Verallgemeinerung eines Satzes über homogene Linearformen

Von L. RÉDEI in Szeged und H. J. WEINERT in Potsdam

Die Begriffsbildungen der vorangehenden Arbeit [1] verallgemeinern wir auf folgende Weise: Es sei $m > 1$ eine ganze Zahl und $R = \mathfrak{Z}/(m)$ der Restklassenring des Ringes $\mathfrak{Z}$ der ganzen Zahlen modulo m. Wir betrachten Systeme von r homogenen Linearformen in n Unbestimmten

$$\left.\begin{aligned} (1) \qquad L_\varrho(x_1, x_2, \ldots, x_n) &= \sum_{\nu=1}^{n} a_{\varrho,\nu} x_\nu \\ (2) \qquad K_\varrho(x_1, x_2, \ldots, x_n) &= \sum_{\nu=1}^{n} b_{\varrho,\nu} x_\nu \end{aligned}\right\} \quad (\varrho = 1, \ldots, r)$$

aus $R[x_1, x_2, \ldots, x_n]$. Ein n-tupel

$$(3) \qquad (\xi_1, \xi_2, \ldots, \xi_n) \in R^{[n]} = R \times R \times \ldots \times R$$

heiße *zulässig*, wenn wenigstens ein ξ_ν kein Nullteiler von R ist. Wir nennen ein System (1) (modulo m) *gleichverteilt*, wenn $m | r$ gilt und für jedes zulässige n-tupel (3) die r Werte

$$(4) \qquad L_\varrho(\xi_1, \xi_2, \ldots, \xi_n) = \sum_{\nu=1}^{n} a_{\varrho,\nu} \xi_\nu \qquad (\varrho = 1, \ldots, r)$$

gleichverteilt sind, d. h. alle Restklassen modulo m gerade $\frac{r}{m}$-mal ergeben. Dagegen sagen wir, daß die Systeme (1) und (2) *wertgleich* sind, wenn für jedes zulässige n-tupel (3) die r Werte $L_\varrho(\xi_1, \xi_2, \ldots, \xi_n)$ in ihrer Gesamtheit mit den r Werten $K_\varrho(\xi_1, \xi_2, \ldots, \xi_n)$ übereinstimmen. Weiterhin bezeichnen wir als *volles System* in n Unbestimmten das aus allen $r = m^n$ paarweise voneinander verschiedenen Linearformen von der Form (1) bestehende System.

Schließlich sagen wir, daß modulo m der *Gleichverteilungssatz* gilt, wenn *ein System* (1) *von r homogenen Linearformen in n Unbestimmten modulo m genau dann gleichverteilt ist, wenn* $m^n | r$ *gilt und es aus* $s = \frac{r}{m^n}$ *vollen Systemen besteht.* Dagegen sei modulo m der *Wertgleichheitssatz* erfüllt, wenn *zwei Systeme* (1) *und* (2) *von je r homogenen Linearformen in n Unbestimmten modulo m genau dann wertgleich sind, wenn diese Systeme übereinstimmen, also* $L_\varrho(x_1, x_2, \ldots, x_n) = K_\varrho(x_1, x_2, \ldots, x_n)$ *bei geeigneter Numerierung gilt.*

Für den Fall, daß der Modul $m=p$ eine Primzahl ist, haben wir in [1] den Gleichverteilungssatz bewiesen und den ihm entsprechenden Wertgleichheitssatz erwähnt. In dieser Note werden wir folgendes zeigen:

Satz 1. *Für jeden Modul m folgt aus dem Gleichverteilungssatz der Wertgleichheitssatz und umgekehrt.*

Satz 2. *Der Wertgleichheitssatz gilt für jeden Modul $m=p^\mu$, wobei p eine Primzahl ist.*

Bezüglich der Frage, ob Satz 2 auch für $m\neq p^\mu$ gilt, haben wir bisher nur Vermutungen.

