

ÜBER DIE EINSTUFIG NICHTKOMMUTATIVEN RINGE

MASATOSHI IKEDA

Dem Andenken meines verehrten Lehrers TADASI NAKAYAMA gewidmet

1. Einleitung

In der Arbeit [2] hat L. Rédei den Begriff des einstufig nichtkommutativen Ringes eingeführt, und die allen möglichen Typen der einstufig nichtkommutativen *endlichen* Ringe aufgezählt. Sie bestehen aus drei Grundtypen und ihren homomorphen Bildern¹⁾. In der oben genannten Arbeit hat Rédei einstufig nichtkommutativen *unendlichen* Ringes ganz kurz erwähnt, und nur darauf hingewiesen, dass man nicht einmal weiss, ob solche Ringe überhaupt existieren. In der vorliegenden Arbeit handelt es sich um die Nichtexistenz der einstufig nichtkommutativen unendlichen Ringe. Obwohl die Nichtexistenz der allgemeinen unendlichen Ringe vom genannten Charakter hoch glaubwürdig scheint, kann ich doch zur Zeit die Aufgabe in ihrer vollen Allgemeinheit nicht lösen, sondern ich kann nur zeigen, dass ein einstufig nichtkommutativer Ring mit einer zusätzlichen Bedingung notwendigerweise endlich wird. Im folgenden soll nämlich der untenbenannte Satz bewiesen werden.

SATZ. R sei ein Ring, dessen Restklassenring R/N nach dem Radikal N einen endlichen Rang über dem Zentrum besitzt. Ist R ein einstufig nichtkommutativer Ring, so ist R notwendigerweise ein endlicher Ring.

Es soll hier noch folgendes hervorgehoben werden. Die zusätzliche Bedingung, die im obigen Satz vorausgesetzt worden ist und dem Satz einen Schönheitsfehler beibringt, ist nur deswegen benötigt, weil die Nichtexistenz des Schiefkörpers, der ein einstufig nichtkommutativer *Ring* ist, nicht leicht nachweisbar ist.

Bevor wir zum Beweis kommen, schicken wir der Vollständigkeit halber die Definition des n -stufig nichtkommutativen Ringes voran.

Received June 29, 1965.

¹⁾ Vgl. Rédei [2].

Der Begriff des n -stufig nichtkommutativen Ringes wird nach der Induktion über n eingeführt. Ein assoziativer Ring heisst 0-stufig nichtkommutativ, wenn er ein kommutativer Ring ist; ein assoziativer Ring R heisst n -stufig nichtkommutativ, wenn alle echten Unterringe von R höchstens $(n-1)$ -stufig nichtkommutativ, aber R selbst nicht $(n-1)$ -stufig nichtkommutativ ist.

Ist ein Ring R n -stufig nichtkommutativ, so ist, wie man leicht durch Induktion beweisen kann, ein beliebiges homomorphes Bild von R höchstens n -stufig nichtkommutativ. Wie man gleichfalls durch Induktion bestätigen kann, ist ein n -stufig ($n < 0$) nichtkommutativer Ring durch geeignete $n+1$ Elemente erzeugbar. Ein einstufig nichtkommutativer Ring ist insbesondere durch beliebige zwei nicht vertauschbare Elemente erzeugbar.

2. Hilfssätze

Um den Satz zu beweisen, benötigen wir einige Hilfssätze, die im folgenden zusammengestellt werden.

HILFSSATZ 1. *K sei ein Schiefkörper endlichen Ranges über dem Zentrum. Dann ist K niemals ein einstufig nichtkommutativer Ring.*

