BAYERISCHE AKADEMIE DER WISSENSCHAFTEN
MATHEMATISCH-NATURWISSENSCHAFTLICHE KLASSE

SITZUNGSBERICHTE

JAHRGANG
1974

MÜNCHEN 1975

VERLAG DER BAYERISCHEN AKADEMIE DER WISSENSCHAFTEN
In Kommission bei der C. H. Beck'schen Verlagsbuchhandlung München

Bemerkungen zur elementaren Algebra II; Über trinomische Gleichungen mit quadratischer Diskriminante und rationale Punkte auf gewissen algebraischen Flächen

Von **Hermann Schmidt** in Würzburg

Vorgelegt am 7. Juni 1974

Einleitung

Die folgenden Betrachtungen können als kleiner Beitrag zur Weiterführung der vor Jahren von E. Noether in ihrer bekannten Abhandlung [6] eingeführten Methode zur Gewinnung von algebraischen Gleichungen mit vorgeschriebener Gruppe durch Parameterdarstellung der Koeffizienten gelten, wenngleich zum Verständnis unserer einfachen Überlegungen die Kenntnis dieser größeren Zusammenhänge nicht erforderlich ist (vgl. das Summar). Dort werden zunächst die Wurzeln als Unbestimmte angesehen und die Lösung der Aufgabe von der (im allgemeinen schwer zu prüfenden) Existenz einer n-gliedrigen Rationalbasis für den zur Gruppe gehörigen Invariantenkörper abhängig gemacht. Damit kommt man in den Fällen $n \leq 4$ zum Ziel, und die Ergebnisse sind in der Arbeit Seidelmann [8] niedergelegt. (Ein Irrtum sei vermerkt: Bei den zyklischen Gleichungen 4. Grades S. 232 IV darf der Fall $f = 0$ nicht ausgeschlossen werden, wie etwa das Beispiel der zyklischen Gleichung $x^4 - 5x^2 + 5 = 0$ zeigt.)

Wir legen hier von vornherein eine spezielle Gleichungsform zugrunde und ziehen nur die alternierende Gruppe mit ihren Untergruppen in Betracht. Dies bewirkt, daß die entstehende Bedingungsgleichung für die Diskriminante (bei Ausschließung einiger Werte für die Charakteristik) stets parametrisiert werden kann, was, falls das mittlere Gleichungsglied gerade das vorletzte ist, fast unmittelbar, allgemein aber durch ein schrittweises Reduktionsverfahren einzusehen ist. Dies wird in § 1 etwas all-

gemeiner (unabhängig von der Anwendung auf die Diskriminante) für Gleichungen durchgeführt, die (bei passendem Grundkörper) auch als Gleichungen spezieller algebraischer Flächen aufgefaßt werden können, die sich als rational erweisen und deren rationale Punkte gefunden werden. Nach einer kleinen Abschweifung mehr zahlentheoretischer Natur in § 2 folgt die Anwendung auf das Ausgangsproblem in § 3, besonders Satz 4. Zum Schluß bringen wir Bemerkungen zur Berechnung ganzzahliger Lösungen im Falle $n = 3$, wo ja diese Aufgabe in die Lehre von den positiv definiten quadratischen Formen bzw. die Theorie des quadratischen Zahlkörpers $Q(\sqrt{-3})$ fällt. Entsprechend werden bei der betreffenden Aufgabe in den höheren Fällen quadratische Zahlkörper eine Rolle spielen (was aber erst aufgrund der Parameterdarstellung zum Vorschein kommt), so der reelle Zahlenkörper $Q(\sqrt{5})$ für $n = 5$. – Erwähnt sei noch, daß die Frage, wann sich die Gruppe reduziert, nicht allgemein behandelt wurde; es kann dies schon über dem Körper $K(u, v)$ der unbestimmten Parameter u, v der Fall sein, wie etwa das Beispiel (15)'' für $k = 2$, $m = 0$ lehrt.

§ 1. Rationale Punkte auf speziellen algebraischen Flächen

Satz 1. *Es sei K ein Körper, in dem jede Gleichung $x^m = c$ ($c \in K$, m ungerade) lösbar ist (z. B. der Körper $\mathbf{R}$ der reellen Zahlen). Vorgelegt sei die Gleichung*

$$Z^2 = aX^n + bY^l, \text{ in der} \tag{1}$$

$$a, b \in K, ab \neq 0, (n, l) = 1. \tag{1}_0$$

Falls, was keine Einschränkung bedeutet, noch n ungerade ist, erhält man genau alle Lösungen von (1) mit $X \neq 0, X, Y \in K$ in der Form

$$X = t^h,\ Y = t^\varrho u,\ Z = t^\sigma v, \tag{2}$$

worin ϱ, σ geeignete ganze Zahlen ≥ 0 sind, ferner $h \in \mathbf{N}$ und

$$at := v^2 - bu^l, \tag{3}$$

während das Paar u, v alle Elemente von $K \times K$ mit $t \neq 0$ durchläuft.

Es sei nämlich zunächst X, Y, Z eine gegebene Lösung dieser Art. Bei beliebiger Wahl der natürlichen Zahl $h \equiv 1\ (2)$ und von $\varrho, \sigma \in \boldsymbol{N}_0$ können dann $t, u, v \in K$ so bestimmt werden, daß (2) gilt, und es ist dann

$$t^{2\sigma} v^2 = a t^{hn} + b t^{\varrho l} u^l.$$

Jetzt werde für h eine ungerade Lösung der Kongruenz $hn \equiv 1\,(l)$ gewählt; eine solche gibt es, da $(n, l) = 1$ nach Vor. $(1)_0$, ferner ein gerades $h = h_0$ nur für ungerades l auftreten kann, worauf dann $h = h_0 + l \equiv 1\,(2)$ wird. Mit den Werten

$$\varrho := \frac{hn-1}{l}, \quad \sigma := \frac{hn-1}{2}$$

ist dann (3) erfüllt.

Umgekehrt erfüllen die Werte (2) mit t aus (3) bei dieser Wahl der Exponenten und für beliebige $u, v \in K$ mit $t \neq 0$ die Gleichung (1) mit $X \neq 0$.

