Die einstufig nichtregulären Ringe

Von LADISLAUS RÉDEI in Szeged

Die nullteilerfreien Ringe nennen wir auch *regulär.*

Einstufig nichtregulär nennen wir jeden nichtregulären Ring, dessen echte Unterringe regulär sind. Diese Ringe sind endlich, undzwar gilt der folgende:

Satz. *Die sämtlichen einstufig nichtregulären Ringe sind die Zeroringe von Primzahlordnung und die direkten Summen von zwei endlichen Primkörpern.*

Dabei nennen wir einen Zeroring einen Ring, dessen Quadrat 0 ist, ferner verstehen wir unter der Ordnung einer endlichen Struktur die Anzahl ihrer Elemente. Die Ordnung einer solchen Struktur S werde mit $O(S)$ bezeichnet. Stets bezeichnen p und q Primzahlen.

Ist R ein Zeroring mit $O(R)=p$, so enthält R Nullteiler, ferner hat R überhaupt keine echten Unterringe, weshalb R tatsächlich einstufig nichtregulär ist.

Ferner sei jetzt $R=K+L$ die direkte Summe von zwei Körpern K und L mit $O(K)=p$, $O(L)=q$. Zwei von 0 verschiedene Elemente von R haben (dann und) nur dann ein verschwindendes Produkt, wenn das eine in K, das andere in L liegt, also die zwei miteinander R erzeugen. Hiernach ist R wieder einstufig nichtregulär.

Umgekehrt bezeichnen wir fortan mit R einen einstufig nichtregulären Ring. Wir haben zu beweisen, daß R einer der vorher betrachteten Ringe ist. Freilich ist $R\neq 0$.

Erstens sei R endlich. Es bezeichne $\mathfrak{n}$ das Radikal von R. Nur die Fälle $\mathfrak{n}=R$, 0 sind möglich, da sonst $\mathfrak{n}$ ein echter Unterring von R mit Nullteilern wäre, entgegen der Voraussetzung.

Im Fall $\mathfrak{n}=R$ sind alle Elemente von R nilpotent. Sofort folgt hieraus die Existenz eines Elementes $\varrho(\neq 0)$ von R mit $\varrho^2=0$. Dabei läßt sich ϱ so wählen, daß seine additive Ordnung $o^+(\varrho)$ eine Primzahl p ist, denn um dies zu erreichen genügt es ϱ mit einer passenden ganzen rationalen Zahl zu multiplizieren. Wegen

$$\varrho^2=0, \quad o^+(\varrho)=p$$

ist der durch ϱ erzeugte Unterring von R ein Zeroring p-ter Ordnung. Da dieser nicht nullteilerfrei ist, so muß er sogar gleich R sein.

Im Fall $n=0$ ist R halbeinfach, also gilt nach dem Satz von WEDDERBURN—ARTIN eine Zerlegung

$$R=S_1+\cdots+S_k \qquad (k\geqq 1)$$

in eine direkte Summe von vollen Matrizenringen $S_1,\ldots,S_k$ über endlichen Körpern. Jedoch müssen diese Matrizenringe den Rang 1 haben, d. h. lauter Körper sein, denn sonst hätte R echte Unterringe mit Nullteilern. Da ferner R Nullteiler hat, so muß $k>1$ sein. Da endlich die echten Unterringe von R nullteilerfrei sind, so muß $k=2$ bestehen, auch müssen S_1, S_2 Primkörper sein.

Zweitens sei R unendlich. Hieraus leiten wir ziemlich mühsam einen Widerspruch ab, womit wir den Satz bewiesen haben werden.

