ACTA ARITHMETICA
XXX (1976)

Über Permutationsgruppen die durch Tschebyscheff-Polynome erzeugt werden

von

RUDOLF LIDL und WINFRIED B. MÜLLER (Wien)

Sei $\mathrm{GF}(q)$ das Galoisfeld der Ordnung q. Ein Polynom $f(x) \in \mathrm{GF}(q)[x]$ heißt ein Permutationspolynom von $\mathrm{GF}(q)$, wenn die Abbildung

$$\pi\colon\ a \to f(a), \qquad a \in \mathrm{GF}(q),$$

eine Permutation der Elemente von $\mathrm{GF}(q)$ ist. Analog nennt man einen Polynomvektor

$$\big(f(x, y), g(x, y)\big) \in \big(\mathrm{GF}(q)[x, y]\big)^2$$

Permutationspolynomvektor von $\mathrm{GF}(q)$, wenn die Abbildung

$$\pi\colon\ (a, b) \to \big(f(a, b), g(a, b)\big), \qquad (a, b) \in \mathrm{GF}(q)^2,$$

eine Permutation der Elemente von $\mathrm{GF}(q)^2$ ist.

In mehreren bisherigen Arbeiten über Permutationspolynome und Permutationspolynomvektoren hat man sich mit dem Problem befaßt, abgeschlossene Klassen von Permutationspolynomen und Permutationspolynomvektoren gegenüber der Komposition zu finden und die durch diese Klassen erzeugten Permutationsgruppen zu studieren. Dabei wurden vor allem Klassen von Dickson-Polynomen (vgl. [1]) und die aus ihnen durch Verallgemeinerung folgenden Klassen von Tschebyscheff-Polynomvektoren untersucht.

Das Dickson-Polynom $g_k(a, x)$ über $\mathrm{GF}(q)$ wird für natürliches k definiert durch

$$g_k\Big(a, u + \frac{a}{u}\Big) = u^k + \frac{a^k}{u^k}, \tag{1}$$

mit $a \in \mathrm{GF}(q)$ und $u \in \mathrm{GF}(q^2)$. Mittels der Waringschen Formel bekommt man die Darstellung

$$g_k(a, x) = \sum_{t=0}^{\left[\frac{k}{2}\right]} \frac{k}{k-t}\binom{k-t}{t}(-a)^t x^{k-2t}. \tag{2}$$

Die in (1) definierten Dickson-Polynome kann man folgenderweise verallgemeinern:

$$
\begin{aligned}
g_1^{(k)}(a, x, y) &= u^k + v^k + \frac{a^k}{u^k v^k}, \\
g_2^{(k)}(a, x, y) &= u^k v^k + \frac{a^k}{u^k} + \frac{a^k}{v^k},
\end{aligned} \tag{3}
$$

für $x = u + v + \frac{a}{uv}$, $y = uv + \frac{a}{u} + \frac{a}{v}$ und $a \in \mathrm{GF}(q)$, $u, v \in \mathrm{GF}(q^6)$. Wegen des Zusammenhanges der Polynome $g_k(a, x)$ mit den Tschebyscheff-Polynomen $T_k(x)$ erster Art (vgl. etwa [4]),

$$
g_k(a, x) = 2(\sqrt{a})^k T_k\left(\frac{x}{2\sqrt{a}}\right), \tag{4}
$$

werden die Polynome $g_1^{(k)}(a, x, y)$ und $g_2^{(k)}(a, x, y)$ nach [3] Tschebyscheff-Polynome in 2 Veränderlichen über $\mathrm{GF}(q)$ genannt. Der Polynomvektor

$$
\mathfrak{g}_k = \left(g_1^{(k)}(a, x, y), g_2^{(k)}(a, x, y)\right)
$$

wird als Tschebyscheff-Polynomvektor bezeichnet. Wie im eindimensionalen Fall erhält man mit Hilfe der Waringschen Formel

$$
\begin{aligned}
g_1^{(k)}(a, x, y) &= \sum_{i=0}^{\left[\frac{k}{2}\right]} \sum_{j=0}^{\left[\frac{k}{3}\right]} \frac{k(-1)^i a^j}{k-i-2j} \binom{k-i-2j}{i+j} \binom{i+j}{i} x^{k-2i-3j} y^i, \\
g_2^{(k)}(a, x, y) &= \sum_{i=0}^{\left[\frac{k}{2}\right]} \sum_{j=0}^{\left[\frac{k}{3}\right]} \frac{k(-1)^i a^{i+2j}}{k-i-2j} \binom{k-i-2j}{i+j} \binom{i+j}{j} x^i y^{k-2i-3j}.
\end{aligned} \tag{5}
$$

