Konstruktion endlicher auflösbarer Gruppen

R. Laue, Lehrstuhl II für Mathematik
Universität Bayreuth

Ein wesentlicher Schritt zur Konstruktion endlicher auflösbarer Gruppen ist nach [3] die Bestimmung der Konjugiertenklassen von p'-Gruppen in $GL(n,p)$. Man kann sich nach [3] dabei auf einige kleinere Untergruppen von $GL(n,p)$ beschränken. Hier betrachten wir die monomiale Gruppe $M_n = Z_{p-1} \wr S_n$ und Untergruppen der Ordnung q, wobei $2 \neq q | p-1$ gilt und p, q Primzahlen sind.

1. Repräsentantensysteme

Sei $GF(p)^* = \langle z \rangle$. Dann hat $x = z^{\frac{p-1}{q}}$ die Ordnung q. Zu geeigneter Basis hat ein $u \in GL(n,p)$ der Ordnung q die Matrixdarstellung $u = diag(x^{e_1}, \ldots, x^{e_n})$. Die Abbildung

$$log_x : (B_n)_q \longrightarrow V(n,q) : diag(x^{e_1}, \ldots, x^{en}) \longmapsto (e_1, \ldots, e_n)$$

ist dann ein Homomorphismus der q-Sylowgruppe $(B_n)_q$ der Basisgruppe B_n von M_n in $V(n,q)$, der die Operation von S_n überträgt. Ist $GF(q)^* = \langle y \rangle$, so ist

$$log_y : V(n,q) \longrightarrow [-1, q-2]^n : (e_1, \ldots, e_n) \longmapsto (a_1, \ldots, a_n)$$

mit $a_i = -1$ falls $e_i = 0$ und $a_i = c$ falls $e_i = y^c$ eine Abbildung, die die Operation von S_n überträgt.

Erzeuger von Untergruppen der Ordnung q von B_n transformieren wir durch beide Abbildungen, um durch die *lexikographisch kleinsten* $(a_1, \ldots, a_n)$ die Konjugiertenklassen von Untergruppen von B_n einfach beschreiben zu können.

Repräsentanten $(a_1, \ldots, a_n)$, die ein $a_i = -1$ enthalten, ergeben sich aus den Repräsentanten für $n-1$ durch Voranstellen einer -1. Für die Tupel $(a_1, \ldots, a_n)$ ohne -1 können wir mit Permutationen $0 \leq a_1 \leq a_2 \leq \ldots \leq a_n$ erreichen. Potenzieren in B_n geht über in die Addition einer Konstanten aus Z_{q-1} zu jedem a_i. Die lexikographisch kleinsten Repräsentanten der $S_n \times Z_{q-1}$

Bahnen besitzen mindestens einen 0-Eintrag und lassen sich durch keine Subtraktion eines festen a_i von allen a_j und zyklisches Vertauschen der i-ten Position an die erste Stelle auf ein lexikographisch kleineres Tupel transformieren. Das ergibt für kleine n folgende Repräsentantensysteme:

$$\begin{array}{ll} n=1: & \{(0)\}. \\ n=2: & \{(-1,0)\} \cup \{(0,i) \mid 0 \le i \le \frac{q-1}{2}\}. \\ n=3: & \{(-1,i,j) \mid (i,j) \text{ Repräsentant für } n=2\} \cup \\ & \{(0,i,j) \mid 0 \le i \le \frac{q-1}{3}, 2\cdot i \le j \le q-1-i\} \\ & \text{zusätzlich} \quad (0, \frac{q-1}{3}, 2\cdot\frac{q-1}{3}) \quad \text{falls} \quad q \equiv 1 mod 3. \end{array}$$

$$\begin{array}{ll} n=4: & \{(-1,i,j,k) \mid (i,j,k) \text{ Repräsentant für } n=3\} \cup \{(0,0,0,k) \mid 0 \le k < q-1\} \cup \\ & \{(0,0,j,j) \mid 0 \le j \le \frac{q-1}{2}\} \cup \{(0,0,j,k) \mid 1 \le j < k < q-1\} \cup \\ & \{(0,i,j,k) \mid 1 \le i \le \frac{q-1}{4}, 2\cdot i \le j < q-1, u \le k < q-i-1 \\ & \text{mit} \quad u = i+j \quad \text{falls} \quad j \le \frac{q-1}{2} \quad \text{und} \quad u = i+j+1 \quad \text{sonst } \} \\ & \text{zusätzlich} \quad (0, \frac{q-1}{4}, 2\cdot\frac{q-1}{4}, 3\cdot\frac{q-1}{4}) \quad \text{falls} \quad q \equiv 1 mod 4. \end{array}$$

