Über eindeutig umkehrbare Polynome in endlichen Körpern.

Von LADISLAUS RÉDEI in Szeged.

Wir legen einen endlichen Körper k mit q Elementen und der Charakteristik p zu Grunde und nennen ein (ganzes oder gebrochenes) Polynom[1]) $f(x)$ umkehrbar (nämlich eindeutig umkehrbar), wenn $y=f(x)$ für jedes y eine, folglicherweise nur eine Lösung hat. Mit anderen Worten heißt das, daß die Abbildung $x\to f(x)$ eine Permutation der Elemente von k ist. Wohlbekannte wichtige Beispiele sind die linearen ganzen Polynome. Allgemein ist mit $f(x)$ und $g(x)$ auch $f(g(x))$ umkehrbar. Aus beiden folgt, daß mit $f(x)$ auch alle

$$Tf(Sx) \tag{1}$$

umkehrbar sind, wobei S und T beliebige (nichtsinguläre) lineare ganze Substitutionen bedeuten. Bekantlich ist x^n dann und nur dann umkehrbar, wenn $(n, q-1)=1$ ist.

Für viele Zwecke erweitert man k durch Hinzunahme eines unendlichen Elementes ∞ mit den üblichen Rechnungsregeln zu einer Menge k'. Das bisherige behält auch für k' statt k seinen guten Sinn, und dabei werden sogar die gebrochenen linearen Polynome $\frac{ax+b}{cx+d}$ $(ad-bc\neq 0)$ umkehrbar (in k'). Entsprechend läßt sich das über (1) gesagte für die gebrochenen linearen Substitutionen verallgemeinern. Sind S und T solche Substitutionen, so nennen wir bei festem $f(x)$ alle Polynome (1) äquivalent, insbesondere im Fall $T=S^{-1}$ ähnlich. Äquivalente Polynome sind also gleichzeitig umkehrbar in k'. Umkehrbarkeit von $f(x)$ für k und k' kommen auf dasselbe hinaus dann und nur dann, wenn der Zähler von $f(x)$ von größerem Grad als der Nenner, d. h. $f(\infty)=\infty$ ist. Da letzteres für ein passendes $Sf(x)$ statt $f(x)$ der Fall ist, so läßt sich die Frage der Umkehrbarkeit auf die in k zurückführen.

[1]) „Gebrochenes Polynom" bedeutet den Quotienten zweier ganzen Polynome.

Beschränkt man sich auf die Polynome vom Grad $\leqq q-1$, was offenbar gestattet ist, so sind alle verschiedenen umkehrbaren ganzen Polynome bekanntlich durch

$$\sum \bar{a}_i[1-(x-a_i)^{q-1}] \tag{2}$$

angegeben, wobei man über alle Elemente $a_1, \ldots, a_q$ von k zu summieren hat und $\bar{a}_1, \ldots, \bar{a}_q$ eine Permutation von ihnen ist. Somit gibt es insgesamt $q!$ solche Polynome. Für (2) läßt sich übrigens im Fall $q>2$ wegen $\sum a_i=0$ und $(x-a_i)^q=x^q-a_i^q$ die durchsichtigere Form

$$-\sum \bar{a}_i x^{q-1}-\sum \bar{a}_i a_i x^{q-2}-\ldots-\sum \bar{a}_i a_i^{q-1} \tag{2'}$$

geben. Zu (2) ähnlich sind die

$$\frac{1}{h(x)}\sum \bar{a}_i h(a_i)[1-(x-a_i)^{q-1}] \tag{3}$$

alle (ganzen und gebrochenen) umkehrbaren Polynome vom Grad $\leqq q-1$, wobei $h(x)$ alle nullstellenfreien ganzen Polynome vom Grad $\leqq q-1$ bedeutet. (Natürlich brauchen hier Zähler und Nenner nicht teilerfremd zu sein, und so ist in (3) über Eindeutigkeit keine Rede mehr.)

