

## 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

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

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 ( $a, b, t \in S$  fest;  $t$  invertierbar), so ist  $S$  endlich; ist darüber hinaus  $p$  eine Primzahl mit  $p^2 \mid \text{Char. } S$ , so ist die Menge

$$\{c \in S \mid pc \equiv 0 \pmod{p^2}\}$$

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  $d^4 \leq q-4$ , 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  $\Phi$  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)  $T^x - T^y \equiv F \pmod{\Phi}$  ist für alle  $F \in \mathbb{Z}[T^{-1}, T]$  lösbar.

II. Ist  $\Phi$  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

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

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

Die Aussage in Abschnitt 2 motiviert die Definition:

Ein Ideal  $\Phi$  von  $R_T$  heißt  $d$ -Ideal, wenn die Kongruenz

$$(2) \quad T^x - T^y \equiv F \pmod{\Phi}$$

für alle  $F \in R_T$  lösbar ist.

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

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

(a) Ist  $\Phi_1$   $d$ -Ideal, so ist auch  $\Phi_2$   $d$ -Ideal.

(b) Ist  $\Phi_2$  kein  $d$ -Ideal, so ist auch  $\Phi_1$  kein  $d$ -Ideal.

4. Die folgende Aussage wird später benötigt:

$\Phi$  sei  $d$ -Ideal. Dann gilt für jedes  $\Phi$  echt enthaltende Ideal  $\Phi_1$  von  $R_T$ :

(a) Es gibt eine kleinste natürliche Zahl  $f$  mit  $T^f \equiv 1 \pmod{\Phi_1}$ .

(b) Die Kongruenz

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

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  $T^u - T^v \equiv F_1 \pmod{\Phi}$  lösbar. Für die so bestimmten  $u, v$  gilt  $u - v \neq 0$ ,  $T^{u-v} \equiv 1 \pmod{\Phi_1}$ ; also gilt (a). Aus (2) folgt für  $F \in \Phi_1$ :  $T^{x-y} \equiv 1 \pmod{\Phi_1}$ , 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  $\Phi$  kein  $d$ -Ideal:

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

Der Beweis wird indirekt geführt. Angenommen,  $\Phi$  sei doch  $d$ -Ideal.

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

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

und die Kongruenzen

- (3)  $\pi \equiv T^y (T^f x - 1) \equiv T^y x \pi D \pmod{\Phi}$ ,  
 (4)  $\pi A \equiv T^v (T^f u - 1) \equiv T^v u \pi D \pmod{\Phi}$

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

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

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

und die Kongruenzen

- (5)  $\pi \equiv T^y (T^f x - 1) \equiv T^y \left( x(\pi D + ABE) + \binom{x}{2} A^2 B^2 E^2 \right) \pmod{\Phi}$ ,  
 (6)  $AB \equiv T^v (T^f u - 1) \equiv T^v \left( u(\pi D + ABE) + \binom{u}{2} A^2 B^2 E^2 \right) \pmod{\Phi}$

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

$$D \equiv 0 \pmod{AB}.$$

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

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

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

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

$$(7) \quad T^x - T^y \equiv F \pmod{A}$$

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),  $B|A$  und der Irreduzibilität von  $B$  gibt es dann für alle  $\beta \in R[\alpha]$  natürliche Zahlen  $x, y, z$  mit

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

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

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

Ist aber  $\text{Char. } R = 0$ , so sei  $C(T)$  das Minimalpolynom von  $\alpha$  über  $\mathbb{Z}$ . Aus (8) erhält man die Lösbarkeit von  $T^x - T^y = G \pmod{C}$  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  $C \pmod{p}$  den Faktor  $T - t$ , ist also  $\pmod{p}$  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  $\alpha$  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  $y \geq z$  angenommen werden. Dann ist  $\alpha^x = \alpha^z(\alpha^{y-z} + 1)$ , also für  $y = z$ :  $2|\alpha^x$ , und für  $y > z$ :  $\alpha^{y-z} + 1|1$ . 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  $\Phi$  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

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

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

Denn da  $\Phi$  nichttrivial ist, gibt es ein  $A \in \Phi$  von  $\pmod{\pi}$  positivem Grad mit  $\Phi \subseteq (A, \pi)$ . Nach Abschnitt 3 ist  $(A, \pi)$  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,  $\Phi$  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,  $\pi \mid p = \text{Char. } R/\pi R$ .