Zusatz. Ist $l \mid (n-1)$ oder $l \mid (n+1)$, so kann $h = 1$ genommen werden und man erhält unmittelbar für beliebiges K alle Lösungen mit $X \neq 0$ in der Form

$$(4)_a \qquad aX = v^2 - bu^l,\ Y = uX^{\frac{n-1}{l}},\ Z = vX^{\frac{n-1}{2}} \qquad \text{für } \begin{cases} l \mid (n-1) \\ l \mid (n+1) \end{cases}$$

$$(4)_b \qquad \frac{a}{X} = v^2 - bu^l,\ Y = uX^{\frac{n+1}{l}},\ Z = vX^{\frac{n+1}{2}}$$

$$n \equiv 1\,(2), u, v \in K,\ v^2 - bu^l \neq 0.$$

Im allgemeinen aber wird man zur Anwendung von Satz 1 einen beliebigen Körper K erst zu einem Körper K^* erweitern müssen, der die gemachte Voraussetzung erfüllt (im Einzelfall wird es nach Ermittlung eines passenden h auch genügen, wenn diese für $m = h$ zutrifft); man erhält dabei keine Auskunft darüber, für welche Werte u, v aus K^* man Lösungswerte $\in K$ erhält. Sei beispielsweise über $K = \boldsymbol{Q}$ (rationaler Zahlenkörper) die Gleichung gegeben

(5) $\quad Z^2 = X^7 + 16\,Y^{12}$, die für $X = 2,\ Y = 1, Z = 12$

erfüllt ist.

Die nach unserem Verfahren bestimmte Parameterdarstellung

$$X = t^7,\ Y = t^4 u,\ Z = t^{24} v \text{ mit } t := v^2 - 16u^{12}$$

ergibt aber diese Lösung (in $\boldsymbol{R}$) nur für $t = \sqrt[7]{2}$, also gewiß nicht für rationale u, v.

Gleichwohl gibt es aber eine ähnliche, wenn auch nicht ganz so bequem zu erhaltende Parameterdarstellung auch über einem beliebigen Körper, die aber nicht aus Polynomen zu bestehen braucht (worauf wir schon bei $(4)_b$ verzichtet haben).

Satz 2: *K sei ein beliebiger Körper, und für*

$$(1) \qquad Z^2 = aX^n + bY^l \text{ bzw. } (1)'\ Z^2 = (aX^n + bY^l)Y$$

gelte Voraussetzung $(1)_0$. Dann lassen sich in endlich vielen Schritten drei Potenzprodukte $t^{\alpha_j} u^{\beta_j} v^{\gamma_j} (\alpha_j, \beta_j, \gamma_j \in \mathbf{Z}, j = 1,2,3)$ sowie ein Polynom (Binom) $P(u,v) \in K[u,v]$ derart herstellen, daß diese genau alle Lösungskomponenten $X, Y, Z \in K$ mit $XYZ \neq 0$ liefern, wenn u,v alle Paare aus $K \times K$ durchläuft, für die $uv \cdot P(u,v) \neq 0$ ist, und dann $t = P(u,v)$ gesetzt wird.

Zum Beweis betrachten wir zunächst Gleichung (1), worin jetzt ohne Einschränkung $n > l$ angenommen sei. Für $l = 1$ ist nichts zu beweisen: man setze $X = u$, $Z = v$, $bY = v^2 - au^n$. Nun sei $1 < l < n$. Dann bestimmen wir, was stets möglich ist, $\varrho \in \boldsymbol{N}$ so, daß $\varrho l =: 2\sigma$ gerade und weiter

$$(6) \qquad 0 \leq n_1 := |n - \varrho l| \leq l,$$

wobei von selbst $n_1 \neq 0, l$, da $(n,l) = 1$.

Es sei ferner $\varepsilon := sg(n - \varrho l)$ (für l gerade kann nach Belieben $\varepsilon = +1$ oder -1 erreicht werden). Dann machen wir die birationale („monomiale") Transformation

$Y = X^\varrho \cdot Y_1, Z = X^\sigma \cdot Z_1$, nebst $X = X_1^\varepsilon$, wodurch (da $X = 0$ ausgeschlossen ist) die Gleichung hervorgeht

$$Z_1^2 = aX_1^{n_1} + bY_1^l,$$

in der nun $1 \leq n_1 < l$, und $(l, n_1) = 1$. So fortfahrend erhält man schließlich eine Gleichung mit kleinstem Exponenten 1, womit das Verfahren zum Abschluß kommt. Dieser Fall war soeben

behandelt worden, und durch Rücksubstitution erhält man die Behauptung.

Im Beispiel (5) (wo die Rolle von X und Y vertauscht ist, d. h. $n = 12$, $l = 7$ zu setzen ist) erhält man in zwei Schritten mit

$$\varrho_1 = 2,\ \sigma_1 = 7,\ \varepsilon_1 = -1$$
$$\varrho_2 = \sigma_2 = 3,\ \varepsilon_2 = 1 \text{ bezw. } \varrho_2' = \sigma_2' = 4,\ \varepsilon_2' = -1$$

die beiden Darstellungen

$$\left.\begin{aligned} X &= u^{-2}P^{-5} = u'^{-2}P'^{7} \\ Y &= u^{-1}P^{-3} = u'^{-1}P'^{4} \\ Z &= vu^{-7}P^{-18} = u'^{-7}v'P'^{24} \end{aligned}\right| \text{ mit } \left\{\begin{aligned} P &= P(u,v) = v^2 - 16u^2 \\ P' &= P(u',v') = \tfrac{1}{P} \text{ vermöge} \\ u' &= \tfrac{u}{P},\ v' = \tfrac{v}{P}; \end{aligned}\right.$$

$u = \frac{1}{8}$, $v = \frac{3}{2}$, $P = 2$ rational für $X = 2$, $Y = 1$, $Z = 12$ (die durch die birationale Transformation $u' = \frac{u}{P}, v' = \frac{v}{P}$ ineinander übergehen).

