# Bemerkung zu meiner Arbeit „Über die Gleichungen dritten und vierten Grades in endlichen Körpern“[1]).

Von L. RÉDEI in Szeged.

Nach zwei Arbeiten von SKOLEM[2]), [3]) über die Lösbarkeit der Kongruenzen dritten Grades nach einem Primzahlmodul habe ich in der Arbeit [1]) unter anderem die Anzahl der Wurzeln dieser Kongruenzen in jedem Falle genau bestimmt (s. Satz 1 in der Arbeit [1])). Mein Resultat bezieht sich viel allgemeiner auf die ähnliche Frage über die Gleichungen dritten Grades im endlichen Körper $k$ mit $q$ Elementen, unterworfen der einzigen Einschränkung, daß die Charakteristik $p$ von 2, 3 verschieden ist. Hier werde ich diese Frage auf eine andere Art behandeln, und so wird die Antwort in einer neuen, überraschend eleganter Form erscheinen. Als wesentlich neues stellt sich heraus, daß die Anzahl der Wurzeln nur von einer Invariante (s. unten) der Gleichung abhängt[4]), und dabei erscheinen (im Gegensatz zur Arbeit [1])) beide Fälle $3|q-1$, $3|q+1$ in völliger Symmetrie. Ich hoffe, daß nach diesem Anfang

---

[1]) *Dieser Band*, S. 96—105. Diese Arbeit wird durch die vorliegende in keiner Hinsicht überflüssig gemacht. Die auf S. 97. aus dem *Zentralblatt für Math.* zitierten Resultate von SKOLEM sind mit der Einschränkung $a \not\equiv 0 \pmod{p}$ zu verstehen, was das Referat unbemerkt ließ. Ohne diese Einschränkung lauten die Resultate einfacher (vgl. S. 104, Fußanmerkung [8])).

[2]) TH. SKOLEM, Zwei Sätze über kubische Kongruenzen, *Det Kongelige Norske Videnskaber Selskab Forhandlinger*, **10** (1937), S. 89—92. Diese Arbeit ist mir erst neulich bekannt geworden. Der Inhalt ist im wesentlichen die erste Hälfte von Satz 1 meiner Arbeit [1]) für den Spezialfall, daß $k$ ein Primkörper ist, und ein Teil der darauffolgenden Formel $(16_2)$. SKOLEM bedient sich in seiner Arbeit eines biquadratischen (Dirichletschen) Zahlkörpers.

[3]) Zitiert in der Arbeit [1]) auf S. 97.

[4]) Das ist merkwürdig aus dem Grunde, daß es drei Möglichkeiten (keine, eine oder drei Wurzeln) gibt. Im „klassischen“ Fall, wo $k$ der Körper der reellen Zahlen ist, gibt es nur zwei Möglichkeiten (eine oder drei Wurzeln).

sich auch die Gleichungen höheren Grades in endlichen Körpern ähnlich behandeln lassen werden. Das klingt nicht unglaublich, da dieses Problem im bekannten Satz von KÖNIG-RADOS eine Antwort gewonnen hat, und zwar bestimmt dieser die Anzahl der Wurzeln einer Gleichung (vom Grade $\leq q-2$) in $k$ aus einer einzigen Invariante, dem Rang der aus den Koeffizienten gebildeten zyklischen Matrix[5]). Ich bemerke noch, daß ich einige Hilfsmittel allgemeiner entwickle, als das zu unserem obigen Zweck nötig ist; auch werde ich am Schluß der Arbeit zeigen, wie die hier zu gewinnende neue Form von Satz 1 der Arbeit [1]) sich auch aus diesem Satz herleiten läßt. Übrigens haben die „alte" und „neue" Form der Lösung unseres Problems jede einen Vorteil über den anderen.

Ein Polynom in $k$ nennen wir kurz ein $k$-Polynom. Irgendein Polynom mit rationalen Koeffizienten läßt sich üblicherweise auch als ein $k$-Polynom auffassen, wenn nur die Koeffizienten für $p$ ganz sind (d. h. einen, zu $p$ primen Nenner haben). Den (eindeutig bestimmen) endlichen Erweiterungskörper vom Grade $n$ über $k$ bezeichnen wir mit $k_n$.

