Sonderabdruck aus
ARCHIV DER MATHEMATIK
Vol. XXVII, 1976 BIRKHÄUSER VERLAG, BASEL UND STUTTGART Fasc. 3

Taktische Konfigurationen und die Gleichung $at^x + bt^y = c$ in kommutativen Ringen mit Eins

Von
ARNOLD NEUMAIER

0. Eine Klasse von taktischen Konfigurationen I mit den Eigenschaften (u. a.):

(I) Durch je zwei Punkte von I geht mindestens ein Block,

(II) Je zwei Blöcke von I haben mindestens einen Punkt gemeinsam,

kann charakterisiert werden durch die Lösbarkeit der Gleichung

(III) $$t^x - t^y = c$$

für alle c aus einem Ring S durch ganze Zahlen x, y; dabei ist t ein geeignetes invertierbares Element von S und die additive Gruppe von S fungiert als punkt- und blocktransitive Gruppe von Automorphismen von I (Abschnitt 12).

In dieser Arbeit werden einerseits notwendige, andererseits hinreichende Bedingungen für die Lösbarkeit von (III) hergeleitet, z. B.

a) Ist S ein assoziativer und kommutativer Ring mit Eins, und ist $at^x + bt^y = c$ für alle $c \in S$ durch ganze Zahlen x, y lösbar (a, b, t S fest; t invertierbar), so ist S endlich; ist darüber hinaus p eine Primzahl mit $p^2 \mid \text{Char. } S$, so ist die Menge

$$\{c \in S \mid p\,c \equiv 0 \bmod p^2\}$$

ein maximales Ideal von S (Abschnitt 10).

b) Ist S ein endlicher Körper mit q Elementen, t ein von 0 verschiedenes Element von S, und gilt für den Exponenten $d^{-1}(q-1)$ von t die Ungleichung $d^4 \leqq q - 4$, so ist (III) für alle $c \in S$ durch ganze Zahlen x, y lösbar (Abschnitt 11).

1. S sei kommutativer, assoziativer Ring mit Eins, $S^\times$ die Menge der invertierbaren Elemente von S. Weiter seien $a, b \in S$, $t \in S^\times$ fest gewählt.

Die Gleichung $at^x + bt^y = c$ ist genau dann für alle $c \in S$ lösbar, wenn gilt:

(a) $a \in S^\times$, $-a^{-1}b$ *ist eine Potenz von* t;

(b) *Die Gleichung* $t^x - t^y = c$ *ist für alle* $c \in S$ *lösbar.*

Denn gelten (a) und (b), so ist nach (a) $-a^{-1}b = t^w$, und nach (b) gibt es u, v mit $t^u - t^v = a^{-1}c$. Damit ist $at^u + bt^{v-w} = c$.

Ist andererseits $at^x + bt^y = c$ für alle $c \in S$ lösbar, so gibt es speziell u, v, w, z mit $at^u + bt^v = 0$ und $at^w + bt^z = 1$. Mit der Abkürzung $a' = t^w - t^{z+u-v}$ rechnet man leicht $aa' = 1$, $-a'b = t^{u-v}$ nach; daher gilt (a). Ist weiter $at^x + bt^y = ac$, so ist $t^x + t^{y+u-x} = c$, und daraus ergibt sich (b).

2. T sei eine Unbestimmte über dem Ring $\mathbb{Z}$ der ganzen Zahlen.

Satz. I. *Die Gleichung* $t^x - t^y = c$ *sei für alle* $c \in S$ *lösbar. Dann gibt es ein Ideal* Φ *von* $\mathbb{Z}[T^{-1}, T]$ *derart, daß gilt:*

(a) *S ist zum Restklassenring $\mathbb{Z}[T^{-1}, T]/\Phi$ isomorph und es gibt einen Isomorphismus, der t auf T abbildet.*

(b) $T^x - T^y \equiv F \bmod \Phi$ *ist für alle* $F \in \mathbb{Z}[T^{-1}, T]$ *lösbar.*

II. *Ist Φ ein Ideal von $\mathbb{Z}[T^{-1}, T]$ und gelten die Aussagen* (a) *und* (b), *so ist* $t^x - t^y = c$ *für alle* $c \in S$ *lösbar.*

Man kann nämlich

$$\Phi = \{F(T) \in \mathbb{Z}[T^{-1}, T] \mid F(t) = 0 \text{ in } S\}$$

setzen und erhält (a) und (b) unmittelbar. II ist trivial.