Im Falle der Gleichung (1)′ haben wir wegen der unsymmetrischen Form die beiden Fälle

$$\alpha)_0 \qquad 1 = l < n \quad \text{und} \quad \beta)_0 \qquad 1 = n \leq l$$

vorweg zu behandeln. Beidemale setzen wir

$$(7) \qquad Z = vY, \text{ so daß} \qquad v^2Y = aX^n + bY^l$$

weiter zu untersuchen ist. Die Formeln

$$\overline{\alpha)_0} \qquad X = u;\ (v^2 - b)Y = au^n;\ Z = vY \qquad \text{und}$$
$$\overline{\beta)_0} \qquad Y = u;\ aX = u(v^2 - bu^{l-1});\ Z = uv$$

enthalten die gewünschten Parameterdarstellungen ($a \neq 0$, $XYZ \neq 0$).

Damit läßt sich jetzt die allgemeine Gleichung (1)′ erledigen. Wenn

$\alpha)$ $1 < l < n$ setzen wir

$$Y = X^{\varrho}Y_1,\ Z = X^{\sigma}Z_1,\ X = X_1^{\varepsilon} \text{ wo } \varrho, n_1, \varepsilon \text{ wie bei (6)}$$

bestimmt werden, jedoch diesmal

$$(l+1)\varrho =: 2\sigma$$

gerade sein soll. Man erhält durch Einsetzen

$$Z_1^2 = (aX_1^{n_1} + bY_1^{l})Y_1 \text{ mit } 1 \leq n_1 \leq l.$$

Im Falle

$\beta)$ $1 < n < l$

werde

$$1 \leq l_1 = |l - n\varrho| < n,\ sg(l - n\varrho) = \varepsilon,\ n\varrho = 2\sigma$$

gesetzt, ferner

$$X = Y^{\varrho}X_1,\ Z = Y^{\sigma+\frac{1-\varepsilon}{2}}Z_1,\ Y = Y_1^{\varepsilon}.$$

Es kommt dann

$$Z_1^2 = (aX_1^{n} + bY_1^{l_1})Y_1 \qquad \text{mit } 1 \leq l_1 < n.$$

Jedesmal hat der kleinere der beiden Exponenten um mindestens eine Einheit abgenommen, so daß nach endlich vielen Schritten einer der Fälle $\alpha)_0$, $\beta)_0$ erreicht wird. Damit ist der Beweis zu Satz 2 abgeschlossen.

Übrigens läßt sich für ungerade $n = 2k+1$, was hier eine echte Einschränkung bedeutet, die Gleichung (1)′ im Falle $\alpha)$ vermöge $X = X'/Y'$, $Y = 1/Y'$, $Z = Z'/Y'^{k+1}$ birational auf $Z'^2 = aX'^n + bY'^{n-l}$, das heißt auf die Gleichung (1) mit $n - l$ statt l zurückführen. Die betreffenden Parameterdarstellungen gehen z. B. im Falle $\alpha)_0$ $(l = 1)$ durch $u = 1/u'$, $v = v'/u'^k$ in einander über ($(4)_a$ in gestrichenen Parametern und Unbekannten).

Es sei noch bemerkt, daß es bei $K = \boldsymbol{R}$ oder $K = \boldsymbol{C}$ klassische Bedingungen für die Rationalität einer Fläche $Z^2 = f(X, Y)$ gibt $(f(X, Y) \in K[X, Y])$; vgl. etwa Castelnuovo-Enriques [3], 738–740; Baker [1], 130/131; [2] 35/37; Conforto [4] 411ff. Doch dürfte die Heranziehung dieser Sätze für unsere Zwecke kaum von Nutzen sein, da es uns um fertige Darstellungen von der Art zu tun ist, daß nicht nur die Parameterfunktionen in $K(u, v)$ liegen, wo K der gegebene Körper ist, sondern außerdem alle Lösungswerte $\in K$ auch für Parameterwerte aus K hervor-

gehen, was bei den Formeln (2) (3) nicht allgemein, wohl aber bei Satz 2 gewährleistet ist.

§ 2. Verallgemeinerung eines Satzes von Mordell

Noch einfacher als die Gleichungen (1), (1)' ist die folgende Gleichung für $n+1$ Unbekannte aus K zu behandeln:

$$z^l = H(y_0, y_1, \ldots y_{n-1}), \tag{8}$$

wo rechts eine homogene Funktion vom Grade $k(\gtrless 0)$ aus $K(y_0, y_1, \ldots y_{n-1})$ steht, $n \geq 2$, $(l,k) = 1$. Gesucht sind alle Lösungen mit $y_0 z \neq 0$. Für solche kann man setzen

$$y_\nu =: t_\nu y_0; \text{ man erhält mit } H := H(1, t_1, t_2, \ldots t_{n-1})$$

$l' \mid k' \mid$ $\qquad\qquad z^l = y_0{}^k H (\neq 0).$

Es sei ferner $k'l - l'k = 1, k'$ und $l' \in \boldsymbol{Z}$ und v durch

$-l \mid -k \mid$ $\qquad\qquad z^{l'} = y_0{}^{k'} v^{-1}$

erklärt. Durch Potenzieren mit den angegebenen Exponenten und Multiplikation ergibt sich dann sofort

$$\begin{aligned} z &= v^k H^{k'} \\ y_0 &= v^l H^{l'} \\ y_\nu &= t_\nu v^l H^{l'} \quad (\nu = 1, 2, \ldots n-1), \end{aligned} \tag{9}$$

und umgekehrt ist für jede Wahl von $v, t_\nu \in K$, für die $vH \neq 0$, auch das Wertsystem (9) eine Lösung der gewünschten Art; so erhalten wir alle solchen Lösungen.