Wir geben eine Gleichung dritten Grades in $k$ in der allgemeinen Form

$$f(x) = a_0x^3 + a_1x^2 + a_2x + a_3 = 0 \qquad (a_0 \neq 0) \tag{1}$$

an, und setzen voraus, daß die Diskriminante $\neq 0$ ist. Dann sind die Wurzeln $x_1, x_2, x_3$ verschieden, sie liegen in $k_1$, $k_2$ oder $k_3$. Wir setzen

$$y_1 = x_2 - x_3, \quad y_2 = x_3 - x_1, \quad y_3 = x_1 - x_2 \tag{2}$$

und ähnlich

$$z_1 = y_2 - y_3, \quad z_2 = y_3 - y_1, \quad z_3 = y_1 - y_2, \tag{3}$$

d. h.

$$z_i = x_1 + x_2 + x_3 - 3x_i \qquad (i = 1, 2, 3), \tag{4}$$

führen dann die Invariante[6]) ·

$$\Delta = -\frac{(z_1 z_2 z_3)^2}{27\,(y_1 y_2 y_3)^2} \tag{5}$$

ein. Offenbar ist $\Delta$ eine (rationale) symmetrische Funktion der $x_i$, die sich also durch die $a_i$ ausdrücken läßt. Genauer gesagt, $(y_1 y_2 y_3)^2$ und $z_1 z_2 z_3$ sind für sich symmetrisch in den $x_i$. Das erste von ihnen ist die Diskriminante von (1):

$$D = (y_1 y_2 y_3)^2 = (x_1 - x_2)^2 (x_2 - x_3)^2 (x_3 - x_1)^2, \tag{6}$$

---

[5]) Leider läßt sich dieser Rang schwer bestimmen. Das ist der Grund, daß der König-Radossche Satz bisher keine Anwendung fand. Es scheint eine schwere, aber sich lohnende Aufgabe zu sein, aus diesem Satz meine Resultate über die Anzahl der Wurzeln der Gleichungen dritten und vierten Grades abzuleiten.

[6]) Es ist nämlich $\Delta$ eine absolute Invariante gegenüber linearer Transformationen $x = ux' + v$ von (1).

das zweite ist:

$$P = z_1 z_2 z_3 = \frac{27}{a_0} f\left(\frac{x_1+x_2+x_3}{3}\right) = \frac{27}{a_0} f\left(\frac{-a_1}{3a_0}\right). \tag{7}$$

Dann gilt[7])

$$J = -\frac{P^2}{27D}. \tag{8}$$

Weiter führen wir für jede natürliche Zahl $n$ die $k$-Polynome

$$\varphi_n(x) = \binom{n}{1} + \binom{n}{3}x + \binom{n}{5}x^2 + \ldots = \frac{1}{2\sqrt{x}}\left((1+\sqrt{x})^n - (1-\sqrt{x})^n\right) \tag{9}$$

ein. Abgesehen vom uninteressanten Fall $p \mid n$ ist $\varphi_n(x)$ vom Grade $\left[\frac{n-1}{2}\right]$, wobei $[x]$ die größte ganze Zahl $\leq x$ bezeichnet. Zu unserer Frage über (1) wird $\varphi_n(x)$ nur für $n = q+1$, $\left[\frac{q+1}{3}\right]$ in Betracht kommen, ausführlich geschrieben:

$$\varphi_{q+1}(x) = 1 + x^{\frac{q-1}{2}} \tag{10}$$

und

$$\varphi_{\frac{q-1}{3}}(x) = \binom{\frac{q-1}{3}}{1} + \binom{\frac{q-1}{3}}{3}x + \binom{\frac{q-1}{3}}{5}x^2 + \ldots + \binom{\frac{q-1}{3}}{\frac{q-4}{3}}x^{\frac{q-7}{6}} \tag{11}$$

$$(3 \mid q-1),$$

bzw.

