Navorsings- en oorsigartikels

Primitiewe elemente vir kommutatiewe ringuitbreidings

H. J. Schutte

Departement Wiskunde, Universiteit van Stellenbosch, Stellenbosch 7600

Ontvang 12 Mei 1990; aanvaar 22 Februarie 1991

UITTREKSEL

Die bestaan van primitiewe elemente vir integriteitsgebiede word behandel met verwysing na die alombekende stelling oor primitiewe elemente vir uitbreidings van liggame. Primitiewe elemente vir uitbreidings van 'n kommutatiewe ring R , met eenheidselement, word vervolgens beskou waar R slegs eindig veel minimale priemideale het waarvan die deursnede nul is. Hierdie geval word gereduseer na uitbreidings van integriteitsgebiede.

ABSTRACT

Primitive elements for commutative ring extensions

The existence of primitive elements for integral domain extensions is considered with reference to the well known theorem about primitive elements for field extensions. Primitive elements for extensions of a commutative ring R with identity are considered, where R has only a finite number of minimal prime ideals with zero intersection. This case is reduced to the case for ring extensions of integral domains.

AMS (American Mathematical Society) onderwerpklassifikasie: Primêr 13B02
Sekondêr 13B25

1. Inleiding

Algebraïese en transendente elemente oor 'n kommutatiewe ring R met eenheidselement word gedefinieer soos vir uitbreidings van liggame.¹ Schutte bewys dat as S 'n unitêre uitbreiding van R is (d.w.s. R en S het dieselfde identiteitselement), R 'n ring met nul priemradikaal, en $\alpha \in S$ is algebraïes oor R , dan is alle elemente van $R[\alpha]$ algebraïes oor R .² Dit word aanvaar dat R slegs 'n eindige aantal minimale priemideale het. As nog 'n element $\beta \in S$ aan $R[\alpha]$ gadjungeer word, dan kan dit gebeur dat $R[\alpha, \beta]$ transendente elemente oor R het.³ Dit word trouens bewys dat as die minimale priemideale in R paarsgewys komaksimaal is, dan is 'n nodige en voldoende voorwaarde vir 'n unitêre uitbreiding S van R om transendente elemente oor R te hê, dat vir elke priemideaal P_i in R daar 'n element $\alpha_i \in S$ bestaan wat algebraïes is oor R en waarvan die definiërende ideaal in $R[x]$ bevat is in $P_i[x]$.⁴

'n Primitiewe element oor R vir die ringuitbreiding $R[\alpha, \beta]$ is 'n element $\gamma \in R[\alpha, \beta]$ sodat $R[\gamma] = R[\alpha, \beta]$. Uit die opmerkings hierbo volg dit dat as α en β algebraïes oor R is, dan is dit nie moontlik om 'n element $\gamma \in R[\alpha, \beta]$ te vind sodat $R[\gamma] = R[\alpha, \beta]$ nie as $R[\alpha, \beta]$ elemente het wat transendent oor R is. Om sake nog verder te bemoeilik kan bewys word dat as $t \in S$ transendent is oor R , en die k minimale priemideale in R is paarsgewys komaksimaal, dan bestaan elemente $\alpha_1, \alpha_2, \dots, \alpha_k$ in S wat algebraïes is oor R met $R[t] = R[\alpha_1, \alpha_2, \dots, \alpha_k]$.⁵ Primitiewe elemente (as hulle bestaan) van uitbreidings van R , wat verkry word deur algebraïese elemente oor R aan R te adjungeer, kan dus algebraïes of transendent oor R wees.

Daar is min bekend oor primitiewe elemente vir

ringuitbreidings. Die enigste teorema wat in die literatuur beskikbaar is, is die bekende stelling vir eindige uitbreidings van liggame.

In hierdie artikel sal ons 'n nodige en voldoende voorwaarde vir bepaalde ringuitbreidings $R[\alpha, \beta]$, α en β algebraïes oor R , gee vir die bestaan van 'n primitiewe element oor R . Ook word voldoende voorwaardes gegee waaronder integrale uitbreidings van 'n integriteitsgebied primitiewe elemente het.

2. Primitiewe elemente vir integriteitsgebiede

Laat S 'n integriteitsgebied met 'n eenheidselement wees. Ons sal die ideaal wat in S voortgebring word deur die elemente $a_1, a_2, \dots, a_n \in S$ deur $(a_1, a_2, \dots, a_n)$ aandui. As α en β algebraïes oor S en $S[\alpha, \beta]$ 'n integriteitsgebied is, dan is dit duidelik dat α en β algebraïes is oor die liggaam van kwosiente $Q(S)$ van S en dat $Q(S)[\alpha, \beta]$ 'n uitbreidingsliggaam van $Q(S)$ is. As die definiërende veelterm van α in $Q(S)[x]$ $f(x)$ is, dan $S[\alpha] \cong S[x]/((f(x)) \cap S[x])$ waar $(f(x))$ die ideaal is wat deur $f(x)$ voortgebring word in $Q(S)[x]$. Die veelterm $f(x)$ kan sô gekies word dat sy koëffisiënte in S is. So 'n veelterm sal 'n definiërende veelterm van α in $S[x]$ genoem word.