3. R sei ein Hauptidealring, T transzendent über R. Mit R_T soll der Ring

$$R_T := R[T^{-1}, T]$$

bezeichnet werden. Für $F \in R_T$, $F \neq 0$, also

$$F = \sum_{i=j}^{k} a_i T^i \qquad (a_j, a_k \neq 0) \tag{1}$$

sei — in Abweichung von der üblichen Definition — der Grad von F definiert als $|F| := k - j$. F soll normiert heißen, wenn in (1) $j = 0$ und $a_k = 1$ ist.

Mit $(A_1, \ldots, A_n)$ soll das von $A_1, \ldots, A_n$ erzeugte Ideal von R_T bezeichnet werden.

Die Aussage in Abschnitt 2 motiviert die Definition:

Ein Ideal Φ von R_T heißt d-Ideal, wenn die Kongruenz

$$T^x - T^y \equiv F \bmod \Phi \tag{2}$$

für alle $F \in R_T$ lösbar ist.

Ein triviales, immer vorhandenes d-Ideal ist $\Phi = R_T$. Unmittelbar aus der Definition folgt:

Φ_1, Φ_2 seien Ideale von R_T, $\Phi_1 \subseteq \Phi_2$. Dann gilt:

(a) *Ist Φ_1 d-Ideal, so ist auch Φ_2 d-Ideal.*

(b) *Ist Φ_2 kein d-Ideal, so ist auch Φ_1 kein d-Ideal.*

4. Die folgende Aussage wird später benötigt:

Φ sei d-Ideal. Dann gilt für jedes Φ echt enthaltende Ideal Φ_1 von R_T:

(a) *Es gibt eine kleinste natürliche Zahl f mit* $T^f \equiv 1 \bmod \Phi_1$.

(b) *Die Kongruenz*

$$T^y(T^{fz} - 1) \equiv F \bmod \Phi$$

ist für alle $F \in \Phi_1$ lösbar.

(c) *Es ist* $\Phi_1 = (\Phi, T^f - 1)$.

Beweis. Wähle ein $F_1 \in \Phi_1 - \Phi$. Nach Voraussetzung ist $T^u - T^v \equiv F_1 \bmod \Phi$ lösbar. Für die so bestimmten u, v gilt $u - v \neq 0$, $T^{u-v} \equiv 1 \bmod \Phi_1$; also gilt (a). Aus (2) folgt für $F \in \Phi_1$: $T^{x-y} \equiv 1 \bmod \Phi_1$, also $x - y = fz$ mit ganzem z und man erhält (b). Aus (b) ergibt sich schließlich $\Phi_1 \subseteq (\Phi, T^f - 1)$; die umgekehrte Inklusion folgt aus (a) und $\Phi \subseteq \Phi_1$.

5. *$\pi \in R$ sei Primelement, $A, B, C \in R_T$, A, B normiert. In den folgenden beiden Fällen ist Φ kein d-Ideal:*

(a) $\Phi = (AB + \pi C, \pi^2)$, $|A| > 0$, $|B| > 0$.
(b) $\Phi = (A^2 B + \pi C, \pi A, \pi^2)$, $|A| > 0$.

Der Beweis wird indirekt geführt. Angenommen, Φ sei doch d-Ideal.