Beweis. Sei u_i ($i = 1, \dots, n$) ein Basissystem von K über dem Zentrum Z von K , und sei

$$u_i u_j = \sum_k \alpha_{i,j}^k u_k \text{ mit } \alpha_{i,j}^k \in Z.$$

Ferner sei $Z_0 = P[\alpha_{i,j}^k]$ der über dem Primkörper P von K durch die Elemente $\alpha_{i,j}^k$ erzeugte Unterring von Z . Dann ist $K_0 = \sum_i Z_0 u_i$ ein nichtkommutativer Unterring von K . Wäre K ein einstufig nichtkommutativer Ring, so müsste $K = K_0$ sein. Demnach folgte, dass $Z = Z_0$ ist. Nach einem Satz von Zariski²⁾ wäre dann $[Z : P] < \infty$, folglich $[K : P] < \infty$. Sei nun v_i ($i = 1, \dots, m$) ein Basissystem von K über P , und sei

$$v_i v_j = \sum_k \beta_{i,j}^k v_k \text{ mit } \beta_{i,j}^k \in P.$$

Ferner sei $\{a_1, a_2\}$ ein Erzeugendensystem des einstufig nichtkommutativen Ringes K , und sei

$$a_i = \sum_j r_i^j v_j \text{ mit } r_i^j \in P.$$

²⁾ Vgl. Zariski [3].

Da jedes Element von K als Produktsumme von a_i darstellbar ist, sieht man sofort ein, dass der Primkörper P unter diesen Umständen durch die Elemente $\beta_{i,j}^k, \gamma_j^i$ erzeugbar sein würde. Wäre nun die Charakteristik von K gleich Null, so wäre P der Körper der rationalen, was aber unmöglich ist, denn die Anzahl der Primzahlen, die in den Nennern von $\beta_{i,j}^k$ bzw. γ_j^i vorhanden sind, ist endlich. Die Charakteristik von K würde also von Null verschieden sein. Als endliche Erweiterung eines endlichen Körpers P wäre dann K selbst endlich und kommutativ, was doch ein Widerspruch ist. Somit wurde der Hilfssatz bewiesen.

HILFSSATZ 2. R sei ein halbeinfacher Ring endlichen Ranges über dem Zentrum. Dann ist R niemals einstufig nichtkommutativ.

Beweis. Zunächst zeigen wir, dass ein primitiver Ring endlichen Ranges über dem Zentrum niemals einstufig nichtkommutativ sein kann. Ein primitiver Ring R lässt sich als dichter Ring der linearen Transformationen eines Vektorraumes über einem Schiefkörper K darstellen. Ist der Rang $[V : K] > 1$, so seien x_i ($i = 1, 2$) K -linear unabhängige Elemente von V . Wäre nun R einstufig nichtkommutativ, so würde der Unterring $T = \{a \in R \mid x_i a = 0\}$ kommutativ sein. Andererseits gibt es in T zwei Elemente a_i ($i = 1, 2$) derart, dass $x_2 a_i = x_i$ ($i = 1, 2$) ist. Dann ist ersichtlich $x_2(a_1 a_2) = 0$ und $x_2(a_2 a_1) = x_1$. Die Elemente a_1 und a_2 sind also nicht vertauschbar, was aber ein Widerspruch sein würde. Es müsste also $[V : K] = 1$ sein, demnach müsste R ein Schiefkörper sein. Nach dem Hilfssatz 1 kann aber ein Schiefkörper endlichen Ranges über dem Zentrum niemals ein einstufig nichtkommutativer Ring sein. Somit wurde gezeigt, dass ein primitiver Ring endlichen Ranges über dem Zentrum niemals einstufig nichtkommutativ sein kann. Nun sei R ein halbeinfacher Ring mit einem endlichen Rang über dem Zentrum. Wäre R einstufig nichtkommutativ, so würde, für beliebiges primitives Ideal P von R , der Restklassenring R/P höchstens einstufig sein. Da aber der Restklassenring R/P einen endlichen Rang über dem Zentrum besitzt, kann er, wie oben gezeigt, niemals einstufig nichtkommutativ sein, demnach folgte, dass R/P kommutativ sein muss. Daraus folgte aber, dass R selbst kommutativ ist, was ein Widerspruch ist. Somit wurde die Behauptung bewiesen.