Die bekende stelling oor primitiewe elemente vir eindige liggaamsuitbreidings sê dat as $F(\alpha_1, \beta_1)$ 'n algebraïese uitbreiding van 'n liggaam F is en β_1 separabel oor F is, dan gee enige waarde k uit F 'n primitiewe element $\gamma = \alpha_1 + k\beta_1$ vir $F(\alpha_1, \beta_1)$ oor F , mits $\alpha_1 + k\beta_1 \neq a_i + k\beta_i$ waar α_i enigeen van α_1 se toegevoegdes is, insluitende α_1 , en β_i een van β_1 se toegevoegdes is ($\beta_i \neq \beta_1$).⁶ As F 'n eindige liggaam is, dan is $F(\alpha_1, \beta_1)$ altyd 'n enkelvoudige uitbreiding.⁷ As F oneindig

is, is daar slegs eindig veel ongeskikte keuses van k , aangesien die vergelykings $\alpha_i + k\beta_i = \alpha_i + k\beta_j$ slegs eindig veel moontlike oplossings k in F het.

Ons neem aan S het oneindig veel elemente. Terwyl daar 'n oorvloed van primitiewe elemente van die vorm $\alpha + k\beta$, $k \in S$, vir $Q(S)[\alpha, \beta]$ is, hoef $S[\alpha, \beta]$ geen primitiewe element oor S te hê nie.

Voorbeeld: Neem die ring van heelgetalle Z as S en $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$. Veronderstel $\gamma = \sqrt{2} + k\sqrt{3}$ is 'n primitiewe element vir $Q(Z)[\sqrt{2}, \sqrt{3}]$ oor $Q(Z)$. Dan is $(\sqrt{2} + k\sqrt{3})^3 = (2 + 9k^2)\sqrt{2} + (6k + 3k^3)\sqrt{3} \in Q(Z)[\gamma]$.

Omdat ook $\sqrt{2} + k\sqrt{3} \in Q(Z)[\gamma]$ en al die koëffisiënte van hierdie twee uitdrukkings inverses vir alle waardes van $k (\neq 0)$ in $Q(Z)$ het, volg dat $\sqrt{2}, \sqrt{3} \in Q(Z)[\alpha]$. Ons sal later aantoon dat $Z[\sqrt{2}, \sqrt{3}]$ geen primitiewe element oor Z het nie. (Kyk die opmerking voor Stelling 2.)

Aangesien $S[\alpha, \beta] = S[\gamma]$ as die ideale (α, β) en (γ) dieselfde is, bestaan daar klaarblyklik 'n primitiewe element vir $S[\alpha, \beta]$ oor S as $S[\alpha, \beta]$ 'n hoofideaaldomein (h.i.d.) is. Selfs as S 'n h.i.d. is, is dit uitsonderlik vir $S[\alpha, \beta]$ om 'n h.i.d. te wees. Al is $S[\alpha, \beta]$ nie 'n h.i.d. nie, kan dit egter nog gebeur dat (α, β) 'n hoofideaal is. Byv., $Z[\sqrt{-5}, \frac{1}{2}]$ is nie 'n h.i.d. nie,⁸ maar $\sqrt{-5}, \frac{1}{2} = \left(\frac{1}{\sqrt{-5}}\right)$.

Alle primitiewe elemente vir $S[\alpha, \beta]$ oor S is ook primitiewe elemente vir $Q(S)[\alpha, \beta]$ oor $Q(S)$. Om primitiewe elemente van die vorm $\alpha + k\beta$ vir $S[\alpha, \beta]$ oor S te vind is dit daarom voldoende om na te gaan onder welke voorwaardes 'n primitiewe element van die vorm $\alpha + k\beta$ vir $Q(S)[\alpha, \beta]$ oor $Q(S)$ een is vir $S[\alpha, \beta]$ oor S . As $S[\alpha, \beta] = S[\gamma]$ dan is klaarblyklik

$$\alpha = \sum_{i=0}^p \tau_i \gamma^i, \tau_i \in S, \text{ en } \beta = \sum_{i=0}^q s_i \gamma^i, s_i \in S,$$

vir een of ander p en q . As egter $\alpha + k\beta$, $k \in S$, 'n primitiewe element vir $Q(S)[\alpha, \beta]$ oor $Q(S)$ is, weet ons slegs dat $S[\alpha, \beta] \cong S[\gamma]$.

Laat α en β algebraïes wees oor $Q(S)$, soos tevore.

Stelling 1: Laat $\gamma = \alpha + k\beta$, $k \in S$, 'n primitiewe element van $Q(S)[\alpha, \beta]$ oor $Q(S)$ wees en laat $S[\gamma] \subseteq S[\alpha, \beta]$, dan bestaan daar 'n element $m \in S$, $m \neq 0$, sodat γ 'n primitiewe element is van $S'[\alpha, \beta]$ oor $S' = S[m^{-1}]$.

Bewys: Laat $[Q(S)[\alpha, \beta]:Q(S)] = n$. Dan

$$\beta = \sum_{i=0}^{n-1} s_i \gamma^i, s_i \in Q(S). \text{ Laat } s_i = s_i/v_i (s_i, v_i \in S) \text{ en stel}$$

$m = v_0 \dots v_{n-1}$. Dan $m \in S$ en $v_i^{-1} \in S[m^{-1}] = S'$. Gevolglik $\beta \in S'[\gamma]$ en $\alpha = \gamma - k\beta \in S'[\gamma]$. Dus $\alpha, \beta \in S'[\gamma]$ en $S'[\alpha, \beta] \subseteq S'[\gamma]$. Aangesien $S[\gamma] \subseteq S[\alpha, \beta]$, volg dit dat $S'[\gamma] \subseteq S'[\alpha, \beta]$ en dus $S'[\gamma] = S'[\alpha, \beta]$.