Fall (a). Setze $\Phi_1 = (AB, \pi)$. Mit den Bezeichnungen von Abschnitt 4 gilt: Das durch $T^f - 1 \equiv \pi D \bmod \Phi$ definierte $D \in R_T$ erfüllt

$$T^{fx} - 1 \equiv x \pi D \bmod \Phi \quad \text{für alle} \quad x \in \mathbb{Z},$$

und die Kongruenzen

$$\pi \equiv T^y (T^{fx} - 1) \equiv T^y x \pi D \bmod \Phi, \tag{3}$$

$$\pi A \equiv T^v (T^{fu} - 1) \equiv T^v u \pi D \bmod \Phi \tag{4}$$

sind lösbar. Aus (4) folgt mit Hilfe von (3) $u \equiv 0 \bmod \pi$, aus (4) dann der Widerspruch $\pi A \equiv 0 \bmod \Phi$.

Fall (b). Es ist $A^3 B = A(A^2 B + \pi C) - C(\pi A) \equiv 0 \bmod \Phi$. Setze $\Phi_1 = (AB, \pi)$. Mit den Bezeichnungen von Abschnitt 4 gilt: Die durch $T^f - 1 \equiv \pi D + ABE \bmod \Phi$ definierten $D, E \in R_T$ erfüllen

$$T^{fx} - 1 \equiv x(\pi D + ABE) + \binom{x}{2} A^2 B^2 E^2 \bmod \Phi,$$

und die Kongruenzen

$$\pi \equiv T^y (T^{fx} - 1) \equiv T^y \left(x(\pi D + ABE) + \binom{x}{2} A^2 B^2 E^2 \right) \bmod \Phi, \tag{5}$$

$$AB \equiv T^v (T^{fu} - 1) \equiv T^v \left(u(\pi D + ABE) + \binom{u}{2} A^2 B^2 E^2 \right) \bmod \Phi \tag{6}$$

sind lösbar. Wegen $AB \not\equiv 0 \bmod \Phi$ folgt aus (6) zunächst $u \neq 0$, dann (AB ist normiert!) $\pi u \not\equiv 0 \bmod AB$, und (6) mod AB genommen liefert schließlich

$$D \equiv 0 \bmod AB.$$

Zusammen mit (5) ergibt das aber den Widerspruch $\pi \equiv 0 \bmod AB$.

Damit ist in beiden Fällen gezeigt, daß die Annahme, Φ sei d-Ideal, falsch war.

6. Satz. *Enthält R unendlich viele Elemente, und ist Φ ein d-Ideal von R_T, so ist der größte gemeinsame Teiler aller Elemente von Φ eine Einheit.*

Beweis. A sei Teiler aller Elemente von Φ. Dann ist $\Phi \subseteq (A)$, und (A) ist nach Abschnitt 3 d-Ideal; daher ist die Kongruenz

(7) $$T^x - T^y \equiv F \bmod A$$

für alle $F \in R_T$ lösbar.

Angenommen, A ist keine T-Potenz. Dann enthält A einen irreduziblen Polynomfaktor B, der keine T-Potenz ist. Man kann also zu R eine Lösung $\alpha \neq 0$ der Gleichung $B(x) = 0$ adjungieren. Wegen (7), $B \mid A$ und der Irreduzibilität von B gibt es dann für alle $\beta \in R[\alpha]$ natürliche Zahlen x, y, z mit

(8) $$\alpha^x - \alpha^y = \beta\, \alpha^z .$$

Für $\beta = 1$ ergibt sich: α ist absolutalgebraisch und ganz.

Ist jetzt zuerst Char. $R = p$ eine Primzahl, so ist α als absolutalgebraische Zahl $\neq 0$ eine s-te Einheitswurzel für ein gewisses s. Für β in (8) gibt es also höchstens s^3 Möglichkeiten im Widerspruch dazu, daß R unendlich viele Elemente enthält.

Ist aber Char. $R = 0$, so sei $C(T)$ das Minimalpolynom von α über $\mathbb{Z}$. Aus (8) erhält man die Lösbarkeit von $T^x - T^y = G \bmod C$ für alle $G \in \mathbb{Z}_T$. Daher ist (C) d-Ideal von $\mathbb{Z}_T$.

