Über die Gleichungen dritten und vierten Grades in endlichen Körpern.

Von LADISLAUS RÉDEI in Szeged.

Ist irgendein Körper k mit einer Charakteristik $\neq 2, 3$ zu Grunde gelegt, so lassen sich bekanntlich die Gleichungen dritten und vierten Grades durch eine lineare Transformation auf die Form

$$x^3 + ax + b = 0, \tag{1}$$

$$x^4 + Ax^2 + Bx + C = 0 \tag{2}$$

bringen, weiter sind sie (durch Radikale) auflösbar. Selbst die Berechnung der Wurzeln wird für (1) durch die Formel von CARDANO ermöglicht, bzw. für (2) mit Hilfe einer kubischen Resolvente auf den vorigen Fall zurückgeführt. Dabei erfordern die auftretenden Radikale in vielen Fällen eine Erweiterung des Grundkörpers, bekanntlich eventuell auch bei der Berechnung der Wurzeln, die in k liegen. So ist das klassische Problem entstanden, wie es sich mit den in k liegenden Wurzeln verhält, und zwar was ihre Zahl ist, wann und wie sie sich durch ein endliches Rechenverfahren (eine „Wurzelformel") ohne eine Erweiterung von k berechnen lassen?

Bekanntlich sind diese Fragen im historisch ersten Fall vollkommen erledigt, wenn k der Körper der reellen Zahlen ist. Für andere Grundkörper ist das Problem im allgemeinen nicht gelöst worden. Ich kann nur die bekannte Tatsache nennen, daß die in k liegenden Wurzeln (auch bei Gleichungen höheren Grades) sich mit endlich vielen Versuchen bestimmen lassen, wenn k (der absolut rationale Zahlkörper oder allgemeiner) ein absolut algebraischer Zahlkörper endlichen Grades ist.

Von nun an beschäftigen wir uns mit dem Fall, wo k ein endlicher Körper[1]) ist. Merkwürdigerweise fehlten bisher in diesem, für die Zahlentheorie sehr wichtigen und auch an sich interessanten Fall die entspre-

[1]) Man kann also (1) und (2) auch als Kongruenzen nach einem Primidealmodul in einem absolut algebraischen Zahlkörper endlichen Grades deuten.

chenden Untersuchungen, außer einer unlängst erschienenen kleinen Arbeit von SKOLEM[2]), obwohl sich jetzt die aufgeworfenen Fragen im großen Teil und teilweise sehr elegant beantworten lassen. Eine vollständige Beantwortung ist mir aber nicht gelungen[3]).

Bevor wir unsere Resultate zusammenstellen, rekapitulieren hier kurz die Auflösung der Gleichungen (1) und (2).

Die drei Wurzeln von (1) sind nach der Formel von CARDANO

$$x_1 = \sqrt[3]{\alpha} + \sqrt[3]{\alpha'}, \quad x_2 = \varrho\sqrt[3]{\alpha} + \varrho'\sqrt[3]{\alpha'}, \quad x_3 = \varrho'\sqrt[3]{\alpha} + \varrho\sqrt[3]{\alpha'}, \tag{3}$$

wobei 1, ϱ, ϱ' die drei Werte von $\sqrt[3]{1}$ sind[4]),

$$\alpha = -\frac{b}{2} + \frac{1}{18}\sqrt{-3D}, \quad \alpha' = -\frac{b}{2} - \frac{1}{18}\sqrt{-3D} \tag{4}$$

und

$$D = -4a^3 - 27b^2 \tag{5}$$

die Diskriminante von (1) ist; die Radikale $\sqrt{-3D}$, $\sqrt[3]{\alpha}$ sind beliebig, aber fest zu wählen, während $\sqrt[3]{\alpha'}$ nach

$$\sqrt[3]{\alpha}\sqrt[3]{\alpha'} = -\frac{a}{3} \tag{6}$$

zu bestimmen ist.

