Beiträge zur Algebra und Geometrie
4 (1975), 9–14

Über die Untergruppen der elementarabelschen Gruppen

LOTHAR TESCHKE

Die vorliegende Arbeit beschäftigt sich mit den elementarabelschen Gruppen, also den endlichen abelschen Gruppen mit Primzahlexponent. Obwohl diese Gruppen strukturell gut überschaubar sind und auch für die Anzahl der Untergruppen mit gegebener Ordnung explizite Formeln vorliegen, scheint eine Aufzählung der Untergruppen mit Hilfe gewisser, in natürlicher Weise gewonnener Parametersysteme noch nicht vorgenommen worden zu sein. Wir wollen eine solche Aufzählung geben, wobei wir ein kombinatorisches Ergebnis von PÓLYA und ALEXANDERSON [1] heranziehen werden.

1. Bezeichnungen

Es sei $\mathfrak{G}$ die Gruppe bestehend aus den p^m m-Tupeln

$$(a_1, a_2, \ldots, a_m),$$

wobei die Koordinaten a_i aus dem Galois-Feld $GF(p)$ von p Elementen (p Primzahl) zu wählen sind. Die Verknüpfung der m-Tupel soll in der Weise geschehen, daß entsprechende Koordinaten addiert werden.
Wir vereinbaren weiter, daß ein m-Tupel, bei dem gewisse der m Koordinaten mit $k_1, k_2, \ldots, k_r$ bezeichnet sind, eine Untermenge von $\mathfrak{G}$ repräsentieren soll, und zwar die Menge der m-Tupel, die dadurch entsteht, daß sämtliche k_i unabhängig voneinander alle Elemente von $GF(p)$ durchlaufen. Danach gilt z. B. $\mathfrak{G} = (k_1, k_2, \ldots, k_m)$.

2. Untergruppen der Ordnung p

Für $0 \leqq r \leqq m$ ist bekanntlich die Anzahl der Untergruppen der Ordnung p^r von $\mathfrak{G}$ gleich dem Gaußschen Binomialkoeffizienten

$$\begin{bmatrix} m \\ r \end{bmatrix} = \frac{(p^m - 1)(p^{m-1} - 1) \cdots (p^{m-r+1} - 1)}{(p - 1)(p^2 - 1) \cdots (p^r - 1)},$$

falls man noch zusätzlich

$$\begin{bmatrix} m \\ 0 \end{bmatrix} = 1$$

setzt (vgl. z. B. [2], S. 109).
So ist speziell

$$\begin{bmatrix} m \\ 1 \end{bmatrix} = \frac{p^m - 1}{p - 1} = p^{m-1} + p^{m-2} + \cdots + p + 1$$

die Anzahl der Untergruppen der Ordnung p von $\mathfrak{G}$, die gemäß der in 1. getroffenen Vereinbarung folgendermaßen angegeben werden können:

$$\begin{array}{lll} 1 & \text{Untergruppe } \mathfrak{H}^{(1)} & = (0, 0, \ldots, 0, k_1), \\ p & \text{Untergruppen } \mathfrak{H}^{(1)}_{u_1} & = (0, 0, \ldots, 0, k_1, u_1 k_1), \\ & \vdots & \\ p^s & \text{Untergruppen } \mathfrak{H}^{(1)}_{u_1 \ldots u_s} & = (\underbrace{0, \ldots, 0}_{m-s-1}, k_1, u_1 k_1, u_2 k_1, \ldots, u_s k_1), \\ & \vdots & \\ p^{m-1} & \text{Untergruppen } \mathfrak{H}^{(1)}_{u_1 \ldots u_{m-1}} & = (k_1, u_1 k_1, u_2 k_1, \ldots, u_{m-1} k_1), \end{array}$$

wobei die Parameter u_i unabhängig voneinander alle Elemente von $GF(p)$ durchlaufen sollen und jeweils für eine bestimmte Gruppe fest zu wählen sind.
Denn zunächst sind die angegebenen Mengen von p Elementen Untergruppen von $\mathfrak{G}$, da offensichtlich die Verknüpfung nicht aus ihnen herausführt. Zum anderen sind die aufgeführten $(p^m - 1)/(p - 1)$ Untergruppen paarweise verschieden, wie sich aus der allgemeinen Betrachtung in 3.2. ergibt.