Hat nun C einen Grad > 1, so gibt es eine ganze Zahl t mit $C(t) \neq \pm 1$. Ist p ein Primteiler von $C(t)$, so enthält $C \bmod p$ den Faktor $T - t$, ist also mod p reduzibel. Nach Abschnitt 5 ist dann (C, p^2) kein d-Ideal; (C, p^2) enthält aber das d-Ideal (C) — im Widerspruch zu Abschnitt 3.

Hat C aber den Grad 1, so ist α ganzrational. $\beta = 1$ in (8) ergibt die Lösbarkeit von $\alpha^x = \alpha^y + \alpha^z$ in natürlichen Zahlen x, y, z. O.B.d.A. kann $y \geqq z$ angenommen werden. Dann ist $\alpha^x = \alpha^z(\alpha^{y-z} + 1)$, also für $y = z$: $2 \mid \alpha^x$, und für $y > z$: $\alpha^{y-z} + 1 \mid 1$. In beiden Fällen ergibt sich $\alpha = \pm 2$; dann prüft man aber leicht die Unlösbarkeit von (8) für $\beta = 5$ nach.

Also führt die Annahme, A sei keine T-Potenz, zu einem Widerspruch. Daher ist jeder Teiler aller Elemente von Φ eine T-Potenz, d.h. eine Einheit.

Ist R ein unendlicher Körper, so wird jedes Ideal vom größten gemeinsamen Teiler seiner Elemente erzeugt. Daher gilt in diesem Fall:

R sei ein unendlicher Körper. Dann besitzt R_T kein nicht-triviales d-Ideal.

7. Bekanntlich enthält ein Ideal von $R[T]$, wenn der g.g.T. seiner Elemente eine Einheit ist, stets ein Element des Ringes R selbst. Das überträgt sich sofort auf Ideale von R_T. Ist weiter

$$a_1\, a_2 \in \Phi \cap R, \quad (a_1, a_2) = 1 ,$$

so ist

$$\Phi = (\Phi, a_1) \cdot (\Phi, a_2) \subsetneqq (\Phi, a_1) .$$

Diese Zerlegungsmöglichkeit rechtfertigt die besondere Untersuchung derjenigen d-Ideale, die eine Potenz eines Primelements von R enthalten. In dieser Hinsicht gilt zunächst:

$\pi \in R$ sei Primelement, Φ ein nichttriviales d-Ideal von R_T. Ist dann $\pi^s \in \Phi$, so ist der Restklassenkörper $R/\pi R$ endlich.

Denn da Φ nichttrivial ist, gibt es ein $A \in \Phi$ von mod π positivem Grad mit $\Phi \subsetneqq (A, \pi)$. Nach Abschnitt 3 ist (A, π) ein d-Ideal, und das ist äquivalent damit,

daß (A) ein d-Ideal von $R/\pi R[T, T^{-1}]$ ist. Außerdem ist (A) nichttrivial, und nach dem Ergebnis am Ende von Abschnitt 6 muß $R/\pi R$ endlich sein.

8. Satz. *R enthalte unendlich viele Elemente, Φ sei nichttriviales d-Ideal, $\pi \in R$ sei Primelement und $\pi^s \in \Phi$, $\pi^{s-1} \notin \Phi$. Dann gilt:*

(a) *Der Restklassenkörper $R/\pi R$ ist endlich, $\pi | p = \text{Char. } R/\pi R$.*

(b) *Ist $s = 1$, so ist $\Phi = (A, \pi)$ mit einem normierten Polynom A von positivem Grad. (Typ 1).*

Ist $s > 1$, so ist $\Phi = (AB, \pi A, \pi^s)$ mit einem normierten, $\bmod \pi$ *irreduziblen Polynom A von positivem Grad und einem normierten Polynom B mit $(A, B, \pi) = (1)$. (Typ s).*

Teil (a) folgt sofort aus Abschnitt 7.

