Die Klassifikation der endlichen einfachen Gruppen

Dieter Held

Fachbereich Mathematik

Johannes Gutenberg-Universität

55099 Mainz, Germany

Aus: Forschungsmagazin der Johannes Gutenberg-Universität Mainz, 1/86.

1 Einleitung

Ende des Jahres 1964 traf an den Zentren der mathematischen Forschung eine Nachricht ein, die von den Gruppentheoretikern als eine Sensation empfunden wurde. Die Nachricht bestand aus einer Beschreibung einer bis dahin unbekannten endlichen einfachen Gruppe – heute durch J_1 bezeichnet – mit 175.560 Elementen. Zvonimir Janko – damals am Institute of Advanced Studies in Canberra – hatte, als er versuchte, eine allgemein als zutreffend angesehene Behauptung nun wirklich zu beweisen, ein hypothetisches Gegenbeispiel zur Behauptung studiert und dann zeigen können, daß dieses Gegenbeispiel tatsächlich existiert und sich als eine neue einfache Gruppe erwies. Wenn sich damals – Anfang der 60er Jahre – ein junger Mathematiker, angezogen von den geheimnisvollen Objekten, welche die einfachen Gruppen wohl für die meisten Mathematiker darstellen, äußerte, daß er sich ihrem Studium widmen wolle, konnte er nicht selten hören, daß ein solches Unterfangen wenig Sinn haben werde, da die Experten auf diesem Gebiet demnächst gezeigt haben würden, daß alle endlichen einfachen Gruppen bereits bekannt seien. Für eine solche Meinung gab es gewichtige Gründe. Bis auf die fünf einfachen Gruppen $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$, die Emile Mathieu in den 60er und

70er Jahren des vorigen (neunzehnten) Jahrhunderts entdeckt hatte, traten alle anderen bekannten einfachen Gruppen als Mitglieder unendlicher Serien von einfachen Gruppen auf, und es gab für alle diese Serien eine ihnen im wesentlichen gemeinsame Konstruktion. Dies war nicht stets von vornherein klar gewesen, es stellte sich aber später immer wieder heraus: So konstruierte z. B. Michio Suzuki 1960 eine neue unendliche Serie einfacher Gruppen; Rimhak Ree zeigte darauf, daß die neue Suzuki-Serie mit Hilfe einer Variation des bekannten Konstruktionsprinzips erhalten werden konnte. Dabei entdeckte Ree selbst zwei neue Serien einfacher Gruppen, indem er die Variation, die zur Suzuki-Serie führte, weiter ausnutzte. Alle späteren Versuche, auf ähnliche Weise zu weiteren neuen einfachen Gruppen zu gelangen, scheiterten. Die Ansicht, daß Anfang der 60er Jahre alle endlichen einfachen Gruppen bekannt seien, war weit verbreitet und schien gerechtfertigt.

2 Gruppen, Homomorphismen, Einfachheit

Was ist nun überhaupt eine Gruppe? Eine Gruppe ist zunächst einmal eine Menge G, die mindestens ein Element enthält, zusammen mit einer Verknüpfung $\circ$, so daß die Verknüpfung $a \circ b$ von Elementen a und b aus G wieder in G liegt. Um klarzumachen, was hier gemeint ist, betrachten wir die beiden Mengen $Z_\infty = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ und $Z_2 = \{1, -1\}$. Die Menge Z_∞ ist die Menge der ganzen Zahlen; offensichtlich ist Z_2 eine Teilmenge von Z_∞. Mit Z_∞ assoziieren wir die Verknüpfung $+$, wobei $+$ die übliche Addition zweier Zahlen sein soll; das soll bedeuten, daß je zwei Elemente von Z_∞ durch $+$ verknüpft werden können. Z. B.: Wir wissen, daß die Elemente -20 und 10 zu

Z_∞ gehören; die Verknüpfung von -20 und 10 durch $+$ liefert $-20+10=-10$; wir stellen fest, daß -10 wieder zu Z_∞ gehört. Es ist ganz offensichtlich, daß für jede Wahl zweier Elemente von Z_∞ ihre Verknüpfung durch $+$ (ihre Summe) wieder ein Element von Z_∞ ist. Während Z_∞ unendlich viele Elemente enthält, besitzt Z_2 genau zwei – daher endlich viele – Elemente. Verwenden wir als Verknüpfung auf Z_2 ebenfalls $+$, so stellen wir fest, daß diese Verknüpfung von Elementen in Z_2 wegen $1+1=2$ aus Z_2 herausführt. Betrachten wir jedoch Z_2 zusammen mit der Verknüpfung $*$, wobei wir unter $*$ die übliche Multiplikation verstehen, so gilt offenbar für Elemente x und y von Z_2, daß $x*y$ wieder in Z_2 liegt; es gilt nämlich $1*1=1$, $1*-1=-1$ und $-1*-1=1$.