3. Untergruppen der Ordnung p^r, $0 \leqq r \leqq m$

Nun wollen wir in Verallgemeinerung von 2. Untergruppen der Ordnung p^r betrachten:

3.1. Ein m-Tupel repräsentiert vereinbarungsgemäß eine Untermenge von p^r Elementen von $\mathfrak{G}$, wenn r Koordinaten gleich gewissen k_i, z. B. $k_1, k_2, \ldots, k_r$, sind. Die übrigen $m-r$ Koordinaten sollen jetzt Linearkombinationen zwischen diesen k_i und bestimmten Parametern u_j sein, die wie bisher alle Elemente von $GF(p)$ durchlaufen sollen, aber für eine bestimmte Menge fest zu wählen sind. Dabei sollen in einer solchen Linearkombination nur diejenigen der r Variablen k_i vorkommen, die links von der betrachteten Koordinate stehen.
Für $m = 4$ und $r = 2$ kann man z. B. auf diese Weise folgende Untermengen von $\mathfrak{G}$ bilden:

$$\begin{array}{lll} 1 & \text{Untermenge } \mathfrak{H}^{(2)} & = (0, 0, k_1, k_2), \\ p & \text{Untermengen } \mathfrak{H}^{(2)}_{u_1} & = (0, k_1, u_1 k_1, k_2), \\ p^2 & \text{Untermengen } \bar{\mathfrak{H}}^{(2)}_{u_1 u_2} & = (0, k_1, k_2, u_1 k_1 + u_2 k_2), \\ p^2 & \text{Untermengen } \bar{\bar{\mathfrak{H}}}^{(2)}_{u_1 u_2} & = (k_1, u_1 k_1, u_2 k_1, k_2), \\ p^3 & \text{Untermengen } \mathfrak{H}^{(2)}_{u_1 u_2 u_3} & = (k_1, u_1 k_1, k_2, u_2 k_1 + u_3 k_2), \\ p^4 & \text{Untermengen } \mathfrak{H}^{(2)}_{u_1 u_2 u_3 u_4} & = (k_1, k_2, u_1 k_1 + u_2 k_2, u_3 k_1 + u_4 k_2). \end{array}$$

Wie man sich schnell überzeugen kann, führt aus den so erklärten Mengen die Verknüpfung nicht heraus, es handelt sich also um Untergruppen von $\mathfrak{G}$. Außerdem sind diese Untergruppen paarweise verschieden, was sich aus den in 3.2. folgenden Betrachtungen ergibt. Wegen

$$p^4 + p^3 + 2p^2 + p + 1 = \begin{bmatrix} 4 \\ 2 \end{bmatrix}$$

haben wir in unserem Spezialfall alle Untergruppen gefunden.

Wir wollen nun zeigen, daß auch im allgemeinen Fall durch unser Vorgehen eine Aufzählung der Untergruppen p^r-ter Ordnung geleistet wird. Die Untergruppeneigenschaft liegt auf der Hand. Der Nachweis für die Vollständigkeit der Aufzählung aller Untergruppen der Ordnung p^r ist erbracht, sobald wir gezeigt haben, daß die Anzahl der konstruierten Untergruppen $\begin{bmatrix} m \\ r \end{bmatrix}$ ist. Wir unterteilen zu diesem Zweck die Gesamtheit der gebildeten Untergruppen wie folgt in Klassen: Zwei Untergruppen liegen genau dann in derselben Klasse, wenn in den sie repräsentierenden m-Tupeln die k_i jeweils in denselben Koordinaten stehen.
Ist dabei α die Anzahl der für die Klasse als variabel angesehenen Koeffizienten u_j, so soll die Klasse als α-Klasse bezeichnet werden.