Neem aan dat die definiërende veelterm $f(x)$ en $g(x)$ van α en β in $S[x]$ grade n_1 en n_2 het respektiewelik en dat $\gamma = \alpha + k\beta$, $k \in S$, 'n primitiewe element van

$Q(S)[\alpha, \beta]$ oor $Q(S)$ is. Veronderstel verder dat γ die wortel van 'n onherleibare monieke veelterm $h(x) \in S[x]$ is (d.w.s. die koëffisiënt van die hoogste mag van x in die definiërende veelterm van γ is een). Stel die graad van $h(x)$ is $n = n_1 \cdot n_2$. Elke moontlike som $\sum s_i \gamma^i = \beta$, $s_i \in S$, kan nou modulo $h(x)$ gereduseer

word na een van die vorm $\sum_{i=0}^{n-1} s_i \gamma^i = \beta$, $s_i \in S$. Netso

ook $\alpha = \sum_{i=0}^{n-1} \tau_i \gamma^i$, $\tau_i \in S$. Die probleem is om geskikte waardes vir s_i en τ_i ($i = 0, \dots, n-1$) in S te vind wat α en β gee.

Let op dat $\alpha + k\beta = \gamma = \sum_{i=0}^{n-1} (\tau_i + ks_i) \gamma^i$. Uit die

lineêre onafhanklikheid van $1, \gamma, \dots, \gamma^{n-1}$ in $S[\gamma]$ volg dat $\tau_i + ks_i = 0$ ($i \neq 1$), en $\tau_1 + ks_1 = 1$. Omge-

keerd, as $\beta = \sum_{i=0}^{n-1} s_i \gamma^i$ en $\tau_i = -ks_i$ ($i \neq 1$),

$\tau_1 = 1 - ks_1$, dan $\alpha = \sum_{i=0}^{n-1} \tau_i \gamma^i$. As daar dus geskikte

waardes s_i in S bestaan, dan is daar ook reeds geskikte waardes τ_i in S .

Om geskikte waardes s_i (s_i beskou as 'n onbekende)

te vind, reduseer $\beta = \sum_{i=0}^{n-1} s_i (\alpha + k\beta)^i$ modulo $f(x)$ en

$g(x)$ na $\beta = \sum_{i=0}^{n_1-1} \sum_{j=0}^{n_2-1} \ell_{ij} \alpha^i \beta^j$ waar die koëffisiënte ℓ_{ij} li-

neêre uitdrukkings in $s_0, \dots, s_{n-1}$ met koëffisiënte in $Q(S)$ is. Die versameling $\{\alpha^i \beta^j \mid 0 \leq i \leq n_1 - 1; 0 \leq j \leq n_2 - 1\}$ is 'n basis vir $Q(S)[\gamma]$ en dus is $\ell_{ij} = 0$ ($i \neq 0, j \neq 1$), $\ell_{01} = 1$.

As vir 'n geskikte keuse van $k \in S$ hierdie stelsel lineêre vergelykings oplossings $s_0, \dots, s_{n-1} \in S$ het, dan is $\alpha + k\beta$ 'n primitiewe element van $S[\alpha, \beta]$ oor S .

As hierdie metode in die geval $Z[\sqrt{2}, \sqrt{3}]$ aangewend word, kan maklik ingesien word dat vir geen $k \in Z$ is $\sqrt{2} + k\sqrt{3}$ 'n primitiewe element van $Z[\sqrt{2}, \sqrt{3}]$ oor Z nie.

Die volgende stelling gee 'n voldoende voorwaarde vir 'n primitiewe element $\alpha + k\beta$ van $Q(S)[\alpha, \beta]$ oor $Q(S)$ om ook een te wees vir $S[\alpha, \beta]$ oor S .

Stelling 2: As $S[\gamma]$ 'n eenduidige faktoriserings-gebied (e.f.g.) is en die definiërende veelterm $g(x)$ van β in $S[x]$ is 'n moniek, dan is $\gamma = \alpha + k\beta$, $k \in S$, 'n primitiewe element van $S[\alpha, \beta]$ oor S as dit ook een is vir $Q(S)[\alpha, \beta]$ oor $Q(S)$.

Bewys: Laat $g(x) = (x - \beta)g_1(x)$ met $x - \beta$ en $g_1(x)$ in $(Q(S)[\gamma])[x]$. Volgens 'n bekende stelling is die koëffisiënte van sowel $x - \beta$ as $g_1(x)$ in $S[\gamma]$, want $g(x)$ is 'n moniek.⁹ Dus $\beta \in S[\gamma]$, en gevolglik $\alpha = \gamma - k\beta \in S[\gamma]$. Soos tevore volg nou dat $S[\gamma] = S[\alpha, \beta]$.

Gevolgtrekking: As die element $m \in S$ van stelling 1 nie die eenheidselement van S is nie, en die definiërende veelterm $g(x)$ van β in $S[x]$ is 'n moniek, dan is $S[\gamma]$ nie 'n eenduidige faktoriserings-gebied nie, mits $S[\gamma] \subseteq S[\alpha, \beta]$.

Bewys: Veronderstel $S[\gamma]$ is 'n e.f.g. Dan volg uit stelling 2 dat γ 'n primitiewe element van $S[\alpha, \beta]$ oor S is. Uit stelling 1 volg dan dat $m = 1$, in stryd met ons aanname.

Voorbeeld: Beskou $Z[\alpha, \beta]$ met $\gamma = \alpha + k\beta$, $k \in Z$, $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$. Klaarblyklik is $Z[\gamma] \subseteq Z[\alpha, \beta]$ en $x^2 - 3$ 'n moniek. Ook weet ons reeds dat in hierdie geval $m \neq 1$ vir alle $k \in Z$. Dus geld vir alle $k \in Z$ dat $Z[\gamma]$ nie 'n e.f.g. is nie. (Vgl. met die opmerking volgende op voorbeeld 2 hierna.)