Bezeichnet man nun mit $G_q(a)$ die Menge aller Permutationen von $\mathrm{GF}(q)$, die durch Polynome $g_k(a, x)$ dargestellt werden, so wurde in [6] gezeigt, daß $G_q(a)$ genau für $a = 0$, $a = 1$ und $a = -1$ abgeschlossen bezüglich der Komposition ist, also eine Gruppe bildet. Ebenso wurde in [3] bewiesen, daß auch die Menge $G_q^2(a)$ aller Permutationen von $\mathrm{GF}(q)^2$, die durch die Polynomvektoren $\mathfrak{g}_k = \left(g_1^{(k)}(a, x, y), g_2^{(k)}(a, x, y)\right)$ erzeugt werden, für $a = 0$, $a = 1$ und $a = -1$ und keine anderen eine Gruppe bildet.

Die Struktur der Gruppen $G_q(0)$, $G_q(1)$ und $G_q(-1)$ wurde bereits in [2] und [6] untersucht. Es wurde gezeigt, daß die Gruppe $G_q(0)$ isomorph zu einer primen Restklassengruppe der ganzen Zahlen ist und daß die Gruppen $G_q(1)$ und $G_q(-1)$ isomorph zu Faktorgruppen von primen Restklassengruppen der ganzen Zahlen nach elementar abelschen 2-Gruppen

sind. In [3] und [4] wurden die von der Klasse der Tschebyscheff-Polynomvektoren erzeugten Permutationsgruppen als Untergruppen der symmetrischen Gruppe auf den Elementen von $\mathrm{GF}(q)^2$ untersucht. Dabei stellte sich heraus, daß $G_q^2(0)$ isomorph zur Faktorgruppe einer primen Restklassengruppe der ganzen Zahlen nach einer elementar abelschen 2-Gruppe ist. Die Gruppen $G_q^2(1)$ und $G_q^2(-1)$ sind zueinander und zur Faktorgruppe einer primen Restklassengruppe der ganzen Zahlen nach der zyklischen Untergruppe der Ordnung 6 isomorph. Somit sind also alle hier untersuchten Permutationsgruppen abelsch.

Das Hauptziel der vorliegenden Arbeit ist es, Beziehungen und Vergleiche zwischen den einzelnen von Tschebyscheff- bzw. Dickson-Polynomen erzeugten Permutationsgruppen herzustellen. Da für den eindimensionalen Fall vor kurzem auch alle zyklischen Permutationsgruppen ermittelt werden konnten ([2], [7]), liegt es nahe, auch alle zyklischen Permutationsgruppen zu bestimmen, welche durch Polynomvektoren in 2 Unbestimmten induziert werden. Dabei stellt sich heraus, daß im Gegensatz zum eindimensionalen Fall die Gruppen $G_q^2(a)$ nur mehr für „triviale" q zyklisch sind.

Bezeichne im weiteren $P(m)$ stets die prime Restklassengruppe der ganzen Zahlen modulo einer ganzen Zahl m. Aus [3], [4] und [6] stellen wir die folgenden Ergebnisse zusammen:

(i) $G_q(0) \cong P(q-1)$;

(ii) $G_q(1) \cong P\left(\frac{q^2-1}{2}\right)/(1, -1, q, -q)$ für $q \neq 2^n$,
$G_q(1) \cong P(q^2-1)/(1, -1, q, -q)$ für $q = 2^n$;

(iii) $G_q(-1) \cong P\left(\frac{q^2-1}{2}\right)/(1, q)$ für $q \equiv 1 \bmod 4$,
$G_q(-1) \cong P(q^2-1)/(1, q)$ für $q \equiv 3 \bmod 4$,
$G_q(-1) = G_q(1)$ für $q = 2^n$;

(iv) $G_q^2(0) \cong P(q^2-1)/(1, q)$;

(v) $G_q^2(1) \cong P\left((q^2-1)(q^2+q+1)\right)/(1, q, q^2, q^3, q^4, q^5)$;

(vi) $G_q^2(-1) \cong G_q^2(1)$.