3.2. Die so erklärten Klassen sind trivialerweise nicht leer. Außerdem sind sie paarweise elementefremd.
Denn bei zwei verschiedenen Klassen stehen die k_i, $1 \leqq i \leqq r$, in den sie repräsentierenden m-Tupeln nicht alle in denselben Koordinaten. Es muß deshalb eine natürliche Zahl s geben, so daß in der s-ten Koordinate des einen m-Tupels ein k_j und des anderen eine Linearkombination steht. Wählen wir s mit dieser Eigenschaft minimal, so hätte das repräsentierende m-Tupel einer in beiden Klassen liegenden Untergruppe (in diesem m-Tupel sind die u_i also fest zu wählen) einmal die Form

$$(\ldots, k_1, \ldots, k_2, \ldots, k_{j-1}, \ldots, k_j, \ldots)$$

und zum anderen die Form

$$(\ldots, k_1, \ldots, k_2, \ldots, k_{j-1}, \ldots, u_{t+1}k_1 + u_{t+2}k_2 + \cdots + u_{t+j-1}k_{j-1}, \ldots).$$

Im ersten m-Tupel ist die s-te Koordinate unabhängig von der Festlegung der Variablen $k_1, k_2, \ldots, k_{j-1}$ frei wählbar, während diese Koordinate im zweiten m-Tupel durch die Wahl dieser Variablen eindeutig festgelegt ist. Beide m-Tupel können also niemals dieselbe Untergruppe repräsentieren.
Zur Bestimmung der Anzahl der Untergruppen in einer α-Klasse betrachten wir zwei Untergruppen $\bar{\mathfrak{H}}$ und $\bar{\bar{\mathfrak{H}}}$ aus einer solchen Klasse. Das repräsentierende m-Tupel von $\bar{\mathfrak{H}}$ werde durch das α-Tupel $(\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_\alpha)$ und von $\bar{\bar{\mathfrak{H}}}$ durch $(\bar{\bar{u}}_1, \bar{\bar{u}}_2, \ldots, \bar{\bar{u}}_\alpha)$ festgelegt. Die Variablen $k_1, k_2, \ldots, k_r$ stehen in beiden m-Tupeln in denselben Koordinaten, in den übrigen Koordinaten befinden sich Linearkombinationen. Steht in irgendeiner Koordinate des m-Tupels von $\bar{\mathfrak{H}}$ die Linearkombination

$$\bar{u}_{t+1}k_1 + \bar{u}_{t+2}k_2 + \cdots + \bar{u}_{t+j}k_j, \tag{1}$$

so finden wir in derselben Koordinate des m-Tupels von $\bar{\bar{\mathfrak{H}}}$ die Linearkombination

$$\bar{\bar{u}}_{t+1}k_1 + \bar{\bar{u}}_{t+2}k_2 + \cdots + \bar{\bar{u}}_{t+j}k_j, \qquad 1 \leqq j \leqq r. \tag{2}$$

Gilt nun $\bar{\mathfrak{H}} = \bar{\bar{\mathfrak{H}}}$, so muß zu jedem j-Tupel $(\bar{k}_1, \bar{k}_2, \ldots, \bar{k}_j)$ ein j-Tupel $(\bar{\bar{k}}_1, \bar{\bar{k}}_2, \ldots, \bar{\bar{k}}_j)$ existieren, so daß (1) für

$$k_1 = \bar{k}_1, k_2 = \bar{k}_2, \ldots, k_j = \bar{k}_j$$

denselben Wert liefert wie (2) für

$$k_1 = \bar{\bar{k}}_1, k_2 = \bar{\bar{k}}_2, \ldots, k_j = \bar{\bar{k}}_j.$$

Wählt man nun ein $\bar{k}_l$ gleich Eins und alle übrigen $\bar{k}_i$ gleich Null, so ergibt sich durch Betrachtung der vorangehenden Koordinaten