Insbesondere sei jetzt $\chi(K) = 0$ und mit $0 \neq d \in K$ gesetzt $H(y) = \left(\sum_{\nu=0}^{n-1} y_\nu\right)^{n+1} : d \prod_{\nu=0}^{n-1} y_\nu$, sodaß $k = 1$; dazu werde $l = 1$ gewählt, sodaß $k' = 1$, $l' = 0$ angenommen werden darf. Dieser für (8) (9) ganz triviale Fall führt im Anschluß an Mordell [4] zu bemerkenswerten Folgerungen. Mit $y_0 - z =: x_0$ geht jetzt (8) über in

$$\left(x_0 + \sum_{\nu=1}^{n-1} y_\nu + z\right)^{n+1} - d x_0 z \prod_{\nu=1}^{n-1} y_\nu = d z^2 \prod_{\nu=1}^{n-1} y_\nu. \tag{10}$$

Durch passende Wahl der Parameter kann die rechte Seite zu einer beliebigen Größe $c(\neq 0) \in K$ gemacht werden. Nach (9) ist hierzu nur erforderlich, daß bei $\prod_{\nu=1}^{n-1} t_\nu \neq 0$ mit $T = 1 + \sum_{\nu=1}^{n-1} t_\nu$ $(v T^2)^{n+1} = c d \prod_{\nu=1}^{n-1} t_\nu$, oder also $T \neq 0$ und

(11) $c d \prod_{\nu=1}^{n-1} t_\nu =$ einer $(n+1)$-ten Potenz t_n^{n+1} eines Elements $\neq 0$ von K wird. Das läßt sich bei Vorgabe von $t_\nu \in K$ mit $t_2 t_3 t_4 \ldots t_n \neq 0$ durch Auflösung von (11) nach t_1 erreichen; alsdann nehme man (unter Beachtung der wegen $\chi(K) = 0$ erfüllbaren Bedingung $T \neq 0$) $v = t_n / T^2$, wodurch $H = c \left(\frac{T}{t_n}\right)^{n+1}$ hervorgeht.

Mit Rücksicht auf (9) (10) wird schließlich

$$x_\nu := y_\nu = t_\nu t_n T^{-2} \qquad (\nu = 1, \ldots n-1)$$

(12)
$$x_n := z = vH = c \frac{T^{n-1}}{t_n^n}$$

$$x_0 = \frac{t_n}{T^2} - x_n = \frac{t_n^{n+1} - c T^{n+1}}{t_n^n T^2}$$

Damit hat man

Satz 3: *Die Gleichung*

$$\left(\sum_{\nu=0}^{n} x_\nu\right)^{n+1} - d \prod_{\nu=0}^{n} x_\nu = c \qquad (c, d \in K, 0 \neq cd)$$

hat wenn $\chi(K) = 0$ die $(n-1)$-parametrige Lösungsschar (12) mit $x_\nu \in K$. Dabei durchlaufen die Parameter t_ν $(\nu \geq 2)$ alle Werte $\neq 0$ aus K, für die mit $t_1 = t_n^{n+1} : c d \prod_{\nu=2}^{n-1} t_\nu$ der Wert $T = 1 + \sum_{\nu=1}^{n-1} t_\nu \neq 0$ ausfällt.

Für $n = 2$ wurde dieser Satz von Mordell [5] im Zusammenhang mit der Lösung von $X_0^3 + X_1^3 + X_2^3 = R$ angegeben, wofür nur $d = 24$, $c = 8R$ zu nehmen ist, ferner $x_\nu = X_{\nu+1} + X_{\nu+2}$, Indizes mod 3.

§ 3. Diskriminanten trinomischer Gleichungen

Es sei nunmehr

(13) $f(x) = x^n - Ax^{n-l} + B$, worin A, B zunächst Unbestimmte über $\boldsymbol{Q}$ sein mögen, und $1 \leq l \leq n-1$. Zur Berechnung der Diskriminante benützen wir die Formel

(14) $D = D(f) = (-1)^{\binom{n}{2}} n^n \prod_{j=1}^{n-1} f(y_j)$, worin y_j die Nullstellen von $f'(x) = (n(x^l - A) + lA)x^{n-l-1}$ (in einem Erweiterungskörper) sind. Es ist

$$f(y_j) = B + y_j^{n-l}(y_j^l - A) = B - \frac{l}{n} A y_j^{n-l}, \text{ somit}$$

$$(-1)^{\binom{n}{2}} D = n^n \prod_{\lambda=0}^{l-1} (B - \frac{l}{n} A(\omega^\lambda y_0)^{n-l}) \cdot B^{n-l-1}, \text{ wenn}$$

ω eine primitive $l$te Einheitswurzel bedeutet, und $y_0^l = \frac{n-l}{n} A$ ist.

Für $(n, l) = 1$ ist nun ω^{n-l} ebenfalls primitive $l$te Einheitswurzel, somit wird

(15) $(-1)^{\binom{n}{2}} D = (n^n B^l - l^l (n-l)^{n-l} A^n) B^{n-l-1}$.

Ist dagegen $(n, l) = h > 1$, $n = hn'$, $l = hl'$, so ist ω^{n-l} primitive l'te Einheitswurzel, und es wird

(15)' $(-1)^{\frac{n}{2}(n+n'-2)} D(f) = h^n B^{h-1} D^h(\varphi)$, wenn

(16) $f(x) = \varphi(x^h)$ geschrieben wird. Übrigens folgt (15)' für jedes Polynom der Form (16) auch unmittelbar aus (14) $(B := \varphi(0))$.

Ist nun K ein beliebiger Körper, A, $B \in K$, so bleiben (15) (15)' richtig, wenn nur, falls die Charakteristik $\chi \neq 0$, die ganzzahligen Koeffizienten $c = n^n$, ... durch die Körperelemente $c \cdot e$ ersetzt werden, wo e die Eins des Körpers bedeutet. Nunmehr werde gefordert

(17) $ABD \neq 0, \chi \neq 2$. Dann hat die Gleichung $f(x) = 0$ in einem Erweiterungskörper n verschiedene Wurzeln, und die Galoissche Gruppe des (separablen) Wurzelkörpers ist genau dann die alternierende oder eine Untergruppe, wenn man hat

(18) $D = C^2$ mit $C(\neq 0)$ aus K. Schreibt man noch

$n = 2k + \gamma$, $n - l - 1 = 2m + \delta$ $(k, m \in \boldsymbol{Z}, \gamma, \delta = 0$ oder $1)$,

so geht die Bedingung (18) im Falle (15) über in

(19) $Z^2 = (aX^n + bY^l)Y^\delta$, das heißt eine Gleichung der Form (1) oder (1)′, wie sie in § 1 behandelt wurden. Hierbei ist jetzt

