h. $|K| = p^{2k}$) hermitesche Räume, wobei der Automorphismus A auf K, der das Skalarprodukt erzeugt, durch $Ax = x^{p^k}$ gegeben ist. Daher kann man von den Gruppen $PSO(n, p^k)$ und $PSU(n, p^{2k})$ sprechen. Die Gruppe $PSU(n, p^{2k})$ ist für $n \geq 3$ einfach, ausgenommen $PSU(3, 4)$. Die kleinste neue einfache Gruppe, die wir dadurch erhalten, ist $PSU(3, 9)$, sie hat die Ordnung 6048.

Dazu gibt es noch die Gruppe $\Omega(V) = \langle \{A^{-1}B^{-1}AB \mid A, B \in SO(V)\} \rangle$, die Kommutatorgruppe von $SO(V)$. Faktorisiert man wie immer das Zentrum heraus, erhält man die Gruppe $P\Omega(V) = \Omega(V)/Z(\Omega(V))$. $P\Omega(n, p^k)$ ist für $n \geq 5$ einfach.

4.4 Weitere Gruppen vom Lie-Typ

Neben den sogenannten *klassischen linearen Gruppen* PSL, PSp, PSU und $P\Omega$ aus den vorigen Kapiteln gibt es noch weitere einfache Gruppen vom Lie-Typ – insgesamt unterscheidet man 16 verschiedene Gruppen. Die übrigen beruhen auf den sogenannten Ausnahme-Lie-Algebren (auf die ich nicht näher eingehen möchte). Sie werden auch *twisted groups* genannt.

5 Sporadische Gruppen

Besonderes Kopfzerbrechen bereiteten den Gruppentheoretikern die sogenannten *sporadischen Gruppen*. Die ersten fünf ihrer Art wurden um 1865 vom französischen Mathematiker Émile Mathieu entdeckt. Die kleinste unter ihnen ist die Gruppe mit dem Namen M_{11} und 7920 Elementen. Sie lässt sich als Untergruppe von S_{11} schreiben.

Es dauerte ein ganzes Jahrhundert bis Zvonimir Janko 1965 die sechste sporadische Gruppe mit der Ordnung 175560 fand. Drei Jahre später überraschte John H. Conway mit der Entdeckung dreier weiterer Gruppen, die auf dem sogenannten *Leech-Gitter* beruhen, das es erlaubt, 24-dimensionale Einheitskugeln dicht zu packen.

Bis 1980 waren schließlich alle sporadischen Gruppen entdeckt. Die größte von ihnen hat die Ordnung

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000

und wird scherzhaft das *Monster* genannt. Sie ist Untergruppe der Gruppe der Drehungen eines 196883-dimensionalen Raumes. Bemerkenswert daran ist, dass die nächstgrößere Zahl 196884 als Koeffizient in der elliptischen modularen Funktion

$$j(q) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots$$

vorkommt, die eine entscheidende Rolle in der Theorie elliptischer Kurven spielt (die ihrerseits ihre bekannteste Anwendung im Beweis des berühmten Satzes von Fermat findet). Der Beweis, dass es sich nicht um einen Zufall handelt (!), brachte Richard Borcherds eine Fields-Medaille ein.

Sämtliche sporadischen Gruppen sind in der folgenden Tabelle aufgelistet:

Name	**Ordnung**	**Entdecker**
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	Mathieu
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	Mathieu
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	Mathieu
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu
J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	Janko
J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	Hall, Wales
J_3	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$	Higman, McKay
J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$	Benson, Conway, Janko, Norton, Parker, Thackray
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	Higman, Sims
MC	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	McLaughlin
Sz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	Suzuki
C_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$	Conway
C_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway
C_3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway
He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$	Held, Higman, McKay
F_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	Fischer
F_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	Fischer
F_{24}	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$	Fischer
Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$	Lyons, Sims
O	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$	O'Nan, Sims
R	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$	Conway, Rudvalis, Wales

F_5	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$	Conway, Fischer, Harada, Norton, Smith
F_3	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$	Smith, Thompson
F_2	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$	Fischer, Leon, Sims
F_1	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot$ $31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$	Fischer, Griess

6 Eindeutigkeitsbeweise

Auch wenn es teilweise alles andere als trivial ist, die Einfachkeit von Gruppen zu beweisen, so liegt die Hauptschwierigkeit beim Klassifizierungssatz darin, zu zeigen, dass es außer den gefundenen Gruppen keine weiteren gibt. Als mächtiges Hilfsmittel bei den einfachen Betrachtungen, die ich im Folgenden vornehmen werde, erweisen sich die Sylowsätze.