$$\varphi_{\frac{q+1}{3}}(x) = \binom{\frac{q+1}{3}}{1} + \binom{\frac{q+1}{3}}{3}x + \binom{\frac{q+1}{3}}{5}x^2 + \ldots + \binom{\frac{q+1}{3}}{\frac{q-2}{3}}x^{\frac{q-5}{6}} \tag{12}$$

$$(3 \mid q+1).$$

Alle drei (wie überhaupt jedes $\varphi_n(x)$ mit $2 \mid n$) sind symmetrische Polynome, selbst (10) ist das eine der Eulerschen Polynome[8]) $1 \pm x^{\frac{q-1}{2}}$. Wir betonen, daß diese Polynome (10), (11), (12) (von (1) nicht) nur von $k$ abhängen.

Der angekündigte Satz lautet so:

---

[7]) Ausführlich lautet $P = \frac{1}{a_0^3}(2a_1^3 - 9a_0a_1a_2 + 27a_0^2a_3)$. Der zweite Faktor spielt in der Theorie der Invarianten eine Rolle. Nimmt man (1) in der Form $x^3 + ax + b = 0$ an, so ist einfach $D = -4a^3 - 27b^2$, $P = 27b$, $\Delta = \frac{27b^2}{4a^3 + 27b^2}$.

[8]) Diese zerfallen voll in $k$ und haben zu Nullstellen alle (von 0 verschiedenen) Quadrate bzw. Nichtquadrate in $k$.

Satz 1. *Bezeichne $\nu$ die Anzahl der Wurzeln von* (1) *in $k$. Den Fall $\Delta = 0$ schließen wir aus*[9]). *Es ist dann und nur dann $\nu = 1$, wenn*

$$\varphi_{q+1}(-3\Delta) = 0. \tag{13}$$

*Im anderen Fall ist $\nu = 0$ oder 3, letzteres dann und nur dann, wenn*

$$\varphi_{\left[\frac{q+1}{3}\right]}(\Delta) = 0. \tag{14}$$

Die erste Hälfte des Satzes werden wir als Spezialfall aus folgendem allgemeinen Satz gewinnen[10]):

Satz 2. *Die Diskriminante eines $k$-Polynoms ohne mehrfachen Teiler ist dann und nur dann ein Quadrat in $k$; wenn die Anzahl der irreduzibilen Faktoren von geradem Grad eine gerade Zahl ist.*

Da die multiplikative Gruppe der von 0 verschiedenen Elemente von $k$ zyklisch und von gerader Ordnung ist, so genügt es wegen der multiplikativen Eigenschaft der Diskriminante zu beweisen, daß die Diskriminante eines irreduzibilen $k$-Polynoms $f(x)$ vom Grade $n$ dann und nur dann ein Quadrat in $k$ ist, wenn $n$ ungerade ist. Die Wurzeln von $f(x)$ liegen $k_n$. Mit Hilfe eines erzeugenden Automorphismus $S$ von $k_n/k$ lassen sie sich in der Form $S^i\alpha\,(i = 0, \ldots, n-1)$ annehmen. Die Diskrikriminante von $f(x)$ ist das Quadrat von

$$\delta = \prod_{0 \leq i < j \leq n-1} (S^i\alpha - S^j\alpha).$$

Da offenbar $S\delta = (-1)^{n-1}\,\delta$ gilt, so liegt $\delta$ dann und nur dann in $k$, wenn $n-1$ gerade, d. h. $n$ ungerade ist. Satz 2 ist also richtig.

Insbesondere für das $k$-Polynom $f(x)$ in (1) spricht dieser Satz aus, daß es dann und nur dann einen irreduzibilen Faktor zweiten Grades, d. h. eine einzige Nullstelle in $k$ hat, wenn $D$, d. h. nach (8), $-3\Delta$ kein Quadrat in $k$ ist. Nach (10) ist die Bedingung hierfür eben (13), womit wir die erste Hälfte von Satz 1 bewiesen haben.

