Zur Theorie der Gleichungen in endlichen Körpern.

Von LADISLAUS RÉDEI in Szeged.

1. Wir legen einen beliebigen endlichen Körper k von q Elementen und der Karakteristik p zu Grunde, wobei dann q eine Potenz der Primzahl p ist, und untersuchen in ihm die Lösbarkeit einer Gleichung $F=0$, wobei

$$F=F(x_1, \ldots, x_n) \tag{1}$$

ein beliebiges nichtkonstantes Polynom g-ten Grades in den n Unbestimmten $x_1, \ldots, x_n$ ist. Da jedes Element von k der Gleichung $x^q-x=0$ genügt, verlieren wir nichts an Allgemeinheit, indem wir F reduziert d. h. in jedem x_i vom Grade $\leqq q-1$ annehmen. Obzwar sich unsere Betrachtungen auch auf die Gleichung $F=1$ mit homogenem F beziehen (man schreibe sie hierzu in der Form $F-1=0$), werden wir uns mit ihr am Ende der Arbeit besonders beschäftigen und für sie schärfere Resultate bekommen.

CHEVALLEY[1]) bewies eine Vermutung von ARTIN über die Anzahl der gemeinsamen Lösungen eines Systems von Gleichungen in k. Der Satz lautet insbesondere für unseren Fall so: Ist $g<n$ und die Gleichung $F=0$ lösbar, so hat sie mindestens zwei Lösungen[2]). WARNING[3]) hat dann den Satz durch genauere Aussagen über die Anzahl der Lösungen verschärft. Seine Hauptresultate sind (wieder für den Fall einer Gleichung) im folgenden Satz enthalten: Ist $g<n$ und die Gleichung $F=0$ lösbar, so ist die Anzahl der Lösungen $\equiv 0 \pmod p$[2]) und $\geqq q^{n-g}$. Selbst die Frage der Lösbarkeit lassen beide Arbeiten unberührt, abgesehen von einigen ganz einfachen Beispielen von WARNING für unlösbare Gleichungen.

---

[1]) C. CHEVALLEY, Démonstration d'une hypothèse de M. Artin, *Abh. math. Sem. d. Hansischen Univ.*, **11** (1936), S. 73–75.

[2]) Für Gleichungssysteme ebenso, wobei dann g die Summe der Grade der einzelnen Gleichungen ist.

[3]) E. WARNING, Bemerkungen zur vorstehenden Arbeit von Herrn Chevalley, *Abh. math. Sem. d. Hansischen Univ.*, **11** (1936), S. 76–83.

2. Wir nennen den Rang r von F die kleinste natürliche Zahl, für die es eine nichtsinguläre homogene lineare Substitution der $x_1, \ldots, x_n$ gibt, durch die F in ein Polynom von r Unbestimmten übergeführt wird. Immer ist $r \leqq n$.

Vermutung. *Ist k ein Primkörper und $g \leqq r$, so ist $F = 0$ lösbar.*

Für ein beliebiges k wäre dies falsch nach dem Beispiel 2 von WARNING (s. [3]) S. 83), das etwas verallgemeinert so lautet: Ist k kein Primkörper, so ist die Gleichung

$$a_1 x_1^{q-1} + \ldots + a_n x_n^{q-1} + c = 0 \qquad (n \text{ beliebig})$$

unlösbar, wenn die Koeffizienten außer c dem in k enthaltenen Primkörper angehören. Das kommt nämlich einfach davon, daß x^{q-1} nur die Werte 0, 1 annimmt, die im Primkörper von k sind. Auch sieht man leicht, daß in diesem Beispiel $r = n$ ist (also r beliebig groß sein kann), wenn man nur $a_1, \ldots, a_n \neq 0$ wählt. Sonst könnte man nämlich für die x_i homogene lineare Ausdrücke $x_i = l_i(y_1, \ldots, y_n)$ mit nichtverschwindender Determinante D einsetzen, so daß

$$a_1 l_1^{q-1} + \ldots + a_n l_n^{q-1}$$

ein Polynom in $y_1, \ldots, y_{n-1}$ ist. Dann verschwindet die nach y_n genommene Derivierte:

$$-a_1 \alpha_1 l_1^{q-2} - \ldots - a_n \alpha_n l_n^{q-2} = 0,$$

wobei α_i der Koeffizient von y_n in l_i ist. Wegen $D \neq 0$ lassen sich aber die $y_1, \ldots, y_n$ so wählen, daß alle $l_1, \ldots, l_n$ verschwinden bis auf ein beliebiges l_j. Das ergibt $\alpha_j = 0$ $(j = 1, \ldots, n)$, was doch wegen $D \neq 0$ ein Widerspruch ist.