---

[2]) TH. SKOLEM, Die Anzahl der Wurzeln der Kongruenz $x^3 + ax + b \equiv 0$ mod p für die verschiedenen Paare a, b, *Det Kongl. Norske Vid. Selskab Forhandl.*, **14** (1942), S. 161—164. Mir war diese Arbeit bisher nicht zugänglich. Nach dem Referat im *Zentralblatt f. Math.*, **28** (1944), S. 203 sollte der Inhalt der Arbeit folgendes sein: „Für eine Primzahl $p \equiv 1$ mod 3 hat die Titelkongruenz der Reihe nach für $p-1$, $\frac{1}{2}p(p-1)$, $\frac{1}{3}(p-1)^2$, $\frac{1}{6}(p-4)(p-1)$ Paare a, b zwei, eine, keine oder drei Wurzeln. Für $p \equiv 2$ mod 3 und zwar $p > 2$ sind die entsprechenden Anzahlen $p-1$, $\frac{1}{2}(p-2)(p-1)$, $\frac{1}{3}(p+1)(p-1)$, $\frac{1}{6}(p-2)(p-1)$." Das ist aber falsch schon aus dem Grunde, daß die Summe der angeführten vier Anzahlen (in beiden Fällen) p^2-p ist, wobei es doch p^2 Paare a, b gibt. Siehe die Verbesserung im Anhang am Ende meiner Arbeit [insbesondere [8]], wo ich kurz auf ähnliche Fragen über (1) und (2) eingehe. Hier erwähne ich, daß ich vorliegende Arbeit mit weniger vollkommenen Resultaten unlängst auch im *Math. u. Naturwiss. Anzeiger d. Ung. Akad.* publiziert habe (in ungarischer Sprache).

[3]) Ich konnte nämlich in einigen Fällen keine Wurzelformel für die in k liegenden Wurzeln von (1) und (2) angeben, mit der man ohne Körpererweiterung auskommt, noch konnte ich den entsprechenden Unmöglichkeitsbeweis erbringen, was auch kein leichtes Problem zu sein scheint.

[4]) Wie üblich, bezeichnen wir die Elemente des in k enthaltenen Primkörpers ebenso wie die absolut rationalen Zahlen, woraus aber kein Mißverständnis entstehen wird.

Die vier Wurzeln von (2) sind

$$x_1=\frac{1}{2}(\quad \sqrt{y_1}-\sqrt{y_2}-\sqrt{y_3}), \tag{7}$$

$$x_2=\frac{1}{2}(-\sqrt{y_1}+\sqrt{y_2}-\sqrt{y_3}), \tag{8}$$

$$x_3=\frac{1}{2}(-\sqrt{y_1}-\sqrt{y_2}+\sqrt{y_3}), \tag{9}$$

$$x_4=\frac{1}{2}(\quad \sqrt{y_1}+\sqrt{y_2}+\sqrt{y_3}), \tag{10}$$

wobei y_1, y_2, y_3 die drei Wurzeln der kubischen Resolvente

$$y^3+2Ay^2+(A^2-4C)y-B^2=0 \tag{11}$$

bedeuten; die Radikale $\sqrt{y_1}$, $\sqrt{y_2}$, $\sqrt{y_3}$ sind mit der Einschränkung

$$\sqrt{y_1}\,\sqrt{y_2}\,\sqrt{y_3}=-B \tag{12}$$

(sonst beliebig) zu wählen. Hieraus folgt

$$y_1=(x_1+x_4)^2,\quad y_2=(x_2+x_4)^2,\quad y_3=(x_3+x_4)^2. \tag{13}$$

Man kann auch so verfahren, daß man nur ein Radikal $r=\sqrt{y_i}$ bestimmt, mit dem dann (2) in die Gleichung

$$\left(x^2+rx+\frac{r^3+Ar-B}{r}\right)\left(x^2-rx+\frac{r^3+Ar+B}{r}\right)=0 \tag{14}$$

zerfällt, so daß man zur Berechnung der x_i nur noch die Auflösung von zwei quadratischen Gleichungen braucht. Die Diskriminanten von (2) und (11) sind gleich.

Wir bezeichnen mit q die Anzahl der Elemente von k und mit $\chi_e(x)$ einen beliebigen Charakter e-ten Grades in der multiplikativen Gruppe $q-1$-ter Ordnung, gebildet aus allen Elementen $x(\neq 0)$ von k $(e|q-1)$. Insbesondere bedeutet dann $\chi_e(x)=1$, daß $x(\neq 0)$ eine e-te Potenz ist. Für χ_2 schreiben wir einfach χ.