Für das übrige setzen wir in $k_2$:

---

[9]) Im Fall $\Delta = 0$ ist $P = 0$, nach (7) hat also (1) die Wurzel $\frac{-a_1}{3a_0}$; dann ist nach Satz 1 der Arbeit [1]) $\nu = 1$ oder 3, je nachdem $D$ kein Quadrat oder ein Quadrat in $k$ ist. — Im Fall $\Delta \neq 0$ darf man in (13) und (14) $\Delta$ durch $\Delta' = \frac{1}{\Delta}$ ersetzen; das ist von Vorteil, wenn die Gleichung $x^3 + ax + b = 0$ vorgelegt wird, denn dann berechnet man $\Delta' = 1 + \frac{4a^3}{27b^2}$ einfacher als $\Delta$ (vgl. [7])).

[10]) Mir war dieser einfache Satz bisher unbekannt. Für die Neuheit des Satzes spricht auch die Arbeit [2]) von Skolem, die im wesentlichen einen (verhältnismäßig komplizierten) Beweis für den Spezialfall enthält, wo $k$ ein Primkörper und das vorgelegte Polynom vom dritten Grade ist.

(15) $\varrho = \frac{-1+\sqrt{-3}}{2}$ $\left(\varrho^2 = \frac{-1-\sqrt{-3}}{2},\ \varrho^3 = 1\right)$.

Im Fall $3|q-1$ liegen $\varrho$, $\varrho^2$ in $k$, im Fall $3|q+1$ sind sie konjugiert in $k_2/k$.

Zunächst wollen wir (14) umgestalten. Für irgendein $c$ ($\neq 0$) in $k$ ist $\varphi_n(c)=0$ nach (9) äquivalent mit

(16) $$\left(\frac{1+\sqrt{c}}{1-\sqrt{c}}\right)^n = 1.$$

Nach (8) können wir also (14) in der Form

(17) $$\left(\frac{P+\sqrt{-27D}}{P-\sqrt{-27D}}\right)^{\left[\frac{q+1}{3}\right]} = 1$$

schreiben. Der Nenner ist nach (6), (7) und (3) gleich

$$(y_1-y_2)(y_2-y_3)(y_3-y_1)-3y_1y_2y_3\sqrt{-3}.$$

Wegen (2) ist

(18) $$y_1+y_2+y_3=0,$$

und so bekommen wir weiter

$$(y_1-y_2)(y_1+2y_2)(-2y_1-y_2)+3y_1y_2(y_1+y_2)\sqrt{-3},$$

d. h.

$$-2y_1^3+3y_1^2y_2(-1+\sqrt{-3})+3y_1y_2^2(1+\sqrt{-3})+2y_2^3.$$

Dies ist nach (15) gleich $-2(y_1-\varrho y_2)^3$. Ähnliches gilt für den Zähler in (17) (mit $\varrho^2$ statt $\varrho$), und so geht dies in

(19) $$\left(\frac{y_1-\varrho^2 y_2}{y_1-\varrho y_2}\right)^{3\left[\frac{q+1}{3}\right]} = 1$$

über. Das ist die gewünschte andere Form von (14).

Zur zweiten Hälfte von Satz 1 genügt es zu beweisen, daß (19) im Fall $\nu=3$ richtig, im Fall $\nu=0$ falsch ist. Wir schicken die Bemerkung voraus, daß die Zuordnung $x \to x^q$ ein erzeugender Automophismus für jeden Relativkörper $k_n/k$ ist. Im Fall $\nu=0$ wählen wir die Numerierung so, daß $x_1^q = x_2$ (also auch $x_2^q = x_3$, $x_3^q = x_1$) gilt. Dann gilt gleiches für die $y_i$.