Auch läßt sich r in der Vermutung nicht durch ein kleineres ersetzen. Hierfür führen wir gleich zwei Beispiele an. Wir betrachten im Primkörper k mit $p \geqq 3$ die Gleichungen

$$x_1^{p-1} + \ldots + x_n^{p-1} + c = 0,$$

$$x_1^{\frac{p-1}{2}} + \ldots + x_n^{\frac{p-1}{2}} + c = 0.$$

In ihnen ist $r = n$, denn obiger Beweis gilt auch jetzt. Sie sind für $n < p-1$, $c = 1$ bzw. $n < \frac{p-1}{2}$, $c = \frac{p-1}{2}$ unlösbar, da $x^{\frac{p-1}{2}}$ nur die Werte 0, ± 1 annimmt. (Dagegen sind sie, wie leicht zu sehen, für $n \geqq p-1$ bzw. $n \geqq \frac{p-1}{2}$ und beliebiges c lösbar, entsprechend der Vermutung).

Nachdem wir uns überzeugt haben, daß die Vermutung (in zwei Richtungen) scharf ist, werden wir im Laufe unserer Betrachtungen

— die übrigens fast ausschließlich einen beliebigen k betreffen — sehen, daß die Vermutung berechtigt zu sein scheint.

3. Wir führen das Ideal

$$\mathfrak{J} = (x_1^q - x_1, \ldots, x_n^q - x_n) \tag{2}$$

ein und beweisen folgendes:

Kriterium 1. *$F = 0$ ist dann und nur dann nicht lösbar, wenn*

$$F^{q-1} - 1 \equiv 0 \pmod{\mathfrak{J}} \tag{3}$$

d. h. mit irgendwelchen Polynomen $H_1, \ldots, H_n$ in $x_1, \ldots, x_n$

$$F^{q-1} - 1 = H_1(x_1^q - x_1) + \ldots + H_n(x_n^q - x_n) \tag{4}$$

ist. Man darf annehmen, daß H_i $(i = 1, \ldots, n-1)$ in jedem $x_{i+1}, \ldots, x_n$ vom Grade $\leqq q-1$ ist. Zugleich ist dann das Maximum der Grade von $H_1, \ldots, H_n$ gleich $gq - g - q$.

Man kann nämlich in

$$F^{q-1} - 1 \equiv R \pmod{\mathfrak{J}} \tag{5}$$

das Polynom R reduziert annehmen. Bekanntlich verschwindet R für alle $x_1, \ldots, x_n$ dann und nur dann, wenn $R = 0$ ist[4]). Weiter sind die zwei Seiten von (5) als Funktionen in k offenbar gleich. Die linke Seite verschwindet für alle $x_1, \ldots, x_n$ dann und nur dann, wenn $F = 0$ keine Lösung hat, womit die erste Behauptung des Kriteriums bewiesen ist.

Die zweite Behauptung beweisen wir in $n-1$ Schritten. Als erster Schritt reduzieren wir H_1 nach $x_2, \ldots, x_n$, d. h. bestimmen in

$$H_1 = h_2(x_2^q - x_2) + \ldots + h_n(x_n^q - x_n) + H_1'$$

die Polynome $h_2, \ldots, h_n, H_1'$ so, daß letzteres in jedem der $x_2, \ldots, x_n$ vom Grade $\leqq q - 1$ ist. Die rechte Seite von (4) geht dann in

$$H_1'(x_1^q - x_1) + [H_2 + h_2(x_1^q - x_1)](x_2^q - x_2) + \ldots + [H_n + h_n(x_1^q - x_1)](x_n^q - x_n)$$

über. Die neu aufgetretenen Faktoren bezeichnen wir wieder mit $H_1, \ldots, H_n$ und sehen, daß der auf H_1 bezügliche Teil der Behauptung schon bewiesen ist. Nach diesem beendeten ersten Schritt verfahren wir im zweiten Schritt ähnlich, aber so, daß wir am ersten Produkt auf der rechten Seite von (4) nichts mehr ändern und H_2 nur noch nach $x_3, \ldots, x_n$ reduzieren. Auf diesem Weg sieht man die Behauptung leicht ein.

