

IDEMPOTENTE VOORTBRINGERS VAN MATRIKSALGEBRAS



IDEMPOTENTE VOORTBRINGERS VAN MATRIKSALGEBRAS

MAGDALEEN SUZANNE MARAIS

Tesis ingelewer ter gedeeltelike voldoening aan die graad van Magister in die Natuurwetenskappe aan die Universiteit Stellenbosch.



Promotor: Prof. L. van Wyk

Augustus 2007

VERKLARING

Ek, die ondergetekende, verklaar hiermee dat die werk in hierdie tesis vervat, my eie oorspronklike werk is en dat ek dit nie vantevore in die geheel of gedeeltelik by enige universiteit ter verkryging van 'n graad voorgelê het nie.

Handtekening: _____ Datum: _____

OPSOMMING

'n Uiteensetting word gegee van [12], 'n artikel deur N. Krupnik, wat 'n bespreking is van die minimum aantal idempotente voortbringers van 'n volledige matriksalgebra $M_n(F)$ oor 'n liggaam F , asook van direkte somme van volledige matriksalgebras oor F . Daar sal byvoorbeeld bewys word dat, indien $n \geq 2$, dan is die minimum aantal idempotente voortbringers van 'n volledige $n \times n$ matriksalgebra oor 'n liggaam gelyk aan 2 of 3. Krupnik het 'n foutiewe stelling in ([12], Stelling 5) gemaak, naamlik dat die minimum aantal idempotente voortbringers van m kopieë van 'n oneindige liggaam F , as 'n algebra oor F , $m - 1$ is. Hierdie fout is deur A.V. Kelarev, A.B. van der Merwe en L. van Wyk in [11] geïdentifiseer en reggestel. Die tesis sluit ook 'n uiteensetting van hierdie regstelling in. Verder word 'n uiteensetting gegee van die hoofresultaat in [5], waarin E. Formanek aantoon dat, indien $n \geq 2$, dan is daar 'n nie-nulwordende sentrale polinoom vir $M_n(F)$, met F enige liggaam. Laasgenoemde resultaat word gebruik in die uiteensetting van [12].

ABSTRACT

An exposition is given of [12], a paper by N. Krupnik, which is a discussion of the minimum number of idempotent generators of a complete matrix algebra $M_n(F)$ over a field F , as well as direct sums of complete matrix algebras over F . It will, for example, be proved that, if $n \geq 2$, then the minimum number of idempotent generators of a $n \times n$ matrix algebra is equal to 2 or 3. Krupnik made an incorrect statement in ([12], Theorem 5), namely that the minimum number of idempotent generators of m copies of an infinite field F , as an algebra over F , is $m - 1$. This error was identified and corrected by A.V. Kelarev, A.B. van der Merwe and L. van Wyk in [11]. The thesis also includes an exposition of this correction. Furthermore an exposition will be given of the main result of [5], where E. Formanek showed that, if $n \geq 2$, then there is a non-vanishing central polynomial for $M_n(F)$, with F any field. The last mentioned result will be used in the exposition of [12].

My opregte dank en waardering aan prof. L. van Wyk. Sy kennis, toewyding en leiding
het vir my insig en sekuriteit gegee en my deurlopend gemotiveer.

Inhoudsopgawe

Inleiding	1
1. Die minimum aantal idempotente voortbringers van volledige matriksalgebras oor 'n liggaam	10
2. Die minimum aantal idempotente voortbringers van direkte somme van volledige matriksalgebras oor 'n liggaam	28
3. Sentrale Polinome	62
Verwysings	81
Lys van Simbole	83
Indeks	84

Inleiding

Die tesis is 'n uiteensetting van [12], wat 'n bespreking van die bepaling van die minimum aantal idempotente voortbringers van volledige matriksalgebras oor 'n willekeurige liggaam F , asook van direkte somme van volledige matriksalgebras oor F , is.