Opmerking: As $f(x)$ die definiërende veelterm van α in $S[x]$ is en β is separabel oor S , dan het $f(\gamma - kx)$ en $g(x)$ die grootste gemene deler (g.g.d.) $x - \beta$ in $(Q(S[\gamma])[x])$ vir 'n geskikte keuse van $k \in S$ en dus is $\beta \in S[\gamma]$. As die algoritme vir die bepaling van die g.g.d. uitgevoer kan word in $(S[\gamma])[x]$ dan klaarblyklik $\beta \in S[\gamma]$.

Voorbeeld: 1. Die integriteitsgebied $Z[e^{2\pi i/5}]$ is 'n e.f.g.¹⁰ Die getal $e^{2\pi i/5}$ is 'n wortel van $x^4 + x^3 + x^2 + x + 1 = 0$, terwyl die definiërende veelterme van $\cos \frac{2\pi}{5}$ en $i \sin \frac{2\pi}{5}$ die onherleibare veelterme $4x^2 + 2x - 1$ en $16x^4 + 20x^2 + 5$ respektiewelik is. In $(Z[\frac{1}{5}])[x]$ is beide hierdie veelterme monieke en $[Z[\frac{1}{5}][e^{2\pi i/5}]]$ is 'n e.f.g. Aangesien $i \sin \frac{2\pi}{5}$ 'n wortel is van $x^2 + 1 \left((1 - \cos^2 \frac{2\pi}{5}) \in \left(Z \left[\cos \frac{2\pi}{5} \right] \right)[x] \right)$ volg uit die dimensies van die uitbreidings $Q(Z)(e^{2\pi i/5}) : Q(Z)$ en $Q(Z) \left(\cos \frac{2\pi}{5} \right) : Q(Z)$ dat $e^{2\pi i/5}$ 'n primitiewe element van $Q(Z) \left(\cos \frac{2\pi}{5}, i \sin \frac{2\pi}{5} \right)$ oor $Z[\frac{1}{5}]$ is. Uit stelling 2 volg nou dat $e^{2\pi i/5}$ 'n primitiewe element vir $(Z[\frac{1}{5}]) \left(\cos \frac{2\pi}{5}, i \sin \frac{2\pi}{5} \right)$ oor $Z[\frac{1}{5}]$ is.

Voorbeeld: 2. Laat $S = Z[\frac{1}{5}]$, Z die ring van heelgetalle. Laat $\alpha = \sqrt{2}$ en $\beta = \sqrt{3}$, $f(x) = x^2 - 2$, $g(x) = x^2 - 3$, $\gamma = \sqrt{2} + \sqrt{3}$. Dan is $f(\gamma - x) = x^2 - 2(\sqrt{2} + \sqrt{3})x + 3 + 2\sqrt{2}\sqrt{3} \in (S[\gamma])[x]$. Die algoritme vir die berekening van die g.g.d. van $g(x)$ en $f(\gamma - x)$ gee $f(\gamma - x) - 1 \cdot g(x) = -2(\sqrt{2} + \sqrt{3})(x - \sqrt{3}) \in (S[\gamma])[x]$. Daar $-2(\sqrt{2} + \sqrt{3}) \left[-(\sqrt{2} + \sqrt{3}) \frac{(\sqrt{2} - \sqrt{3})^2}{2} \right] = 1$ en $\frac{(\sqrt{2} - \sqrt{3})^2}{2} \in S[\gamma]$ volg dat $-2(\sqrt{2} + \sqrt{3})$ 'n eenheid in $S[\gamma]$ is, en gevolglik is $x - \sqrt{3} \in (S[\gamma])[x]$. Dus is $\sqrt{3} \in S[\gamma]$ en $S[\sqrt{2} + \sqrt{3}] = S[\sqrt{2}, \sqrt{3}]$.

Opmerking: Die algebraïese heelgetalle in die liggaam $Q(\sqrt{2} + \sqrt{3})$, Q die liggaam van rasionale getalle, is van die vorm $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, waar a en c heelgetalle is, en b en d is óf beide heelgetalle óf beide halwes van onewe heelgetalle.¹¹ Dui hierdie ring van algebraïese heelgetalle aan met D . D is 'n Euklidiese integriteitsgebied en dus 'n e.f.g.

As aan enige e.f.g. D 'n element x geadjungeer word wat deur $cx = 1$ (d.w.s. $x = c^{-1}$) gedefinieer is, en $c = p_1^{t_1} p_2^{t_2} \dots p_t^{t_t}$ is die priemfaktorontbinding van c in D , dan het $p_i (i = 1, 2, \dots, t)$ inverses in $D[c^{-1}]$. Aangesien alle elemente van D van die vorm $\frac{d}{c^s}$, $d \in D$, ($s = 0, 1, 2, \dots$) is, kan hulle op een-eenduidige manier in priemfaktore ontbind word waarby $p_i (i = 1, 2, \dots, t)$ uitgesluit is. Dus is $D[c^{-1}]$ 'n e.f.g. Gevolglik is $D[\frac{1}{5}]$ 'n e.f.g. en aangesien klaarblyklik $D[\frac{1}{5}] = (Z[\frac{1}{5}]) (\sqrt{2}, \sqrt{3})$, volg uit voorbeeld 2 dat $(Z[\frac{1}{5}]) (\sqrt{2} + \sqrt{3}) = D[\frac{1}{5}]$ 'n e.f.g. is.