Der folgende Hilfssatz ist fast trivial, aber der Vollständigkeit halber wird der Beweis gegeben,

HILSSATZ 3. *R sei ein durch ein Element erzeugter Ring, der keine additive Torsion besitzt. Dann gibt es unendlich viele Primzahlen p derart, dass $pR \cong R$ ist.*

Beweis. $I[x]$ sei der Polynomring über dem Integritätsbereich der ganzen Zahlen, und $I_0[x]$ der Ring der Polynome ohne Konstante. Der Ring R ist dann zum Restklassenring $I_0[x]/A$ von $I_0[x]$ nach einem Ideal A isomorph. Andererseits ist ein beliebiges Primideal von $I_0[x]$ entweder von der Form (px) oder $(px, f_0(x))$ oder $(g_0(x))$, wobei p eine Primzahl, $f_0(x)$ bzw. $g_0(x)$ Polynome der Form $xh(x)$ mit einem primitiven irreduziblen (nicht konstanten) Polynom $h(x)$ in $I[x]$ ist. Nun sei $A = \bigcap_i Q_i$ eine Darstellung von A als Durchschnitt der Primärideale Q_i , und P_i sei das Q_i zugehörige Primideal. Es gibt dann mindestens ein Primideal P_i vom dritten Typus, denn sonst würde $I_0[x]/A$ eine additive Torsion besitzen. Ein solches Primideal sei $P = (g_0(x))$ mit $g_0(x) = a_1x + \dots + a_nx^n$ ($n > 1$). Den Restklassenring $I_0[x]/P$ bezeichnen wir mit S . Wäre nun $pS = S$ für unendlich viele Primzahlen p , so würde $p(I_0[x] + P) = I_0[x] + P$ für die betreffenden Primzahlen p sein. Das heisst, dass P ein Polynom der Form $b_1x + \dots + b_mx^m$ mit $b_1 \not\equiv 0(p)$, $b_2 \equiv \dots \equiv b_m \equiv 0(p)$ für jede betreffende Primzahl p enthalten würde. Wie man leicht daraus schliessen kann, würde dann $a_2 \equiv \dots \equiv a_n \equiv 0(p)$ für alle betreffenden Primzahlen p sein, woraus folgte, dass $g_0(x)$ von der Form a_1x ist. Das ist aber ein Widerspruch. Es gibt also unendlich viele Primzahlen p derart, dass $pS \cong S$ ist. Demnach folgt sofort, dass $pR \cong R$ für diese Primzahlen p ist.

HILFSSATZ 4. *R sei ein Ring, dessen Restklassenring R/N nach dem Radikal N einen endlichen Rang über dem Zentrum besitzt. Ist R ein stufig nichtkommutativer Ring, so besteht R aus lauter additiven Torsionen. Die additive Ordnung jedes Elements ist eine Potenz einer festen Primzahl.*

Beweis. R_0 sei die Gesamtheit der additiven Torsionen von R , und Z sei das Zentrum von R . Evident ist R_0 ein Ideal von R . Nehmen wir zunächst an, dass $R \not\cong R_0$ und $Z \not\subset R_0$ ist. Dann gibt es sicher, für beliebiges Element $\rho \in R_0 - Z$, ein Element σ , das mit ρ nicht vertauschbar ist. R ist demnach durch ρ und σ erzeugbar. Der Restklassenring $\bar{R} = R/R_0$ ist nun durch ein Element erzeugbar und ohne additive Torsion. Also nach dem Hilfssatz 3 gibt es zwei voneinander verschiedene Primzahlen p und q derart, dass $p\bar{R} \cong \bar{R}$