Beweis von (b). Setze $\Phi_0 = \Phi \cap R[T]$. Dann ist Φ_0 ein Ideal von $R[T]$, dessen Elemente als größten gemeinsamen Teiler eine Einheit besitzen. Nach Rédei ([1], § 120—121, S. 461—468) wird Φ_0 erzeugt von einer Menge der Form $\pi^{s_0} A_0, \ldots, \pi^{s_r} A_r$ $(r \geqq 1, s_0 = 0, A_r = 1)$ mit

$$|A_{i+1}| < |A_i|, s_i < s_{i+1}, A_i \in (A_{i+1}, \pi^{s_{i+2} - s_{i+1}}); \quad A_i \text{ normiert.} \tag{9}$$

Wegen $\Phi = \{T^i F_0 | F_0 \in \Phi_0, i \in \mathbb{Z}\}$ ist also $\Phi = (\pi^{s_0} A_0, \ldots, \pi^{s_r} A_r)$. Ist $r = 1$, so ist mit $s = s_1$, $A = A_0$: $\Phi = (A, \pi^s)$; für $s = 1$ ist das die Behauptung. Für $s > 1$ muß wegen Abschnitt 5(a) $A \bmod \pi$ irreduzibel sein. Mit $B = 1$ ist das wieder die Behauptung. Ist $r > 1$, so ist nach (9) $A_0 = A_1 B_1 + \pi^{s_2 - s_1} C_1$. Wären A_1 und $B_1 \bmod \pi$ nicht teilerfremd und $A \bmod \pi$ ein gemeinsamer normierter Teiler von positivem Grad, so wäre $A_0 \equiv 0 \bmod (A^2, \pi)$, $A_0 = A^2 B + \pi C$, also $\Phi \subseteqq (A^2 B + \pi C, \pi A, \pi^2)$ im Widerspruch zu Abschnitt 5(b). Also ist $(A_1, B_1, \pi) = (1)$ und daher sind die Kongruenzen

$$AB \equiv A_1 B_1 + \pi^{s_2 - s_1} C_1 \bmod \pi^{s_2}, \quad A \equiv A_1, B \equiv B_1 \bmod \pi^{s_2 - s_1}$$

unter der Nebenbedingung $|A| = |A_1|$, $|B| = |B_1|$ nach dem Henselschen Lemma lösbar. Damit ist

$$\Phi \subseteqq (AB, \pi^{s_1} A, \pi^{s_2}), \tag{10}$$

wobei die Gleichheit genau für $r = 2$ gilt. Wegen

$$\Phi \subseteqq (AB, \pi^{s_1}), \quad |B| = |B_1| = |A_0| - |A_1| > 0, \quad |A| = |A_1| > 0$$

und Abschnitt 5(a) ist $s_1 = 1$. Wegen $\Phi \subseteqq (A, \pi^{s_2}) \subseteqq (A, \pi^2)$ muß ebenso $A \bmod \pi$ irreduzibel sein.

Wäre nun $r > 2$, so wäre $A_1 \in (A_2, \pi)$, $0 < |A_2| < |A_1|$, also A_1 und daher auch $A \bmod \pi$ reduzibel, Widerspruch.

Somit ist $r = 2$ und mit $s = s_2$ folgt die Behauptung aus (10).

9. Die Beschränkung in den Sätzen der Abschnitte 6 und 8 auf Ringe mit unendlich vielen Elementen ist wesentlich. Aber die Untersuchung der d-Ideale über endlichen Hauptidealringen, also Körpern läuft parallel zur Untersuchung der

d-Ideale vom Typ 1 über unendlichen Ringen. Denn: Jeder endliche Körper ist darstellbar als Restklassenkörper eines geeigneten Hauptidealrings R_0 modulo einem Primelement $\pi \in R_0$: $R = R_0/\pi R_0$. Jedes Ideal Φ von R_T ist Hauptideal, $\Phi = (A)$, und Φ ist genau dann d-Ideal, wenn $\Phi_0 = (A, \pi)$ d-Ideal von $R_0[T, T^{-1}]$ ist.

Ist umgekehrt R_0 ein (unendlicher) Hauptidealring, und ist $\Phi_0 = (A, \pi)$ ein Ideal von R_0, so ist Φ_0 genau dann d-Ideal, wenn $\Phi = (A)$ d-Ideal über $R = R_0/\pi R_0$ ist, und in diesem Fall ist R nach Abschnitt 7 endlich.