3. Primitiewe elemente vir algebraïese ringuitbreidings

Laat R 'n kommutatiewe ring met eenheidselement wees wat slegs 'n eindige aantal minimale priemideale $P_1, P_2, \dots, P_k$ het waarvan die deursnede nul is. Laat α en β elemente uit 'n unitêre uitbreidingsring S van R wees wat algebraïes is oor R . Die ideaal voortgebring deur P_i in $R[\alpha, \beta]$ word aangedui met $P_i R[\alpha, \beta]$. Klaarblyklik $P_i[\alpha, \beta] = P_i R[\alpha, \beta]$. Ook is $P_i[\alpha, \beta] \cap R = P_i$.¹² Dui die beelde van α en β onder die kanoniese homomorfie $R[\alpha, \beta] \rightarrow R[\alpha, \beta] / P_i[\alpha, \beta]$ met $\bar{\alpha}$ en $\bar{\beta}$ aan. Dan $R[\alpha, \beta] / P_i[\alpha, \beta] \cong (R/P_i)[\bar{\alpha}, \bar{\beta}]$. Voorts, as 'n element $\bar{\gamma} \in (R/P_i)[\bar{\alpha}, \bar{\beta}]$ algebraïes is oor R/P_i , dan is $\gamma \in R[\alpha, \beta]$ algebraïes oor R waar γ 'n oerbeeld van $\bar{\gamma}$ in $R[\alpha, \beta]$ is.¹³ As α algebraïes oor R is en $\bar{\alpha}$ is algebraïes oor R/P_i , dan is die definiërende ideaal van $\bar{\alpha}$ in $(R/P_i)[x]$ die beeld onder die kanoniese homomorfie $R[x] \rightarrow (R/P_i)[x]$ van die ideaal $(I, P_i[x])$ voortgebring deur I en $P_i[x]$ in $R[x]$, waar I die definiërende ideaal van α in $R[x]$ is.¹⁴

Definisie: 'n Ring $T (\supseteq R)$ word algebraïes oor R genoem as elke element van T algebraïes oor R is.

Stelling 3: $R[\alpha, \beta]$ is algebraïes oor R as en slegs as daar 'n minimale priemideaal P in R bestaan sodanig dat sowel $\bar{\alpha}$ as $\bar{\beta}$ algebraïes oor R/P is.

Bewys. Veronderstel $R[\alpha, \beta]$ is algebraïes oor R . Laat $\{a_i\}$ die versameling van alle koëffisiënte van die definiërende veelterme van α in $R[x]$ wees en $\{b_i\}$ dié van β .

Omdat die nulradikaal van R die nulideaal is, moet R minstens twee minimale priemideale hê, tensy die nulideaal self die enigste minimale priemideaal in R is, in welke geval die stelling triviaal is.

Veronderstel nou daar is geen minimale priemideaal P sodanig dat sowel $\bar{\alpha}$ as $\bar{\beta}$ algebraïes oor R/P is nie. As $\{a_i\} \not\subseteq P$ en $\{b_i\} \not\subseteq P$, P minimaal priem in R , dan is sowel $\bar{\alpha}$ as $\bar{\beta}$ algebraïes oor R/P , in stryd met ons aanname. Dus $\{a_i\} \subseteq P$ of $\{b_i\} \subseteq P$. Ook is dit nie die geval dat $\{a_i\} \subseteq P$ en $\{b_i\} \subseteq P$ nie, want R het minstens twee minimale priemideale, sê P_1 en P_2 , en as $\{a_i\} \subseteq P_1$

en $\{b_i\} \subseteq P_1$, dan is $\bar{\alpha}$ en $\bar{\beta}$ algebraïes oor R/P_2 , in stryd met ons aanname. Die versameling minimale priemideale in R word dus in twee eksklusiewe klasse A en B verdeel: As $P \in A$ dan $\{a_i\} \subseteq P$ en as $P \in B$ dan $\{b_i\} \subseteq P$. Maar dan bevat $R[\alpha, \beta]$ 'n element wat transcendent is oor R in stryd met die oorspronkslike aanname.¹⁵ Dus bestaan daar 'n minimale priemideaal P in R sodat $\bar{\alpha}$ sowel as $\bar{\beta}$ algebraïes is oor R/P .

Die bewys van die omgekeerde is soortgelyk aan die bewys van proposisie 6 in Schutte 1987 waarin ons $(R/P)[\bar{\alpha}, \bar{\beta}]$ vir S neem en in aanmerking neem dat $Q(R/P)^*[\bar{\alpha}', \bar{\beta}']$ 'n eindig dimensionale vektorruimte oor $Q(R/P)^*$ is.

Klaarblyklik kan hierdie resultaat uitgebrei word na alle eindig voortgebringde uitbreidings $R[\alpha_1, \alpha_2, \dots, \alpha_n]$ van R .

Laat α en β algebraïes oor R wees met P soos hierbo.

Gevolgtrekking 1: $\gamma \in R[\alpha, \beta]$ is 'n primitiewe element van $R[\alpha, \beta]$ oor R as, en slegs as, $\bar{\alpha} \in (R/P)[\bar{\alpha}, \bar{\beta}]$ 'n primitiewe element van $(R/P)[\bar{\alpha}, \bar{\beta}]$ oor R/P is en die beperking van die kanoniese homomorfie $R[\alpha, \beta] \rightarrow R[\alpha, \beta]/P[\alpha, \beta] (\cong (R/P)[\bar{\alpha}, \bar{\beta}])$ tot $R[\gamma]$ die kern $P[\alpha, \beta]$ het.

Bewys: As ons in gedagte hou dat $R[\gamma] \rightarrow (R/P)[\bar{\alpha}, \bar{\beta}]$ 'n surjeksie is, volg die stelling onmiddellik.

Hierdie kriterium kan enigsins verswak word in die geval waar $(R/P)[\bar{\alpha}, \bar{\beta}]$ 'n integriteitsgebied is.