$$\bar{\bar{k}}_l = 1 \qquad \text{und} \qquad \bar{\bar{k}}_i = 0 \qquad \text{für } i \neq l,$$

und man erhält

$$\bar{u}_{t+l} = \bar{\bar{u}}_{t+l}, \qquad 1 \leqq l \leqq j.$$

Wir haben somit gezeigt, daß $\bar{\mathfrak{H}}$ genau dann mit $\bar{\bar{\mathfrak{H}}}$ übereinstimmt, wenn die α-Tupel ihrer u_i gleich sind. Da für jede Koordinate u_i eines α-Tupels die Werte $0, 1, \ldots, p-1$ möglich sind, enthält jede α-Klasse genau p^α verschiedene Untergruppen.

3.3. Weiterhin beachten wir, daß der Gaußsche Binomialkoeffizient $\begin{bmatrix} m \\ r \end{bmatrix}$, wenn wir einmal p für den Moment als Variable ansehen, nicht nur eine rationale, sondern, wie in [1] gezeigt wird, sogar eine ganze rationale Funktion von p ist:

$$\begin{bmatrix} m \\ r \end{bmatrix} = \sum_{\alpha=0}^{r(m-r)} A_{m,r,\alpha} \cdot p^\alpha.$$

In [1] wird für die ganzen rationalen Zahlen $A_{m,r,\alpha}$ folgende kombinatorische Interpretation gegeben: In einem rechtwinkligen Koordinatensystem sei ein „Zickzackweg" ein kürzester Weg zwischen den Punkten $(0, 0)$ und $(r, m-r)$, wobei man nur Strecken benutzen darf, die parallel zu den Achsen verlaufen und Punkte mit ganzen Zahlen als Koordinaten verbinden. Es gilt dann:
$A_{m,r,\alpha}$ ist gleich der Anzahl der „Zickzackwege", deren Fläche unter dem Weg α ist; diese Fläche ist begrenzt durch den Weg, die x-Achse und die Gerade $x = r$.

3.4. Wir geben nun eine eineindeutige Abbildung zwischen der Menge der „Zickzackwege" mit der Eigenschaft, daß die Fläche unter ihnen α ist, und der Menge der α-Klassen an, womit der Vollständigkeitsnachweis erbracht ist.
Es sei ein „Zickzackweg" von $(0, 0)$ bis $(r, m-r)$ gegeben, so daß die Fläche unter dem Weg gleich α ist. Diese Fläche zerlegen wir durch Parallelen zur y-Achse in Rechtecke R_s, deren Basisseite die Strecke von $(r-s, 0)$ bis $(r-s+1, 0)$ mit der Länge 1 sei, $1 \leqq s \leqq r$ (vgl. Abb. 1). Bezeichnen wir die Höhe von R_s mit h_s, so gilt infolgedessen

$$\sum_{s=1}^{r} h_s = \alpha. \tag{3}$$

Die endliche Folge $h_1, h_2, \ldots, h_r$ besteht aus nichtnegativen Zahlen und muß, da es sich bei einem „Zickzackweg" um einen kürzesten Weg handeln soll, schwach monoton fallend sein. Umgekehrt kennzeichnet eine endliche Folge nichtnegativer

Zahlen $h_1, h_2, \ldots, h_r$ eindeutig einen „Zickzackweg", unter dem die Fläche α ist, falls sie schwach monoton fallend ist und (3) erfüllt.