Wir wollen nun bestimmte $(Z_\infty,+)$ und $(Z_2,*)$ gemeinsame Eigenschaften hervorheben. Unter dem Paar $(G,\circ)$ werden wir vorübergehend $(Z_\infty,+)$ oder/und $(Z_2,*)$ verstehen; das heißt: Ist für uns $G=Z_\infty$, so soll $\circ=+$ gelten; ist aber $G=Z_2$, so sei $\circ=*$.

Dann hat $(G, \circ)$ folgende Eigenschaften:

A1) Sind a und b Elemente aus G, so gibt es ein eindeutig bestimmtes Element $a \circ b$ in G.

A2) Sind a, b, c Elemente aus G, so gilt $(a \circ b) \circ c = a \circ (b \circ c)$.

A3) Es gibt genau ein Element n aus G derart, daß $n \circ a = a \circ n = a$ gilt für alle a aus G.

A4) Ist a in G, so gibt es genau ein b in G mit $a \circ b = b \circ a = n$.

Das Nachprüfen der behaupteten Eigenschaften von $(G, \circ)$ ist leicht: Im Falle $G = Z_\infty$ hat man z. B. $n = 0$, während $n = 1$ im Falle $G = Z_2$ gilt.

Sehen wir jetzt von der speziellen Bedeutung, die wir $(G, \circ)$ gegeben haben ab und verlangen, daß das Paar $(G, \circ)$ mit der nichtleeren Menge G und der Verknüpfung $\circ$ die Eigenschaften A1 bis A4 besitzt, so erhalten wir die Definition einer Gruppe. Wir sagen also: $(G, \circ)$ ist eine Gruppe, falls $(G, \circ)$ die Eigenschaften A1 bis A4 hat.

Gilt für alle a, b in G die Gleichung $a \circ b = b \circ a$, so nennt man G eine abelsche oder kommutative Gruppe. Wir demonstrieren später, daß es nichta-

belsche Gruppen gibt. Ist eine Teilmenge U von G, welche n enthält, bezüglich $\circ$ eine Gruppe, so nennt man $(U, \circ)$ eine Untergruppe von $(G, \circ)$. Man sieht, daß $(\{n\}, \circ)$ die Untergruppe von $(G, \circ)$ ist, die nur ein Element enthält.

Im folgenden werden wir der Einfachheit halber eine Gruppe $(G, \circ)$ kurz mit G bezeichnen. Wir haben gesehen, daß es sowohl unendliche als auch endliche Gruppen gibt. In diesem Artikel soll bis auf das Beispiel Z_∞ nur von endlichen Gruppen die Rede sein. Ist G eine endliche Gruppe, so bezeichnen wir durch $|G|$ die Anzahl der Elemente von G. Ein Satz von Lagrange besagt, daß für eine Untergruppe U von G die „Ordnung“ $|U|$ von U ein Teiler der Ordnung $|G|$ von G ist. Unter den abelschen Gruppen werden diejenigen Gruppen „einfache“ Gruppen genannt, deren Ordnung eine Primzahl ist. So ist zum Beispiel Z_2 eine einfache Gruppe. Übrigens könnte man unter den natürlichen Zahlen die Primzahlen „einfache Zahlen“ nennen, da sie multiplikativ nicht aus anderen Zahlen zusammengesetzt sind.

Die Anwendung des Satzes von Lagrange auf eine abelsche einfache Gruppe A zeigt sogleich, daß eine Untergruppe von A – wenn sie von A verschieden ist – die Ordnung 1 haben muß, also nur aus dem Element n besteht; denn Teiler einer Primzahl p sind nur p und 1.

Ein fundamentales Ergebnis in der Theorie der endlichen Gruppen ist der Satz von Sylow: Ist G eine endliche Gruppe der Ordnung $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, wobei die p_i Primzahlen und die α_i ganze nichtnegative Zahlen sind, so gibt es Untergruppen von G der Ordnungen $p_i^{\beta_i}$ für alle ganzen Zahlen β_i mit $0 \leq \beta_i \leq \alpha_i$

und $1 \leq i \leq k$.

Ein Beispiel: Hat die Gruppe G die Ordnung $60 = 2^2 \cdot 3 \cdot 5$, so gibt es Untergruppen der Ordnungen 1, 2, 2^2, 3 und 5 in G. Aus dem Satz von Sylow folgt, daß eine Gruppe A, welche nur die Untergruppen A und $\{n\}$ besitzt, eine Ordnung haben muß, die eine Primzahl oder 1 ist. Es ist leicht zu zeigen,daß eine Gruppe von Primzahlordnung abelsch sein muß.

Wir wollen jetzt erklären, was man im allgemeinen – also auch im nichtabelschen Fall – unter einer einfachen Gruppe zu verstehen hat.

Sei G eine fest gewählte endliche Gruppe, und sei H irgendeine endliche Gruppe. Wir betrachten eine Abbildung f der Elemente von G in die Gruppe H hinein. Unsere Abbildung f soll folgende Eigenschaften haben:

1) Ist g aus G, so ist das Bildelement $f(g)$ in H eindeutig bestimmt;

2) sind a und b Elemente aus G, so gilt $f(a \circ b) = f(a) \overline{\circ} f(b)$; hier bedeutet $\circ$ auf der linken Seite der Gleichung die Verknüpfung auf G und $\overline{\circ}$ auf der rechten Seite die Verknüpfung auf H.