Zuerst betrachten wir den Fall, daß R durch ein Element erzeugbar ist. Dann ist R das homomorphe Bild des durch ein Element erzeugten freien Ringes. Dieser läßt sich als $x\mathfrak{J}[x]$ annehmen, wobei $\mathfrak{J}$ den Ring der ganzen rationalen Zahlen und x eine Unbestimmte bezeichnet. (Also ist $x\mathfrak{J}[x]$ der Unterring des Polynomringes $\mathfrak{J}[x]$ bestehend aus den durch x teilbaren Elementen von diesem.) Die Ideale von $x\mathfrak{J}[x]$ sind $x\mathfrak{a}$, wobei $\mathfrak{a}$ die Ideale von $\mathfrak{J}[x]$ bezeichnet.[1]) Folglich läßt sich nach dem Homomorphiesatz

$$R=x\mathfrak{J}[x]/x\mathfrak{a} \tag{1}$$

ansetzen. Freilich ist $\mathfrak{a}\neq 0$. Wir bezeichnen mit $d(x)(\in\mathfrak{J}[x])$ den größten gemeinsamen Teiler der Elemente von $\mathfrak{a}$, so normiert, daß der Anfangskoeffizient positiv ist. Dann gilt

$$\mathfrak{a}=d(x)\mathfrak{a}_0, \tag{2}$$

wobei $\mathfrak{a}_0$ ein primitives Ideal von $\mathfrak{J}[x]$ ist, dessen Elemente nämlich 1 zum größten gemeinsamen Teiler haben. Das ist bekanntlich gleichbedeutend damit, daß $\mathfrak{a}_0$ sowohl ein von 0 verschiedenes konstantes Element, als auch ein Hauptpolynom (d. h. ein Polynom mit dem Anfangskoeffizienten 1) enthält. Folglich gilt

$$\mathfrak{a}_0\supseteqq(h(x),n), \tag{3}$$

wobei $h(x)$ ein in $\mathfrak{a}_0$ enthaltenes Hauptpolynom kleinsten Grades und n die in $\mathfrak{a}_0$ enthaltene kleinste natürliche Zahl bezeichnet. (Der Fall $h(x)=n=1$, $\mathfrak{a}_0=(1)$ kommt auch in Frage.) Da der Faktorring $x\mathfrak{J}[x]/x\mathfrak{a}_0$ offenbar endlich ist, muß $d(x)$ wegen (2) und der Annahme von 1 verschieden sein.

[1]) Vgl. RÉDEI, *Algebra* I (Leipzig, 1959), S. 470—471.

Für beliebige Mengen $\mathfrak{A}$, $\mathfrak{B}$ bezeichnen wir mit $\mathfrak{A}-\mathfrak{B}$ üblicherweise die Menge der in $\mathfrak{B}$ nicht enthaltenen Elemente von $\mathfrak{A}$ und beweisen den folgenden:

Hifssatz. *Gelten*

$$f(x),\ g(x) \in x\mathfrak{J}[x]-x\mathfrak{a} \tag{4}$$

und

$$f(x)g(x) \in x\mathfrak{a}, \tag{5}$$

so gibt es Polynome $\mathfrak{F}(x)$ *und* $\mathfrak{G}(x)$ *in* $x\mathfrak{J}[x]$ *mit*

$$\mathfrak{F}(f(x))+\mathfrak{G}(g(x)) \equiv x \pmod{x\mathfrak{a}}. \tag{6}$$

Zum Beweis bezeichnen wir mit $\overline{\varphi(x)}$ für jedes $\varphi(x)\ (\in x\mathfrak{J}[x])$ die Restklasse $\varphi(x) \pmod{x\mathfrak{a}}$. Wegen (1) und (4) sind $f(x)$, $g(x)$ von 0 verschiedene Elemente von R, ferner ist ihr Produkt nach (5) gleich 0, also erzeugen sie den ganzen Ring R. Da insbesondere $\bar{x} \in R$ ist, so folgt hieraus der Hilfssatz sofort.

Es ist $x \nmid d(x)$. Denn ist $x \mid d(x)$, so setze man

$$f(x)=g(x)=pnd(x) \tag{7}$$

mit einer beliebigen Primzahl p. Wegen (2) und (3) sind dann für (7) die Bedingungen (4) und (5) erfüllt, weshalb sich der Hilfssatz anwenden läßt. Also entsteht nach Einsetzen von (7) in (6) und nochmaliger Berücksichtigung von (2):

$$\mathfrak{H}(pnd(x)) \equiv x \pmod{xd(x)}$$

mit einem $\mathfrak{H}(x)(\in x\mathfrak{J}[x])$. Hieraus folgt $d(x) \mid x$, also $d(x)=x$,

$$\mathfrak{H}(pnx) \equiv x \pmod{x^2}.$$

Da dies falsch ist, so ist $x \nmid d(x)$ bewiesen.