(20) $a = (-1)^{k-1} l^l (n-l)^{n-l}$, $b = (-1)^k n^n$, und

$A = X$, $B = Y$, $C = ZY^m$ gesetzt. Damit kann jetzt Satz 2 herangezogen werden, wobei aber, da dieser sich nur auf $ab \neq 0$ bezieht (was in den Beweisen entscheidend benützt wird), nunmehr weitere Einschränkungen bezüglich der Charakteristik gemacht werden müssen. So kommt man zu

Satz 4: *Es sei K ein Körper der Charakteristik χ mit*

$\chi \nmid nl(n-l)$. *Die Gleichung (13) mit $AB \neq 0$ hat, wenn* $(n,l) = 1$, *genau dann über K die alternierende Gruppe oder eine Untergruppe derselben, wenn A, B bezw. aus zwei in endlich vielen Schritten konstruierbaren Potenzprodukten*

$$Q(u,v)^{\alpha_j}\ u^{\beta_j}\ v^{\gamma_j} \qquad (\alpha_j, \beta_j, \gamma_j \in Z),\ Q(u,v) \in K[u,v]$$

für zwei Werte $u, v \in K$ mit $uvQ(u,v) \neq 0$ hervorgehen.

Wenn $(n,l) > 1$ ist (vgl. (15)′, (16)), gelangt man entsprechend zu $C^2 = (-1)^k h^n D'^h B^{n-l-1}$, wobei gesetzt ist $D' = (-1)^{\binom{n'}{2}} D(\varphi) B^{-(n'-l'-1)}$. Mit $h = 2q + \vartheta$ ($\vartheta = 0$ oder 1) und $C =: Zh^k D'^q B^m$ hat man jetzt die Bedingung

$$Z^2 = (-1)^k h^\gamma D'^\vartheta B^\delta \qquad \text{zu erfüllen.}$$

Für $\vartheta = 1$ ist dies eine Gleichung der Form (19) mit

$a' = (-1)^{k-1} h^\gamma l'^{l'} (n'-l')^{n'-l'}$, $b' = (-1)^k h^k n'^{n'}$ statt a, b,

so daß unter der Voraussetzung $\chi \nmid hn'l'(n'-l')$ wieder Satz 2 anwendbar ist. Für $\vartheta = 0$ ist stets $\gamma = 0$, $\delta = 1$, so daß gesetzt werden kann

$B = (-1)^k v^2$, $A = u$ beliebig, doch mit $BD' \neq 0, u, v \in K$.

Man hat die einfache Gleichung

(15)″ $$x^{2k} - ux^{2m+2} + (-1)^k v^2 = 0,$$

die sich der Aussage des Satzes 4 für $\alpha_j = 0$ unterordnet.

Sonderfälle

Wir geben hier eine übersichtliche Zusammenstellung für den nächstliegenden Fall $l = n - 1$, wo man ohne den allgemeinen Satz 2 schon mit $(4)_{a,b}$ auskommt. Die Werte von a, b sind aus (20) zu entnehmen.

$n = 2k + 1$ ungerade

$a = (-1)^{k-1}(2k)^{2k}$, $b = (-1)^k(2k+1)^{2k+1}$, $\chi \neq 2k(2k+1)$

$(2k)^{2k} A = (2k+1)^{2k+1} u^{2k} + (-1)^{k-1} v^2$, $B = uA$, $C = vA^k$

oder mit

$$u = \frac{2kp}{2k+1}, \quad v = (2k+1)(2k)^k q$$

(21) $A = (2k+1)P, B = 2kpP, C = (2k)^k(2k+1)^{k+1} qP^k$,

wo

$$P := p^{2k} + (-1)^{k-1}(2k+1)q^2.$$

$n = 3$ $4A = 27u^2 + v^2$, $4B = u(27u^2 + v^2)$, $\chi \neq 6$.

Mit $u = \frac{2}{3} p$, $v = 6q$ ergibt sich

$A = 3(p^2 + 3q^2)$, $B = 2p(p^2 + 3p^2)$
(Seidelmann [8], 17 (5)) und mit

$3u = -u'$, $v = u' + 2v'$

(21)′ $A = u'^2 + u'v' + v'^2$, $B = -\frac{u'A}{3}$ (Perron [7], b))

$n = 5$ (Bring-Jerrardsche Form der Gleichung 5. Grades).
$A = 5(p^4 - 5q^2)$, $B = 4p(p^4 - 5q^2)$.

$n = 2k$ gerade.

Man setze $2k =: l', l = 2k - 1 = n'$ (ungerade)
$a' := (-1)^k(2k)^{2k}$, $b' := (-1)^{k-1}(2k-1)^{2k-1}$,
damit $(4)_b$ anwendbar wird. Man erhält schließlich

(22) $A = 2kpQ^{-1}$, $B = (2k-1)Q^{-1}$,
$C = (2k-1)^k(2k)^k qQ^{-k}$, wo $\chi \neq 2k(2k-1)$,
$Q := p^{2k} + (-1)^k(2k-1)q^2$

$n = 4$ $A = 4pQ^{-1}$, $B = 3Q^{-1}$, $C = 144qQ^{-2}$,
$Q = p^4 + 3q^2$.

Ersetzt man noch q durch $p^{k-1}q$, so wird aus (21) ($\underline{n = 2k+1}$)

$$(21)^* \quad A = (2k+1)p^{2k-2}\ P^*, B = 2kp^{2k-1}P^*,$$
$$C = (2k)^k(2k+1)^{(k-1)(2k+1)}\ qP^*, \text{ wo}$$
$$P^* = p^2 + (-1)^{k-1}(2k+1)q^2 \text{ und aus (22) } (\underline{n = 2k})$$

$$(22)^* \quad A = \frac{2k}{p^{2k-3}Q^*},\ B = \frac{2k-1}{p^{2k-2}Q^*},\ C = \frac{(2k-1)^k(2k)^k q}{p^{(k-1)(2k-1)}Q^{*k}} \text{ mit}$$

$$Q^* = p^2 + (-1)^k(2k-1)q^2$$

Für $k = 2$ vgl. Seidelmann ([8], 233 für $e = 0$).