Eine solche Abbildung f nennt man einen Homomorphismus der Gruppe G in die Gruppe H. Die Untermenge von H, die aus allen $f(g)$ besteht, wenn g alle Elemente von G durchläuft, bezeichnen wir mit $f(G)$. Es ist leicht zu sehen, daß $f(G)$ eine Untergruppe von H ist. Es gibt stets einen Homomorphismus von G in eine beliebige Gruppe H; einen solchen erhält man, wenn man die Abbildung Ψ betrachtet, die $\Psi(g) = n_H$ für alle g aus G erfüllt; hierbei ist n_H das unter A3 geforderte „neutrale“ Element aus H; offenbar gilt $|\Psi(G)| = 1$.

Wir sind jetzt in der Lage folgende Definition auszusprechen:

Definition 1 *Eine endliche Gruppe G heißt einfach, wenn für jede endliche Gruppe H und jeden Homomorphismus f von G in H stets $|f(G)| = |G|$ oder $|f(G)| = 1$ gilt. – Die Analogie zwischen den endlichen einfachen Gruppen und den „einfachen“ Zahlen ist auffallend.*

Wir ziehen noch einmal unsere Gruppen $(Z_\infty, +)$ und $(Z_2, *)$ heran, um ein nichttriviales Beispiel für einen Homomorphismus zu geben: Dazu definieren wir die Abbildung Θ von Z_∞ in Z_2 durch die Forderung, daß jede gerade Zahl in Z_∞ unter Θ auf 1 in Z_2 und jede ungerade Zahl in Z_∞ unter Θ auf -1 in Z_2 abgebildet wird. Dann ist Θ offenbar ein Homomorphismus von Z_∞ in Z_2; die Gruppe Z_∞ hat unendlich viele Elemente, während $\Theta(Z_\infty)$ aus genau zwei Elementen besteht und mit Z_2 zusammenfällt.

Man kann zeigen, daß die eben angeführte Definition der Einfachheit einer endlichen Gruppe im abelschen Fall genau zu den Gruppen mit Primzahlordnung führt. Gruppen von Primzahlordnung haben eine sehr einfache Struktur. Jedes ihrer Elemente ist eine Potenz eines beliebigen vom neutralen Element n verschiedenen Elementes; hier ist Potenz im Sinne der jeweiligen Verknüpfung zu verstehen: Hat z. B. die Gruppe Z die Ordnung 5, so hat man $Z = \{n, x, x^2, x^3, x^4\}$, wobei man irgendein von n verschiedenes Element x aus Z nehmen kann; hier haben wir $x \circ x = x^2$, $x \circ x \circ x = x^3$ usw. gesetzt; es gilt $x^5 = n$. Vom gruppentheoretischen Standpunkt aus kann man sagen, daß

die Struktur der abelschen einfachen Gruppen bekannt ist; da jedes Element als Potenz eines festen Elementes erhalten werden kann, kann man in einer solchen Gruppe mühelos rechnen.

3 Nichtabelsche einfache Gruppen

Wir wollen uns daher im folgenden nur mit den nichtabelschen endlichen einfachen Gruppen beschäftigen. Die Ordnung der kleinsten (nichtabelschen) einfachen Gruppe ist 60. Die Ordnungen unter 1000 sind 60, 168, 360, 504 und 660. Für die fünf Mathieu-Gruppen gilt $|M_{11}| = 7.920$, $|M_{12}| = 95.040$, $|M_{22}| = 443.520$, $|M_{23}| = 10.200.960$ und $|M_{24}| = 244.823.040$.

Für jede natürliche Zahl $m \geq 3$ gibt es eine einfache Gruppe, die durch $GL(m, 2)$ bezeichnet wird und welche die Ordnung $2^{m(m-1)/2} \cdot \prod_{i=2}^{m} (2^i - 1)$ hat. Die unendliche Folge der Ordnungen der einfachen Gruppen $GL(m, 2)$ beginnt mit 168, 20.160, 9.999.360. Eine weitere unendliche Serie von einfachen Gruppen bilden die sogenannten alternierenden Gruppen. Die kleinste Gruppe dieser Serie hat die Ordnung 60; es folgen die Ordnungen 360, 2.520, 20.160, 181.440. Alle Ordnungen der hier aufgeführten Gruppen sind durch 2 teilbar. Dies ist nicht zufällig, sondern im allgemeinen so, wie Walter Feit und John G. Thompson 1963 in einer 250 Seiten langen Arbeit [2] bewiesen haben. Man muß sich vor Augen halten, daß ja 1963 noch nicht alle einfachen Gruppen bekannt waren; der Satz von Feit und Thompson besagte daher: Eine nichtabelsche endliche einfache Gruppe, sei sie schon bekannt oder noch unbekannt, muß eine

gerade Ordnung haben. Dieses Resultat hatte die Arbeit der Gruppentheoretiker einen großen Schritt vorangebracht, denn die Anwendung des Satzes von Sylow liefert die Existenz von Untergruppen der Ordnung 2 in nichtabelschen einfachen Gruppen. Elementare Überlegungen zeigen, daß dann sogar 4 ein Teiler der Ordnungen solcher Gruppen sein muß.