Betrachten wir zuerst den Fall $3|q-1$. Dann ist der Exponent in (19) gleich $q-1$, und so läßt sich dies in der Form

(19′) $$\left(\frac{y_1-\varrho^2 y_2}{y_1-\varrho y_2}\right)^q = \frac{y_1-\varrho^2 y_2}{y_1-\varrho y_2}$$

schreiben. Ist $\nu=3$, so liegt jedes $y_i$ in $k$, und dann ist (19′) richtig. Ist dagegen $\nu=0$, so ist die linke Seite von (19′) mit Rücksicht auf (18) gleich

$$\frac{y_2-\varrho^2 y_3}{y_2-\varrho y_3}=\varrho\,\frac{\varrho y_2-y_3}{\varrho^2 y_2-y_3}=\varrho\,\frac{y_1+(1+\varrho)y_3}{y_1+(1+\varrho^2)y_2}=\varrho\,\frac{y_1-\varrho^2 y_2}{y_1-\varrho y_2},$$

folglich ist jetzt (19′) falsch.

Betrachten wir nun den Fall $\nu=0$. Jetzt ist der Exponent in (19) $q+1$, und so läßt sich dies in der Form

$$\left(\frac{y_1-\varrho^2 y_2}{y_1-\varrho y_2}\right)^q=\frac{y_1-\varrho y_2}{y_1-\varrho^2 y_2} \tag{19″}$$

schreiben. Wegen $\varrho^q=\varrho^2$ ist dies im Fall $\nu=3$ richtig. Dagegen im Fall $\nu=0$ ist die linke Seite nach einer ähnlichen Rechnung wie oben das $\varrho^2$-fache der rechten Seite, und so ist jetzt (19″) falsch. Damit haben wir Satz 1 bewiesen.

Um zu zeigen, daß sich Satz 1 auch aus Satz 1 der Arbeit [1]) gewinnen läßt, beweisen wir als Vorbereitung folgenden, auch an sich interessanten Satz (den wir zum genannten Zweck nur für $e=3$ anwenden werden).

Wir bezeichnen mit $\alpha, \alpha'$ entweder ein Elementenpaar in $k$ oder ein (über $k$) konjugiertes Elementenpaar in $k_2$, beidesmal eingeschränkt durch $\alpha \neq \pm\alpha'$, so daß also

$$\alpha=r(1+\sqrt{s}),\qquad \alpha'=r(1-\sqrt{s})\qquad (r,s\neq 0) \tag{20}$$

gesetzt werden kann mit eindeutig bestimmten $r, s$ in $k$. Dann gilt der:

Satz 3. *Ist $\alpha, \alpha' \in k$ und $\alpha\alpha'$ eine $e$-te Potenz in $k$ mit $e \mid q-1, 2 \nmid e$, so ist $\alpha$ (zugleich auch $\alpha'$) dann und nur dann eine $e$-te Potenz in $k$, wenn*

$$\varphi_{\frac{q-1}{e}}(s)=0. \tag{21}$$

*Ist $\alpha, \alpha' \in k$, $e \mid q+1$ $(e>0)$, so ist $\alpha$ (zugleich auch $\alpha'$) dann und nur dann eine $e$-te Potenz in $k_2$, wenn*

$$\varphi_{\frac{q+1}{e}}(s)=0. \tag{22}$$

Im ersten Fall ist nämlich $(\alpha\alpha')^{\frac{q-1}{e}}=1$, ferner ist $\alpha$ dann und nur dann eine $e$-te Potenz in $k$, wenn $\alpha^{\frac{q-1}{e}}=1$ ist. Da die linke Seite eine $e$-te Einheitswurzel in $k$, also gewiß $\neq -1$ ist, so darf diese Bedingungsgleichung durch

$$\alpha^{2\frac{q-1}{e}}=\left(\frac{\alpha}{\alpha'}\right)^{\frac{q-1}{e}}=1$$

ersetzt werden. Nach (20) und (16) ist dies in der Tat äquivalent mit (21).