und $q\bar{R} \cong \bar{R}$ ist. Daraus folgt, dass $pR \cong R$, und folglich, dass die Unterringe pR und qR kommutativ sind. Das ergibt $[p\rho, p\sigma] = [q\rho, b\sigma] = 0$, woraus folgt aber $[\rho, \sigma] = 0$, was ein Widerspruch ist. Es muss also entweder $R = R_0$ oder $R_0 \subset Z$ sein. Um den Hilfssatz zu beweisen, nehmen wir an, dass $R \neq R_0$ ist, und zeigen, dass ein Widerspruch daraus folgt. Wie eben besagt, ist R_0 unter dieser Annahme in Z enthalten. Zunächst zeigen wir, dass $\bar{R} = R/R_0$ kommutativ sein muss. Wäre nämlich \bar{R} nichtkommutativ, so wäre er einstufig nichtkommutativ. Stimmt er mit seinem Radikal überein, so würde $\bar{R} \cong \bar{R}^2$ sein, also wäre $\bar{R} = \bar{R}/\bar{R}^2$ als additive Gruppe durch zwei Elemente erzeugbar, folglich wäre sie keine vollständige Gruppe. Es gäbe also eine Primzahl p derart, dass $p\bar{R} \cong \bar{R}$ ist. Also wäre $p\bar{R} \cong \bar{R}$, und wegen der einstufig Nichtkommutativität von \bar{R} wäre $p\bar{R}$ ein kommutativer Ring. Wäre nun $\{\bar{\rho}, \bar{\sigma}\}$ ein beliebiges Erzeugendensystem von \bar{R} , so würde $[p\bar{\rho}, p\bar{\sigma}] = p^2[\bar{\rho}, \bar{\sigma}] = 0$ sein, während $[\bar{\rho}, \bar{\sigma}] \neq 0$ wäre. Das würde aber im Widerspruch mit der Tatsache stehen, dass \bar{R} keine Torsionen besitzt. Wäre nun \bar{R} von Radikal \bar{N} verschieden, so wäre der Restklassenring \bar{R}/\bar{N} höchstens einstufig nichtkommutativ. Da aber \bar{R}/\bar{N} ersichtlich einen endlichen Rang über dem Zentrum besitzt, könnte er nach dem Hilfssatz 2 nicht einstufig nichtkommutativ sein, sondern kommutativ. \bar{P} sei ein primitives Ideal von \bar{R} , dann wäre der Restklassenring \bar{R}/\bar{P} , wie eben besagt, ein kommutativer Körper, der durch zwei Elemente erzeugbar ist und folglich ein endlicher Körper ist. Wäre die Charakteristik von \bar{R}/\bar{P} , so wäre $p\bar{R} \cong \bar{R}$, woraus folgte, dass $p\bar{R}$ ein kommutativer Ring ist. Also würde $[p\bar{\rho}, p\bar{\sigma}] = p^2[\bar{\rho}, \bar{\sigma}] = 0$ für beliebiges Erzeugendensystem von \bar{R} sein, was aber mit der Tatsache, dass \bar{R} ohne additive Torsion ist, im Widerspruch stehen würde. \bar{R} muss somit kommutativ sein. Folglich ist $[a, b] \in R_0$ für beliebiges Paar der Elemente von R . Nun sei $\{\rho, \sigma\}$ ein beliebiges Erzeugendensystem, und m sei die additive Ordnung von $[\rho, \sigma]$. Dann folgt aus $m[\rho, \sigma] = [m\rho, \sigma] = [\rho, m\sigma] = 0$, dass mR in Z enthalten ist. Wählen wir jetzt ein Erzeugendensystem $\{\rho, \sigma\}$ so aus, dass die additive Ordnung m von $[\rho, \sigma]$ möglichst klein wird. Dann ist m eine Primzahl. Wäre m keine Primzahl, so gäbe es einen Primteiler p von m derart, dass $pR \cong R$ ist, denn mR ist im Zentrum von R enthalten. Da pR kommutativ sein würde, $[p\rho, p\sigma] = p[p\rho, \sigma] = 0$, wobei $[p\rho, \sigma] = p[\rho, \sigma]$ von Null verschieden sein würde, denn sonst würde m der Primzahl p gleich sein. Die Elemente $p\rho$ und σ wären dann