4 Die alternierenden Gruppe

Bevor wir auf den Klassifikationssatz für die endlichen einfachen Gruppen etwas näher eingehen, wollen wir die kleinste nichtabelsche einfache Gruppe beschreiben. Diese Gruppe hat die Ordnung 60 und die Bezeichnung A_5. Sie ist Mitglied der oben schon erwähnten unendlichen Serie der alternierenden Gruppen A_m für ganze Zahlen $m \geq 2$. Es gilt $|A_m| = (1 \cdot 2 \cdot 3 \cdot ... \cdot m)/2$; die Ordnung von A_m ist also gleich $\frac{m!}{2}$. Man hat daher $|A_5| = (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5)/2 = 60$. Alle Gruppen A_m mit $m \geq 5$ sind nichtabelsche einfache Gruppen. Die nun folgende Definition von A_5 liefert durch analoge Betrachtungen unmittelbar alle übrigen Gruppen A_m.

Wir stellen uns vor, es seien fünf Objekte gegeben. Diese Objekte symbolisieren wir durch die Ziffern 1, 2, 3, 4 und 5; das soll heißen: 1 ist das Objekt Nummer 1, 2 das Objekt Nummer 2, usw. Unsere Objekte können wir durch Nebeneinanderschreiben von links nach rechts anordnen. Als Standardanordnung wählen wir $O_1 =< 1, 2, 3, 4, 5 >$. Andere Anordnungen sind z. B. $O_2 =< 2, 1, 3, 4, 5 >$, $O_3 =< 1, 3, 2, 4, 5 >$, $O_4 =< 5, 4, 3, 2, 1 >$. Wieviele

solche Anordnungen gibt es? Nun, es stehen uns im ganzen fünf Objekte zur Verfügung: Um die erste Stelle in $<,,,,>$ zu besetzen, haben wir fünf Möglichkeiten; um die zweite Stelle zu besetzen, haben wir noch vier Möglichkeiten, da für die erste Stelle schon ein Objekt verbraucht ist; für die dritte Stelle bleiben drei Möglichkeiten, da ja für die erste und die zweite Stelle schon zwei von den fünf Objekten verbraucht sind, usw. Es folgt daher, daß es genau $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5! = 120$ verschiedene mögliche Anordnungen für unsere fünf Objekte gibt; oben haben wir vier dieser 120 Anordnungen explizit angegeben.

Den Übergang von der Standardanordnung O_1 auf eine beliebige Anordnung O_i nennt man eine Permutation der Objektmenge (oder Ziffernmenge) $\{1, 2, 3, 4, 5\}$. Betrachten wir einmal den Übergang $O_1 \rightarrow O_2$ von O_1 auf O_2. Man kann $O_1 \rightarrow O_2$ folgendermaßen beschreiben: 1 geht auf 2, 2 geht auf 1, 3 geht auf 3, 4 geht auf 4, 5 geht auf 5. Für diesen Übergang $O_1 \rightarrow O_2$ führen wir die Bezeichnung $(1, 2)$ ein. Dies soll uns sagen, daß 1 auf 2 geht, daß 2 auf 1 geht und daß alle übrigen Objekte festbleiben. Betrachten wir den Übergang $O_1 \rightarrow O_4$, so erhalten wir als neue Bezeichnung für diese Permutation $(1, 5)(2, 4)$: Das bedeutet, daß 1 auf 5, daß 5 auf 1, daß 2 auf 4, daß 4 auf 2 übergeht und daß 3 festbleibt. Man muß hierbei stets beachten, daß in einer Klammer ( ) aufeinanderfolgende Elemente aufeinander abgebildet werden und daß das letzte Element einer Klammer auf das erste derselben abgebildet wird; deshalb bezeichnen z. B. $(1, 2, 3, 4)$ und $(3, 4, 1, 2)$ dieselbe Permutation. Betrachten wir z. B. die Permutation $(1, 2, 3)$. Welchen Übergang beschreibt sie? Da hier 1 in 2, 2 in 3 und 3 in 1 übergeht, und die Objekte 4 und 5 nicht vorkommen, erhält man den Übergang $< 1, 2, 3, 4, 5 > \rightarrow < 2, 3, 1, 4, 5 >$; die

Objekte 4 und 5 behalten jeweils ihre Plätze. Die Permutation zum Übergang $O_1 \to O_1$ bezeichnen wir mit E; hier bleibt jedes Element auf seinem Platz. Nichts wird bewegt; E nennt man die identische Permutation.