Die Anzahl der p-Sylowgruppen (d.h. jener Untergruppen einer Gruppe G, die die Ordnung p^k haben, wobei $p^k \,\big|\, |G|$ und $p^{k+1} \nmid |G|$) sei c_p. Sie erfüllt die Eigenschaften $c_p \,\big|\, |G|$ und $c_p \equiv 1 \mod p$. Ist $c_p = 1$, so ist die einzige p-Sylowgruppe ein Normalteiler. Diese Eigenschaften werden im Folgenden verwendet:

Proposition 7 Sei G eine einfache Gruppe der Ordnung p^k, wobei p Primzahl und $k \geq 1$ ist. Dann ist $k = 1$ und G eine zyklische Gruppe.

Beweis: Für $k \geq 2$ gibt es nach dem ersten Sylowsatz einen nichttrivialen Normalteiler vom Index p. Also muss $k = 1$ sein. Es gibt jedoch nur eine Gruppe der Ordnung p, nämlich die zyklische.

□

Proposition 8 Seien p, q Primzahlen und $a \geq 1$. Ist G eine Gruppe der Ordnung $p^a q$, dann ist G nicht einfach.

Beweis: Angenommen, G sei einfach. Dann folgt aus $c_p \,|\, q$ und $c_p \neq 1$, dass $c_p = q$ sein muss. Nehmen wir nun weiter an, je zwei p-Sylowgruppen hätten trivialen Durchschnitt. Dann enthält jede von ihnen $p^a - 1$ Elemente, deren Ordnung eine Potenz von p ist, insgesamt gibt es also $(p^a - 1)q$ Elemente von solcher Ordnung. Es bleiben nur noch q Elemente übrig, und diese müssen dann die einzige q-Sylowgruppe bilden, im Widerspruch zur Einfachheit.
Also gibt es zwei verschiedene p-Sylowgruppen P_1, P_2 mit nichttrivialem Durchschnitt $D = P_1 \cap P_2$. Wir wählen P_1, P_2 derart, dass $|D|$ maximal wird. Setze $B_1 := N_{P_1}(D)$ und $B_2 := N_{P_2}(D)$. Es gilt dann $T := \langle B_1, B_2 \rangle \leq N_G(D)$

und daher $D \trianglelefteq T$. Ist $|T| = p^t$, dann gibt es eine p-Sylowgruppe P_3, in der T enthalten ist. Es folgt

$$P_1 \cap P_3 \geq P_1 \cap T \geq B_1 \geq D$$

Wegen der Maximalität von $|D|$ muss folglich $B_1 = D$ gelten. Nach dem zweiten Sylowsatz gibt es jedoch eine Gruppe $B \leq P_1$, $D \subsetneqq B$, in der D als Normalteiler enthalten ist. Daraus ergibt sich der Widerspruch $D \subsetneqq B \subseteq N_{P_1}(D) = B_1 = D$.
Also muss $|T| = p^t q$ für geeignetes t sein. Sei Q eine q-Sylowgruppe von T. Q und P_1 haben dann sicher trivialen Durchschnitt, es folgt somit $|P_1 Q| = |P_1||Q| = p^a q = |G|$ und daher $P_1 Q = G$.
Definiere nun $K := \langle \{gDg^{-1} \mid g \in G\} \rangle$. Dann ist K jedenfalls ein Normalteiler von G, denn jeder innere Automorphismus bildet K auf K ab. Jedes $g \in G$ lässt sich nun in der Form $g = pq$ mit $q \in Q \leq T \leq N_G(D)$ und $p \in P_1$ schreiben. Dann ist

$$gDg^{-1} = pqDq^{-1}p^{-1} = pDp^{-1} \leq P_1$$

Somit ist $K \neq G$, und wegen $\{e\} \neq D \subseteq K$ ist auch $K \neq \{e\}$. Damit ist jedoch K nichttrivialer Normalteiler von G, ein Widerspruch.