Der Satz in Abschnitt 8 ist in gewisser Hinsicht bestmöglich: Es gibt (wenigstens für $R = \mathbb{Z}$) d-Ideale von jedem vorgeschriebenen Typ. Für die d-Ideale vom Typ 1 mit mod π irreduziblem A konnte ich jedoch weitergehende Aussagen gewinnen. Genau dann ist nämlich R_T/Φ ein endlicher Körper und aus dem Satz in Abschnitt 11 erhält man mit der Konstruktion aus Abschnitt 2 solche d-Ideale.

10. S sei wieder ein kommutativer, assoziativer Ring mit Eins, t ein invertierbares Element von S.

Satz. *Ist die Gleichung $t^x - t^y = c$ für alle $c \in S$ lösbar, so ist S endlich. Ist darüber hinaus p eine Primzahl mit $p^2 \mid$ Char. S, so ist das Ideal*

$$S_p := \{c \in S \mid p\,c \equiv 0 \bmod p^2\} \tag{11}$$

ein maximales Ideal von S.

Dabei ist $n =$ Char. S die kleinste natürliche Zahl mit $n \cdot 1 = 0$.

Beweis. Nach Abschnitt 2 ist das zugeordnete $\mathbb{Z}_T$-Ideal Φ ein d-Ideal, enthält also nach der Bemerkung am Anfang von Abschnitt 7 ein Element $n \in \mathbb{Z}$. Wegen $T^x - T^y - 1 \in \Phi$ (für gewisse x, y) enthält Φ ein normiertes Polynom F. F habe den Grad s. Dann enthält $S \cong \mathbb{Z}_T/\Phi$ höchstens n^s Elemente und ist somit endlich. Ist jetzt $n =$ Char. S, $p^2 \mid n$, so ist $\Phi = (\Phi, n) \subseteq (\Phi, p^2) \not\ni p$. Da Φ d-Ideal ist, ist auch (Φ, p^2) d-Ideal vom Typ 2 und nach Abschnitt 8 $(\Phi, p^2) = (AB, pA, p^2)$ mit einem mod p irreduziblen A. Daher ist

$$\{F(T) \mid F(t) \in S_p\} = \{F \in \mathbb{Z}_T \mid p\,F \in (AB, pA, p^2)\} = (A, p)\,. \tag{12}$$

Ist nun $G(t) \notin S_p$, so ist $G \notin (A, p)$, also, da A mod p irreduzibel ist:

$$\{F(T) \mid F(t) \in (S_p, G(t))\} = (A, G, p) = (1) = \mathbb{Z}_T\,.$$

Folglich ist $(S_p, G(t)) = S$, d.h. S_p ist maximal. (Daß S_p Ideal ist, ist klar.)

11. Satz. *K sei ein endlicher Körper der Ordnung q, t ein festes von 0 verschiedenes Element von K. f sei die kleinste natürliche Zahl mit $t^f = 1$, $f = d^{-1}(q-1)$. Ist dann $q \geqq d^4 + 2d^2N_0 + 4$, so besitzt die Gleichung $at^x + bt^y = c$ für $abc \neq 0$ mehr als N_0 modulo f inkongruente Lösungen (x, y).*

$N = N(a, b, c)$ sei die Anzahl der modulo f inkongruenten Lösungen von

$$A = at^x + bt^y - c = 0\,.$$

χ sei ein vom Hauptcharakter verschiedener Charakter der additiven Gruppe von K. Für diesen gilt:

$$\sum_{k\in K}\chi(kA)=\begin{cases}q & \text{für } A=0,\\ 0 & \text{sonst.}\end{cases} \tag{13}$$