Im folgenden verwenden wir für die Permutationen der Menge {1,2,3,4,5} nur noch unsere Kurzbezeichnungen. Die Menge S_5 der 120 Permutationen ist eine Gruppe. Um dies sagen zu können, müssen wir auf S_5 eine Verknüpfung $\circ$ vereinbaren, so daß $(S_5, \circ)$ die Eigenschaften A1 bis A4 besitzt. Wie man nun zwei Elemente aus S_5 verknüpft, werden wir an einigen Beispielen klarmachen. Der Einfachheit halber werden wir für zwei Elemente a und b aus S_5 anstelle von $a \circ b$ einfach ab schreiben und ab das Produkt von a und b nennen; hierbei hat man die Reihenfolge zu beachten.

Seien $a = (1,2)(3,4)$, $b = (1,3)(2,4)$, $u = (1,3)$, $v = (2,3)$ Elemente aus S_5. Wir „berechnen“ $ab = (1,2)(3,4)(1,3)(2,4)$ zu $(1,4)(2,3)$; dieses Ergebnis erhalten wir, indem wir auf jeweils eine der Ziffern 1, 2, 3, 4, 5 von links nach rechts die aufeinanderfolgenden Permutationen des Produktes ab anwenden: Also, was geschieht mit 1?; die Permutation $(1,2)$ schickt 1 auf 2, $(3,4)$ läßt 2 fest, $(1,3)$ läßt 2 fest, $(2,4)$ schickt 2 auf 4. Wir wissen jetzt, daß ab die Ziffer 1 auf 4 abbildet. Was geschieht mit 4 unter ab?; $(1,2)$ läßt 4 fest, $(3,4)$ schickt 4 auf 3, $(1,3)$ schickt 3 auf 1, $(2,4)$ läßt 1 fest. Also erhalten wir, daß die Ziffern 1 und 4 unter Anwendung von ab miteinander vertauscht werden. Ebenso sieht man, daß die Ziffern 2 und 3 unter ab vertauscht werden. Damit erhalten wir $ab = (1,4)(2,3)$. Man bemerke, daß die Ziffer 5 weder von a noch von b oder ab bewegt wird. Die Permutation ab beschreibt übrigens den Übergang

$< 1, 2, 3, 4, 5 > \rightarrow < 4, 3, 2, 1, 5 >$ in unserer ursprünglichen Schreibweise.

Man stellt fest, daß $ab = ba$ gilt. Wir nennen deshalb die beiden Elemente a und b vertauschbar. Daß nicht alle Elemente von S_5 vertauschbar sind, sieht man anhand der Gleichungen

$$uv = (1, 3)(2, 3) = (1, 2, 3)$$

und

$$vu = (2, 3)(1, 3) = (1, 3, 2)$$

Da uv die Ziffer 3 auf 1 abbildet, aber vu die Ziffer 3 auf 2 abbildet, muß $uv \neq vu$ gelten.

Daß S_5 mit der angegebenen Verknüpfung eine Gruppe ist, prüft man nun mühelos nach. Z. B. spielt E die Rolle des neutralen Elementes von S_5. Wir haben unter anderem gezeigt, daß S_5 eine nichtabelsche Gruppe der Ordnung 120 ist.

Eine Permutation der Form (r, s), wobei r und s zwei verschiedene Elemente der Menge {1,2,3,4,5} sind, heißt Transposition. Eine Transposition ist eine Vertauschung zweier Ziffern. Wir benötigen noch die Tatsache, daß jede Permutation als Produkt von Transpositionen geschrieben werden kann. Nehmen wir z. B. die Permutation $x = (1, 3, 2, 5, 4)$. Man sieht, daß man x als Produkt der Transpositionen $(1, 3)$, $(1, 2)$, $(1, 5)$, $(1, 4)$ erhält, wenn man diese vier Transpositionen in der angegebenen Reihenfolge miteinander multipliziert. Es ist leicht zu sehen und für unsere Überlegungen wichtig, daß die Untermenge A_5

von S_5, die aus allen Permutationen besteht, die als ein Produkt einer geraden Anzahl von Transpositionen geschrieben werden können, eine Untergruppe von S_5 ist. Die Untergruppe A_5 hat genau 60 Elemente und ist die kleinste nichtabelsche einfache Gruppe. Daß A_5 einfach ist, ist so einfach nicht zu zeigen. Wir überzeugen uns jedoch schnell davon, daß A_5 nicht abelsch ist. Die Elemente $(1,2,3)$ und $(1,2,3,4,5)$ sind beide als Produkte von jeweils einer geraden Anzahl von Transpositionen darstellbar. Da $(1,2,3)(1,2,3,4,5) = (1,3,2,4,5)$ jedoch $(1,2,3,4,5)(1,2,3) = (1,3,4,5,2)$ gilt, kann A_5 nicht abelsch sein; denn das erste Produkt schickt 2 in 4 und das zweite Produkt schickt 2 in 1. – Indem wir in unseren Überlegungen die Zahl 5 durch eine beliebige Zahl m, die größer als 1 ist, ersetzen, erhalten wir für jedes solche m die sogenannte alternierende Gruppe A_m des Grades m und der Ordnung $\frac{m!}{2}$. Ist $m \geq 5$, so ist die Gruppe A_m nichtabelsch und einfach.