Gevolgtrekking 2: As $(R/P)[\bar{\alpha}, \bar{\beta}]$ 'n integriteitsgebied is en $\bar{\gamma}$ is 'n primitiewe element van $(R/P)[\bar{\alpha}, \bar{\beta}]$ oor R/P , dan is $\gamma \in R[\alpha, \beta]$ 'n primitiewe element van $R[\alpha, \beta]$ oor R as, en slegs as, die kern K van die homomorfie $R[\gamma] \rightarrow (R/P)[\bar{\alpha}, \bar{\beta}] = (R/P)[\bar{\gamma}]$ 'n priemideaal in $R[\alpha, \beta]$ is.

Bewys: As γ 'n primitiewe element van $R[\alpha, \beta]$ oor R is, dan is die gevolgtrekking duidelik.

Om die omgekeerde te bewys moet ons eers aantoon dat $P[\alpha, \beta]$ 'n minimale priemideaal in $R[\alpha, \beta]$ is. Klaarblyklik is $P[\alpha, \beta]$ priem in $R[\alpha, \beta]$, want die kern van die homomorfie $R[\alpha, \beta] \rightarrow (R/P)[\bar{\alpha}, \bar{\beta}]$ is $P[\alpha, \beta]$. Laat $Q \subseteq P[\alpha, \beta]$ 'n priemideaal in $R[\alpha, \beta]$ wees. Dan is $R \cap Q$ 'n priemideaal in R en $R \cap Q \subseteq P$. Aangesien P 'n minimale priemideaal in R is, het ons $R \cap Q = P$. Maar $P[\alpha, \beta]$ is die kleinste ideaal in $R[\alpha, \beta]$ wat P omvat. Dus $Q = P[\alpha, \beta]$. Aangesien $K \subseteq P[\alpha, \beta]$ en K priem is in $R[\alpha, \beta]$ volg dit dat $K = P[\alpha, \beta]$. Uit gevolgtrekking 1 het ons nou dat $R[\gamma] = R[\alpha, \beta]$.

Opmerking: Daar dit soms moeilik is om in 'n gegewe ring te bepaal of 'n ideaal priem is of nie, is die laaste kriterium nie van veel nut om primitiewe elemente mee op te spoor nie. Dat dit wel nut het, toon die volgende voorbeeld.

Voorbeeld: laat $R = S[t]$, $S = Z[\frac{1}{2}]$, Z die ring van heelgetalle en t algebraïes oor S met definiërende ideaal die ideaal voortgebring deur die veelterm

$x^2 - x$ in $S[x]$. Dus $R \cong S[x]/(x^2 - x)$. Adjungeer α en β aan R waarvan die definiërende ideale voortgebring word deur $x^2 - 2$ en $x^2 - 3$ in $R[x]$. Laat P die ideaal (t) wees in R . Elke ideaal I eg bevat in (t) , moet voortgebring word deur elemente van die vorm st , $s \in S$, want $t^2 = t$, waaruit volg dat $S[t]/I$ nuldelaars bevat. Dus is (t) 'n minimale priem ideaal in R en $P[\alpha, \beta]$ is priem in $R[\alpha, \beta]$, soos aangetoon in die bewys van gevolgtrekking 2. Ook geld $(R/P)[\bar{\alpha}, \bar{\beta}] \cong S[\sqrt{2}, \sqrt{3}]$. Uit 'n vorige voorbeeld weet ons dat $\sqrt{2} + \sqrt{3}$ 'n primitiewe element van $S[\sqrt{2}, \sqrt{3}]$ oor S is. Die kern van die kanoniese homomorfie $(S[t])[\alpha, \beta] \rightarrow S[\sqrt{2}, \sqrt{3}]$ is $P[\alpha, \beta]$, di. $(t)[\alpha, \beta]$, en die kern van $S[(t)[\alpha, \beta]] \rightarrow S[\sqrt{2}, \sqrt{3}]$ is $(t)[\alpha + \beta]$. Aangesien $(S[t])[\alpha, \beta] = (S[\alpha, \beta])[t]$ is $\alpha + \beta$ klaarblyklik 'n primitiewe element van $(S[t])[\alpha, \beta]$, oor $S[t]$. Uit gevolgtrekking 2 het ons dat die ideaal $(t)[\alpha + \beta]$ 'n priem ideaal in $(S[t])[\alpha, \beta]$, is en dieselfde is as die ideaal $(t)[\alpha, \beta]$, in hierdie ring. Trouens, $(t)[\alpha + \beta]$ is 'n minimale priemideaal in $(S[t])[\alpha, \beta]$.

4. Uitbreidings van direkte somme

Ons beskou nou die geval van kommutatiewe ringe met eenheidselement wat die direkte som is van twee ideale: $R = R_1 + R_2$. Die volgende stelling kan maklik uitgebrei word tot direkte somme van meer as twee ideale.

Stelling 4: Laat S 'n unitêre uitbreiding van R wees met identiteit e en laat $e = e_1 + e_2$, $e_i \in R_i$. Laat $\alpha \in S$ en laat I 'n ideaal van $R[x]$ wees sodat $I \cap R = (0)$. Dan is α algebraïes oor R met definiërende ideaal I in $R[x]$ as, en slegs as, of $\alpha_1 := e_1\alpha$ algebraïes oor R_1 is met definiërende ideaal $I_1 := e_1I$ of $\alpha_2 := e_2\alpha$ algebraïes oor R_2 is met definiërende ideaal $I_2 := e_2I$. Ook $R[x] = R_1[x_1] \oplus R_2[x_2]$.