Daher ist

$$qN=\sum_{x,y \bmod f}\ \sum_{k\in K}\chi(kA)\,,$$

also

$$qN-f^2=\sum_{x,y \bmod f}\ \sum_{\substack{k\in K\\ k\neq 0}}\chi(kA)\,.$$

Quadrieren liefert

$$(qN-f^2)^2=\sum_{x,y \bmod f}\ \sum_{\substack{k\in K\\ k\neq 0}}\ \sum_{x',y' \bmod f}\ \sum_{\substack{k'\in K\\ k'\neq 0}}\chi(kA-k'A')\,,$$

wobei $A'=at^{x'}+bt^{y'}-c$. Summation über alle $a, b, c\in K$ ergibt mit (13):

$$\sum_{a,b,c\in K}(qN-f^2)^2=\sum_{x,y \bmod f}\ \sum_{\substack{k\in K\\ k\neq 0}}q^3=q^3f^2(q-1)\,, \tag{14}$$

denn alle Beiträge mit $k'\neq k$ oder $x'\neq x$ oder $y'\neq y$ ergeben die Summe 0. Für $e\neq 0$, $u, v \bmod f$ ist $N(aet^u, bet^v, ce)=N(a,b,c)$; daher sind für $abc\neq 0$ jeweils $(q-1)f^2$ gleiche unter den N und aus (14) folgt:

$$f^2(q-1)(qN-f^2)^2\leqq\sum_{a,b,c\in K}(qN-f^2)^2=q^3f^2(q-1)$$

oder

$$(qN-f^2)^2\leqq q^3\quad\text{für}\quad abc\neq 0,\quad N=N(a,b,c)\,.$$

Es folgt für $q\geqq d^4+2d^2N_0+4$:

$$f^2-qN\leqq q^{3/2}=\left(\frac{q^2}{d^2}\cdot qd^2\right)^{1/2}\leqq\frac{1}{2}\left(\frac{q^2}{d^2}+qd^2\right)=$$

$$=\left(\frac{q-1}{d}\right)^2-q\cdot\frac{q-(d^4+4)}{2d^2}-\frac{1}{d^2}\leqq f^2-qN_0-\frac{1}{d^2}\,,$$

$$\text{also}\quad N\geqq N_0+\frac{1}{qd^2}>N_0\,.$$

Kombiniert man dieses Ergebnis mit dem Satz aus Abschnitt 1, so ergibt sich mit $N_0=0$ das folgende

Korollar. *Unter den selben Voraussetzungen wie oben ist die Gleichung $at^x+bt^y=c$ sicher dann für alle $c\in K$ lösbar, wenn $a\neq 0$, $-a^{-1}b$ eine Potenz von t und $d^4\leqq q-4$ ist.*

12. Satz. a) *Folgender Sachverhalt liege vor:*

(i) *I ist taktische Konfiguration.*

(ii) *Durch je zwei Punkte von I geht mindestens ein Block. Je zwei Blöcke von I haben mindestens einen Punkt gemeinsam.*

(iii) *Γ ist punkt- und blocktransitive abelsche Gruppe von Automorphismen von I.*

(iv) *Δ ist Quotientenmenge von I in Γ; α ist Multiplikator von Δ; die Potenzen von α sind transitiv auf Δ.*

Dann gibt es einen (assoziativen und kommutativen) Ring S mit Eins und ein invertierbares Element $t \in S$ derart, daß $S^+ \cong \Gamma$ und die Gleichung

$$t^x - t^y = c \tag{15}$$

für alle $c \in S$ durch ganze Zahlen x, y lösbar ist. t hat dieselbe (multiplikative) Ordnung wie α.

b) *S sei ein (assoziativer und kommutativer) Ring mit Eins, t ein invertierbares Element von S und die Gleichung* (15) *sei für alle $c \in S$ durch ganze Zahlen x, y lösbar. Dann gibt es eine taktische Konfiguration I, eine Gruppe $\Gamma \cong S^+$, eine Teilmenge Δ von Γ und einen Automorphismus α von Γ (von derselben Ordnung wie t) derart, daß* (i)—(iv) *erfüllt sind.*

(Bezüglich der Begriffe s. Dembowski [2], Kap. 3, S. 52—83.)