Diese Formeln scheinen aber wenig geeignet zu sein, um aus ihnen in unserer Frage weitere Folgerungen zu ziehen. Auf anderem Wege werden wir gewinnen den folgenden

Satz. *Es sei $p\neq 2$ und bedeute n eine natürliche Zahl mit $(n, q+1)=1$. Man wähle ein Nichtquadratelement α in k und setze*

$$g(x)=\sum_{i\geqq 0}\binom{n}{2i}\alpha^i x^{n-2i}, \quad h(x)=\sum_{i\geqq 0}\binom{n}{2i+1}\alpha^i x^{n-2i-1} \tag{4}$$

d. h. in durchsichtigerer Form

$$(x+\sqrt{\alpha})^n=g(x)+h(x)\sqrt{\alpha} \qquad (g(x), h(x) \text{ Polynome in } k), \tag{4'}$$

welche letztere Gleichung natürlich im endlichen Körper k_2 vom zweiten Grade über k zu deuten ist. Dann ist das gebrochene Polynom

$$f_n(x)=\frac{g(x)}{h(x)} \tag{5}$$

vom Grade n und umkehrbar in k. Dabei hängt $f_n(x)$ von α nur unwesentlich ab, da es bei Ersetzung von α durch $\alpha\beta^2$ $(\beta\neq 0)$ in das äquivalente Polynom $\beta f_n\left(\frac{x}{\beta}\right)$ übergeht. Deshalb werde α im folgenden festgehalten.

Bezeichnet P_n die Permutation $x\to f_n(x)$ der Elemente von k, so ist ihre Ordnung die kleinste natürliche Zahl r mit

$$n^r\equiv 1 \pmod{q+1}, \tag{6}$$

d. h. r ist der zu n gehörende Exponent für den Modul $q+1$. Folglich ist die Ordnung von P_n ein Teiler der Eulerschen Funktion $\varphi(q+1)$. Insbesondere ist also $P_n = 1$ dann und nur dann, wenn $q+1 \mid n-1$.

Alle verschiedenen P_n (bei festem k und α) bilden eine Abelsche Gruppe der Ordnung $\varphi(q+1)$ nach der Produktregel

$$P_m P_n = P_{mn} \tag{7}$$

mit der Ergänzung, daß jede der Aussagen

$$P_m = P_n, \quad m \equiv n \pmod{q+1} \tag{8}$$

eine Folge der anderen ist.[2])

Über (7) *hinaus gilt*

$$f_m(f_n(x)) = f_{mn}(x). \tag{9}$$

Zum Beweis schicken wir die Bemerkung voraus: Alle n-ten Einheitswurzeln in k_2 liegen schon in k.

Ist nämlich $\varrho^n = 1$ (ϱ in k_2), so läßt sich hier n durch

$$d = (n, q^2-1) = (n, (q+1)(q-1)) = (n, q-1)$$

ersetzen. Da aber die Gleichung $x^d = 1$ wegen $d \mid q-1$ so viel Wurzeln in k hat, wie der Grad ist, muß ϱ in der Tat in k liegen.

Jetzt zeigen wir zunächst, daß $f_n(x)$ wirklich vom Grade n ist. Sonst hätten nämlich $g(x)$, $h(x)$ einen gemeinsamen Teiler (in k), der aber auch in der linken Seite von (4′) aufgehen muß. Dieser offenbare Widerspruch beweist die Behauptung.

Dann haben wir zu zeigen, daß $h(x)$ nullstellenfrei ist. Deshalb werde $h(\xi) = 0$ mit einem ξ in k angenommen. Nach (4′) gilt dann

$$(\xi + \sqrt{\alpha})^n = g(\xi). \tag{10}$$

Durch Normenbildung folgt hieraus, daß zunächst $g^2(\xi)$, gleichzeitig also wegen $2 \nmid n$ auch $g(\xi)$ eine n-te Potenz in k ist. Das ergibt nach (10)

$$\left(\frac{\xi + \sqrt{\alpha}}{\eta}\right)^n = 1$$

mit einem η in k. Da aber der Klammerausdruck in k_2 und nicht in k ist, haben wir mit obiger Bemerkung einen Widerspruch erhalten und so die Behauptung bewiesen.

Hiernach existiert $f_n(x)$ für jedes x in k. Zeigen wir also, daß $f_n(x)$ in k keinen Wert zweimal annimmt, so wird daraus schon die Umkehrbarkeit von ihr folgen.