Bewys: Laat $I (\neq (0))$ 'n ideaal in $R[x]$ wees sodat $I \cap R = (0)$ en laat $\alpha \in S$ 'n element wees wat algebraïes is oor R , waar S dieselfde identiteit e as R het. Neem aan I is die definiërende ideaal van α in $R[x]$. Laat voorts $f(x) \in I$ en stel $e = e_1 + e_2$, $e_i \in R_i$. Dan is e_i 'n idempotent in R en is dit die identiteitselement van R_i ($i = 1, 2$). Stel $f(x) = f_1(x) + f_2(x)$ waar $f_i(x) = e_i f(x) \in R_i[x]$ ($i = 1, 2$). Elke $f_i(x)$ is nul of van graad ten minste een. Want as $f_i(x) = c \in R_i$, $c \neq 0$, dan is $e_i f(x) = e_i c = c \in I$ (omdat $e_1 e_2 = 0$), strydig met die gegewe $I \cap R = (0)$. Voorts, nie sowel $f_1(x)$ as $f_2(x)$ is nul nie, want $f(x) \neq 0$.

As beide $f_1(x)$ en $f_2(x)$ nie-nul is, dan $0 = e_i f(x) = f_i(e_i \alpha)$ daar $e_1 e_2 = 0$ en $e_i^2 = e_i$ ($i = 1, 2$). Klaarblyklik $\alpha = \alpha_1 + \alpha_2$ waar $\alpha_i = e_i \alpha$. Dus impliseer $f(x) = 0$ dat $f_i(\alpha_i) = 0$ ($i = 1, 2$). As egter $f_1(x) = 0$ vir alle $f(x) \in I$ (d.i. $I \subseteq R_2[x]$) dan is $\alpha_1 := e_1 \alpha$ transcendent oor R_1 . Want as $g(\alpha_1) = 0$ met $0 \neq g(x) \in R_1[x]$, dan is $h(x) := g(x) + f(x) \in R_2[x]$, 'n veelterm nie in I sodat

$$h(x) = h(\alpha_1 + \alpha_2) = g(\alpha_1) + f(\alpha_2) = 0,$$

strydig met ons aanname.

Ook geld $\alpha_1 \alpha_2 = 0$ en $\tau_i \alpha_j = 0$, $i \neq j$, $\tau_i \in R_i$. Dus

$R_1[\alpha_1] \cap R_2[\alpha_2] = (0)$. Dus $R[\alpha] = R_1[\alpha_1] \oplus R_2[\alpha_2]$.

Veronderstel, omgekeerd, dat $I \subseteq R[x]$ is gegee soos tevore, en dat vir elke $f(x) \in I$ geld dat $f(x) = f_1(x) + f_2(x)$ met $0 \neq f_1(x) \in R_1[x]$ vir ten minste een waarde van i , en dat elemente α_1 en α_2 in 'n uitbreidingsring S bestaan sodat $f_1(\alpha_1) = f_2(\alpha_2) = 0$ met $e_i \alpha_i = \alpha_i$ ($i = 1, 2$). Dan is $\alpha := \alpha_1 + \alpha_2$ algebraïes oor R met definiërende ideaal I in $R[x]$. Want $f(\alpha) = f(\alpha_1 + \alpha_2) = f(e_1 \alpha + e_2 \alpha)$ en dus volg dat

$$\begin{aligned} f(e_1 \alpha + e_2 \alpha) &= e_1 f(e_1 \alpha + e_2 \alpha) + e_2 f(e_1 \alpha + e_2 \alpha) \\ &= f_1(\alpha_1) + f_2(\alpha_2) = 0, \end{aligned}$$

want $e_1 e_2 = 0$ en $e_i^2 = e_i$. Let op dat as $I \subseteq R_1[x]$, sê, dws. $f_2(x) = 0$ vir alle $f(x) \in I$ en $f(\alpha_1) = 0$ waar $e_1 \alpha_1 = \alpha_1 \in S$, terwyl $\alpha_2 (= e_2 \alpha_2)$ transcendent is oor R_2 , dan klaarblyklik is $\alpha := \alpha_1 + \alpha_2$ 'n element wat algebraïes is oor R sodanig dat $f(\alpha) = 0$ vir alle $f(x) \in I$. Klaarblyklik is $R[\alpha] = R_2[\alpha] \oplus R_1[\alpha]$ soos tevore.

Beskou nou die geval waar 'n verdere element $\beta \in S$ geadjungeer word aan $R[\alpha]$. Uit stelling 4 volg dat elemente β_1 en β_2 bestaan sodat $R[\alpha, \beta] = R_1[\alpha_1, \beta_1] + R_2[\alpha_2, \beta_2]$ met $\beta = \beta_1 + \beta_2$, $\beta_i = e_i \beta$ ($i = 1, 2$). As $R_1[\alpha_1, \beta_1]$ en $R_2[\alpha_2, \beta_2]$ primitiewe elemente γ_1 en γ_2 oor R_1 en R_2 respektiewelik het, dan klaarblyklik is $\gamma := \gamma_1 + \gamma_2$ 'n primitiewe element van $R[\alpha, \beta]$ oor R .

Voorbeelde: Beskou die direkte som $R = Z_6 = R_1 \oplus R_2$ waar $R_1 \cong Z_3$ en $R_2 \cong Z_2$. R_1 het die elemente 0, 2, 4 en R_2 het die elemente 0, 3.