Den Erweiterungskörper vom Relativgrad n über k bezeichnen wir mit k_n, der also der endliche Körper mit q^n Elementen ist. Insbesondere ist $k_1=k$. Unter allen k_n $(n>1)$ werden uns nur k_2, k_3, k_4 interessieren. Für k_n $(n>1)$ werde der Charakter mit $\chi_e(x, k_n)$ bezeichnet.

Den Zerfällungskörper der Gleichungen (1), (2) und $x^3-1=0$ bezeichnen wir der Reihe nach mit Z_1, Z_2, Z. Diese sind also die kleinsten Körper über k, in denen die genannten Gleichungen ihre sämtlichen Wurzeln haben. Offenbar ist $Z_1=k$, k_2 oder k_3 und $Z_2=k$, k_2, k_3 oder k_4. Weiter gilt entweder

$$Z=k,\quad \chi(-3)=1 \qquad (3|q-1) \tag{15$_1$}$$

oder

$$(15_2) \qquad Z = k_2, \quad \chi(-3) = -1 \qquad (3 \mid q+1).$$

Man kann Z auch als den kleinsten Körper über k definieren, in dem $\chi_3(x, Z)$ sinnvoll ist.

Wir nehmen an, daß die Diskriminanten unserer Gleichungen (1), (2) und die Koeffizienten a, b, B nicht verschwinden, wodurch wir nur leichte Fälle ausgeschlossen haben, insbesondere auch das Vorhandensein von mehrfachen Wurzeln.

Satz 1. *Die Gleichung* (1) *hat genau eine Wurzel in k dann und nur dann, wenn* $\chi(D) = -1$ *ist. Im anderen Fall* $\chi(D) = 1$ *liegt* α *in* Z *und dann hat* (1) *keine oder drei Wurzeln in k, je nachdem* $\chi_3(\alpha, Z) \neq 1$ *oder* $= 1$ *ist. Die Anwendung dieses Satzes macht keine Erweiterung von k nötig, das ja klar ist mit Ausnahme des Falles* $\chi(D) = 1$, $Z = k_2$ (*d. h.* $3 \mid q+1$). *Aber in diesem Fall genügt es nur die Entwicklungsglieder der Potenz*

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

zu berechnen, die eine gerade Potenz von $\sqrt{-3D}$ *enthalten, da ihre Summe offenbar dann und nur dann* $= 1$ *ist, wenn* $\chi_3(\alpha, Z) = 1$ *gilt*[5]).

Satz 2. *Hat* (1) *genau eine Wurzel in k, so läßt sie sich statt* (3) *auch durch die Formel*

$$(16_1) \qquad -\frac{3}{a}\left(\alpha^{\frac{q+2}{3}} + \alpha'^{\frac{q+2}{3}}\right) \qquad (3 \mid q-1)$$

bzw.

$$(16_2) \qquad \alpha^{\frac{2q-1}{3}} + \alpha'^{\frac{2q-1}{3}} \qquad (3 \mid q+1)$$

angeben. Keine dieser Formeln macht eine Erweiterung von k nötig und man braucht nicht einmal dann die Quadratwurzel aus $-3D$ *zu berechnen, wenn diese in k liegt, da die ungeraden Potenzen des Radikals* $\sqrt{-3D}$ *wegen der Addition herausfallen.*

Hat (1) *drei Wurzeln in k und liegt erstens der Fall* $3 \mid q-1$ (*d. h.* $Z = k$) *vor, so bestimmen sich die Wurzeln nach* (3) *ohne Erweiterung von k, da jetzt die vorkommenden Radikale in k liegen. Endlich möge* (1) *ebenfalls drei Wurzeln haben und es liege zweitens der Fall* $3 \mid q+1$ (*d. h.* $Z = k_2$) *vor. Es bedeute dann* 3^ν *die größte, in* $q+1$ *enthaltene Dreierpotenz* ($\nu \geqq 1$). *Gilt* ($\nu = 1$ *oder* $\nu \geqq 2$ *und über* $\chi_3(\alpha, k_2) = 1$ *hinaus sogar*)

$$(17) \qquad \chi_{3^\nu}(\alpha, k_2) = 1,$$

[5]) Obiges folgt nämlich daraus, daß jetzt $\sqrt{-3D}$ nicht in k, sondern erst in k_2 liegt, sonst wäre das falsch.