$d(x)$ enthält keine mehrfachen Faktoren $(\neq 1)$. Gilt nämlich

$$u(x)^2 \mid d(x)$$

mit einem $u(x)$ $(\in \mathfrak{J}[x], \neq \pm 1)$, so sind (4) und (5) für

$$f(x)=g(x)=\frac{nxd(x)}{u(x)}$$

erfüllt. Nach Einsetzen in (6) folgt

$$\mathfrak{H}\left(\frac{nxd(x)}{u(x)}\right) \equiv x \pmod{xd(x)\mathfrak{a}_0}$$

mit einem $\mathfrak{H}(x)\ (\in x\mathfrak{J}[x])$. Sofort ergibt dies $u(x) \mid x$. Da dies nach Vorigem falsch ist, so ist die Behauptung richtig.

$d(x)$ ist prim (d. h. eine Primzahl oder ein irreduzibles Hauptpolynom). Ist nämlich die Behauptung falsch, so hat $d(x)$ zwei verschiedene Primfaktoren $u(x)$, $v(x)$. Ist außerdem $n>1$, so sind (4) und (5) für

$$f(x)=xd(x),\quad g(x)=\frac{nxd(x)}{v(x)}$$

erfüllt. Nach Einsetzen in (6) folgt ähnlich wie vorher $u(x)|x$. Da dies falsch ist, so muß $n=1$, d. h. $\mathfrak{a}_0=(1)$, $\mathfrak{a}=(d(x))$ sein. Für diesen Fall nehme man eine Primzahl p mit $p\nmid d(x)$ zu Hilfe. Dann sind (4) und (5) für

$$f(x)=\frac{pxd(x)}{u(x)},\quad g(x)=\frac{pxd(x)}{v(x)}$$

erfüllt, also entsteht nach Einsetzen in (6)

$$\mathfrak{F}\left(\frac{pxd(x)}{u(x)}\right)+\mathfrak{G}\left(\frac{pxd(x)}{v(x)}\right)\equiv x\pmod{xd(x)},$$

weshalb

$$0\equiv 1\pmod{p,d(x)}$$

ist. Folglich muß $d(x)$ konstant, d. h. eine natürliche Zahl d sein. Für diesen restlichen Fall gehen die obigen $u(x)$, $v(x)$ in gewisse Primzahlen u, v $(uv|d)$ über. Offenbar sind (4) und (5) für

$$f(x)=\frac{dx^2}{u},\quad g(x)=\frac{dx^2}{v}$$

erfüllt. Nach Einsetzen in (6) hat man

$$\mathfrak{F}\left(\frac{dx^2}{u}\right)+\mathfrak{G}\left(\frac{dx^2}{v}\right)\equiv x\,(\mathrm{mod}\,dx).$$

Da dies offenbar falsch ist, so ist die Behauptung bewiesen.

Da hiernach $d(x)$ prim und von x verschieden, also $(xd(x))$ ein Primideal von $x\mathfrak{J}[x]$ ist, anderseits R Nullteiler enthält, so folgt aus (1) und (2), daß notwendig $\mathfrak{a}_0\neq(1)$ ist.

$\mathfrak{a}_0$ ist ein Primideal von $\mathfrak{J}[x]$. Sonst gäbe es nämlich zwei Polynome $u(x)$, $v(x)$ mit

$$u(x),\,v(x)\in\mathfrak{J}[x]-\mathfrak{a}_0,\quad u(x)v(x)\in\mathfrak{a}_0.$$

Da dann (4) und (5) für

$$f(x)=xd(x)u(x),\quad g(x)=xd(x)v(x)$$

erfüllt sind, so folgt aus (6) sofort $d(x)\,|\,1$. Da dies falsch ist, so ist die Behauptung richtig.