Zu diesem Zweck schreiben wir die Definition von $f_n(x)$ nach (4′)

---

[2]) Somit ist die Gruppe der P_n isomorph zur Gruppe der primen Restklassen mod $q+1$.

und (5) in der Form

$$\left(\frac{x+\sqrt{\alpha}}{x-\sqrt{\alpha}}\right)^n = \frac{f_n(x)+\sqrt{\alpha}}{f_n(x)-\sqrt{\alpha}}. \tag{11}$$

Wird also $f_n(\xi)=f_n(\eta)$ angenommen mit ξ, η in k, so gilt

$$\left(\frac{(\xi+\sqrt{\alpha})(\eta-\sqrt{\alpha})}{(\xi-\sqrt{\alpha})(\eta+\sqrt{\alpha})}\right)^n = 1.$$

Wieder nach der vorangeschickten Bemerkung muß hier die Basis der Potenz in k liegen. Da aber Zähler und Nenner konjugiert sind und ersterer gleich

$$(\xi\eta-\alpha)+(\eta-\xi)\sqrt{\alpha}$$

ist, so folgt, daß hier der eine Klammerausdruck verschwindet. Der erste verschwindet nicht, denn dann wäre obige Potenz $(-1)^n=-1(\neq 1)$. Also ist $\xi=\eta$. Hiermit haben wir bewiesen, daß $f_n(x)$ umkehrbar ist.

Nach (11) ist

$$\frac{f_{mn}(x)+\sqrt{\alpha}}{f_{mn}(x)-\sqrt{\alpha}} = \left(\left(\frac{x+\sqrt{\alpha}}{x-\sqrt{\alpha}}\right)^n\right)^m = \left(\frac{f_n(x)+\sqrt{\alpha}}{f_n(x)-\sqrt{\alpha}}\right)^m = \frac{f_m(f_n(x))+\sqrt{\alpha}}{f_m(f_n(x))-\sqrt{\alpha}}.$$

Dies beweist (9), also auch (7).

Die Behauptung über (8) beweisen wir so. Zu $P_m=P_n$ ist notwendig und hinreichend, daß $f_m(\xi)=f_n(\xi)$ d. h. nach (11)

$$\left(\frac{\xi+\sqrt{\alpha}}{\xi-\sqrt{\alpha}}\right)^m = \left(\frac{\xi+\sqrt{\alpha}}{\xi-\sqrt{\alpha}}\right)^n \tag{12}$$

für jedes ξ in k gilt. Wir bezeichnen mit m_0, n_0 den kleinsten nichtnegativen Rest von m bzw. n mod q^2-1. Dann dürfen wir in (12) m, n durch m_0, n_0 ersetzen, weil $\frac{\xi+\sqrt{\alpha}}{\xi-\sqrt{\alpha}}$ in k_2 und $\neq 0$ ist. Zugleich nehmen wir $m_0 \leqq n_0$ an, das offenbar gestattet ist, und setzen

$$n_0-m_0 = qu+v \qquad (0 \leqq u, v \leqq q-1). \tag{13}$$

Dann lautet (12):

$$\left(\frac{\xi+\sqrt{\alpha}}{\xi-\sqrt{\alpha}}\right)^{qu+v} = 1. \tag{14}$$

Da aber $x \to x^q$ der einzige nicht identische Automorphismus des Relativkörpers k_2/k ist, schreibt sich (14) anders so:

$$\left(\frac{\xi+\sqrt{\alpha}}{\xi-\sqrt{\alpha}}\right)^{v-u} = 1. \tag{15}$$

Und zwar ist das Bestehen von (15) für alle ξ in k notwendig und hinreichend, damit $P_m=P_n$ ist. Da aber $x^{v-u}=1$ wegen $|v-u| \leqq q-1$

nur im Fall $v-u=0$ q verschiedene Wurzeln haben kann, so haben wir für $P_m=P_n$ die notwendige und hinreichende Bedingung $u=v$ erhalten. Dies findet nach (13) dann und nur dann statt, wenn $q+1 \mid n_0-m_0$ d. h. $q+1 \mid n-m$ ist. Damit haben wir (8) bewiesen.

Hieraus folgt auch schon, daß es insgesamt nur $\varphi(q+1)$ verschiedene P_n gibt. Es ist also nur noch übrig die Ordnung von P_n zu bestimmen. Diese ist die kleinste natürliche Zahl r, für die $P_n^r=1$, d. h. nach (7) $P_{nr}=1$ gilt. Wieder nach (7) ist $P_1 P_n=P_n$, $P_1=1$, und somit lautet vorige Gleichung: $P_{nr}=P_1$. Nach (8) darf man hierfür (6) schreiben, und das bedeutet eben, daß die Behauptung über die Ordnung von P_n richtig ist. Damit haben wir den Satz bewiesen.