Beweis von Satz 1. Als erstes sei modulo m der Gleichverteilungssatz erfüllt. Es genügt, die Annahme zum Widerspruch zu führen, daß zwei nichtidentische Systeme (1) und (2) modulo m wertgleich sind. Dabei möge in (1) ein und dieselbe Linearform maximal s-mal auftreten. Dann ist (1) ein Teilsystem von s vollen Systemen. Wechselt man in letzterem (1) gegen (2) aus, so entsteht ersichtlich wieder ein gleichverteiltes System von sm^n Linearformen, welches nicht aus s vollen Systemen besteht, im Widerspruch zum Gleichverteilungssatz.

Umgekehrt sei der Wertgleichheitssatz modulo m erfüllt. Wir nehmen jetzt an, daß es ein gleichverteiltes System (1) von r Linearformen modulo m gibt, welches nicht aus vollen Systemen besteht. Dieses System (1) nehmen wir in m^n Exemplaren und erhalten ein ebenfalls gleichverteiltes System von rm^n Linearformen, welches dann auch nicht aus vollen Systemen besteht. Es ist also von dem aus r vollen Systemen bestehenden System verschieden, aber mit diesem wertgleich. Dies widerspricht der Gültigkeit des Wertgleichheitssatzes.

Beweis von Satz 2. Wir schicken für $m=p^\mu$ folgende Hilfsüberlegungen voraus:

1. Die Anzahl der zulässigen n-tupel $(\xi_1, \xi_2, \ldots, \xi_n)$ beträgt

$$P(n,\mu) = m^n-(m-\varphi(m))^n = (p^\mu)^n-(p^{\mu-1})^n = p^{n(\mu-1)}(p^n-1).$$

2. Es sei $a_1x_1+a_2x_2+\ldots+a_nx_n\in R[x_1, x_2, \ldots, x_n]$ eine Linearform, in der wenigstens ein Koeffizient nicht Nullteiler von R ist; ohne Beschränkung der Allgemeinheit gelte etwa $p\nmid a_1$. Dann gibt es genau

$$P(n-1,\mu) = p^{(\mu-1)(n-1)}(p^{n-1}-1)$$

zulässige n-tupel $(\xi_1, \xi_2, \ldots, \xi_n)$, die

$$a_1\xi_1+a_2\xi_2+\ldots+a_n\xi_n \equiv cp^\varkappa \pmod{p^\mu} \tag{5}$$

erfüllen, wobei $1\leqq\varkappa\leqq\mu$ und $c\in\mathfrak{J}$ gilt. In der Tat gibt es zu jedem der $P(n-1,\mu)$ zulässigen $(n-1)$-tupeln $(\xi_2, \ldots, \xi_n)$ genau ein ξ_1, welches (5) erfüllt. Dagegen führt ein nicht zulässiges $(n-1)$-tupel $(\xi_2, \ldots, \xi_n)$ auch zu einem ξ_1 mit $p|\xi_1$, sodaß keine weiteren zulässigen Lösungen von (5) entstehen.

3. Es sei $a_1x_1+a_2x_2+\ldots+a_nx_n\in R[x_1, x_2, \ldots, x_n]$ eine Linearform mit $p^\tau|a_\nu$ $(1\leqq\tau<\mu)$ für alle a_ν, aber $p^{\tau+1}\nmid a_\nu$ für wenigstens ein a_ν. Wir schreiben dafür auch $p^\tau\|(a_1, \ldots, a_n)$, also p^τ ist der genaue p-Teiler des größten gemeinsamen Teilers

der a_ν. Dann gibt es genau $p^\tau P(n-1, \mu)$ zulässige n-tupel $(\xi_1, \xi_2, \ldots, \xi_n)$, die

$$a_1\xi_1 + a_2\xi_2 + \ldots + a_n\xi_n \equiv 0 \pmod{p^\mu} \tag{6}$$

erfüllen. In der Tat erhalten wir mit $a_\nu = p^\tau a'_\nu$ für jedes c mit $0 \leqq c < p^\tau$ gemäß 2. und

$$a'_1\xi_1 + a'_2\xi_2 + \ldots + a'_n\xi_n \equiv p^{\mu-\tau}c \bmod p^\mu \tag{7}$$

jeweils $P(n-1, \mu)$ n-tupel, die (6) erfüllen. Diese $p^\tau P(n-1, \mu)$ zulässigen n-tupel sind auch paarweise verschieden und die sämtlichen, welche (6) erfüllen. Letzteres erkennt man daraus, daß jede Lösung von (6) wegen

$$a_1\xi_1 + a_2\xi_2 + \ldots + a_n\xi_n = p^\tau p^{\mu-\tau}c$$

mit einem geeigneten $c \in \mathfrak{J}$ auch

$$a'_1\xi_1 + a'_2\xi_2 + \ldots + a'_n\xi_n = p^{\mu-\tau}c$$

erfüllt, also eine Lösung von (7) ist.