Die Formeln geben Anschluß an die Theorie der quadratischen Zahlen und dürften für arithmetische Untersuchungen zweckmäßig sein, wie wir sie im folgenden nur für $n = 3$ durchführen.

§ 4. Ganzzahlige Lösungen (n = 3)

Wenn a, b ganzzahlig sind, liegt es nahe, auch nach ganzzahligen Lösungen für die Gleichungen (1) (1)′ des Satzes 2 zu fragen. Wir beschränken uns hier auf den einer trinomischen kubischen Gleichung entspringenden Sonderfall $n = 3, l = 2$ der Gleichung (15) in der Form

$$(23) \qquad 4A^3 = 27B^2 + C^2$$

wo man bei vorgeschriebenem A aufgrund der Lehre von den (positiv definiten) quadratischen Formen bezw. der Theorie des imaginär-quadratischen Zahlkörpers $K(\varepsilon)$ alle Lösungen finden kann $\left(\varepsilon := \frac{-1+i\sqrt{3}}{2}\right)$. Ein rationaler Algorithmus, der ohne sonstige Hilfsmittel im Prinzip zu jedem A alle etwa vorhandenen Lösungen ergibt, ist z. B. in dem Patz-Arwinschen Kettenbruchverfahren verfügbar (vgl. [9] insb. (6.1) (6.2) und Satz 1). Doch dürfte es im allgemeinen günstiger sein, die Tatsache auszunützen, daß $\boldsymbol{Z}(\varepsilon)$ Hauptidealring ist. Bedeutet $\mathfrak{N}$ die Bildung der Norm in $\boldsymbol{Q}(\varepsilon)$, so besagt Gleichung (23)

$$A^3 = \mathfrak{N}\left(\frac{C}{2} - \frac{i\sqrt{3}}{2}\cdot 3B\right) = \mathfrak{N}(K - 3B\varepsilon) = \mathfrak{N}(3B - \varepsilon K),$$

wo jetzt $K := \frac{C-3B}{2} \in \mathbf{Z}$, da ja nach (23) $B \equiv C\,(2)$ (Vgl. hierzu Perron [7] (2)ff.). Andererseits ist nach (21)′ für jede Lösung $A = \mathfrak{N}(u' - \varepsilon v')$, $u', v' \in Q$, woraus sofort folgt, daß auch $A = \mathfrak{N}(U_0 - \varepsilon V_0)$, wo $U_0, V_0 \in \mathbf{Z}$. Zu gegebenem A dieser Form findet man dann (nach einem z. B. bei der Quadratsummendarstellung natürlicher Zahlen geläufigen) Verfahren alle B, C folgendermaßen: Das System $\mathfrak{S}$ der Primfaktoren π in $Z(\omega)$ (mit Vielfachheiten) für A^3 ist durch dasjenige für A (je bis auf eine Einheit) vollständig bestimmt. Man treffe eine bestimmte Wahl, so daß $A^3 = \prod_{\pi \in \mathfrak{S}} \pi$ und teile $\mathfrak{S}$ auf alle möglichen Arten in zwei Systeme $\mathfrak{P}$, $\overline{\mathfrak{P}}$ auf, wobei $\overline{\mathfrak{P}}$ genau die konjugierten Primfaktoren zu denen von $\mathfrak{P}$ enthalten soll (in dem Paar $\mathfrak{P}, \overline{\mathfrak{P}}$ wird die Reihenfolge nicht berücksichtigt). Dann ist für jede Lösung B, C die Zahl $3B - \varepsilon K$ für passendes $\mathfrak{P}$ assoziiert zu $\prod_{\pi \in \mathfrak{P}} \pi =: U - \varepsilon V$.[1] Es ist dann, entsprechend der Multiplikation mit den Einheiten $1, \varepsilon, \varepsilon^2$, zu prüfen, ob in einer Zeile (U^*, V^*) des Schemas

$$\begin{pmatrix} U, V \\ V, -U-V \\ -U-V, U \end{pmatrix} \tag{24}$$

eine durch 3 teilbare Zahl U^* auftritt. Jedesmal hat man dann mit

$$B := \frac{U^*}{3}, \quad K := V^*, \quad C := 3B + 2K = U^* + 2V^*$$

eine Lösung, wenn nur C nicht verschwindet. Dieser Ausnahmefall erscheint offenbar genau dann, wenn

(25) $A = 3A_1^2$ mit $A_1 \in \mathbf{Z}$. Damit sind, abgesehen von Vorzeichenumkehr bei B, C oder beiden, alle Möglichkeiten erschöpft.

---

[1] Die komplexe Primzahl π soll genau so oft als Faktor im Produkt auftreten, wie es die Vielfachheit in $\mathfrak{S}$ bezw. $\mathfrak{P}$, d. h. also in dem betreffenden Hauptdivisor angibt.

Die wegen
$-\varepsilon\cdot(U^*-\varepsilon^2 V^*)=V^*-\varepsilon U^*$ dem Übergang von $\mathfrak{P}$ zu $\overline{\mathfrak{P}}$ entsprechende Vertauschung von U^* mit V^* gibt nichts neues, da V^* schon in der ersten Spalte von (24) vorkommt, nur daß anstelle von $C=V^*+2U^*$ jetzt $C'=V^*-2(U^*+V^*)=-C$ entsteht womit die oben bereits festgesetzte Nichtberücksichtigung von $\overline{\mathfrak{P}}$ neben $\mathfrak{P}$ gerechtfertigt ist.

Jeder Darstellung $A=\mathfrak{N}(U_0-\varepsilon V_0)$ mit $\prod_{\pi\in\mathfrak{Q}_0}\pi=U_0-\varepsilon V_0$ entspricht durch Potenzieren insbesondere eine Darstellung $A^3=\mathfrak{N}\prod_{\pi\in\mathfrak{Q}_0}\pi^3=\mathfrak{N}(U_0-\varepsilon V_0)^3$, in der
$U-\varepsilon V=(U_0-\varepsilon V_0)^3$, $V=3U_0V_0(U_0+V_0)$, so daß man mit $B=V/3$ sicher zu einer Lösung gelangt, wenn nur

(26) $\qquad -C=(U_0-V_0)(2U_0+V_0)(2V_0+U_0)\neq 0$ wird.