Wie schon in [2] gezeigt wurde, ist $G_q(1)$ stets homomorphes Bild der Gruppe $G_q(-1)$. Wir zeigen nun

Satz 1. *Die Gruppe $G_q(-1)$ ist stets homomorphes Bild der Gruppe $G_q^2(0)$. Der Homomorphismus ist ein Isomorphismus genau für $q = 2$ und $q \equiv 3 \bmod 4$.*

Beweis. Im folgenden bezeichne $A \xrightarrow{f} B$ stets, daß B homomorphes Bild von A ist.

a) $q \equiv 1 \bmod 4$. Dann gilt

$$(6)\quad G_q^2(0) \cong P(q^2-1)/(1,q) \xrightarrow{f} P(q^2-1)/\left(1, q, 1+\frac{q^2-1}{2}, q+\frac{q^2-1}{2}\right)$$
$$\cong P\left(\frac{q^2-1}{2}\right)/(1,q) \cong G_q(-1).$$

b) $q \equiv 3 \bmod 4$. In diesem Fall gilt

$$(7)\quad G_q^2(0) \cong P(q^2-1)/(1,q) \cong G_q(-1).$$

c) $q \equiv 0 \bmod 2$. Dann gilt

$$(8)\quad G_q^2(0) \cong P(q^2-1)/(1,q) \xrightarrow{f} P(q^2-1)/(1,-1,q,-q) \cong G_q(-1).$$

Da im Fall a) stets gilt:

$$1 \not\equiv 1+\frac{q^2-1}{2} \bmod (q^2-1), \quad 1 \not\equiv q+\frac{q^2-1}{2} \bmod (q^2-1),$$
$$q \not\equiv 1+\frac{q^2-1}{2} \bmod (q^2-1), \quad q \not\equiv q+\frac{q^2-1}{2} \bmod (q^2-1),$$

ist der Homomorphismus f in (6) nie ein Isomorphismus. Der Isomorphismus in (7) ist klar. Für $q=2$ ist der Homomorphismus f in (8) wegen $1 \equiv -1 \bmod 2$ ein Isomorphismus. Für $q>2$ gilt jedoch stets $1 \not\equiv -1 \bmod (q^2-1)$ und $1 \not\equiv -q \bmod (q^2-1)$.

Da die Gruppe $G_q(-1)$ nach [2] genau für die Zahlen $q=2,3,4$ und 5 zyklisch ist und bekanntlich jedes homomorphe Bild einer zyklischen Gruppe zyklisch ist, bekommt man auf Grund von Satz 1 nach leichter Rechnung

Satz 2. *Die Gruppe $G_q^2(0)$ ist außer für $q=2,3$ nie zyklisch.*

Satz 3. *Die Gruppe $G_{2^s}^2(0)$ ist für ungerades s homomorphes Bild der Gruppe $G_{2^s}^2(1)$.*

Beweis. Da für ungerades s gilt $(2^{2s}-1, 2^{2s}+2^s+1) = 1$, können wir folgende Kette von Homomorphismen betrachten:

$$G_{2^s}^2(1) \cong P\big((2^{2s}-1)(2^{2s}+2^s+1)\big)/(1, 2^s, 2^{2s}, 2^{3s}, 2^{4s}, 2^{5s})$$
$$\cong [P(2^{2s}-1)/(1,2^s)] \otimes [P(2^{2s}+2^s+1)/(1, 2^s, 2^{2s})]$$
$$\xrightarrow{f} P(2^{2s}-1)/(1,2^s) \cong G_{2^s}^2(0),$$

womit die Behauptung gezeigt ist.

Bemerkung. Dieselbe Schlußkette läßt sich für $q=2^s$ mit geradem s nicht anwenden, da dann wegen $2^{2s}+2^s+1 \equiv 0 \bmod 3$ und $2^{2s}-1 \equiv 0 \bmod 3$ diese beiden Zahlen nicht relativ prim sind.