nicht vertauschbar, demnach würden sie den Ring R erzeugen. Für dieses Erzeugendensystem würde aber die additive Ordnung von $[\rho, \sigma]$ gleich p sein, was mit der Minimalität von m im Widerspruch stehen würde. Also ist $m = p$ eine Primzahl. Aus $p[\rho, \sigma]$ folgt, wie schon oben gezeigt, dass pR in Z enthalten ist. Also ist $p[a, b] = 0$ für jedes Paar der Elemente von R . Nun sei $\{\rho, \sigma\}$ ein beliebiges Erzeugendensystem von R . Dann ist $[\rho, \sigma] = \tau$, wie oben besagt, im Ideal R_0 enthalten; R_0 ist seinerseits in Z enthalten. Also ist $\rho[\rho, \sigma] = \rho\tau = \tau\rho = [\rho, \sigma]\rho \in R_0$, daraus folgt $\rho^2\sigma - \sigma\rho^2 = 2\tau\rho \in R_0$, $\rho^3\sigma - \sigma\rho^3 = 3\tau\rho^3 \in R_0$, u.s.w. Endlich bekommt $\rho^b\sigma - \sigma\rho^b = p\tau\rho^{b-1} = 0$, woraus folgt, dass $\xi^b \in Z$ für beliebiges Element ξ von R , denn ein nicht im Zentrum enthaltenes Element kann stets in einem geeigneten Erzeugendensystem von R enthalten sein. Nun sei L ein maximales Linksideal von R , das das Ideal $pR + R_0 (\subseteq Z)$ enthält. Die Existenz solches Ideal folgt aus der Tatsache, dass die Vereinigungsmenge einer aufsteigenden Reihe der echten Linksideale von R einen kommutativen Ring bildet, denn alle echten Linksideale sind kommutative Ringe. Da $[\rho, \sigma]$ in R_0 enthalten ist, ist das Linksideal L ein zweiseitiges Ideal, daraus folgt, dass der Restklassenring R/L ein Schiefkörper ist. Da aber der Schiefkörper R/L einen endlichen Rang über dem Zentrum besitzt, kann er nach dem Hilfssatz 1 niemals ein einstufig nichtkommutativer Ring sein. R/L ist also ein kommutativer Körper, der durch zwei Elemente erzeugbar ist und folglich ein endlicher Körper ist. Die Charakteristik von R/L ist p , denn L enthält pR . Nun sei R/L durch ein Element $\bar{\xi}$ erzeugt, dessen Vertreter mit ξ bezeichnet wird. Dann ist $\xi^{p^f} \equiv \xi \pmod{L}$ mit einer passenden ganzen Zahl f . Da aber ξ^b in Z enthalten ist, lässt sich das Element ξ als Summe $z + \lambda$ mit $z \in Z$ und $\lambda \in L$ darstellen. Daraus folgt, dass das Element ξ mit allen Elementen von L vertauschbar ist, denn L ist kommutativ. Das ist aber unmöglich, weil der nichtkommutative Ring R durch ξ und L erzeugbar ist. Somit wurde gezeigt, dass $R = R_0$ sein muss. Um den Rest der Behauptung zu beweisen, bezeichnen wir mit R_p die Gesamtheit der Elemente von R , deren additive Ordnung Potenz einer Primzahl p ist. Dann bildet R_p ersichtlich ein Ideal von R , und R ist als direkte Summe von R_p darstellbar. Wenn kein von R_p mit R übereinstimmt, so sind sie alle kommutativ, folglich ist R selbst kommutativ, was aber ein Widerspruch ist. Es gibt also eine Primzahl p derart, dass $R_p = R$ ist. W.z.b.w.

HILFSSATZ 5. *R sei ein einstufig nichtkommutativer Ring, dessen Restklassenring R/N nach dem Radikal N einen endlichen Rang besitzt. Wenn R vom Radikal N verschieden ist, so ist der Restklassenring R/N ein endlicher Körper.*