so läßt sich in (3)

$$(18) \qquad \sqrt[3]{\alpha}=\left(-\frac{a}{3}\right)^{-q_0}\alpha^{\frac{2q_0+1}{3}},\quad \sqrt[3]{\alpha'}=\left(-\frac{a}{3}\right)^{-q_0}\alpha'^{\frac{2q_0+1}{3}}$$

einsetzen, wobei q_0 *durch*

$$(19) \qquad q_0=\pm\frac{q+1}{3^\nu}\equiv 1 \pmod 3$$

bestimmt ist, so daß also die Exponenten in (18) *ganz sind. Dadurch sind die rechten Seiten in* (3) *in gewisse Relativspuren in* k_2/k *übergegangen, und so geschieht die Berechnung der Wurzeln wieder ohne die Erweiterung von* k.[6])

Bemerkung. Nach diesem Satz ist zur Berechnung der in k liegenden Wurzeln von (1) nur dann der Erweiterungskörper k_2 heranzuziehen, mit dem man dann aber auch schon auskommt, wenn $9|q+1$ (also $\nu\geqq 2$), $\chi(D)=1$, $\chi_3(\alpha, k_2)=1$ (also drei Wurzeln in k liegen) und $\chi_{3^\nu}(\alpha, k_2)\neq 1$ ist. Es gelang mir nicht diesen restlichen Fall noch mehr einzuschränken. Es scheint hier eine ähnliche Erscheinung (wenn auch in kleinerem Ausmaße) vorzuliegen, wie der „Casus irreducibilis" in dem Fall, wo k der Körper der reellen Zahlen ist und drei reelle Wurzeln vorhanden sind.

Satz 3. *Es habe die kubische Resolvente* (11) *von* (2) *genau* m *Wurzeln in* k *und es gebe unter ihnen genau* m' *Quadrate in* k. *Je nach den Fällen* $m>m'$, $m=m'$ *hat die Gleichung* (2) *keine bzw. genau* $m+1$ *Wurzeln in* k. *Dabei sind für das Paar* m, m' *offenbar nur die Fälle möglich:* 0, 0; 1, 0; 1, 1; 3, 1; 3, 3.

Bemerkung. Eine interessante Folgerung dieses Satzes ist, daß die Gesamtzahl der Wurzeln der Gleichungen (2) und (11) immer ungerade ist. Insbesondere hat also wenigstens eine dieser Gleichungen mindestens eine Wurzel in k.[7]) — Wir können leicht sehen, was man für Körpererweiterungen braucht, wenn man die in k liegenden Wurzeln

---

[6]) Denn die ungeraden Potenzen von $\sqrt{-3D}$ fallen bei der Spurbildung heraus.

[7]) Und zwar gilt das offenbar auch nach Aufhebung der Einschränkung, daß B und die Diskriminante von (2) nicht verschwinden. — Drückt man — C aus den Gleichungen (2), (11) aus, so läßt sich obiges auch so sagen: In k wird jedes Element durch wenigstens eine der Funktionen

$$x^4+Ax^2+Bx,\quad -\frac{x^3+2Ax^2+A^2x-B^2}{4x}$$

angenommen. Hierbei ist aber die Einschränkung $B\neq 0$ wieder unentbehrlich, wie man das gleich sieht. Es läßt sich übrigens zeigen, daß diese Funktionen „ungefähr" $\frac{5}{8}q$ bzw. $\frac{2}{3}q$ verschiedene Elemente annehmen (im Fall $B=0$ treten dafür $\frac{3}{8}q$ bzw. $\frac{1}{2}q$ ein). (Vgl. den Anhang.)