Diese Darstellung ist unabhängig von p. Durch Bestimmen primitiver Elemente und Potenzieren erhält man daraus die Lösung des Ausgangsproblems. Insbesondere erhält man leicht alle Isomorphietypen von Gruppen $(Z_p)^n Z_q$ für $n \le 4$. für $n = 4$ und $GF(p)^* = \langle z \rangle, \quad b = z^{\frac{p-1}{q}}$ und $GF(q)^* = \langle y \rangle$ ist die (a_1, a_2, a_3, a_4) entsprechende Gruppe

$$G = \langle x_1, x_2, x_3, x_4, x_5 | \quad \text{Für} \quad 1 \le i \le j \le 4 \quad \text{ist} \quad x_i^p = 1, [x_i, x_j] = 1, x_5^q = 1, x_i^{x_5} = x_i^{c_i} \rangle$$

wobei

$$c_i = \begin{cases} 1 & \text{falls} \quad a_i = -1 \\ b^{y^{a_i}} & sonst \end{cases} \qquad \text{für} \quad 1 \le i \le 4.$$

Für $n = 2$ wurden die Gruppen implizit von O. Hölder[2] beschrieben, und A. Rottländer [4] zeigte, daß $\frac{q-3}{2}$ dieser Gruppen den gleichen Untergruppenverband besitzen.

2. Anzahlen.

Satz: Sei $k(U, GL(n,p))$ die Anzahl der Konjugiertenklassen zu U isomorpher Untergruppen von $GL(n,p)$. Dann gilt im Falle $U \cong Z_q, \quad q|p-1, \quad q \neq 2$ die Rekursionsformel

$$\begin{aligned} k(Z_q, GL(1,p)) &= 1, \\ k(Z_q, GL(n,p)) &= k(Z_q, GL(n-1,p)) + \frac{1}{q-1} \sum_{d|ggT(n,q-1)} \phi(d) \cdot \frac{\left[\frac{q-1}{d}\right]^{\frac{n}{d}}}{\left(\frac{n}{d}\right)!}, \end{aligned} \tag{1}$$

wobei $[r]^s = r(r+1)\cdots(r+s-1)$ die steigenden Faktoriellen bezeichnet.

Beweis des Satzes. Wie bei den Repräsentantenmengen reicht es hier, nur Tupel $(e_1, \ldots, e_n)$ zu betrachten, bei denen jedes $e_i \neq -1$ ist. Um die Bahnen von Z_{q-1} zu zählen, die auf der Menge der Bahnen von S_n auf der Menge der n-Tupel mit Einträgen aus Z_{q-1} existieren, wenden wir das Lemma von Cauchy-Frobenius an. Zu $a \in Z_{q-1}$ ist $(e_1, \ldots, e_n)^{S_n}$ ein Fixpunkt, wenn die e_i eine Multimenge der Mächtigkeit n bilden, bei der zu jedem a-Zyklus einer Länge l stets l gleiche Elemente auftreten. Nun besitzt a für $d = ggT(a, q-1)$ genau d Zyklen der Länge $\frac{q-1}{d}$. Wir haben also nur dann Fixpunkte, wenn $d|n$ gilt, und dann ist die Anzahl gleich der Anzahl der Bahnen von $S_{\frac{n}{d}}$ auf $\{0, 1, \ldots, q-1\}^{\{1, \ldots, \frac{n}{d}\}}$, also gleich $\frac{1}{\left(\frac{n}{d}\right)!} \cdot \left[\frac{q-1}{d}\right]^{\frac{n}{d}}$, siehe [1, Seite 75].

Da zu festen $d|ggT(n, q-1)$ genau $\phi(d)$ Elemente a mit dieser Bahnenzerlegung existieren, folgt die Formel.

References

[1] Aigner, M.: Combinatorial Theory. Springer Verlag New York 1970.

[2] Hölder, O.: Die Gruppen der Ordnung p^3, pq^2, pqr, p^4 Math. Ann. 43(1893),301-412.

[3] Laue, R.: Zur Konstruktion und Klassifikation endlicher auflösbarer Gruppen. Bayreuther Math. Schr. 9(1982)

[4] Rottländer, A.: Nachweis der Existenz nicht-isomorpher Gruppen von gleicher Situation der Untergruppen. Math. Z. 28(1928),641-653.