5 Der Klassifikationssatz

Im Zuge unserer Erörterungen haben wir bis jetzt als einfache endliche Gruppen einige der „sporadischen“ Gruppen nämlich J_1, M_{11}, M_{12}, M_{22}, M_{23}, M_{24} herausgestellt und die alternierenden Gruppen behandelt. Ferner haben wir die Ordnungen der unendlich vielen einfachen Gruppen $GL(m,2)$ für $m \geq 3$ angegeben. Die Gruppe $GL(m,2)$ gehört zu den sogenannten Gruppen vom Lie-Typ. Die Gruppen vom Lie-Typ zerfallen in 16 jeweils unendliche Serien von einfachen Gruppen; einige dieser Serien hängen von zwei Parametern ab, so daß man für jeden festen Wert von unendlich vielen möglichen Werten eines

Parameters schon unendlich viele einfache Gruppen erhält. Der Bezeichnung „sporadisch“ für die oben aufgeführten Gruppen liegt das Phänomen zugrunde, daß diese Gruppen nicht als Mitglieder unendlicher Serien auftreten.

Wir sind jetzt in der Lage den Klassifikationssatz für die endlichen einfachen Gruppen zu formulieren:

Satz 1 *Jede nichtabelsche endliche einfache Gruppe ist eine Gruppe vom Lie-Typ, eine alternierende Gruppe oder eine der folgenden 26 sporadischen Gruppen:* M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, J_1, J_2, J_3, J_4, HS, $Co1$, $Co2$, $Co3$, He, Mc, Suz, $M(22)$, $M(23)$, $M(24)'$, Ly, Ru, ON, F_5, F_3, F_2, F_1.

Daniel Gorenstein, welcher die Bedeutung der Arbeiten von J. G. Thompson [5] und von W. Feit und J. G Thompson [2] für ein Programm zur Bestimmung aller endlichen einfachen Gruppen frühzeitig erkannt hatte, und dessen nie versiegender Zuversicht in die erfolgreiche Durchführung dieses Vorhabens es schließlich mit zu verdanken war, daß das angestrebte Ziel auch erreicht wurde, beginnt die Einleitung zu seinem Buch „The Classification of Finite Simple Groups“ [3] mit den folgenden Worten: „Never before in the history of mathematics has there been an individual theorem whose proof has required 10,000 journal pages of closely reasoned argument. Who could read such a proof, let alone communicate it to others? But the classification of all finite simple groups is such a theorem – its complete proof, developed over a 30-year period by about 100 group theorists, is the union of some 500 journal articles covering approximately 10,000 printed pages.“ Und einige Zeilen später fährt

Gorenstein fort: „For it is almost impossible for the uninitiated to find the way through the tangled proof without an experienced guide; even the 500 papers themselves require careful selection from among some 2,000 articles on simple group theory, which together include often attractive byways, but which serve only to delay the journey.“

6 Zum Beweis des Satzes

Versetzen wir uns zurück in die Mitte der 60er Jahre. Damals kannte man die 16 Serien der Gruppen vom Lie-Typ, die alternierenden Gruppen, die fünf Gruppen von Mathieu und die Janko-Gruppe J_1. Wie geht man – sich in dieser Situation befindend – vor, wenn man zeigen will, daß alle endlichen einfachen Gruppen bekannt sind? Nun, man nimmt an, daß es unbekannte nichtabelsche einfache Gruppen gibt. Unter allen diesen unbekannten Gruppen gibt es eine Gruppe G minimaler Ordnung. Eine solche Gruppe G hat dann die folgenden Eigenschaften:

a) $|G|$ ist eine gerade Zahl;

b) Ist U eine von G verschiedene einfache Untergruppe von G, so ist U bekannt;

c) G ist eine neue einfache Gruppe.

Das Ziel ist es, unter diesen Voraussetzungen für G einen Widerspruch herzuleiten oder zu zeigen, daß es eine solche Gruppe G tatsächlich gibt, in welchem Falle die Vermutung, daß man schon alle einfachen Gruppen kenne,

falsch war; dieses G gehört dann sogleich zur Menge der bekannten einfachen Gruppen. Man erkennt unschwer den induktiven Charakter des Ansatzes.

Interessant ist, daß man damals – wohl aufgrund der noch nicht genügend ausgereiften Methoden – nicht in der Lage war, eine solche neue einfache Gruppe G minimaler Ordnung zu finden, obwohl es eine solche gab, wie wir heute wissen. Die restlichen sporadischen Gruppen wurden auf den verschiedensten Wegen gefunden.