Hiernach gilt

$$\mathfrak{a}_0 = (h(x), p)$$

mit einer Primzahl p und einem mod p irreduziblen Hauptpolynom $h(x)$. Nach (2) hat man

$$\mathfrak{a} = d(x)\,(h(x), p),$$

wobei nach Obigem $d(x)$ eine Primzahl oder ein nichtkonstantes Primpolynom ist.

Wir zeigen, daß die zweite Möglichkeit nicht zutrifft. Hierzu nehmen wir an, daß $d(x)$ nichtkonstant ist. Für jede ganze Zahl $c(\neq 0)$ sind dann (4) und (5) mit

$$f(x) = x\,d(x), \quad g(x) = cpx$$

erfüllt. Nach (6) gilt also

$$\mathfrak{F}(x\,d(x)) + \mathfrak{G}(cpx) \equiv x \pmod{x\mathfrak{a}}.$$

Es sei α eine komplexe Zahl mit $d(\alpha) = 0$, also $\alpha \neq 0$. Dann folgt

$$\mathfrak{G}(cp\alpha) = \alpha.$$

Wenn α ganz (algebraisch) ist, so folgt hieraus $cp\alpha \mid \alpha$. Da aber dies falsch ist, so folgt, daß α nicht ganz ist. Wählt man nun c so, daß $cp\alpha$ ganz ist, so entsteht dennoch ein Widerspruch. Das beweist die Behauptung, also ist $d(x)$ eine Primzahl q. Somit hat man

$$\mathfrak{a} = q\,(h(x), p).$$

Es ist $q \neq p$, denn im Fall $q = p$ läßt sich der Hilfssatz mit

$$f(x) = g(x) = px$$

anwenden, woraus bei Einsetzen in (6) der Widerspruch p 1 entsteht. Also ist tatsächlich $p \neq q$. Da aber dann (4) und (5) für

$$f(x) = qx, \quad g(x) = xh(x)$$

erfüllt sind, so geht dabei (6) in

$$\mathfrak{F}(qx) + \mathfrak{G}(xh(x)) \equiv x \pmod{qx(h(x), p)}$$

über. Hieraus folgt zunächst $h(x) \neq x$, also folgt für eine komplexe Nullstelle $\alpha(\neq 0)$ von $h(x)$

$$\mathfrak{F}(q\alpha) \equiv \alpha \pmod{pq\alpha}.$$

Dies ist aber unmöglich, da $\alpha(\neq 0)$ ganz ist. Somit haben wir gezeigt, daß R nicht durch ein Element erzeugbar ist.

Im übriggebliebenen Fall bezeichnen ϱ und σ von 0 verschiedene Elemente von R mit

(8) $$\varrho\sigma = 0.$$

Indem wir mit $\{\varrho, \sigma\}$ den durch ϱ und σ erzeugten Unterring von R bezeichnen, so gilt dann

$$R = \{\varrho, \sigma\}, \tag{9}$$

da die rechte Seite Nullteiler hat, also kein echter Unterring von R sein kann. Aus (8) und (9) folgt, daß die Elemente von R sich als eine Summe von Gliedern von der Form

$$c\sigma^i\varrho^k \qquad (i, k \geqq 0;\ i+k \geqq 1;\ c \in \mathfrak{J}) \tag{10}$$

schreiben lassen.

Wir zeigen, daß auch

$$\sigma\varrho = 0 \tag{11}$$

gilt, d. h. R kommutativ ist. Ist nämlich $\sigma\varrho \neq 0$, so gilt wegen $\sigma\varrho \cdot \sigma = 0$ ähnlich wie (9) auch $R = \{\sigma\varrho, \sigma\}$. Also folgt wegen (8), daß sich die Elemente von R als eine Summe von Gliedern von der Form $c\sigma^i$ und $c\sigma^i\varrho$ $(i \geqq 1;\ c \in \mathfrak{J})$ schreiben lassen. Wendet man dies insbesondere auf das Element ϱ an und multipliziert die dadurch sich ergebende Gleichung von links mit ϱ, so entsteht wegen (8) $\varrho^2 = 0$. Dies bedeutet, daß (8) für $\sigma = \varrho$ erfüllt, also R wegen (9) durch das einzige Element ϱ erzeugt is. Da dies der Voraussetzung widerspricht, so ist hiermit (11) bewiesen.