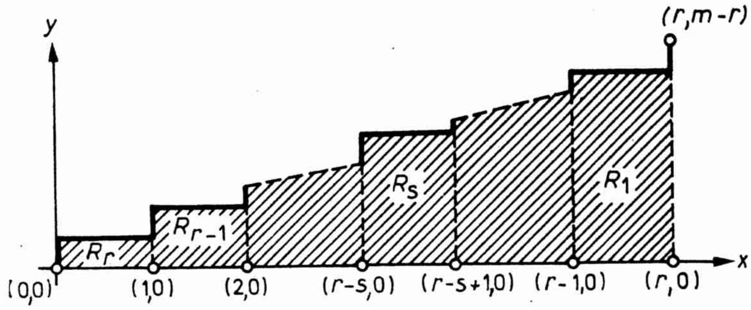

Abb. 1

Wir konstruieren nun zu einem solchen „Zickzackweg" eine α-Klasse durch die Vorschrift, daß

$$k_s \quad \text{in der } (m - r + s - h_s)\text{-ten Koordinate} \tag{4}$$

stehen soll, $1 \leqq s \leqq r$. Da aus $s < s'$ und $h_s \geqq h_{s'}$ sofort $s - h_s < s' - h_{s'}$ folgt, ist die Nummer der Koordinate, in der k_s steht, durch die Angabe von s eindeutig festgelegt. In diesem m-Tupel tauchen genau α Parameter u_j auf. Denn da k_s in der $(m - r + s - h_s)$-ten Koordinate steht, gibt es infolgedessen

$$m - (m - r + s - h_s) = r + h_s - s$$

Koordinaten rechts von k_s. Da noch $k_{s+1}, \ldots, k_r$ rechts von k_s auftauchen, gibt es

$$(r + h_s - s) - (r - s) = h_s$$

Koordinaten rechts von k_s, in denen Linearkombinationen stehen. In allen diesen Linearkombinationen taucht ein Produkt $u_j k_s$ auf. Also liefert jedes k_s genau h_s Parameter u_j. Im ganzen m-Tupel gibt es also nach (3) genau α Parameter u_j.
Damit wird durch (4) jedem „Zickzackweg", unter dem die Fläche α ist, eindeutig eine α-Klasse zugeordnet.
Bei dieser Zuordnung (4) ist jede α-Klasse Bild eines und nur eines „Zickzackweges": Steht nämlich k_s in dem m-Tupel der α-Klasse in der t_s-ten Koordinate, so folgt aus (4) sofort

$$h_s = m - r + s - t_s, \qquad 1 \leqq s \leqq r.$$

Die endliche Folge der so erhaltenen Zahlen $h_1, h_2, \ldots, h_r$ ist schwach monoton fallend, denn aus $t_s < t_{s+1}$ folgt $m - r + s - h_s < m - r + s + 1 - h_{s+1}$ und daraus $h_{s+1} \leqq h_s$. Die Zahlen sind außerdem nichtnegativ, da wegen $t_r \leqq m$

$$h_r = m - r + r - t_r \geqq 0$$

ist. In dem m-Tupel der vorgegebenen α-Klasse tauchen genau α Parameter u_j auf. Wie vorhin gezeigt wurde, liefert jedes k_s genau h_s Parameter u_j. Also muß die Summe aller dieser h_s gleich α sein.
Damit ist vollständig gezeigt, daß durch (4) eine eineindeutige Abbildung der Menge der „Zickzackwege", unter denen die Fläche α ist, auf die Menge der α-Klassen angegeben wird.

3.5. Die in [1] angegebene Beziehung

$$\sum_{\alpha=0}^{r(m-r)} A_{m,r,\alpha} = \binom{m}{r}$$

entspricht bei uns der Tatsache, daß es genau $\binom{m}{r}$ verschiedene Möglichkeiten gibt, $k_1, k_2, \ldots, k_r$ auf die m vorhandenen Koordinaten zu verteilen.

LITERATUR

[1] PÓLYA, G., and G. L. ALEXANDERSON: Gaussian Binomial Coefficients. Elem. Math. *26* (1971), 102–109.
[2] ZASSENHAUS, H.: Lehrbuch der Gruppentheorie I. B. G. Teubner, Leipzig–Berlin 1937.

Manuskripteingang: 4. 10. 1972

VERFASSER:

LOTHAR TESCHKE, Sektion Mathematik/Physik der Pädagogischen Hochschule Halle