Um die letzte Behauptung zu beweisen, bezeichnen wir mit m das Maximum der Grade aller H_i. Da die linke Seite von (4) vom Grad $gq - g$ ist, muß $gq - g \leqq m + q$ sein. Wäre die Behauptung falsch,

[4]) S. in [1]) S. 74.

d. h. es gelte hier das Zeichen $<$, so bedeutet das, daß die Summe S der Glieder $m+q$-ten Grades auf der rechten Seite von (4) verschwindet. Es ist

$$S = H_1^* x_1^q + \ldots + H_n^* x_n^q,$$

wobei H_i^* die Summe der Glieder m-ten Grades von H_i bedeutet. Wir nehmen an, daß rechts das i-te Produkt das letzte nichtverschwindende ist. In x_i ist dieses Produkt von einem Grade $\geqq q$, die voranstehenden aber vom Grade $\leqq q-1$, woraus $S \neq 0$ folgt. Dieser Widerspruch beweist das Kriterium 1.

4. Nennen wir die Summe der Glieder höchsten Grades eines Polynoms seinen Hauptteil, der also immer ein homogenes Polynom ist, und bezeichnen ihn für F mit $\bar{F}$. Ähnlich (aber selbstverständlich ohne einen inneren Zusammenhang in den Bezeichnungen) führen wir das Ideal [vgl. (2)]

$$\bar{\mathfrak{J}} = (x_1^q, \ldots, x_n^q) \tag{6}$$

ein. Offenbar gehören zu $\bar{\mathfrak{J}}$ außer 0 die und nur die Polynome, deren jedes Glied mindestens ein x_i mit einem Exponenten $\geqq q$ enthält.

Satz 1. *$F=0$ ist lösbar, wenn*[5]) *$g \leqq n$ und*

$$\bar{F}^{q-1} \not\equiv 0 \pmod{\bar{\mathfrak{J}}} \tag{7}$$

ist. Schreibt man die linke Seite ausmultipliziert in der Form

$$\bar{F}^{q-1} = \sum_{i_1+\ldots+i_n=g(q-1)} a_{i_1\ldots i_n} x_1^{i_1} \ldots x_n^{i_n}, \tag{8}$$

so bedeutet (7) nichts anderes, als daß nicht alle Koeffizienten $a_{i_1\ldots i_n}$ $(i_1 \leqq q-1, \ldots, i_n \leqq q-1)$ verschwinden.

Zum Beweis nehmen wir an, daß $F=0$ nicht lösbar ist. Nach Kriterium 1 gilt dann (4) mit Polynomen H_i vom Grade $\leqq gq-g-q$. Der Vergleich der Glieder höchsten Grades ergibt:

$$\bar{F}^{q-1} = H_1^* x_1^q + \ldots + H_n^* x_n^q, \tag{9}$$

wobei nämlich H_i^* die Summe der Glieder $gq-g-q$-ten Grades von H_i ist. Aus (9) folgt $\bar{F}^{q-1} \equiv 0 \pmod{\bar{\mathfrak{J}}}$. Wenn also umgekehrt (7) gilt, so ist $F=0$ lösbar, womit Satz 1 bewiesen ist. [Nach [5]) haben wir nur scheinbar mehr als den Satz bewiesen.]

5. Wie wir gesehen haben, umfaßt Satz 1 nur einen kleinen Teil vom Kriterium 1, der nämlich so entstanden ist, daß wir in (3) nur die Glieder höchsten Grades miteinander verglichen haben. Leicht kann

---

[5]) Diese Bedingung $g \leqq n$ ist in der nachfolgenden (7) enthalten, wie man das aus (8) gleich entnimmt, und wäre deshalb ohne weiteres fortzulassen. Wir wollten aber diese „conditio sine qua non" von (7) voranschicken, um den Anschein zu vermeiden, daß der Satz auch für $g > n$ brauchbar wäre. (Vgl. [7]).)

man aus Kriterium 1 weitere Lösbarkeitsbedingungen von weniger Eleganz gewinnen, indem man auch andere Glieder in (4) beachtet. Ein anderes Verfahren wäre, daß man (3) in der äquivalenten Form

$$F^q - F \equiv 0 \pmod{F\mathfrak{J}} \tag{10}$$

schreibt, wobei man die linke Seite leicht berechnet. Wenn man nämlich $F = \Sigma a X$ setzt, wobei die a Elemente von k und die X Potenzprodukte der $x_1, \ldots, x_n$ sind, so ist die linke Seite von (10) auf Grund der Regeln $(u+v+\ldots)^p = u^p + v^p + \ldots$, $a^p = a$ einfach $\Sigma a(X^q - X)$. Uns ist es aber nicht gelungen diesen Weg weiter zu verfolgen.