Beweis. Nach dem Hilfssatz 2 ist der Restklassenring R/N ein kommutativer Ring. Wenn also der Radikal N im Zentrum Z enthalten ist, so ist $[a, b] \in N \subseteq Z$ für beliebiges Paar der Elemente von R . Wie im Beweis des Hilfssatzes 4 gezeigt, gibt es eine Primzahl p , für die $pR \subseteq Z$ und $R_p = R$ gilt. Daraus folgt, dass $p[a, b] = 0$ für beliebiges Paar der Elemente von R ist. Nach demselben Verfahren wie im Beweis des Hilfssatzes 4 kann man dann daraus schliessen, dass $\xi^p \in Z$ für beliebiges Element ξ von R ist. Nun sei P ein primitives Ideal von R , dann ist R/P ein kommutativer Körper, der durch zwei Elemente erzeugbar ist, folglich ein endlicher Körper ist. Unter diesen Umständen kann man daraus nach derselben Methode, die im Beweis des Hilfssatzes 4 verwendet wurde, einen Widerspruch ziehen. Der Radikal N ist also nicht im Zentrum Z enthalten. Es gibt also ein Element ρ von $N - Z$ und ein Element $\sigma \notin N$ derart, dass sie nicht vertauschbar sind. Dann wird R natürlich durch ρ und σ erzeugt, und der Restklassenring R/N wird durch ein Element erzeugt. Die additive Ordnung jedes Elements von R ist nach dem Hilfssatz 4 eine Potenz der Primzahl p . Mit Rücksicht darauf, dass R endlich erzeugbar ist, kann man daraus sofort schliessen, dass pR ein nilpotentes Ideal von R , folglich im Radikal von R enthalten ist. Der Restklassenring R/N ist also eine Algebra über dem Galoisfeld $GF[p]$, und, wie eben besagt, ist durch ein Element erzeugbar. Wenn also R/N kein Körper ist, so enthält er zwei echte Unterringe \bar{T}_1 und \bar{T}_2 derart, dass $R/N = \bar{T}_1 + \bar{T}_2$ ist. Sei T_1 bzw. T_2 das Urbild von \bar{T}_1 bzw. \bar{T}_2 in R . Dann ist das Element σ als Summe der Form $\sigma_1 + \sigma_2$ mit $\sigma_1 \in T_1$ und $\sigma_2 \in T_2$ darstellbar. Da T_1 und T_2 kommutativ sind, so sind die Elemente σ_1 und σ_2 mit ρ vertauschbar, woraus folgt aber, dass σ mit ρ vertauschbar ist, was ein Widerspruch ist. Der Restklassenring R/N ist also ein Körper, der durch ein Element erzeugbar ist, folglich ein endlicher Körper ist. Somit wurde die Behauptung bewiesen.

3. Beweis des Satzes

Nun kommen wir zum Beweis des Satzes. R sei ein einstufig nichtkommutativer Ring, dessen Restklassenring R/N einen endlichen Rang über dem

Zentrum besitzt. Nach dem Hilfssatz 4 besteht R aus additiven Torsionen, deren additive Ordnung Potenz einer Primzahl p ist. Nun sei $\{\rho, \sigma\}$ ein Erzeugendensystem von R , und sei $p^r \rho = p^s \sigma = 0$. Dann ist $p^t a = 0$ für jedes Element a von R , wobei $t = \max(r, s)$ ist. Da $pR \cong R$ ist, ist der Restklassenring $\bar{R} = R/pR$ eine Algebra über dem Galoisfeld $GF[p]$. Mit Rücksicht darauf, dass pR im Radikal N von R enthalten ist, sieht man sofort ein, dass das Radikal \bar{N} von \bar{R} mit N/pR übereinstimmt. Nun zeigen wir, dass \bar{R} eine Algebra mit einer Polynomidentität ist. Stimmt nämlich \bar{R} mit seinem Radikal überein, so ist $\bar{P} \cong \bar{R}^3$, folglich ist \bar{R}^2 ein kommutativer Ring. Daraus folgt dann $[[a, b], [c, d]] = 0$ für beliebige zwei Paare der Elemente von \bar{R} . Ist nun \bar{R} vom Radikal \bar{N} verschieden, so besitzt \bar{R}/\bar{N} ($\cong R/N$) einen endlichen Rang über dem Zentrum, und nach dem Hilfssatz 2 kann er nicht einstufig nichtkommutativ sein. Er ist also kommutativ, woraus folgt dann, dass der Kommutator $[a, b]$ jeden Paars der Elemente von \bar{R} im kommutativen Unter- ringe \bar{N} enthalten ist. Folglich ist $[[a, b], [c, d]] = 0$ für beliebige zwei Paare der Elemente von \bar{R} . Demnach ist \bar{R} jedenfalls eine Algebra mit einer Polynomidentität. Nach einem Satz von Amitsur ist dann das Radikal \bar{N} von \bar{R} ein Nilideal. Für den Beweis des Satzes machen wir noch von der folgenden Tatsache Gebrauch: Ist nämlich ein kommutativer Ring S durch a_i ($i = 1, \dots, r$) mit der Bedingung $a_i^n = 0$ erzeugbar, dann ist $S^{nr} = 0$. Ist nun $\bar{R} = \bar{N}$, so ist $\bar{R} \cong \bar{R}^2$. Der letzere ist also ein kommutativer Nilring, der durch vier Elemente erzeugbar ist. Demnach folgt, dass \bar{R}^3 folglich \bar{R} selbst nilpotent ist. \bar{R} ist also eine durch zwei Elemente erzeugbare nilpotente Algebra über $GF[p]$, die ersichtlich ein endlicher Ring ist. Ist dagegen \bar{R} von seinem Radikal \bar{N} verschieden, so ist \bar{R}/\bar{N} ($\cong R/N$ nach dem Hilfssatz 5 ein endlicher Körper, dessen Absolutgrad mit f bezeichnet wird. Sei $\{\bar{\rho}, \bar{\sigma}\}$ irgendein Erzeugendensystem von \bar{R} , und $\bar{\xi}$ sei ein Vertreter eines erzeugenden Elements des endlichen Körpers R/N . Ferner sei