$C=0$ tritt nur unter der Bedingung (25) auf, andernfalls hat das entstehende Polynom $f(x)=(x-U_0)(x-V_0)(x+U_0+V_0)$ mit den drei verschiedenen Wurzeln U_0, V_0, $-U_0-V_0$ aus K die Identität als Gruppe.

Wir wollen jetzt für einige Sonderfälle die Rechnungen durchführen; die Ergebnisse liefern uns zugleich Belege für grundsätzliche Feststellungen bezüglich der Bestimmung aller ganzzahligen Lösungen. Zunächst führen wir die Bezeichnung ein $\pi_n:=1-n\varepsilon(n=1,2,\ldots)$. π_n braucht nicht Primzahl zu sein, z. B. ist $\pi_4\sim\pi_1\overline{\pi}_2, \pi_9\sim\pi_2\overline{\pi}_3$, dagegen ist π_n prim für $n=1,2,3,5,6$.

Jetzt geben wir uns mit $\eta=a-\varepsilon b, a,b\in\boldsymbol{Z}, \mathfrak{N}(\eta)=:N\neq 0$ die Zahl $A=3N$ vor und bestimmen alle jene ganzzahligen Lösungen, die aus der Darstellung $A^3=\mathfrak{N}(U-\varepsilon V)$ mit

(27) $\qquad U-\varepsilon V=\pi_1^3\eta^3$ bezw. $\pi_1^2\eta^2\overline{\pi}_1\overline{\eta}$ entspringen.

Wenn η Primzahl ist, kommen so alle Lösungen zustande, denn wegen $\sqrt{-3}\sim\pi_1\sim\overline{\pi}_1$ brauchen nur die in (27) angegebenen Primpotenzprodukte in Betracht gezogen zu werden (die acht Möglichkeiten für $\mathfrak{P}$, die in der Tafel S. 131 für ein anderes Paar von Primfaktoren berücksichtigt sind, reduzieren sich aus dem angegebenen Grund hier auf zwei).

Bei der ersten Annahme (27) wird nun jede Zeile des Schemas (24) durch 3 teilbar, so daß wir schreiben können

$$(28)\quad B = \begin{cases} \frac{U}{3} = -a^3 + b^3 - 3ab^2 - 6a^2b = \\ \quad = (b-a)N - 3ab(2a+b) \qquad \text{oder} \\ \frac{V}{3} = 2a^3 - 2b^3 - 3ab^2 + 3a^2b = \\ \quad = (a-b)(a+2b)(2a+b) \qquad \text{oder} \\ -\frac{U+V}{3} = -a^3 + b^3 + 6ab^2 + 3a^2b = \\ \qquad = (b-a)N + 3ab(a+2b) \end{cases}$$

und entsprechend für das jeweils zugehörige C

$$\frac{-C}{3} = \begin{cases} 3(b-a)N + 9ab^2 \\ -9ab(a+b) \\ 3(a-b)N + 9a^2b. \end{cases}$$

Ferner gibt die zweite Annahme (27)

$$U - \varepsilon V = A(a - b - \varepsilon(a+2b))$$

das Schema

$$(29)\quad (U^*, V^*, C) = A \cdot \begin{pmatrix} a-b, a+2b, 3(a+b) \\ a+2b, -(2a+b), -3a \\ -(2a+b), a-b, -3b. \end{pmatrix}.$$

Fälle mit $C = 0$ sind dabei stets wegzulassen.

Für $a = 1, b = n \geq 0$ seien die Schlußformeln nochmals angegeben. Die nach der Bemerkung bei (26) zu reduziblen Gleichungen führenden Fälle sind hier und weiter unten mit einem Stern gekennzeichnet.

$$(28)'\quad B = \begin{cases} (n-1)N - 3n(n+2) \\ -(n-1)(2n+1)(n+2)^*, \\ (n-1)N + 3n(2n+1) \end{cases} \quad \frac{-C}{3} = \begin{cases} 3(n-1)N + 9n^2 \\ -9n(n+1) \\ -3(n-1)N + 9n \end{cases}$$

$$(29)'\quad B, C = N \cdot \begin{cases} -(n-1), 9(n+1) \\ 2n+1, -9 \\ -(n+2), -9n. \end{cases}$$

Für die Bedeutung der zugehörigen zyklischen Gleichungen in der Zahlentheorie des Körpers $\boldsymbol{Z}(\varepsilon)$ sei etwa auf Fueter R., Synthetische Zahlentheorie, De Gruyter 1925, Satz 18, S. 248ff. hingewiesen; dortige Beispiele: $a = 2,\ b = 3, N = 19;$

$$a = 1, n = 2, 3, 5$$
$$N = 7, 13, 31.$$

Da wir hier für $U - \varepsilon V$ nur Ansätze der Form (27), also jedenfalls vom Typ ζ^3 oder $\zeta^2\bar{\zeta}(\zeta \in \boldsymbol{Z}[\varepsilon])$ in Betracht gezogen haben, müssen die Endformeln auch aus den Perronschen Typen [7] für die ganzzahligen Werte $u = a - b, v = a + 2b$ der dortigen (rationalen) Parameter hervorgehen (an geeigneter Stelle). Entsprechendes gilt jedoch nicht allgemein. Vielmehr hat man etwa im Beispiel $A = 91 = \mathfrak{N}(\pi_2\pi_3)$ der folgenden Tafel acht wesentlich verschiedene Wahlen zur Festlegung von $\mathfrak{P}$ bezw. $U - \varepsilon V$ zu betrachten, und in der Hälfte dieser Fälle, nämlich in Zeile 3), 4), 5), 6), ist eine ganzzahlige Darstellung mittels der Perronschen Parameterformeln[1] tatsächlich unmöglich, da eine solche offenbar wegen $\pi_2 \sim \bar{\pi}_2, \pi_3 \sim \bar{\pi}_3$ der betreffenden Primzahlzerlegung von $U - \varepsilon V$ widersprechen würde.