Der Satz von Feit und Thompson legt es nahe, daß den Untergruppen von 2-Potenzordnung einer einfachen Gruppe ganz hervorragende Bedeutung zukommt. Die Gruppe He der Ordnung 4.030.387.200 ist auf folgende Weise entdeckt worden [4]. Nach dem Satz von Sylow besitzt die Gruppe $GL(5,2)$ Untergruppen T der Ordnung 2. Außer dem neutralen Element n besitzt so ein T ein Element t, welches $t^2 = n$ erfüllen muß; ein solches Element wird allgemein als Involution bezeichnet. Das Studium der Untergruppe $C(t)$ derjenigen Elemente von $GL(5,2)$ – für eine gewisse fest gewählte Involution t in $GL(5,2)$ –, die alle mit t vertauschbar sind, liefert $|C(t)| = 2^{10} \cdot 3 \cdot 7$; man nennt $C(t)$ den Zentralisator der Involution t in $GL(5,2)$. Indem man eine analoge Untersuchung für M_{24} anstellt, erfährt man überraschenderweise, daß es in M_{24} eine Involution t_1 gibt derart, daß der Zentralisator $C(t_1)$ von t_1 in M_{24} ebenfalls die Ordnung $2^{10} \cdot 3 \cdot 7$ hat und sogar, daß diese beiden Zentralisatoren die gleiche Struktur haben; es gibt nämlich einen Homomorphismus f von $C(t)$ in $C(t_1)$ mit $f(C(t)) = C(t_1)$ und $f(t) = t_1$. Es stellt sich sogleich die Aufgabe, nach allen endlichen einfachen Gruppen zu fahnden, die eine Involution z enthalten

derart, daß der Zentralisator $C(z)$ von z die gleiche Struktur wir $C(t)$ hat. Natürlich ist die Gruppe vom Lie-Typ $GL(5,2)$ und auch die Mathieu-Gruppe M_{24} eine solche Gruppe. Es stellte sich jedoch 1968 heraus, daß es noch eine dritte einfache Gruppe geben mußte, die bis dahin unbekannte einfache Gruppe der Ordnung $2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$; vgl. [4].

Z. Janko fand die Gruppen J_2 , J_3 und J_4, indem er hypothetische einfache Gruppen untersuchte, die einen „künstlichen“ Zentralisator $C(t)$ einer Involution t enthielten; dabei war ein Zentralisator künstlich, wenn er in keiner der bereits bekannten Gruppen vorkam. Nach unzähligen Versuchen und mit der dadurch gesammelten Erfahrung trat das Unwahrscheinliche ein: Janko stieß auf zwei fruchtbare Zentralisatoren. Der eine lieferte die beiden Gruppen J_2 und J_3, der andere J_4. Die einfache Gruppe J_4 war diejenige sporadische Gruppe, die als letzte entdeckt wurde.

Methoden, wie sie eben anhand von M_{24}, $GL(5,2)$, He, J_2, J_3 und J_4 beschrieben worden sind, lieferten eine große Zahl von Erkennungssätzen. D. h., arbeitete man in einer zunächst noch unbekannten einfachen Gruppe und konnte man z. B. feststellen, daß der Zentralisator einer ihrer Involutionen die gleiche Struktur wie derjenige einer Involution z. B. in J_2 hatte, so wußte man, daß die vorliegende Gruppe J_2 oder J_3 sein mußte.

Erkennungssätze dieser Art sind von ehemaligen Studenten des Fachbereichs Mathematik der Universität Mainz bewiesen worden. Die meisten dieser Ergebnisse sind auch heute noch unverzichtbare Bestandteile des Beweises

des Klassifikationssatzes; sie sind nicht von der Entwicklung immer schärfer werdender Methoden überrollt worden. Es waren vor allem Frau Kai Nah Cheng und die Herren Bert Beisiegel, Ulrich Dempwolff, Franz-Josef Fritz, Wolfgang Lempken, Arthur Reifart, Volker Stingl und Gernot Stroth, die zu den Kennzeichnungen endlicher einfacher Gruppen beitrugen. Im Jahre 1976 hatte Jürgen Bierbrauer seine Kennzeichnung der unendlichen Serie $E_7(2^m)$ von Gruppen vom Lie-Typ fertiggestellt; auf eine Veröffentlichung hatte er jedoch verzichtet, weil sein Ergebnis etwas früher von einem anderen Mathematiker erzielt worden war. Die Bestimmung aller einfachen Gruppen, deren Ordnungen nicht durch 2^{11} teilbar sind – es handelt sich hierbei um eine unendliche Menge einfacher Gruppen –, ist das Werk besonders von B. Beisiegel und V. Stingl; es fließen jedoch Ergebnisse von fast allen eben genannten Gruppentheoretikern ein; dabei müssen auch die Arbeiten von Ulrich Schoenwaelder aus Aachen erwähnt werden, der zeitweilig in der Richtung der Mainzer Forschungsgruppe arbeitete. Das 2^{11}-Resultat schaffte unter anderem mit einem Schlag Klarheit über die von Marshall Hall, Jr. mit Computermethoden ermittelten möglichen Ordnungen einfacher Gruppen unterhalb einer Million.