Hierzu mögen noch einige Bemerkungen stehen:

a) *Ist $p \neq 2$, so gibt es in k zu jedem ungeraden Grad n umkehrbare (ganze oder gebrochene) Polynome.*

Zerlegen wir nämlich n in zwei Faktoren μ, ν so, daß $(\mu, q-1)=(\nu, q+1)=1$ ist. Das ist wegen $(q-1, q+1)=2$ im allgemeinen sogar auf mehrere Arten möglich. Dann ist $f_\nu(x^\mu)$ [desgleichen auch $(f_\nu(x))^\mu$] in der Tat umkehrbar, vom Grade $\mu\nu=n$.

b) *Ist $p \neq 2$, so gibt es in k kein umkehrbares Polynom zweiten Grades.*

Es sei nämlich

$$f(x)=\frac{g(x)}{h(x)} \tag{16}$$

umkehrbar in k, wobei $g(x)$, $h(x)$ ganze Polynome sind und (indem man gleich $f(\infty)=\infty$ annimmt) vom Grade 2 bzw. $\leqq 1$. Dann hat die Gleichung

$$g(x)-yh(x)=0 \tag{17}$$

für jedes y in k genau eine Lösung. Bezeichnet $D(y)$ die nach x genommene Diskriminante dieser Gleichung, so muß also $D(y)=0$ für jedes y gelten. Das ist aber ein Widerspruch, da $D(y)$ offenbar vom ersten oder zweiten Grade ist. (Man hätte **b)** auch einfacher beweisen können.)

c) *Ist $p \neq 2, 3$ und $q \geqq 11$, so gibt es in k kein umkehrbares ganzes Polynom vierten Grades.* Läßt man auch die gebrochenen Polynome zu, so bleibt das für hinreichend große q vermutlich immer noch richtig.

Nehmen wir hierzu ein umkehrbares Polynom $f(x)$ vom vierten Grade wieder in der Form (16) an, wobei jetzt $g(x)$, $h(x)$ vom Grade 4 bzw. $\leqq 3$ ist. Wieder hat dann (17) für jedes y genau eine Lösung. Bei nichtverschwindender Diskriminante $D(y)$ von (17) ist das nach

einer Arbeit[3]) von mir (wegen $p \neq 2, 3$) dann und nur dann der Fall, wenn die kubische Resolvente von (17) keine Lösung hat, woraus ebenfalls nach [3]) folgt, daß $D(y)$ [das ja auch die Diskriminante dieser Resolvente ist] ein Quadratelement sein muß. Das ist im Fall $D(y) = 0$ von selbst erfüllt, gilt also allgemein.

Nunmehr sei $f(x)$ ganz. Dann ist $h(x)$ eine Konstante (wofür man auch 1 nehmen kann) und somit $D(y)$ vom dritten Grade. Als schwache Folgerung aus einem Satz von HASSE[4]) nimmt aber $D(y)$ [im Fall $p \neq 2, 3$; $q \geqq 11$] nicht nur Quadratelemente an, woraus unsere Behauptung folgt.

Ist dagegen $f(x)$ gebrochen, so ist $D(y)$ im allgemeinen vom sechsten Grade. Man kann weiter nicht mehr so schließen wie im vorigen Fall, da Hasses Satz sich nur auf Polynome vom Grade 3 und 4 bezieht. Es scheint aber, daß zum vollständigen Beweis obiger Vermutung nicht viel fehlt.

d) Unseren Satz können wir wie folgt in ein schärferes Licht setzen. Führen wir die lineare Substitution S in k_2 mit

$$Sz = \frac{z + \sqrt{\alpha}}{z - \sqrt{\alpha}}$$

ein. Dann läßt sich (11) so schreiben: $(Sx)^n = Sf_n(x)$, d. h.

$$f_n(x) = S^{-1}(Sx)^n .$$

Hiernach hat das Polynom $f_n(x)$ im Oberkörper k_2 eine einfache Deutung bekommen, woraus man insbesondere sieht, daß $f_n(x)$ *in* k_2 *ein zu* x^n *ähnliches Polynom ist.* (Selbst x^n braucht dabei weder in k noch in k_2 umkehrbar zu sein!) Weniger genau kann man sagen, daß unsere expliziten Beispiele für umkehrbare Polynome im wesentlichen (nämlich von linearen Substitutionen abgesehen) nur die Potenzen x^n sind, wenn man auf obige Weise in den Oberkörper k_2 hinausgreift. Das läßt vermuten, daß mit Hilfe anderer Oberkörper von k sich weitere umkehrbare Polynome in k konstruieren lassen, mir ist aber etwas solches nicht gelungen.

e) Hier wollen wir auf eine an sich sehr merkwürdige Erscheinung hinweisen betreffend alle Polynome $f(x)$ vom dritten Grade in k mit $p \neq 2, 3$, wobei wir uns wieder auf den Fall $f(\infty) = \infty$ beschränken dürfen. *Unter ihnen nehmen* nähmlich x^3 *und das Polynom in* (5)

---

[3]) L. RÉDEI, Über die Gleichungen dritten und vierten Grades in endlichen Körpern, *dieser Band*, S. 96—105.