Satz 4. *Die Gruppe $G_{3^s}^2(0)$ ist stets homomorphes Bild der Gruppe $G_{3^s}^2(1)$.*

Beweis.

$$G_{3^s}^2(1) \cong P\big((3^{2s}-1)(3^{2s}+3^s+1)\big)/(1, 3^s, 3^{2s}, 3^{3s}, 3^{4s}, 3^{5s})$$
$$\cong [P(3^{2s}-1)/(1,3^s)] \otimes [P(3^{2s}+3^s+1)/(1, 3^s, 3^{2s})]$$
$$\xrightarrow{f} P(3^{2s}-1)/(1,3^s) \cong G_{3^s}^2(0).$$

Satz 5. *Die Gruppe $G_q^2(0)$ mit $q \equiv 5 \bmod 6$ ist stets homomorphes Bild der Gruppe $G_q^2(1)$.*

Beweis.

$$G_q^2(1) \cong P\big((q^2-1)(q^3+q+1)\big)/(1, q, q^2, q^3, q^4, q^5)$$
$$\cong [P(q^2-1)/(1,q)] \otimes [P(q^2+q+1)/(1,q,q^2)] \xrightarrow{f} P(q^2-1)/(1,q) \cong G_q^2(0).$$

Mit Hilfe der Sätze 2 bis 5 und (vi) beweisen wir nun

Satz 6. *Die Gruppen $G_q^2(1)$ und $G_q^2(-1)$ sind außer für $q=2$ nie zyklisch.*

Beweis. a) $q=2^s$. Wegen $|G_2^2(1)| = 2$ ist $G_2^2(1)$ zyklisch. Auf Grund der Sätze 2 und 3 kann $G_{2^s}^2(1)$ für ungerades $s>1$ nicht zyklisch sein. Sei also s gerade. Dann gilt

$$G_{2^s}^2(1) \cong P\big((2^{2s}-1)(2^{2s}+2^s+1)\big)/(1, 2^s, 2^{2s}, 2^{3s}, 2^{4s}, 2^{5s}).$$

Wegen

$$2^{2s}-1 = (2^s+1)(2^s-1) \quad \text{und} \quad 2^{2s}+2^s+1 = (2^s-1)^2+3\cdot 2^s$$

können wir durch Wahl eines passenden e erreichen, daß die Zahlen

$$2^s+1, \quad \frac{2^s-1}{3^e}, \quad \frac{2^{2s}+2^s+1}{3}, \quad 3^{e+1}$$

untereinander paarweise teilerfremd sind und somit folgt:

$$(9)\quad P\big((2^{2s}-1)(2^{2s}+2^s+1)\big)/(1, 2^s, 2^{2s}, 2^{3s}, 2^{4s}, 2^{5s})$$
$$\xrightarrow{f} [P(2^s+1)/(1,2^s)] \otimes \left[P\left(\frac{2^s-1}{3^e}\right)\right] \otimes \left[P\left(\frac{2^{2s}+2^s+1}{3}\right)/(1, 2^s, 2^{2s})\right] \otimes$$
$$\otimes [P(3^{e+1})/(1, 2^s, 2^{2s}, 2^{3s}, 2^{4s}, 2^{5s})].$$

In (9) gilt stets

$$(10)\quad 2 \mid \frac{1}{3}\varphi\left(\frac{2^{2s}+2^s+1}{3}\right).$$

Ist nun $\frac{2^s-1}{3^e} = 1$, so folgt $2^s-1 = 3^e$, also $2^s \equiv 1 \bmod 3^e$. Da 2 stets Primitivwurzel $\bmod 3^e$ ist, gilt $s = t\cdot 2\cdot 3^{e-1}$, mit $t>0$. Wir erhalten damit $4^{t\cdot 3^{e-1}}-1 = 3^e$. Wie man leicht sieht, ist diese Gleichung nur