Im zweiten Fall ist $\alpha$ dann und nur dann eine $e$-te Potenz in $k_2$, wenn

$$\alpha^{\frac{q^2-1}{e}}=1$$

ist. Wegen $\frac{q^2-1}{e} = q\frac{q+1}{e} - \frac{q+1}{e}$ und $\alpha'' = \alpha'$ geht diese Gleichung in

$$\left(\frac{\alpha'}{\alpha}\right)^{\frac{q-1}{e}} = 1$$

über. Letztere ist wieder nach (20) und (16) äquivalent mit (22). Satz 3 haben wir also bewiesen.

Nunmehr können wir Satz 1 folgenderweise auch aus dem Satz 1 der Arbeit [1]) gewinnen. Da $\Delta$ eine Invariante ist[6]), dürfen wir uns auf den Spezialfall $x^3+ax+b=0$ von (1) beschränken. Vor (15) haben wir schon gesehen, daß beide Sätze den Fall $\nu=1$ im wesentlichen gleich erledigen. Im anderen Fall ($\nu=0$ oder 3) ist nach dem Satz 1 der Arbeit [1]) dann und nur dann $\nu=3$, wenn

$$\alpha = -\frac{b}{2}+\frac{1}{18}\sqrt{-3D} = -\frac{b}{2}\left(1+\sqrt{\frac{-D}{27b^2}}\right) = -\frac{b}{2}\left(1+\sqrt{\frac{1}{\Delta}}\right)$$

eine dritte Potenz in $k$ $(3|q-1)$, bzw. $k_2$ $(3|q+1)$ ist. Dabei gilt nach (6) der Arbeit [1]) $\alpha\alpha' = \left(\frac{-a}{3}\right)^3$, und so läßt sich Satz 3 mit $e=3, s=\frac{1}{\Delta}$ anwenden. In den bezüglichen Bedigungsgleichungen (21), (22) läßt sich $\frac{1}{\Delta}$ durch $\Delta$ ersetzen, und dann können wir beide in der Form (14) schreiben. Das ist der gewünschte zweite Beweis von Satz 1.[11])

*(Eingegangen am 16. Januar 1947.)*

---

[11]) Wir bemerken noch folgendes. Aus (9) folgt $\varphi_{q-1}(x) = -(1-x)^{-1}\left(1-x^{\frac{q-1}{2}}\right)$ (vgl (10)). Weiter gilt allgemein $\varphi_n(x)\,|\,\varphi_{n'}(x)$ $(n|n')$. Hieraus folgt

$$\varphi_n(x)\,|\,1-x^{\frac{q-1}{2}} \quad (n|q-1), \quad \varphi_n(x)\,|\,1+x^{\frac{q-1}{2}}\,(n|q+1),$$

und so zerfällt $\varphi_n(x)$ $(n|q\pm 1)$ in $k$ voll (vgl. [8])). Dies bezieht sich inbesondere auf $\varphi_{\left[\frac{q+1}{3}\right]}(x)$, und das bedeutet, daß im Satz 1 der Grad von (14) nicht erniedrigt werden kann. — Satz 1 wollen wir noch anders formulieren. Wir bezeichnen das vorhergenannte Polynom mit $A(x)$, setzen $B(x)=\varphi_{q+1}(-3x)=1+x^{\frac{q-1}{2}}$ bzw. $1-x^{\frac{q-1}{2}}$ je nachdem $3|q-1$ oder $3|q+1$ ist, und definieren das (ganze) Polynom $C(x)$ durch

$$1-x^{q-1} = A(x)\,B(x)\,C(x).$$

Dann läßt sich Satz 1 so aussprechen: Im Fall $\Delta \neq 0$ ist $\nu=3,1,0$, je nachdem $A(\Delta), B(\Delta), C(\Delta)=0$ ist. — Fassen wir jetzt $\varphi_n(x)$ als ein ganzzahliges Polynom auf, so läßt sich obiges für den Spezialfall $q=p$ folgenderweise sagen: Für die Primzahlen von der Form $p=nt\pm 1$ hat die Kongruenz $\varphi_n(x)\equiv 0 \pmod p$ so viel Lösungen, wie der Grad ist. — Abgesehen vom Satz 1 gelten die Feststellungen dieser Arbeit auch für $p=3$.