In den Anhängen M und N zu seinem 1911 erschienenen Buch „Theory of Groups of Finite Order“ [1] rätselt W. Burnside – Professor der Mathematik an der Royal Naval Academy – über die Möglichkeit der Existenz nichtabelscher einfacher Gruppen ungerader Ordnung. Er berichtet von Bemühungen der zeitgenössischen Mathematiker, zu zeigen, daß es wenigstens für kleine Ordnungen keine solchen Gruppen gibt.

Burnside geht dort ferner auf die exzeptionelle Natur der Mathieu-Gruppen ein. Er schreibt: „These apparently sporadic simple groups would probably repay a closer examination than they have yet received.“ Mit dieser Bemerkung bewies Burnside eine beträchtliche Weitsicht: Viele der später entdeckten sporadischen einfachen Gruppen involvieren in der einen oder anderen Weise die Mathieu-Gruppen.

Der Abschluß des Beweises des Klassifikationssatzes für endliche einfache Gruppen im Jahre 1981 ist für die Entwicklung der Theorie der endlichen Gruppen ein markanter Einschnitt. Sind doch jetzt die Elementarbausteine – nämlich die einfachen Gruppen – bekannt, aus denen sich endliche Gruppen überhaupt zusammensetzen können.

Literatur

[1] W. Burnside, Theory of Groups of Finite Order, Dover Publications, Inc. (1955); unabridged republication of the second edition published in 1911 by Cambridge University Press.

[2] W. Feit und J. G. Thompson, Sovability of Groups of Odd Order, Pacific J. Math. 13 (1963), 775–1029.

[3] Daniel Gorenstein, The Classification of Finite Simple Groups, Volume 1: Groups of Noncharacteristic 2 Type; Plenum Press New York and London (1983).

[4] D. Held, The Simple Groups related to M_{24}, Journal of Algebra 13, 253-296 (1969).

[5] J. G. Thompson, Nonsolvable Finite Groups all of whose local subgroups are solvable: I–VI. Bull. Amer. Math. Soc. 74 (1968), 383–437; Pacific J. Math. 33 (1970), 451–536; 39 (1971), 483–534; 48 (1973), 511–592; 50 (1974), 215–297; 51 (1974), 573–630.

Die 26 sporadischen einfachen Gruppen

Name	Ordnung	Entdecker/Konstrukteur	Jahr
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11 = 7.920$	Mathieu	1861
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11 = 95.040$	Mathieu	1861
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 443.520$	Mathieu	1873
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 10.200.960$	Mathieu	1873
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 244.823.040$	Mathieu	1873
J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 = 175.560$	Janko	1964
J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7 = 604.800$	Janko/Hall	1966
J_3	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19 = 50.232.960$	Janko/G. Higman, McKay	1966
J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$	Janko/Norton, Parker,	1975
	$= 86.775.571.046.077.562.880$	Benson, Conway, Thackray	
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11 = 44.325.000$	Higman,Sims	1967
Co_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$	Conway	1968
	$= 4.157.776.806.543.360.000$		
Co_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23 = 42.305.421.312.000$	Conway	1968
Co_3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23 = 495.766.656.000$	Conway	1968
He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17 = 4.030.387.200$	Held/G. Higman, McKay	1968
Mc	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 = 898.128.000$	McLaughlin	1968
Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 = 448.345.497.600$	Suzuki	1968
$M(22)$	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 = 64.561.751.654.400$	Fischer	1969
$M(23)$	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	Fischer	1969
	$= 4.089.470.473.293.004.800$		

Name	Ordnung	Entdecker/Konstrukteur	Jahr
$M(24)'$	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$	Fischer	1969
	$= 1.255.205.709.190.661.721.292.800$		
Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$	Lyons/Sims	1970
	$= 51.765.179.004.000.000$		
Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29 = 145.926.144.000$	Rudvalis/Conway, Wales	1972
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/Sims,Leon	1973
	$= 4.154.781.481.226.426.191.177.580.544.000.000$		
ON	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31 = 460.815.505.920$	O'Nan/Sims	1973
F_5	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$	Thompson/Smith	1974
	$= 90.745.943.887.872.000$		
F_3	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19 = 273.030.912.000.000$	Harada, Norton, Scmith	1974
F_1	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3$	Fischer, Griess	1974
	$\cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$		
	$= 808.017.424.794.512.875.886.459.904.961.$		
	$710.757.005.754.368.000.000.000$		

Die Entdeckung einer einfachen Gruppe G beinhaltete nicht immer auch den Beweis ihrer Existenz. Wenn G nicht gerade als Operatorgruppe einer geometrisch strukturierten Objektmenge gefunden wurde, mußte zum Beweis ihrer Existenz oft ein Computer herangezogen werden. Die theoretisch ermittelte Ordnung von G und eine reichhaltige Information über die Untergruppen von G waren gewöhnlich die Ausgangspunkte für eine Computerkonstruktion. Heutzutage sind die Existenzbeweise für die meisten der sporadischen Gruppen computerfrei.