von (2) nach (14) bestimmen will. Es ist ein sehr ungünstiger Fall, wenn (2) genau eine Wurzel in k hat. Hierfür ist nämlich nach Satz 3 notwendig und hinreichend, daß (11) keine Wurzel in k hat. In diesem Fall braucht man den Erweiterungskörper k_3 zu Hilfe zu nehmen, in dem nämlich die y_i liegen, damit kommt man aber auch schon aus, da nach (7)—(10) mit den x_i auch die $\sqrt{y_i}$ in k_3 liegen. Hat weiter (2) genau zwei Wurzeln in k — das ist dann und nur dann der Fall, wenn (11) genau eine Wurzel in k hat, die dort zugleich ein Quadrat ist — so braucht man nach Satz 2 keine Körpererweiterung, denn man kann in (14) für y_i eben diese Wurzel von (11) nehmen. Hat endlich (2) vier Wurzeln in k, d. h. sind alle drei Wurzeln von (11) Quadrate in k, so gilt ähnliches bis auf den in der obigen Bemerkung erwähnten Ausnahmefall, in dem man die Erweiterung k_2 benötigt.

Beweis. Die Diskriminante von (1) drückt sich in den Wurzeln so aus:

$$D = [(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)]^2. \tag{20}$$

Liegen alle x_i in k, so folgt hieraus gleich $\chi(D) = 1$. Liegt kein x_i in k, so ist der Zerfällungskörper von (1) $Z_1 = k_3$, und das bedeutet, daß die Galoissche Gruppe von (1) von der dritten Ordnung ist. Ein erzeugendes Element dieser Gruppe permutiert also die x_i zyklisch. Dabei bleibt das Differenzenprodukt in (20) invariant, letzteres liegt somit in k. Also ist auch in diesem Fall $\chi(D) = 1$. Liegt endlich nur eines der x_i in k, so ist $Z_1 = k_2$ und die Galoissche Gruppe von (1) von der zweiten Ordnung. Das erzeugende Element vertauscht zwei der x_i miteinander, läßt also obiges Differenzenprodukt nicht invariant. Hieraus folgt $\chi(D) = -1$. Mit den bisherigen haben wir eben die erste Behauptung des Satzes 1 bewiesen.

Zum vollständigen Beweis dieses Satzes brauchen wir nur noch den Fall $\chi(D) = 1$ zu betrachten. Dann hat (1) keine oder drei Wurzeln in k, und somit genügt es zu zeigen, daß (1) dann und nur dann wenigstens eine Wurzel in k hat, wenn $\chi_3(\alpha, Z) = 1$ gilt. In der Tat, wenn diese Gleichung gilt, so liegen $\sqrt[3]{\alpha}$, $\sqrt[3]{\alpha'}$ in Z. Da auch ϱ, ϱ' in Z sind, so gilt nach (3) ähnliches auch über die x_i. Andererseits ist der Relativgrad von Z/k höchstens gleich zwei, woraus folgt, daß wenigstens eines der x_i in k ist. Wenn dies umgekehrt der Fall ist, so müssen schon alle x_i in k sein, und das ergibt nach (3), daß $\sqrt[3]{\alpha}$ in Z liegt. Das bedeutet eben $\chi_3(\alpha, Z) = 1$, womit wir Satz 1 bewiesen haben.

Aus Satz 2 brauchen wir nur die Behauptungen über (16_1), (16_2), (18) zu beweisen.

Zum Beweis von (16_1) bemerken wir zuerst, daß jetzt $\chi(D) = -1$,

$\chi(-3)=1$, also $\chi(-3D)=-1$ ist. Hieraus folgt, daß α nicht in k, sondern in k_2 ist. Wir setzen

$$\xi=-\frac{3}{a}\alpha^{\frac{q+2}{3}},\quad \xi'=-\frac{3}{a}\alpha'^{\frac{q+2}{3}}. \tag{21}$$

Nach (6) gilt $\xi^3=(\alpha\alpha')^{-1}\alpha^{q+2}$. Andererseits ist $\alpha^q=\alpha'$, da der Automorphismus $x\to x^q$ von k_2/k die konjugierten Elemente ineinander überführt. Dies ergibt mit dem vorigen $\xi^3=\alpha$, woraus auch $\xi'^3=\alpha'$ folgt. Weiter ist nach (21) und (6)

$$\xi\xi'=\left(-\frac{3}{a}\right)^2\left(-\frac{a}{3}\right)^{q+2}=\left(-\frac{a}{3}\right)^q=-\frac{a}{3},$$

da für jedes Element x von k $x^q=x$ gilt. Wir haben also gewonnen, daß ξ, ξ' solche Kubikwurzeln aus α bzw. α' sind, daß auch (6) gilt. Das beweist nach (3) die Behauptung über (16_1).