für $e = 1$ und $t = 1$ erfüllt und wir bekommen $s = 2$. In diesem Fall gilt jedoch für den direkten Faktor $P(2^s+1)/(1, 2^s)$ in (9): $2 \mid \frac{1}{2}\varphi(5)$, womit wegen (10) im direkten Produkt von (9) zwei Faktoren nicht teilerfremde Ordnungen besitzen und daher das direkte Produkt keine zyklische Gruppe ist. Ist hingegen $\frac{2^s-1}{3^e} > 1$, so gilt $2 \mid \varphi\left(\frac{2^s-1}{3^e}\right)$ und es haben dann in (9) die Ordnungen von $P\left(\frac{2^s-1}{3^e}\right)$ und $P\left(\frac{2^{2s}+2^s+1}{3}\right)/(1, 2^s, 2^{2s})$ stets mindestens den gemeinsamen Teiler 2.

b) $q = 3^s$. Wie sofort aus Satz 4 folgt, ist $G_{3^s}^2(1)$ höchstens dann zyklisch, wenn $G_{3^s}^2(0)$ zyklisch ist. Es bleibt also nur noch zu untersuchen, ob

$$G_3^2(1) \cong P(8 \cdot 13)/(1, 3, 3^2, 3^3, 3^4, 3^5) \cong [P(8)/(1, 3)] \otimes [P(13)/(1, 3, 3^2)]$$

zyklisch ist. Wegen $2 \mid \frac{1}{2}\varphi(8)$ und $2 \mid \frac{1}{3}\varphi(13)$ ist dies nicht der Fall.

c) $q \equiv 5 \bmod 6$. Dann ist $G_q^2(1)$ wegen der Sätze 2 und 5 nicht zyklisch.

d) $q \equiv 1 \bmod 6$. Durch Wahl eines passenden e können wir wiederum erreichen, daß die Zahlen

$$3^{3+1}; \quad \frac{q^2-1}{3^e} \text{ und } \frac{q^2+q+1}{3}$$

paarweise teilerfremd sind. Dann gilt

$$\begin{aligned}(11)\quad G_q^2(1) &\cong P\big((q^2-1)(q^2+q+1)\big)/(1, q, q^2, q^3, q^4, q^5) \\ &\xrightarrow{f} [P(3^{e+1})/(1, q, q^2, q^3, q^4, q^5)] \otimes \left[P\left(\frac{q^2-1}{3^e}\right)/(1, q)\right] \otimes \\ &\qquad \otimes \left[P\left(\frac{q^2+q+1}{3}\right)/(1, q, q^2)\right].\end{aligned}$$

Da stets $2 \mid \frac{1}{3}\varphi\left(\frac{q^2+q+1}{3}\right)$ und wegen $8 \mid \frac{q^2-1}{3}$ auch $2 \mid \frac{1}{2}\varphi\left(\frac{q^2-1}{3^e}\right)$ gilt, haben die Ordnungen der beiden letzten direkten Faktoren in (11) den gemeinsamen Teiler 2, womit gezeigt ist, daß $G_q^2(1)$ in diesem Fall nicht zyklisch ist.

Literaturverzeichnis

[1] L. E. Dickson, *Linear Groups with an Exposition of Galois Field Theory*, New York 1958.

[2] H. Hule und W. B. Müller, *Grupos ciclicos de permutaciones inducidas por polinomios sobre campos de Galois*, Erscheint in Anais da Academia Brasileira de Ciências 44.

[3] R. Lidl, *Tschebyscheffpolynome und die dadurch dargestellten Gruppen*, Monatsh. Math. 77 (1973), S. 132–147.

[4] — *Über die Struktur einer durch Tschebyscheffpolynome in 2 Variablen dargestellten Permutationsgruppe*, Beiträge zur Algebra und Geometrie 3 (1974), S. 41–48.

[5] W. Nöbauer, *Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen*, Monatsh. Math. 69 (1965), S. 230–238.

[6] — *Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen*, J. Reine Angew. Math. 231 (1968), S. 215–219.

[7] — *Über Gruppen von Dickson-Polynomfunktionen und einige damit zusammenhängende zahlentheoretische Fragen*, Monatsh. Math. 77 (1973), S. 330–344.

IV. INSTITUT FÜR MATHEMATIK
TECHNISCHE HOCHSCHULE WIEN

Eingegangen 8. 4. 1974
und in revidierter Form 14. 11. 1974 (560)