□

Proposition 9 Seien p, q, r Primzahlen mit $p > q > r$. Ist G eine Gruppe der Ordnung pqr, dann ist G nicht einfach.

Beweis: Angenommen, G wäre einfach. Es gilt $c_p \mid qr$ und $c_p \equiv 1 \mod p$. Da wegen der Einfachheit nicht $c_p = 1$ sein kann, muss $c_p \geq p + 1 > q, r$ sein. Der einzige Teiler von qr, der damit noch für c_p in Frage kommt, ist $c_p = qr$. Ebenso gilt $c_q \mid pr$, $c_q \neq 1$ und $c_q \equiv 1 \mod q$, damit weiter $c_q \geq q + 1 > r$, also $c_q \geq p$. Zuletzt ergibt sich ebenso $c_r \geq q$.
Je zwei p-Sylowgruppen haben trivialen Durchschnitt, da jedes Element einer p-Sylowgruppe (ausgenommen e) diese bereits erzeugt. Jede p-Sylowgruppe enthält $p - 1$ Elemente der Ordnung p, insgesamt gibt es also $(p-1)qr$ Elemente der Ordnung p. Ebenso gibt es zumindest $(q-1)p$ Elemente der Ordnung q und zumindest $(r-1)q$ Elemente der Ordnung r. Zusammen mit dem Element e ergibt das

$$(p-1)qr+(q-1)p+(r-1)q+1 = pqr-qr+qp-p+rq-q+1 = pqr+(p-1)(q-1) > pqr$$

Elemente, also erhält man einen Widerspruch.

□

Lemma 10 Es habe G eine Untergruppe H vom Index n. Dann hat G einen Normalteiler N, der $n \,\big|\, |G/N|$ und $|G/N| \,\big|\, n!$ erfüllt.

Beweis: Sei jedem Element $g \in G$ die Funktion f_g zugeordnet, die die Linksnebenklassen von H nach dem Schema $aH \mapsto gaH$ auf sich abbildet. Dann ist f_g bijektiv (mit der Inversen $f_{g^{-1}}$), also eine Permutation auf der n-elementigen Menge der Linksnebenklassen von H.
Diese Zuordnung erzeugt einen Homomorphismus $f : G \to S_n$. Sei N dessen Kern. Dann ist $G/N \simeq \operatorname{Im} f \leq S_n$. Daraus folgt $|G/N| \,\big|\, n! = |S_n|$. Andererseits gibt es zu beliebigen Linksnebenklassen aH, bH stets ein Gruppenelement $g = ba^{-1}$, das aH auf bH abbildet. Also besteht die Bahn jeder Linksnebenklasse aH bezüglich der Wirkung durch G/N aus allen n Linksnebenklassen, und da die Mächtigkeit einer Bahn gleich dem Index des Stabilisators und daher ein Teiler der Gruppenordnung ist, folgt $n \,\big|\, |G/N|$.

□

Proposition 11 Seien p, q Primzahlen mit $p > q$. Ist G eine Gruppe der Ordnung p^2q^2, dann ist G nicht einfach.

