Beiträge zur Algebra und Geometrie
2 (1974), 55—59

Reguläre Polynome über endlichen Körpern

RUDOLF LIDL

Sei R ein kommutativer Ring mit Einselement, I ein Ideal von R. Ein Polynomvektor $\mathfrak{F} = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n))$ aus $R[x_1, \ldots, x_n]^n$ heißt Permutationspolynomvektor mod I, wenn die durch $\mathfrak{F}$ induzierte Abbildung von $(R/I)^n$ in sich eine Permutation ist (vgl. dazu [2], [6]). Die Komponenten eines solchen Polynomvektors heißen Permutationspolynome mod I. H. LAUSCH und W. NÖBAUER zeigen in [7] die beiden folgenden Sätze:

Sei Q Primärideal von R mit zugehörigem Primideal P, so daß R/Q endlich ist, $Q \neq P$. Ein Polynomvektor $\mathfrak{F}$ über R ist genau dann ein Permutationspolynomvektor mod Q, *wenn $\mathfrak{F}$ Permutationspolynomvektor* mod P *ist und für seine Funktionaldeterminante $\partial\mathfrak{F}$ gilt: $\partial\mathfrak{F} \equiv 0$* mod P *hat keine Lösung in R.*

Das Polynom $f(x_1, \ldots, x_n)$ ist genau dann Permutationspolynom mod Q, *wenn es Permutationspolynom* mod P *ist und keine der Kongruenzen*

$$\partial_i f(x_1, \ldots, x_n) \equiv 0 \bmod P, \quad i = 1, 2, \ldots, n,$$

eine Lösung in R besitzt.

In [4] wurden für den Fall $n = 1$ und $R =$ Integritätsbereich der ganzen rationalen Zahlen einige in der Literatur behandelte Typen von Permutationspolynomen in einer Unbestimmten daraufhin untersucht, ob sie Permutationspolynome für alle Potenzen einer Primzahl p sind. In dieser Arbeit werden für den Fall daß R ein endlicher Körper $K = GF(q)$ ist, $q = p^e$, p prim, $e \geqq 1$ natürlich, einige Klassen von Polynomvektoren betrachtet.

Definition. Ein Polynomvektor $\mathfrak{F}$ über K heißt *regulär*, wenn seine Funktionaldeterminante $\partial\mathfrak{F} \neq 0$ für alle $(a_1, \ldots, a_n) \in K^n$. Ein Polynom $f(x_1, \ldots, x_n)$ über K heißt regulär, wenn sein Gradient von 0 verschieden ist für alle $(a_1, \ldots, a_n) \in K^n$.

Auf Grund der Kettenregel erhalten wir sofort: Die Menge der regulären Polynomvektoren von $K[x_1, \ldots, x_n]^n$ bildet eine Teilhalbgruppe der Halbgruppe der Polynomvektoren. Ebenso unmittelbar einzusehen ist das Folgende: Die Menge der linearen Polynomvektoren über K ist eine Teilhalbgruppe der Halbgruppe der Polynomvektoren. *Die Menge der linearen Permutationspolynomvektoren bildet eine Untergruppe davon, deren Elemente reguläre Polynomvektoren sind.*

Ist die Char. $K \neq 2$, so wird in [2] gezeigt, daß alle quadratischen Permutationspolynome bis auf lineare Äquivalenz von der Form $x_1 + b_2 x_2^2 + \cdots + b_n x_n^2, b_i \in K$, sind. Daraus folgt: *Jedes quadratische Permutationspolynom ist ein reguläres Polynom.* Weiter gilt: *Der Potenzpolynomvektor* $(x_1^{k_1}, \ldots, x_n^{k_n})$ *ist ein regulärer Polynomvektor genau dann, wenn* $k_i = 1$, $i = 1, 2, \ldots, n$.

Nun untersuchen wir die verallgemeinerten Tschebyscheffpolynome (vgl. dazu [3]) in zwei Unbestimmten auf Regularität. Dazu betrachten wir das Polynom $r(z) = z^3 - u z^2 + v z - b$, $u, v \in K$.