Für die Formel (16_2) ist dagegen $\chi(D)=-1$, $\chi(-3)=-1$, also $\chi(-3D)=1$, und dies bedeutet, daß α jetzt in k liegt. Wir setzen

$$\xi=\alpha^{\frac{2q-1}{3}},\quad \xi'=\alpha'^{\frac{2q-1}{3}}. \tag{22}$$

Jetzt ist $\alpha^q=\alpha$, woraus $\xi^3=\alpha^{2q-1}=\alpha$ folgt. Ähnlich ist $\xi'^3=\alpha'$. Weiter gilt nach (22) und (6)

$$\xi\xi'=\left(-\frac{a}{3}\right)^{2q-1}=-\frac{a}{3}.$$

Wie vorher, folgt hieraus die Richtigkeit der Behauptung über (16_2).

Die dritte Potenz der rechten Seite der ersten Gleichung in (18) ist

$$(\alpha\alpha')^{-q_0}\alpha^{2q_0+1}=\alpha(\alpha\alpha'^{-1})^{q_0}.$$

Da jetzt $\alpha^q=\alpha'$ ist, so läßt sich hierfür $\alpha\alpha^{-q_0(q-1)}$ schreiben. Der zweite Faktor ist aber wegen (17) gleich 1, da der Exponent nach (19) eben $\pm\frac{q^2-1}{3^\nu}$ ist. Das beweist zunächst die Behauptung über die erste Gleichung in (18). Da weiter nach (6) das Produkt aus den rechten Seiten in (18) gleich $-\frac{a}{3}$ ist, so haben wir Satz 2 bewiesen.

Um Satz 3 zu beweisen, zerlegen wir ihn in die folgenden drei Teilbehauptungen, wobei μ die Anzahl der in k liegenden Wurzeln von (2) bedeutet.

1) $\mu=1$ ist dann und nur dann, wenn $m=0$ ist;
2) $\mu=2$ ist dann und nur dann, wenn $m=m'=1$ ist;
3) $\mu=4$ ist dann und nur dann, wenn $m'=3$ ist.

Wir bemerken zuerst die einfache Folgerung aus (7)—(10), daß der aus k nach Adjunktion aller $\sqrt{y_i}$ entstandene Körper mit dem Zer-

fällungskörper Z_2 von (2) identisch ist. Insbesondere können also diese Körper nur gleichzeitig mit k zusammenfallen, was eben die Richtigkeit von 3) bedeutet. Weiter folgt aus unserer Bemerkung, daß Z_2 den Zerfällungskörper von (11) enthält und der Relativgrad eine Zweierpotenz ist. Hieraus folgt, daß die Relativgrade der Zerfällungskörper von (2) und (11) über k nur gleichzeitig durch drei teilbar sein können. Das ist eben die Richtigkeit von 1).

Um auch 2) zu beweisen, nehmen wir zuerst $\mu = 2$ an. Dann ist mit geeigneter Reihenfolge

$$x_1 = u, \quad x_2 = v, \quad x_3 = -\frac{u+v}{2} + w\sqrt{d}, \quad x_4 = -\frac{u+v}{2} - w\sqrt{d},$$

wobei u, v, w, d in k sind und $u \neq v$, $w \neq 0$, $\chi(d) = -1$ gilt. Nach (13) ist dann

$$y_1 = \left(\frac{u-v}{2} - w\sqrt{d}\right)^2, \quad y_2 = \left(\frac{v-u}{2} - w\sqrt{d}\right)^2, \quad y_3 = (u+v)^2.$$