Beweis: Nehmen wir wieder an, G sei einfach. Dann folgt aus $c_p | q^2$ und $c_p \equiv 1 \mod p \Rightarrow c_p \geq p + 1 > q$ diesmal $c_p = q^2$. Angenommen, je zwei p-Sylowgruppen von G hätten trivialen Durchschnitt. Dann gibt es $q^2(p^2 - 1)$ Gruppenelemente, deren Ordnung p^2 teilt. Die übrigen q^2 Elemente müssten dann bereits die einzige q-Sylowgruppe bilden, im Widerspruch zur Einfachheit.
Also gibt es zwei p-Sylowgruppen P_1, P_2 mit einem Durchschnitt $D = P_1 \cap P_2$, der die Ordnung $|D| = p$ haben muss. Nach dem zweiten Sylowsatz ist D Normalteiler sowohl von P_1 als auch von P_2, also $P_1 \leq N_G(D)$ und $P_2 \leq N_G(D)$. Sei nun $T = \langle P_1, P_2 \rangle$. Dann muss auch $T \leq N_G(D)$ und damit $D \trianglelefteq T$ gelten. Daher ist $T \neq G$. Andererseits muss $p^2 = |P_1|$ die Ordnung von T teilen, und wegen $P_1 \neq P_2$ ist $|T| \neq p^2$.
Es bleibt nur übrig, dass $|T| = p^2q$, d.h. T ist eine Untergruppe vom Index q. Nach dem vorigen Lemma hat G damit einen Normalteiler N, der $q \,\big|\, |G/N|$ und $|G/N| \,\big|\, q!$ erfüllt. Wegen der ersteren Bedingung kann N nicht G sein, wegen der zweiteren kann N nicht e sein (weil sonst $q \,|\, (q-1)!$ für die Primzahl q gelten müsste, was unmöglich ist). Insgesamt ergibt sich also ein Widerspruch zur Einfachheit.

□

Satz 12 *Die kleinste nichtzyklische einfache Gruppe hat die Ordnung* 60*. Sie ist bis auf Isomorphie eindeutig bestimmt.*

Beweis: Aufgrund der vorangegangenen Propositionen fallen alle natürlichen Zahlen < 60 als potenzielle Ordnungen nichtzyklischer einfacher Gruppen weg. Die alternierende Gruppe A_5 hat Ordnung $\frac{5!}{2} = 60$. Es bleibt lediglich zu zeigen, dass sie die einzige einfache Gruppe der Ordnung 60 ist.
Dazu genügt der Nachweis, dass jede einfache Gruppe der Ordnung 60 eine Untergruppe vom Index 5 hat. Nach Lemma 10 gibt es dann einen Normalteiler N von G, der $5 \,|\, |G/N|$ erfüllt. Es kann sich also nicht um $N = G$ handeln, daher ist $N = \{e\}$. Aus der Konstruktion in Lemma 10 ergibt sich dann, dass G isomorph zu einer Untergruppe von S_5 ist. S_5 hat jedoch nur eine Untergruppe der Ordnung 60, nmlich A_5. Jede andere Untergruppe U müsste wie A_5 ein Normalteiler sein (Index 2) und daher $A_5 \cap U \trianglelefteq A_5$ erfüllen. Wegen der Einfachheit von A_5 ist dies nur möglich, falls A_5 und U trivialen Durchschnitt haben. Dann wäre jedoch $|A_5 U| = 60^2 = 3600 > |S_5|$, ein Widerspruch.
Zeigen wir nun, dass jede einfache Gruppe G der Ordnung 60 eine Untergruppe vom Index 5 hat. Angenommen, dies wäre nicht der Fall. Es kann auch keine Untergruppen vom Index $2, 3$ oder 4 geben, weil dann (wie oben) G isomorph zu einer Untergruppe von S_2, S_3 oder S_4 sein müsste. Wegen $|G| > 4! = 24$ ist dies aber unmöglich.
Sei nun $p \in \{2, 3, 5\}$ und P eine feste p-Sylowgruppe. Wegen $c_p = [G : N_G(P)]$ muss $c_p > 5$ für jedes p sein, da es keine Untergruppen $U \neq G$ vom Index ≤ 5 gibt. Daraus und aus den Bedingungen $c_2 \,|\, 15$, $c_3 \,|\, 20$, $c_5 \,|\, 12$ sowie $c_p \equiv 1 \mod p$ ergibt sich $c_2 = 15$, $c_3 = 10$, $c_5 = 6$.
Je zwei 3- bzw. 5-Sylowgruppen haben trivialen Durchschnitt, weil jedes Element außer e bereits Erzeuger ist. Es gibt somit $2c_3 = 20$ Elemente der Ordnung 3 und $4c_5 = 24$ Elemente der Ordnung 5.
Angenommen, es gäbe zwei 2-Sylowgruppen P_1, P_2 mit nichttrivialem Durchschnitt D. D hat dann in beiden Gruppen Index 2, also $D \trianglelefteq P_1, P_2$, damit $P_1, P_2 \leq N_G(D)$ und in weiterer Folge $T := \langle P_1, P_2 \rangle \leq N_G(D)$, also $D \trianglelefteq T$. Wegen der Einfachheit von G gilt $T \neq G$. Da T zumindest zwei 2-Sylowgruppen enthält (nämlich P_1 und P_2), enthält T sogar drei 2-Sylowgruppen (die Anzahl muss ungerade sein). Also ist $|T| \geq 12$, im Widerspruch zu $[G : T] > 5$. Daher haben je zwei 2-Sylowgruppen trivialen Durchschnitt, und es gibt $3c_2 = 45$ Elemente in G, deren Ordnung 2 oder 4 ist. Damit enthält jedoch G zumindest $20 + 24 + 45 > 60$ Elemente, ein Widerspruch.