$$\bar{\rho} = \sum_{i=0}^{f-1} \alpha_i \bar{\xi}^i + \bar{\rho}_0$$

$$\bar{\sigma} = \sum_{i=0}^{f-1} \beta_i \bar{\xi}^i + \bar{\sigma}_0$$

mit $\alpha_i, \beta_i \in GF[p]$ und mit $\bar{\rho}_0, \bar{\sigma}_0 \in \bar{N}$. Schliesslich sei $\sum_{i=0}^{f-1} r_i \bar{\xi}^i = \bar{\tau}_0 \in \bar{N}$ mit $r_i \in GF[p]$ eine Relation vom niedrigsten Grade, der $\bar{\xi}$ genügt. Da jedes Element

von R als Summe der Form $\sum_{i=0}^{f-1} \delta_i \bar{\xi}^i + \lambda_0$ mit $\delta_i \in GF[p]$ und $\lambda_0 \in \bar{N}$ eindeutig darstellbar ist, sieht man sofort ein, dass der Radikal \bar{N} durch die Elemente $\bar{\xi}^i \bar{\rho}_0$, $\bar{\xi}^i \bar{\sigma}_0$ und $\bar{\xi}^k \bar{\tau}_0$ ($i, j, k = 0, \dots, f-1$) erzeugbar ist. \bar{N} ist folglich ein kommutativer endlich erzeugbarer Nilring, der also nach der oben erwähnten Tatsache nilpotent ist. \bar{N} ist demnach eine endlich erzeugbare nilpotente Algebra über $GF[p]$, die also ein endlicher Ring ist. Da aber \bar{R}/\bar{N} ein endlicher Körper ist, schliesst man daraus, dass \bar{R} selbst ein endlicher Ring ist. Nun bilde man eine endliche Algebra \bar{R}_1 über $GF[p]$ mit Einselement durch die eventuelle Hinzufügung eines Einselements zu \bar{R} . Dann ist pR/p^3R ein Modul von \bar{R}_1 , der durch zwei Elemente erzeugbar ist. Er ist also ein endlicher Modul. Auf dieselbe Weise ist $p^i R/p^{i-1} R$ ein endlicher Modul für jedes $i = 0, 1, \dots, t-1$. Daraus folgt schliesslich, dass R selbst ein endlicher Ring ist. W.z.b.w.

LITERATURVERZEICHNIS

- [1] Amitsur, S. A.: A generalization of Hilbert's Nullstellensatz, Proc. Amer. Math. Soc. 8, 1957.
- [2] Rédei, L.: Die einstufig nichtkommutativen endlichen Ringe, Acta Sci. Math. Szeged, 18, 1958.
- [3] Zariski, O.: A new proof of Hilbert's Nullstellensatz, Bull. Amer. Math. Soc. 53, 1947.

Ege Universität
Izmir, Türkei