6. Satz 1 macht sehr wahrscheinlich, daß bei festem k, g, n mit $g \leqq n$ die Mehrzahl aller $F = 0$ lösbar ist, und zwar bei wachsendem n in steigerndem Maße. Nämlich lautet (7) im „ungünstigsten" Falle $g = n$ so, daß der Koeffizient $a_{q-1,\ldots,q-1}$ in (8) nicht verschwindet. Da aber das Verschwinden eines bestimmten Koeffizienten in (8) mit einer Wahrscheinlichkeit $\frac{1}{q}$ zu erwarten ist, scheint $F = 0$ für $g = n$ höchstens[6]) nur im $\frac{1}{q}$-ten Teil aller Fälle unlösbar zu sein. Für $n = g+1, g+2, \ldots$ ist die Lage offenbar noch viel günstiger, da durch (7) immer mehr Koeffizienten betroffen werden [schon für $n = g+1$ kommen $\binom{g+q-1}{g}$ Koeffizienten in Betracht].

7. Bezeichnet $\bar{r}$ den Rang von $\overline{F}$ (es ist dann $\bar{r} \leqq r \leqq n$), so zeigen wir, daß Satz 1 im Fall $g > \bar{r}$ über die Lösbarkeit von $F = 0$ nicht entscheidet.[7])

Es gibt nämlich eine nichtsinguläre homogene lineare Substitution σ, die die neuen Unbestimmten $y_1, \ldots, y_n$ einführt und $\overline{F}$ in $\overline{F} = \overline{F}'(y_1, \ldots, y_{\bar{r}})$ überführt. Aus $g > \bar{r}$ folgt

$$\overline{F}'^{q-1} \equiv 0 \pmod{y_1^q, \ldots, y_{\bar{r}}^q}.$$

Die inverse Substitution σ^{-1} führt $\overline{F}'$ zurück in $\overline{F}$ und jedes y_i^q in ein Polynom des Moduls $(x_1^q, \ldots, x_n^q)$ über. So entsteht

$$\overline{F}^{q-1} \equiv 0 \pmod{\overline{\mathfrak{J}}},$$

womit die Behauptung bewiesen ist.

8. Wir zeigen folgendes: Ist k kein Primkörper und enthält jedes Glied von $\overline{F}$ mindestens ein x_i zu einem Exponenten $\geqq p$, so ist die

---

[6]) Man nehme Rücksicht darauf, daß (7) hinreichend, aber nicht notwendig zur Lösbarkeit von $F = 0$ ist.

[7]) Demgemäß hätten wir in Satz 1 die Ungleichung $g \leqq n$ ohne jeden Verlust durch $g \leqq \bar{r}$ ersetzen können. Trotzdem wollten wir das nicht tun, da man doch bei Anwendung des Satzes den Rang von $\overline{F}$ nicht zu berechnen braucht.

Frage der Lösbarkeit von $F=0$ auf Grund von Satz 1 nicht zu entscheiden.

Nämlich ist jetzt offenbar

$$\overline{F}^{\frac{q}{p}} \equiv 0 \pmod{\overline{\mathfrak{J}}}.$$

Also ist (7) wegen $q-1 > \frac{q}{p}$ unmöglich, und das beweist die Behauptung.

9. Wir führen hier für Satz 1 zwei einfache Beispiele an, deren Zahl man leicht vermehren könnte.

Beispiel 1. *Besteht $\overline{F}$ aus dem einzigen Glied $ax_1 \dots x_g$ $(a \neq 0)$, so ist $F=0$ lösbar.*

Beispiel 2. *Ist k ein Primkörper, e die größte ganze Zahl $\leqq \frac{p-1}{g}$,*

$$\overline{F} = a_1 x_1^g + \dots + a_n x_n^g \qquad \left(a_1 \dots a_n \neq 0,\ n \geqq \frac{p-1}{e}\right),$$

so ist $F=0$ lösbar.

Im Beispiel 1 ist nämlich (7) offenbar erfüllt. Für Beispiel 2 ist

$$\overline{F}^{ne} \not\equiv 0 \pmod{\overline{\mathfrak{J}}}, \tag{11}$$

da die linke Seite nach der Polynomialentwicklung das mit keinem anderen aufgehende nichtverschwindende Glied

$$\frac{(p-1)!}{(e!)^n} (a_1 \dots a_n)^e (x_1 \dots x_n)^{ge}$$

enthält, wobei $ge \leqq p-1$ ist. Wegen $ne \geqq p-1$ folgt aus (11) das Bestehen von (7) für diesen Fall, zugleich also die Richtigkeit von Beispiel 2.