Hieraus sieht man, daß y_1, y_2 nicht in k liegen, dagegen y_3 ein Quadrat in k, d. h. $m = m' = 1$ ist, wie behauptet war. Nehmen wir umgekehrt letzteres an. Es liege z. B. y_3 in k, das dann zugleich ein Quadrat in k ist. Wir wenden (14) mit $r = \sqrt{y_3}$ an. Da jetzt r in k ist, so folgt, daß die Faktoren der linken Seite von (14) Polynome in k sind. Berücksichtigt man hierzu auch (13), so sieht man, daß die Gleichungen

$$(23) \qquad (x-x_1)(x-x_2) = 0, \quad (x-x_3)(x-x_4) = 0$$

ihre Koeffizienten in k haben. Die Diskriminanten sind

$$(x_1-x_2)^2, \quad (x_3-x_4)^2,$$

die natürlich in k liegen. Andererseits sind y_1, y_2 wegen der Annahme die Wurzeln einer irreduziblen Gleichung in k, woraus folgt, daß $(y_1-y_2)^2$ in k ist mit $\chi((y_1-y_2)^2) = -1$. Man berechnet aber nach (13)

$$y_1 - y_2 = (x_1+x_4)^2 - (x_2+x_4)^2 = (x_1-x_2)(-x_3+x_4),$$

woraus

$$(y_1-y_2)^2 = (x_1-x_2)^2 (x_3-x_4)^2$$

folgt. Es ergibt sich hieraus, daß genau nur die eine der Gleichungen (23) ein Quadrat in k zur Diskriminante hat. Dies bedeutet $\mu = 2$, womit wir Satz 3 bewiesen haben.

Anhang. Von hier an sollen die Koeffizienten der Gleichungen (1) und (2) keiner Einschränkung mehr unterworfen sein. Wir lassen in diesen Gleichungen die konstanten Glieder b, C alle Elemente von k durchlaufen, und fragen, wie viele Gleichungen (1) bzw. (2) auf diesem Wege (bei festgehaltenem a, A, B) entstehen, die eine vorgegebene Anzahl Lösungen haben. Diese Frage läßt sich offenbar auch so for-

muliren: Wie viele Elemente nehmen die Funktionen

$$x^3+ax, \quad x^4+Ax^2+Bx$$

genau i-mal an, wobei $i=0, 1, 2, 3$ bzw. $0, 1, 2, 3, 4$ sein kann. Mit solchen Fragen (auch allgemeiner für nicht notwendig ganze rationale Funktionen dritten und vierten Grades) werde ich mich in einer anderen Arbeit ausführlich beschäftigen, wobei die vorliegende Arbeit zur Anwendung kommen wird; trotzdem will ich hier die obigen Fragen mit Andeutung des Beweises beantworten.

Satz 4. *Bei festem a bedeute n_i $(i=0, 1, 2, 3)$ die Anzahl derjenigen b, für die die Gleichung* (1) *genau i verschiedene Wurzeln hat.*

Im Fall $a\neq 0$ ist:

$$n_0=\frac{1}{3}q \qquad -\frac{1}{3}\chi(-3) \qquad , \tag{24}$$

$$n_1=\frac{1}{2}q-\frac{1}{2}+\frac{1}{2}\chi(-3)-\frac{1}{2}\chi(-3a), \tag{25}$$

$$n_2= \quad 1 \quad + \quad \chi(-3a), \tag{26}$$

$$n_3=\frac{1}{6}q-\frac{1}{2}-\frac{1}{6}\chi(-3)-\frac{1}{2}\chi(-3a). \tag{27}$$

Im Fall $a=0$ ist:

$$n_0=\frac{q-1}{3}(1+\chi(-3)), \quad n_1=1+\frac{q-1}{2}(1-\chi(-3)), \quad n_2=0, \tag{28}$$
$$n_3=\frac{q-1}{6}(1+\chi(-3)).^{8})$$

Satz 5. *Bei festem A, B bedeute n_i $(i=0, 1, 2, 3, 4)$ die Anzahl derjenigen C, für die die Gleichung* (2) *genau i verschiedene Wurzeln hat.*