Dieses Polynom hat drei nicht notwendig verschiedene Wurzeln in $GF(q^6)$. Diese seien $x, y, \frac{b}{xy}$, dann gilt:

$$r(z) = z^3 - \left(x + y + \frac{b}{xy}\right) z^2 + \left(xy + \frac{b}{x} + \frac{b}{y}\right) z - b = 0.$$

Sei k eine positive ganze Zahl, dann setzen wir

$$r^{(k)}(z) = z^3 - \left(x^k + y^k + \frac{b^k}{x^k y^k}\right) z^2 + \left(x^k y^k + \frac{b^k}{x^k} + \frac{b^k}{y^k}\right) z - b^k = 0.$$

Die k-ten Potenzsummen der Wurzeln von $r(z)$ kann man mit Hilfe der Waringschen Formel durch die Koeffizienten von $r(z)$ ausdrücken und erhält somit für die Tschebyscheffpolynome $g_1^k(u, v, b)$, $g_2^k(u, v, b)$ die folgenden Gleichungen:

$$\begin{aligned} g_1^k(u, v, b) &= x^k + y^k + \frac{b^k}{x^k y^k}, \\ g_2^k(u, v, b) &= x^k y^k + \frac{b^k}{x^k} + \frac{b^k}{y^k}; \end{aligned} \tag{1}$$

dabei gilt

$$\left.\begin{aligned} u &= x + y + \frac{b}{xy} \\ v &= xy + \frac{b}{x} + \frac{b}{y} \end{aligned}\right., \quad x, y \in GF(q^6); \quad u, v, b \in K. \tag{2}$$

Neben der expliziten Darstellung von g_1^k und g_2^k wird in [3] das folgende Kriterium gezeigt (für $n = 1$ siehe [5]):

Die Abbildung $(u, v) \to (g_1^k(u, v, b), g_2^k(u, v, b))$ ist genau dann eine Permutation von K^2, wenn gilt: $(k, q^s - 1) = 1$, $s = 1, 2, 3$ für $b \neq 0$ und $s = 1, 2$ für $b = 0$. (3)

Wir beweisen nun den

Satz. *Der Polynomvektor* $(g_1^k(u, v, b), g_2^k(u, v, b))$ *ist genau dann ein regulärer Permutationspolynomvektor über* K, *wenn gilt*: $b \neq 0$, $(k, p(q^s - 1)) = 1$, $s = 1, 2, 3$.

Beweis. Mit Hilfe der Formel (1) berechnen wir zunächst die Funktionaldeterminante von (g_1^k, g_2^k).

$$D = \begin{vmatrix} \frac{\partial g_1}{\partial x} & \frac{\partial g_1}{\partial y} \\ \frac{\partial g_2}{\partial x} & \frac{\partial g_2}{\partial y} \end{vmatrix} = \begin{vmatrix} \frac{\partial g_1}{\partial u} & \frac{\partial g_1}{\partial v} \\ \frac{\partial g_2}{\partial u} & \frac{\partial g_2}{\partial v} \end{vmatrix} \begin{vmatrix} \frac{\partial u}{\partial x} & \frac{\partial u}{\partial y} \\ \frac{\partial v}{\partial x} & \frac{\partial v}{\partial y} \end{vmatrix}$$

$$= \frac{k^2 (x^k - y^k)}{x^{2k+1} y^{2k+1}} (x^{3k} y^{3k} - b^k x^k y^k (x^k + y^k) + b^{2k}).$$

Wegen (2) folgt:

$$D = \frac{k^2 (x^k - y^k) (x^{3k} y^{3k} - b^k x^k y^k (x^k + y^k) + b^{2k})}{x^{2(k-1)} y^{2(k-1)} (x - y) (x^3 y^3 - b x y (x + y) + b^2)}$$

$$= \frac{k^2}{x^{2(k-1)} y^{2(k-1)}} \sum_{i=0}^{k-1} x^{k-1-i} y^i \left(\sum_{i=0}^{k-1} x^{3(k-1)-2i} y^{3(k-1)-2i} b^i \sum_{r=0}^{i} x^{i-r} y^r \right.$$

$$\left. + \sum_{j=0}^{k-2} x^j y^j b^{2(k-1)-j} \sum_{s=0}^{j} x^{j-s} y^s \right)$$

$$= \frac{k^2}{x^{2(k-1)} y^{2(k-1)}} h(x, y). \tag{4}$$

Daraus folgt $x^{2(k-1)} y^{2(k-1)} \cdot D = k^2 h(x, y)$. Da auf beiden Seiten ein Polynom steht, gilt diese Gleichung für jedes $x \neq 0$, $y \neq 0$ aus einem Erweiterungskörper von K. Ist (g_1^k, g_2^k) ein regulärer Permutationspolynomvektor von K^2, dann folgt aus (3) $(k, q^s - 1) = 1$ und aus obiger Gleichung $(k, p) = 1$.
Ist umgekehrt $(k, p(q^s - 1)) = 1$, dann ist (g_1^k, g_2^k) wegen (3) ein Permutationspolynomvektor. Es bleibt noch zu zeigen, daß dieser Polynomvektor auch regulär ist. Angenommen, es gäbe $u, v \in K$, so daß $D = 0$. Dann gibt es $x, y \in GF(q^6)$, so daß (2) und $h(x, y) = 0$ erfüllt sind. Es folgt also

$$(x - y) (x^3 y^3 - b x y (x + y) + b^2) h(x, y)$$
$$= (x^k - y^k) (x^{3k} y^{3k} - b^k x^k y^k (x^k + y^k) + b^{2k}) = 0.$$