(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, mod  $\pi$  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  $\Phi_0$  ein Ideal von  $R[T]$ , dessen Elemente als größten gemeinsamen Teiler eine Einheit besitzen. Nach Rédei ([1], § 120–121, S. 461–468) wird  $\Phi_0$  erzeugt von einer Menge der Form  $\pi^{s_0} A_0, \dots, \pi^{s_r} A_r$  ( $r \geq 1, s_0 = 0, A_r = 1$ ) mit

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

Wegen  $\Phi = \{T^i F_0 \mid F_0 \in \Phi_0, i \in \mathbb{Z}\}$  ist also  $\Phi = (\pi^{s_0} A_0, \dots, \pi^{s_r} A_r)$ . 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  $\Phi \subseteq (A^2 B + \pi C, \pi A, \pi^2)$  im Widerspruch zu Abschnitt 5(b). Also ist  $(A_1, B_1, \pi) = (1)$  und daher sind die Kongruenzen

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

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

$$(10) \quad \Phi \subseteq (AB, \pi^{s_1} A, \pi^{s_2}),$$

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

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

und Abschnitt 5(a) ist  $s_1 = 1$ . Wegen  $\Phi \subseteq (A, \pi^{s_2}) \subseteq (A, \pi^2)$  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  $\Phi$  von  $R_T$  ist Hauptideal,  $\Phi = (A)$ , und  $\Phi$  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  $\Phi_0$  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  $\pi$  irreduziblem  $A$  konnte ich jedoch weitergehende Aussagen gewinnen. Genau dann ist nämlich  $R_T/\Phi$  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  $tx - ty = c$  für alle  $c \in S$  lösbar, so ist  $S$  endlich. Ist darüber hinaus  $p$  eine Primzahl mit  $p^2 \mid \text{Char. } S$ , so ist das Ideal

$$(11) \quad S_p := \{c \in S \mid pc \equiv 0 \pmod{p^2}\}$$

ein maximales Ideal von  $S$ .

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

**Beweis.** Nach Abschnitt 2 ist das zugeordnete  $\mathbb{Z}_T$ -Ideal  $\Phi$  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  $\Phi$  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  $n = \text{Char. } S$ ,  $p^2 \mid n$ , so ist  $\Phi = (\Phi, n) \subseteq (\Phi, p^2) \neq p$ . Da  $\Phi$   $d$ -Ideal ist, ist auch  $(\Phi, p^2)$   $d$ -Ideal vom Typ 2 und nach Abschnitt 8  $(\Phi, p^2) = (AB, pA, p^2)$  mit einem mod  $p$  irreduziblen  $A$ . Daher ist

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

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  $tf = 1$ ,  $f = d^{-1}(q - 1)$ . Ist dann  $q \geq d^4 + 2d^2N_0 + 4$ , 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

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

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

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

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  $A' = atx' + btv' - c$ . Summation über alle  $a, b, c \in K$  ergibt mit (13):

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

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:

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

oder

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

Es folgt für  $q \geq d^4 + 2d^2 N_0 + 4$ :

$$\begin{aligned} f^2 - qN &\leq q^{3/2} = \left( \frac{q^2}{d^2} \cdot qd^2 \right)^{1/2} \leq \frac{1}{2} \left( \frac{q^2}{d^2} + qd^2 \right) = \\ &= \left( \frac{q-1}{d} \right)^2 - q \cdot \frac{q - (d^4 + 4)}{2d^2} - \frac{1}{d^2} \leq f^2 - qN_0 - \frac{1}{d^2}, \end{aligned}$$

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

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  $d^4 \leq q - 4$  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)  $\Gamma$  ist punkt- und blocktransitive abelsche Gruppe von Automorphismen von  $I$ .

(iv)  $\Delta$  ist Quotientenmenge von  $I$  in  $\Gamma$ ;  $\alpha$  ist Multiplikator von  $\Delta$ ; die Potenzen von  $\alpha$  sind transitiv auf  $\Delta$ .

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

$$(15) \quad t^x - t^y = c$$

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

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  $\Delta$  von  $\Gamma$  und einen Automorphismus  $\alpha$  von  $\Gamma$  (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  $\alpha$  erzeugte Unterring des Endomorphismenrings von  $\Gamma$ ,  $t = \alpha$ . 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  $\Delta x$  ein Block, der  $p$  und  $\xi p$  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  $\Gamma$  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

$$(16) \quad \xi = \xi_0^{\alpha^x - \alpha^y}.$$

Daher ist die Abbildung

$$\kappa: S^+ \rightarrow \Gamma; \quad \gamma \rightarrow \xi_0^\gamma$$

ein surjektiver Homomorphismus. Ist  $\gamma \in \text{Kern } \kappa$ , 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  $\kappa$  sogar ein Isomorphismus zwischen  $S^+$  und  $\Gamma$ . Aus der Lösbarkeit von (16) für  $\xi = \xi_0^\gamma$  ( $\gamma \in S$  beliebig) folgt dann die Lösbarkeit von

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

in ganzen Zahlen  $x, y$ .

b) Setze

$$\Gamma := \{\gamma_a: S \rightarrow S; s \rightarrow s + a \mid a \in S\},$$

$$\alpha: \Gamma \rightarrow \Gamma; \gamma_a \rightarrow \gamma_{ta},$$

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

$I$  bestehe aus der Punktmenge  $S$  und der Blockmenge  $\{T + s \mid s \in S\}$  mit dem Enthaltensein als Inzidenz. Dann ist  $\Gamma \cong S^+$ , und  $\alpha$  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  $\Delta$  ist Quotientenmenge von  $I$  in  $\Gamma$ . Wegen  $\Delta^\alpha = \Delta$ ,  $\Delta = \{\gamma_1^{x^x} \mid x \in \mathbb{Z}\}$  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