Im Fall $B\neq 0$ ist:

$$n_0=\frac{1}{8}q-\frac{1}{8}S_1+\frac{1}{8}S_2-\frac{1}{4}-\frac{1}{8}\chi(-1) \qquad -\frac{1}{2}\sigma_1 \qquad , \tag{29}$$

$$n_1=\frac{1}{3}q+\frac{1}{3}S_1 \qquad +\frac{1}{3} \qquad -\frac{1}{3}\varrho+ \quad \sigma_1 \qquad , \tag{30}$$

$$n_2=\frac{1}{4}q-\frac{1}{4}S_1-\frac{1}{4}S_2 \qquad +\frac{1}{4}\chi(-1)+ \quad \varrho-\frac{1}{2}\sigma_1-\frac{1}{2}\sigma_2, \tag{31}$$

$$n_3= \qquad \qquad \qquad \qquad -\quad \varrho \qquad +\quad \sigma_2, \tag{32}$$

$$n_4=\frac{1}{24}q+\frac{1}{24}S_1+\frac{1}{8}S_2-\frac{1}{12}-\frac{1}{8}\chi(-1)+\frac{1}{3}\varrho \qquad -\frac{1}{2}\sigma_2, \tag{33}$$

---

[8]) Addiert man die n_i für alle a, so ergibt sich, daß es insgesamt $\frac{1}{3}(q^2-1)$, $\frac{1}{2}(q^2-q)+1$, $q-1$, $\frac{1}{6}(q-1)(q-2)$ Gleichungen (1) gibt, die keine, eine, zwei bzw. drei Wurzeln haben. Damit wurden die Angaben in [2]) verbessert und verallgemeinert.

wobei

$$S_1 = \chi(2) \sum_x \chi(x^3 + 2(Ax - B^2)^2), \tag{34}$$

$$S_2 = \chi(-1) \sum_x \chi(x^3 + 2Ax^2 + 4B^2),^{9}) \tag{35}$$

weiter $\varrho = 1$, *wenn* $8A^3 + 27B^2 = 0$, *sonst* $\varrho = 0$ *ist, endlich* σ_1, σ_2 *die Anzahl der verschiedenen Wurzeln der Gleichung* $B^2x^3 + 2Ax + 2 = 0$ *bedeuten, für die* $\chi(x) = -1$ *bzw.* 1 *ist.*

Im Fall $A \neq 0$, $B = 0$ *ist:*

$$n_0 = \frac{5}{8}q - \frac{1}{4} + \frac{1}{8}\chi(-1) + \frac{1}{4}\chi(-A) - \frac{1}{4}\chi(-2A), \tag{36}$$

$$n_1 = \frac{1}{2} - \frac{1}{2}\chi(-A), \tag{37}$$

$$n_2 = \frac{1}{4}q - \frac{1}{2} - \frac{1}{4}\chi(-1) + \frac{1}{2}\chi(-2A), \tag{38}$$

$$n_3 = \frac{1}{2} + \frac{1}{2}\chi(-A), \tag{39}$$

$$n_4 = \frac{1}{8}q - \frac{1}{4} + \frac{1}{8}\chi(-1) - \frac{1}{4}\chi(-A) - \frac{1}{4}\chi(-2A). \tag{40}$$

Im Fall $A = B = 0$ *ist:*

$$n_0 = \frac{q-1}{8}(5 + \chi(-1)),\ n_1 = 1,\ n_2 = \frac{q-1}{4}(1 - \chi(-1)),\ n_3 = 0,$$
$$n_4 = \frac{q-1}{8}(1 + \chi(-1)). \tag{41}$$

Es ist nämlich in jedem Fall $\sum_i n_i = q$, $\sum_i i n_i = q$, wie das auch offenbar sein muß. Deshalb genügt es für die Gleichungen (1) und (2) nur n_1, n_2 bzw. n_1, n_2, n_3 zu bestimmen. Für die Gleichung (1) ist im Fall $a \neq 0$ nach Satz 1 n_1 und n_2 die Anzahl der b, für die $\chi(D) = -1$ bzw. $D = 0$ ist, und so folgen (25), (26) leicht. Fall $a = 0$ leuchtet unmittelbar ein. Für die Gleichung (2) bestimmt sich n_3 ebenfalls leicht. Um auch n_1, n_2 zu bestimmen, zieht man Satz 3 heran, auf die ziemlich komplizierten Rechnungen gehe ich aber, wie gesagt, erst an einer anderen Stelle ein.

(Eingegangen am 22. September 1944.)

[9]) Nach H. Hasse sind die Summen in (34), (35) absolut $\leqq 2\sqrt{q}$.