Auf der folgenden Seite geben wir eine

Tafel aller ganzzahligen Lösungen der Gleichung

$$4A^3 - 27B^2 = C^2$$
$$\text{für } A = 7, 13, 91.$$

$$\pi_2 = 1 - 2\varepsilon, \pi_3 = 1 - 3\varepsilon, \pi_2\pi_3 = -5 - 11\varepsilon, \pi_2\bar{\pi}_3 \sim 1 - 9\varepsilon.$$

Für $A = 3, 9, 21, 39, 93$ ist auf (28)', (29)' mit
$n = 0, 1, 2, 3, 5$ zu verweisen.

---

[1] die ja alle auf solchen Zerlegungen fußen

A	$U - \varepsilon V$	$\lvert B\rvert$, $\lvert C\rvert$	
7	π_2^3	6, 20	*
	$\pi_2^2 \bar{\pi}_2 = 7\pi_2$	7, 7	
13	π_3^3	12, 70	*
	$\pi_3^2 \bar{\pi}_3 = 13\pi_3$	13, 65	
91	1) $\pi_2^3 \pi_3^3$	330, 272	*
	2) $\pi_2^3 \bar{\pi}_3^3$	90, 1672	*
	3) $\pi_2^2 \pi_3^3 \bar{\pi}_2 = 7\pi_2 \pi_3^3$	$7 \cdot$ 41, 127	
	4) $\pi_2 \pi_3^3 \bar{\pi}_2^2 = 7\bar{\pi}_2 \pi_3^3$	$7 \cdot$ 29, 197	
	5) $\pi_2^3 \pi_3^2 \bar{\pi}_3 = 13\pi_2^3 \pi_3$	$13 \cdot$ 5, 131	
	6) $\pi_2^3 \pi_3 \bar{\pi}_3^2 = 13\pi_2^3 \bar{\pi}_3$	$13 \cdot$ 25, 31	
	7) $\pi_2^2 \pi_3^2 \bar{\pi}_2 \bar{\pi}_3 = 91\pi_2 \pi_3$	$91 \cdot$ 2, 16	
	8) $\pi_2^2 \bar{\pi}_3^2 \bar{\pi}_2 \pi_3 = 91\pi_2 \bar{\pi}_3$	$91 \cdot$ 3, 11	

Bemerkung. Von den mit Stern bezeichneten Fällen abgesehen, sind die zugehörigen Gleichungen $x^3 - Ax + B = 0$ alle unzerlegbar, also zyklisch (Satz von Eisenstein).

Auch das Verfahren (27) ist zur Behandlung von $A = 3N$ unzureichend, wenn η keine Primzahl ist. Sei z. B. $A = 273 = \mathfrak{N}(\pi_1 \pi_2 \pi_3)$. Mit $\eta := \pi_2 \pi_3$ entstehen aus (28), (29), je drei Lösungen, ebenso mit $\eta' := \pi_2 \bar{\pi}_3 \sim \pi_9$ aus (28)', (29)' ($n = 9$).

Nun kann aber für $U - \varepsilon V$ auch gesetzt werden $\pi_1^3 H$, wenn H einer der Werte unter 3), 4), 5), 6) in der zweiten Spalte der Tafel ist, beispielsweise der erste. Er liefert vermöge

$$\varepsilon^2 (U - \varepsilon V) = 21(127 - 121\varepsilon)$$ noch die Lösungen

$$\lvert B\rvert = 7 \cdot \begin{Bmatrix} 127 \\ 121, \\ 248 \end{Bmatrix} \quad \lvert C\rvert = 21 \cdot \begin{Bmatrix} 369 \\ 375, \\ 6 \end{Bmatrix} \quad A = 273,$$

die wieder nicht aus einem Ansatz vom Typ ζ^3 oder $\zeta^2 \bar{\zeta}$ mit einem $\zeta = u - \varepsilon v$ bei $u, v \in \boldsymbol{Z}$ entspringen können.

Nachtrag (8. 7. 1974). Nach Einreichung der vorstehenden Note habe ich noch kennen gelernt: Nagell, T., Sur quelques catégories d'équations diophantiennes résolubles par des identités, Acta Arithmetica 9 (1964), 227–235, eine Arbeit, die sich teilweise mit § 1 und § 2 berührt. Aus *Theorem* 5.6. (a.a.O. S. 232/233) kann man nach einer dort allgemein möglichen (und erwünschten) Verschärfung (Ersetzung des Produktes MN durch das kleinste gemeinsame Vielfache $MN:(M,N)$) unseren Zusatz zu Satz 1 erhalten ($N = 2, M = l, P = n$). Ein Gegenstück zu unserem (entscheidenden) Satz 2 wird jedoch dort nicht gegeben. Ferner entsprechen *Theorem* 1.2. zusammen mit der *Bemerkung* (S. 230/232) dem Sonderfall $l \equiv \pm 1 (k)$ unseres Ergebnisses § 2 (9) ($k' = \pm 1, l' = \pm m$ bei $l = mk \pm 1$).

Schriftenverzeichnis

[1] Baker, H. F., Principles of Geometry, Vol. VI Cambridge University Press 1933.

[2] Baker, H. F., Some recent advances in the theory of algebraic surfaces. Proc. London Math. Soc. 12 (1913) 1–40.

[3] Castelnuovo-Enriques, Die algebraischen Flächen vom Gesichtspunkte der birationalen Transformationen aus. Enzyklopädie der mathem. Wissensch. II C 6b, 1915.

[4] Conforto, F., Le superficie razionali. Bologna Zanichelli 1939.

[5] Mordell, L. J., On Ryley's solution of $x^3 + y^3 + z^3 = n$. J. London Math. Soc. 17 (1942) 194–196.

[6] Noether, E., Gleichungen mit vorgeschriebener Gruppe. Math. Ann. 78 (1918), 221–229.

[7] Perron, O., Eine Liste von zyklischen kubischen Gleichungen. J. reine angew. Math. 262/263 (1973) 234–238.

[8] Seidelmann, F., Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitätsbereich. Diss. Erlangen 1916, Auszug Math. Ann. 78 (1918) 230–233.

[9] Schmidt, Hermann, Über das Kettenbruchverfahren von Patz und Arwin zur Darstellung von Zahlen durch positiv definite binäre quadratische Formen. Sitzgsber. Bayer. Akad. Wiss., Math.-nat. Klasse 1966, 5–12.