Hiernach läßt sich das bei (10) gesagte dahin verschärfen, daß sich die Elemente von R in der Form

$$f(\varrho) + g(\sigma) \qquad (f(x), g(x) \in x\mathfrak{J}[x]) \tag{12}$$

schreiben lassen.

Nun bilden die $f(x)$ $(\in x\mathfrak{J}[x])$ mit $f(\varrho) = 0$ ein Ideal $\mathfrak{a}_\varrho$ von $x\mathfrak{J}[x]$. Dieses ist ein Primideal, denn sonst gäbe es zwei Polynome $u(x)$, $v(x)$ aus $x\mathfrak{J}[x] - \mathfrak{a}_\varrho$ mit $u(x)v(x) \in \mathfrak{a}_\varrho$. Das bedeutet $u(\varrho) \neq 0$, $v(\varrho) \neq 0$, $u(\varrho)v(\varrho) = 0$, also das Bestehen von $R = \{u(\varrho), v(\varrho)\}$. Dies hat zur Folge, daß R durch das einzige Element ϱ erzeugt ist. Da aber letzteres falsch ist, so ist $\mathfrak{a}_\varrho$ tatsächlich ein Primideal von $x\mathfrak{J}[x]$.

Genau so wie $\mathfrak{a}_\varrho$ ist auch (das entsprechend zu verstehende) $\mathfrak{a}_\sigma$ ein Primideal von $x\mathfrak{J}[x]$.

Lassen wir $\mathfrak{F}(x)$ und $\mathfrak{G}_j(x)$ je ein Repräsentantensystem der Restklassen von $x\mathfrak{J}[x]$ mod $\mathfrak{a}_\varrho$ bzw. mod $\mathfrak{a}_\sigma$ voneinander unabhängig durchlaufen. Dann kommen alle Elemente von R nach (12) sogar schon unter den

$$\mathfrak{F}(\varrho) + \mathfrak{G}_j(\sigma) \tag{13}$$

vor.

Wir zeigen, daß jedes Element von R nur einmal unter diesen Elementen (13) vorkommt. Offenbar genügt es zu zeigen, daß aus der Annahme

$$\mathfrak{F}(\varrho)+\mathfrak{G}(\sigma)=0 \tag{14}$$

das Verschwinden beider Glieder der linken Seite folgt. Aus (14) folgt wegen (8) sofort $\varrho\mathfrak{F}(\varrho)=0$, d. h. $x\mathfrak{F}(x)\in\mathfrak{a}_\varrho$. Da $\mathfrak{a}_\varrho$ ein Primideal von $x\mathfrak{J}[x]$ ist, so folgt, daß x oder $\mathfrak{F}(x)$ in $\mathfrak{a}_\varrho$ gehört. Da aber aus $x\in\mathfrak{a}_\varrho$ offenbar $\mathfrak{F}(x)\in\mathfrak{a}_\varrho$ folgt, so gilt stets das letztere. Das bedeutet eben $\mathfrak{F}(\varrho)=0$, womit die Behauptung bewiesen ist.

Das Resultat besagt, daß eine direkte Summenzerlegung

$$R=S_1+S_2 \tag{15}$$

gilt, wobei S_1, S_2 mit den Faktorringen

$$x\mathfrak{J}[x]/\mathfrak{a}_\varrho,\quad x\mathfrak{J}[x]/\mathfrak{a}_\sigma$$

isomorphe Unterringe von R sind. Da R unendlich ist, so ist mindestens das eine von S_1 und S_2 ebenfalls unendlich. Da aber jeder unendliche Ring echte Unterringe hat, so folgt aus (15) sofort, daß R echte Unterringe mit Nullteilern besitzt. Mit diesem Widerspruch ist der Beweis des Satzes beendet.

(Eingegangen am 25. August 1959)