Beweis. a) S sei der von 1 und α erzeugte Unterring des Endomorphismenrings von Γ, $t = \alpha$. Dann ist S assoziativer, kommutativer Ring mit Eins und t ist invertierbares Element von S.

p sei ein beliebiger Punkt von I. Für $\xi \in \Gamma$ sei Δx ein Block, der p und ξp enthält, d.h. es gibt $\xi_1, \xi_2 \in \Delta$ mit $\xi p = \xi_1 x$, $p = \xi_2 x$, also $\xi \xi_2 x = \xi_1 x$. Da Γ abelsch und punkttransitiv ist, folgt $\xi \xi_2 = \xi_1$, $\xi = \xi_1 \xi_2^{-1}$.

Für ein festes $\xi_0 \in \Delta$ gibt es nach (iv) ganze Zahlen x, y mit $\xi_1 = \xi_0^{\alpha^x}$, $\xi_2 = \xi_0^{\alpha^y}$, also

$$\xi = \xi_0^{\alpha^x - \alpha^y}. \tag{16}$$

Daher ist die Abbildung

$$\varkappa\colon S^+ \to \Gamma; \quad \gamma \to \xi_0^\gamma$$

ein surjektiver Homomorphismus. Ist $\gamma \in \operatorname{Kern} \varkappa$, also $\xi_0^\gamma = 1$, so ist

$$\xi^\gamma = \xi_0^{(\alpha^x - \alpha^y)\gamma} = \xi_0^{\gamma(\alpha^x - \alpha^y)} = 1 \quad \text{für alle } \xi \in \Gamma,$$

also $\gamma = 0$. Somit ist $\varkappa$ sogar ein Isomorphismus zwischen S^+ und Γ. Aus der Lösbarkeit von (16) für $\xi = \xi_0^\gamma$ ($\gamma \in S$ beliebig) folgt dann die Lösbarkeit von

$$\gamma = \varkappa^{-1}(\xi_0^\gamma) = \varkappa^{-1}(\xi_0^{\alpha^x - \alpha^y}) = \alpha^x - \alpha^y = t^x - t^y$$

in ganzen Zahlen x, y.

b) Setze

$$\Gamma := \{\gamma_a\colon S \to S; s \to s + a \,|\, a \in S\},$$

$$\alpha\colon \Gamma \to \Gamma;\ \gamma_a \to \gamma_{ta},$$

$$T := \{t^x \,|\, x \in \mathbb{Z}\}, \quad \Delta := \{\gamma_a \,|\, a \in T\}.$$

I bestehe aus der Punktmenge S und der Blockmenge $\{T + s \,|\, s \in S\}$ mit dem Enthaltensein als Inzidenz. Dann ist $\Gamma \cong S^+$, und α und t haben dieselbe Ordnung. Mit

den Bezeichnungen von Dembowski [2] ist $I = I(S^+, E, T)$, wobei E die Einsgruppe ist; daher ist (i) und (iii) erfüllt und Δ ist Quotientenmenge von I in Γ. Wegen $\Delta^\alpha = \Delta$, $\Delta = \{\gamma_1^{\alpha^x} \mid x \in \mathbb{Z}\}$ gilt dann auch (iv).

Für zwei Punkte s_1, s_2 sei $s_1 - s_2 = t^x - t^y$ $(x, y \in \mathbb{Z})$. Dann liegen s_1 und s_2 beide in dem Block $T + (s_1 - t^x) = T + (s_2 - t^y)$. Ebenso sei für zwei Blöcke $T + s_1, T + s_2$: $s_1 - s_2 = t^x - t^y$ $(x, y \in \mathbb{Z})$. Dann liegt der Punkt $s_1 + t^y = s_2 + t^x$ in beiden Blöcken. Also gilt auch (ii).

Literaturverzeichnis

[1] L. Rédei, Algebra I. Leipzig 1959.
[2] P. Dembowski, Kombinatorik. Mannheim 1970.

Eingegangen am 31. 5. 1974

Anschrift des Autors:

Arnold Neumaier
Seestraße 117
D-1000 Berlin 65