Ist $x^k - y^k = 0$, dann gilt $x = y$ wegen $(k, q - 1) = 1$, und aus (4) folgt

$$D = \frac{k^2}{x^{4(k-1)}} k \cdot x^{k-1} \left(\sum_{i=0}^{k-1} b^i x^{3(k-1-i)} \right)^2.$$

Aus $x^6 - 2bx^3 + b^2$ folgt aber $x^3 = b$, also gilt $h(x, y) = k^2 b^{k-1} \neq 0$. Aus

$$x^{3k} y^{3k} - b^k x^k y^k (x^k + y^k) + b^{2k} = 0$$

folgt, daß x, y einer der beiden Gleichungen $x^{2k} y^k = b^k$ oder $x^k y^{2k} = b^k$ genügen müssen, d. h., es gilt $x^2 y = b$ oder $x y^2 = b$. Da $h(x, y)$ symmetrisch in x, y ist, gilt

$$h\left(x, \frac{b}{x^2}\right) = k\, b^{2(k-1)} \left(\sum_{i=0}^{k-1} x^{3(k-1-i)} b^i \right)^2$$

für $y = \frac{b}{x^2}$ und eine analoge Formel für $x = \frac{b}{y^2}$. In beiden Fällen ist wegen $(k, p) = 1$ $h(x, y) \neq 0$ im Widerspruch zur Annahme.

Wie in [4] gezeigt wird, sind für $n = 1$ sowohl die Tschebyscheffpolynome als auch die in [8] untersuchten Rédei-Funktionen reguläre Polynome. Wir geben zum Abschluß einen einfachen Zusammenhang zwischen diesen beiden Klassen von regulären Polynomen an. Sei Char. $K \neq 2$. Wir setzen

$$(x + \sqrt{a})^n = r_n(x) + s_n(x) \sqrt{a}, \quad \frac{r_n(x)}{s_n(x)} \text{ ist die Rédei-Funktion;}$$

$$(x - \sqrt{a})^n = r_n(x) - s_n(x) \sqrt{a}.$$

Durch Addition erhalten wir

$$2r_n(x) = (x + \sqrt{a})^n + \left(\frac{x^2 - a}{x + \sqrt{a}} \right)^n = g^k\left(x + \sqrt{a} + \frac{x^2 - a}{x + \sqrt{a}}, x^2 - a\right) = g^k(2x, x^2 - a).$$

Das heißt, das Tschebyscheffpolynom in der Variablen $2x$ und mit „Absolutglied" $x^2 - a$ ist identisch mit dem doppelten Zählerpolynom der Rédei-Funktion.

Ein offenes Problem ist, auf Grund eines analogen Zusammenhanges die den bekannten verallgemeinerten Tschebyscheffpolynomen in mehreren Unbestimmten entsprechenden verallgemeinerten Polynome zu finden, welche Zählerpolynome von verallgemeinerten Rédei-Funktionen in mehreren Unbestimmten sind.

LITERATUR

[1] ALEXANDROV, R. L.: Über die Tschebyscheffsche Gleichung. **Mathematika, Učen. Zap., Gos. Ped. Inst. Sverdlovsk (1967), 3–11.**

[2] LIDL, R.: Über Permutationspolynome in mehreren Unbestimmten. **Monatsh. Math. *75* (1971), 432–440.**

[3] LIDL, R., and C. WELLS: Chebyshev polynomials in several variables. J. reine und angew. Math. *255* (1972), 104–111.
[4] NÖBAUER, W.: Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen. Monatsh. Math. *69* (1965), 230–238.
[5] NÖBAUER, W.: Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen. J. reine u. angew. Math. *231* (1968), 215–219.
[6] NÖBAUER, W.: Zur Theorie der Polynomtransformationen und Permutationspolynome. Math. Ann. *157* (1964), 332–342.
[7] NÖBAUER, W., and H. LAUSCH: Algebra of polynomials. van Nostrand, Amsterdam 1973.
[8] RÉDEI, L.: Über eindeutig umkehrbare Polynome in endlichen Körpern. Acta. Sci. Math. Szeged *11* (1946), 85–92.

Manuskripteingang: 8. 9. 1971

VERFASSER:
RUDOLF LIDL, IV. Institut für Mathematik der Technischen Hochschule Wien