□

Mit ähnlichen Methoden ist es auch möglich, die einfachen Gruppen für etwas höhere Ordnungen zu charakterisieren (etwa bleiben nur noch die Ordnungen $72, 84$ und 90 im Bereich bis 100 übrig, es zeigt sich jedoch, dass die

nächstkleinere nichtzyklische einfache Gruppe erst die Gruppe $PSL(3,2)$ ist, die die Ordnung 168 hat).

Tiefere Methoden werden dazu benutzt, um Ergebnisse wie die folgenden zu beweisen:

Satz 13 (Burnside) *Sind p, q Primzahlen und $k, l \geq 1$, dann gibt es keine einfache Gruppe der Ordnung $p^k q^l$.*

Satz 14 (Feit,Thompson) *Eine einfache endliche nichtzyklische Gruppe hat gerade Ordnung.*

Die Folge der Ordnungen nichtzyklischer einfacher Gruppen beginnt mit den folgenden Werten:

Ordnung	**Gruppe**
$60 = 2^2 \cdot 3 \cdot 5$	$A_5 \simeq PSL(2,4) \simeq PSL(2,5)$
$168 = 2^3 \cdot 3 \cdot 7$	$PSL(2,7) \simeq PSL(3,2)$
$360 = 2^3 \cdot 3^2 \cdot 5$	$A_6 \simeq PSL(2,9)$
$504 = 2^3 \cdot 3^2 \cdot 7$	$PSL(2,8)$
$660 = 2^2 \cdot 3 \cdot 5 \cdot 11$	$PSL(2,11)$
$1092 = 2^2 \cdot 3 \cdot 7 \cdot 13$	$PSL(2,13)$
$2448 = 2^4 \cdot 3^2 \cdot 17$	$PSL(2,17)$
$2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$	A_7
$3420 = 2^2 \cdot 3^2 \cdot 5 \cdot 19$	$PSL(2,19)$
$4080 = 2^4 \cdot 3 \cdot 5 \cdot 17$	$PSL(2,16)$
$5616 = 2^4 \cdot 3^3 \cdot 13$	$PSL(3,3)$
$6048 = 2^5 \cdot 3^3 \cdot 7$	$PSU(3,9)$
$6072 = 2^3 \cdot 3 \cdot 11 \cdot 23$	$PSL(2,23)$
$7800 = 2^3 \cdot 3 \cdot 5^2 \cdot 13$	$PSL(2,25)$
$7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$	M_{11}

Literatur

[1] Gardner, *Geometrie mit Taxis, die Köpfe der Hydra und andere mathematische Spielereien*, Birkhäuser Verlag Basel 1997

[2] Grillet, *Algebra*, John Wiley & Sons 1999

[3] Hungerford, *Algebra*, Springer Verlag New York 1974

[4] Huppert, *Endliche Gruppen I*, Springer Verlag Berlin 1967