10. Aus Beispiel 2 heben wir folgenden Spezialfall hervor:

Ist k ein Primkörper und $g \mid p-1$, so ist die Gleichung

$$a_1 x_1^g + \dots + a_g x_g^g = c \qquad (a_1 \dots a_g \neq 0)$$

lösbar. (Hiervon haben wir die trivialen Fälle $a_1 = \dots = a_g = 1$, $p \geqq 3$, $g = p-1$ oder $\frac{p-1}{2}$ schon in 2. erwähnt.) In der Kongruenzsprache:

Ist $g \mid p-1$ und sind $a_1, \dots, a_g$, c ganze rationale Zahlen, so ist

$$a_1 x_1^g + \dots + a_g x^g \equiv c \pmod{p} \qquad (p \nmid a_1 \dots a_g)$$

lösbar.

Mir war dieser Satz nicht einmal für den Fall $a_1 = \dots = a_g = 1$ bekannt. Auch scheint er nicht mit einfacheren Mitteln beweisbar zu sein.

11. Im folgenden beschäftigen wir uns nur noch mit dem anfangs erwähnten Sonderfall $F=1$ mit homogenem F. (Auch 10. gehörte schon hierher.) Wir bemerken im voraus, daß im Fall $q-1 \mid g$ den bisherigen gegenüber nichts neues gewonnen wird.

Kriterium 2. *$F=1$ mit homogenem F ist dann und nur dann nicht lösbar, wenn*

$$\frac{F^q-F}{F^{\frac{q-1}{\gamma}}-1} \equiv 0 \pmod{\mathfrak{J}} \qquad [\gamma=(g, q-1)] \tag{12}$$

d. h. mit irgendwelchen Polynomen $H_1, \ldots, H_n$ in $x_1, \ldots, x_n$

$$\frac{F^q-F}{F^{\frac{q-1}{\gamma}}-1} = H_1(x_1^q-x_1)+\ldots+H_n(x_n^q-x_n) \tag{13}$$

ist. Insbesondere ist also für $\gamma=1$ immer Lösbarkeit vorhanden[8]*. Für $\gamma>1$ darf angenommen werden, daß H_i $(i=1, \ldots, n-1)$ in jedem $x_{i+1}, \ldots, x_n$ vom Grade $\leq q-1$ ist. Zugleich ist dann das Maximum der Grade von $H_1, \ldots, H_n$ gleich $(g-1)q-\frac{g}{\gamma}(q-1)$.*

Man wende nämlich Kriterium 1 auf unsere Gleichung $F-1=0$ an. Hierfür geht (3) [dessen linke Seite man zuerst in der Form $\frac{F^q-F}{F}$ schreibt] offenbar in

$$\frac{F^q-F}{F-1} \equiv 0 \pmod{\mathfrak{J}} \tag{14}$$

über. Dies gilt also dann und nur dann, wenn $F=1$ nicht lösbar ist. Da aber F homogen vom g-ten Grade ist, sind alle Gleichungen $c^{-g}F=1$ (c konstant, $\neq 0$) gleichzeitig lösbar. Also darf man F in (14) ohne weiteres durch $c^{-g}F$ ersetzen, wodurch man

$$\frac{F^q-F}{F-c^g} \equiv 0 \pmod{\mathfrak{J}} \tag{15}$$

bekommt. Somit wird die erste Behauptung von Kriterium 2 bewiesen, wenn wir zeigen, daß der größte gemeinschaftliche Teiler der linken Seiten aller (15) eben die linke Seite von (12) ist. Dies ist wirklich der Fall, da die c^γ offenbar alle verschiedenen c^g sind und das Produkt der entsprechenden (verschiedenen) Nenner $F-c^\gamma$ eben der Nenner in (12) ist. Die übrigen Behauptungen folgen ebenso wie im Beweis von Kriterium 1.

[8]) Das sieht man auch unmittelbar leicht ein.

12. Wie wir aus Kriterium 1 Satz 1 gewonnen haben, ebenso entsteht jetzt nach Kriterium 2 folgender:

Satz 2. *$F=1$ mit homogenem F ist im Fall $\gamma=(g, q-1)>1$*[9]) *lösbar, wenn*[10]) $g\left(1+\frac{1}{q-1}-\frac{1}{\gamma}\right)\leqq n$ *und*

$$F^{q-\frac{q-1}{\gamma}}\not\equiv 0 \pmod{\mathfrak{F}} \tag{16}$$

ist[11]).

(Eingegangen am 17. Mai 1944.)

[9]) Für $\gamma=1$ ist die Lösbarkeitsfrage nach Kriterium 2 in bejahendem Sinne schon erledigt.

[10]) Auch hierüber gilt ähnliche Bemerkung wie in [5]).

[11]) Man beachte, daß jetzt F sein eigener Hauptteil ist, weshalb die Bezeichnung $\overline{F}$ überflüssig ist.