[4]) H. HASSE, Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, *Abh. Math. Sem. Hamburg*, **10** (1934), S. 325—348, insb. S. 347.

$[f_3(x) =] \frac{x^3+3\alpha x}{3x^2+\alpha}$ *eine Sonderstellung ein, und diese zwei stehen einander* gewissermaßen *dual gegenüber,* wie wir das hier näher ausführen wollen.

Es bezeichne $[f]_i$ $(i=0, \ldots, 4)$ die Anzahl der i-fachen Elemente des Wertevorrats von $f(x)$. (Insbesondere bezeichnet $[f]_0$ die Anzahl der Elemente von k, die durch $f(x)$ nicht angenommen werden.) Zu äquivalenten Polynomen gehören dieselben Zahlen $[f]_i$. Weiter ist $f(x)$ offenbar dann und nur dann umkehrbar in k, wenn $[f]_1 = q$ ist.

In einer Arbeit[5]) werde ich unter anderem die $[f]_i$ genau berechnen. Hieraus entnimmt man folgende Abschätzungen:

$$\left|[f]_0 - \frac{q}{3}\right| \leqq \frac{2}{3}\sqrt{q} + \frac{2}{3}, \quad \left|[f]_1 - \frac{q}{2}\right| \leqq \sqrt{q} + 2, \quad [f]_2 \leqq 4, \quad \left|[f]_3 - \frac{q}{6}\right| \leqq \frac{1}{3}\sqrt{q} + \frac{8}{3}, \tag{18}$$

ausgenommen x^3 und $\frac{x^3+3\alpha x}{3x^2+\alpha}$ (und die äquivalenten Polynome). Für diese zwei verhalten sich die Zahlen $[f]_i$ scharf abweichend nach den Angaben folgender Tabelle:

		$[f]_0$	$[f]_1$	$[f]_2$	$[f]_3$	
Für	x^3	0	q	0	0	$(3 \mid q+1)$
		$\frac{2q-2}{3}$	1	0	$\frac{q-1}{3}$	$(3 \mid q-1)$.
Für	$\frac{x^3+3\alpha x}{3x^2+\alpha}$	$\frac{2q+2}{3}$	0	0	$\frac{q-2}{3}$	$(3 \mid q+1)$
		0	q	0	0	$(3 \mid q-1)$.

Die erste und vierte Zeile dieser Tabelle drückt die schon bekannte Tatsache aus, daß x^3 im Fall $3 \mid q+1$ bzw. $\frac{x^3+3\alpha x}{3x^2+\alpha}$ im Fall $3 \mid q-1$ umkehrbar ist. Im ganzen zeigt aber die Tabelle, daß diese zwei Polynome (was die Vielfachheitszahlen $[f]_i$ anbelangt) ihre Rollen vertauschen, wenn man vom Fall $3 \mid q+1$ zum Fall $3 \mid q-1$ übergeht. Die Sonderstellung dieser zwei Polynome tritt durch die Bemerkung noch klarer hervor, daß es unter den übrigen Polynomen dritten Grades für $q \geqq 11$ keine umkehrbaren gibt, wie man es aus (18) sieht.

f) Nach der Arbeit [3]) können wir die Gleichung

$$\frac{x^3+3\alpha x}{3x^2+\alpha} = y$$

[5]) L. Rédei, Über die Charaktersummen von Hasse und den Wertevorrat der Polynome dritten und vierten Grades in endlichen Körpern. (In Vorbereitung.)

im Fall $3|q-1$ (dann ist die linke Seite umkehrbar) leicht nach x auflösen. Das ergibt

$$x=y+(y^2-\alpha)^{\frac{q-1}{3}}[(y+\sqrt{\alpha})^{\frac{q+2}{3}}+(y-\sqrt{\alpha})^{\frac{q+2}{3}}] \qquad (3|q-1),$$

wie man es auch direkt leicht bestätigt. Die rechte Seite — die offenbar ein Polynom q-ten Grades in k ist, da die ungeraden Potenzen von $\sqrt{\alpha}$ herausfallen — ist also umkehrbar.

(Eingegangen am 21. Juli 1944.)