1. Laat die definiërende ideaal I van α voortgebring word deur $1 \cdot x^2 + 1 \cdot x + 5$ en die definiërende ideaal van β deur $1 \cdot x^4 + 1 \cdot x^2 + 5$ in $Z_6[x]$. Splits $f(x) := 1 \cdot x^2 + 1 \cdot x + 5$ in $f_1(x) := 4 \cdot x^2 + 4 \cdot x + 2 \in R_1[x]$ en $f_2(x) := 3 \cdot x^2 + 3 \cdot x + 3 \in R_2[x]$. Vir $g(x) := 1 \cdot x^3 + 1 \cdot x^2 + 5$ kry ons $g_1(x) := 4 \cdot x^3 + 4 \cdot x^2 + 2 \in R_1[x]$ en $g_2(x) := 3 \cdot x^3 + 3 \cdot x^2 + 3 \in R_2[x]$. Die veelterme $f_1(x)$ en $g_1(x)$ is onherleibaar in $R_1[x]$ terwyl $f_2(x)$ en $g_2(x)$ onherleibaar is in $R_2[x]$. $g(x)$ definieer β .

Pas ons stelling 4 toe op $R_1 \oplus R_2 = Z_6$, volg uit Van der Waerden (1950) §40 dat $R_1[\alpha_1, \beta_1]$ en $R_2[\alpha_2, \beta_2]$ primitiewe elemente γ_1 en γ_2 respektiewelik het. Dus is $\gamma := \gamma_1 + \gamma_2$ 'n primitiewe element van $Z_6[\alpha, \beta]$ oor Z_6 .

2. Neem die definiërende ideaal van α in $Z_6[x]$ weer as $I = (1 \cdot x^2 + 1 \cdot x + 5)$, maar die definiërende ideaal van β as $J = (3 \cdot x^2 + 3 \cdot x + 3) \subseteq Z_6[x]$. Die veelterm $3x^2 + 3x + 3$ is onherleibaar in $R_2[x]$.

Die element $\alpha_1 = e_1 \alpha (= 3\alpha)$ is algebraïes oor R_1 , maar $\beta = e_1 \beta$ is transcendent oor R_1 aangesien $J \subseteq R_2[x]$. Terwyl daar 'n primitiewe element vir $R_2[\alpha_2, \beta_2]$ oor R_2 bestaan in hierdie geval, is daar nie so 'n element vir $R_1[\alpha_1, \beta_1]$ oor R_1 nie. Die rede hiervoor is dat $R_1[\alpha_1, \beta_1]$ 'n transendente uitbreiding van die liggaam $R_1[\alpha_1]$ is en as daar 'n algebraïese primitiewe element vir $R_1[\alpha_1, \beta_1]$ oor R_1 sou bestaan dan sou alle elemente van $R_1[\alpha_1, \beta_1]$ algebraïes oor R_1 wees,¹⁶ terwyl as die primitiewe element transcendent is, dan sal alle elemente van $R_1[\alpha_1, \beta_1]$, nie in R_1 nie, transcendent wees oor R_1 .¹⁷

Literatuurverwysings

- Schutte, H.J. (1988). Transcendental and Algebraic Extensions of commutative Rings, *Quaestiones Mathematicae*, Vol. II(1), 73-89.
- Schutte, H.J. (1988). Transcendental and Algebraic Extensions of commutative Rings, *Quaestiones Mathematicae*, Vol. II(1), 73-89, proposisie 6.
- Schutte, H.J. (1988). Transcendental and Algebraic Extensions of commutative Rings, *Quaestiones Mathematicae*, Vol. II(1), 73-89, §2.
- Schutte, H.J. (1988). Transcendental and Algebraic Extensions of commutative Rings, *Quaestiones Mathematicae*, Vol. II(1), 73-89, proposisie 8.
- Schutte, H.J. (1988). Transcendental and Algebraic Extensions of commutative Rings, *Quaestiones Mathematicae*, Vol. II(1), 73-89, bewys van proposisie 8.
- Van der Waerden, B.L. (1950). *Modern Algebra*, Vol. I (Frederick Ungar Publishing Co. N.Y.) §40.
- Van der Waerden, B.L. (1950). *Modern Algebra*, Vol. I (Frederick Ungar Publishing Co. N.Y.) §37.
- Hardy, G.H. & Wright, E.M. (1945). *An introduction to the Theory of Numbers* (Clarendon Press, Oxford), §14.6.
- Van der Waerden, B.L. (1950). *Modern Algebra*, Vol. I (Frederick Ungar Publishing Co. N.Y.) §23.
- Hardy, G.H. & Wright, E.M. (1945). *An Introduction to the Theory of Numbers* (Clarendon Press, Oxford), §15.8.
- Hardy, G.H. & Wright, E.M. (1945). *An Introduction to the Theory of Numbers* (Clarendon Press, Oxford), §15.8.
- Schutte, H.J. (1988). Transcendental and Algebraic Extensions of Commutative Rings, *Quaestiones Mathematicae*, Vol. II(1), 73-89, §3.
- Schutte, H.J. (1988). Transcendental and Algebraic Extensions of Commutative Rings, *Quaestiones Mathematicae*, Vol. II(1), 73-89, lemma 2.
- Schutte, H.J. (1988). Transcendental and Algebraic Extensions of Commutative Rings, *Quaestiones Mathematicae*, Vol. II(1), 73-89, lemma 1.
- Schutte, H.J. (1988). Transcendental and Algebraic Extensions of Commutative Rings, *Quaestiones Mathematicae*, Vol. II(1), 73-89, proposisie 8.
- Schutte, H.J. (1988). Transcendental and Algebraic Extensions of Commutative Rings, *Quaestiones Mathematicae*, Vol. II(1), 73-89, proposisie 6.
- Van der Waerden, B.L. (1950). *Modern Algebra*, Vol. I (Frederick Ungar Publishing Co. N.Y.) Raadpleeg Luroth se stelling, §63.