Der eigentliche Beweis unseres Satzes 2 beruht nun auf dem Gedanken, daß man von zwei wertgleichen, aber verschiedenen Systemen (1) und (2) zu ebensolchen übergehen könnte, bei denen die Linearform

$$0 = 0x_1 + 0x_2 + \ldots + 0x_n$$

zwar etwa in (1), aber nicht in (2) auftritt. Zunächst kann man nämlich erreichen, daß eine Linearform von (1), etwa L_1, nicht in (2) auftritt und dann zu den Systemen

$$L_\varrho - L_1 \quad \text{und} \quad K_\varrho - L_1 \qquad (\varrho = 1, \ldots, r)$$

übergehen. Weiterhin müssen wertgleiche Systeme, wenn in beiden alle zulässigen n-tupel $(\xi_1, \xi_2, \ldots, \xi_n)$ eingesetzt werden, gleich oft den Wert 0 ergeben.

Für $m = p$ [1]) kommen wir damit rasch zu einem Widerspruch, da die Linearformen

$$\sum a_\nu x_\nu \quad \text{von (1) bzw.} \quad \sum b_\nu x_\nu \quad \text{von (2)}$$

mit $p \nmid (a_1, \ldots, a_n)$ bzw. $p \nmid (b_1, \ldots, b_n)$ gemäß 2. nur für $P(n-1, 1) = p^{n-1} - 1$, die Linearform 0 aber für $p^n - 1$ zulässige n-tupel verschwinden. Für $m = p^\mu$ führen wir einen vollständigen Induktionsschluß nach μ durch, indem wir beide Systeme (1) und (2) modulo p^τ mit $\tau = 1, \ldots, \mu - 1$ betrachten. Die entstehenden Systeme sind auch modulo p^τ wertgleich, mithin nach Induktionsannahme identisch. Dies lehrt, daß in beiden Systemen jeweils gleichviele Linearformen auftreten, für die (mit von selbst klaren Bezeichnungen)

$$\begin{aligned}
&p \nmid (a_1, \ldots, a_n) \quad \text{bzw.} \quad p \nmid (b_1, \ldots, b_n) \\
&p \parallel (a_1, \ldots, a_n) \quad \text{bzw.} \quad p \parallel (b_1, \ldots, b_n) \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&p^{\mu-2} \parallel (a_1, \ldots, a_n) \quad \text{bzw.} \quad p^{\mu-2} \parallel (b_1, \ldots, b_n) \\
&p^{\mu-1} \mid (a_1, \ldots, a_n) \quad \text{bzw.} \quad p^{\mu-1} \mid (b_1, \ldots, b_n)
\end{aligned} \tag{8}$$

[1]) Natürlich ist der Fall $m = p$ schon in [1] erledigt worden.

erfüllt ist. In der letzten Zeile von (8) gilt dabei rechts sogar $p^{\mu-1} \| (b_1, \ldots, b_n)$, während links die Linearform 0 mit $p^{\mu} | (a_1, \ldots, a_n)$ wenigstens einmal auftritt. Die Anwendung von 3. ergibt, daß damit das System (1) für mehr n-tupel $(\xi_1, \xi_2, \ldots, \xi_n)$ verschwindet, als das System (2). Dieser Widerspruch zeigt, daß es modulo p^{μ} keine nichtidentischen, aber wertgleichen Systeme von Linearformen geben kann.

Literatur

[1] L. Rédei—H. J. Weinert, Ein Gleichverteilungssatz für Systeme homogener Linearformen modulo p, *Acta Sci. Math.*, **27** (1966),

(Eingegangen am 3. Februar 1965)