Dit is belangrik om op te let dat 'n algebra skalaar vermenigvuldiging, sowel as ring vermenigvuldiging, het, aangesien dit wil voorkom asof Krupnik die ring vermenigvuldiging vir 'n oomblik agterweë gelaat het toe hy die foutiewe stelling in ([12], Stelling 5) gemaak het dat die minimum aantal idempotente voortbringers van die direkte som F^m , waar F^m m kopieë van die F -algebra $M_1(F) \cong F$ voorstel, met F 'n oneindige liggaam, $m - 1$ is. Hierdie fout is in [11] geïdentifiseer en reggestel. Ons sal hierdie fout, sowel as die regstelling, in Hoofstuk 2 bespreek.

Die hoofresultaat in Hoofstuk 1 is Stelling 1.1 wat handel oor die bepaling van die minimum aantal idempotente voortbringers van 'n volledige matriksalgebra oor 'n willekeurige liggaam F in Stelling 1 in [12].

In Hoofstuk 2 poog ons om Stelling 1.1 na direkte somme van matriksalgebras uit te brei. Ons sal daarin slaag om deur middel van Stelling 2.1, Stelling 2.2, Stelling 2.3 en Stelling 2.4 die minimum aantal idempotente voortbringers van enige direkte som van volledige matriksalgebras oor 'n willekeurige liggaam F te bepaal, behalwe die direkte somme waarin 'n direkte som $M_2^m(F)$, met $m \geq 2$ en $|F| \leq m + 1$, voorkom, of direkte somme waarin 'n direkte som $M_n^m(F)$, met $m \geq 2$, $n \geq 3$ en $|F| \leq m$, voorkom. Verder sal ons deur middel van Stelling 2.1, Gevolg 2.19, Gevolg 2.13 en Gevolg 2.17 'n ondergrens en 'n bogrens vir die minimum aantal idempotente voortbringers van direkte somme waarin 'n direkte som $M_2^m(F)$, met $m \geq 2$ en $|F| \leq m + 1$, voorkom, en direkte somme waarin 'n direkte som $M_n^m(F)$, met $m \geq 2$, $n \geq 3$ en $|F| \leq m$, voorkom, bepaal. Alhoewel die ondergrens oor die algemeen nie direkte relevansie het nie, sal dit uit die ondergrens blyk dat die minimum aantal idempotente voortbringers in bostaande gevalle van n , $|F|$, asook m , afhanklik is. Aan die einde van die Hoofstuk pas ons die resultate van Hoofstukke 1 en 2 op eindig dimensionele semi-eenvoudige algebras oor 'n algebraïes geslote liggaam F toe.

Hoofstuk 3 is 'n uiteensetting van die hoogs nie-triviale bewys van die resultaat van E. Formanek in [5] waarin daar vir elke $n \geq 2$ 'n nie-nulwordende sentrale polinoom vir $M_n(F)$ gekonstrueer word. Hierdie stelling word in Hoofstuk 2 benodig.

Met die term ring bedoel ons deurgaans 'n (nie noodwendig kommutatiewe) ring met identiteit. Laat $n \in \mathbb{N}$. Ons sal die identiteitsmatriks van 'n $n \times n$ matriksalgebra met I_n en die matrikseenhede met e_{mk} ($m, k = 1, 2, \dots, n$) aandui, waar $e_{mk} = (a_{jl})_{j,l=1}^n$, met $a_{mk} = 1$ en $a_{jl} = 0$ vir die oorblywende pare van indekse. Dit wil sê e_{mk} is die matriks met 'n 1 in posisie mk en 0'e andersins. Ons dui die graad van 'n nie-nul polinoom h as $\deg h$ en die polinoomring van polinome in 'n onbekende x oor 'n liggaam F as $F[x]$ aan. Verder sal ons die dimensie van 'n vektorruimte V as $\dim V$ aandui.

Ons aanvaar dat die volgende welbekende definisies en resultate wat ons deurgaans in die tesis gebruik, reeds aan die leser bekend is. Daarom formuleer ons slegs die resultate sonder bewys.

Ons definieer eerstens die begrip algebra, asook 'n paar verwante begrippe.

Definisie 0.1 ([9], Hoofstuk 4, Def 7.1) Laat F 'n liggaam wees. 'n F -algebra \mathbb{A} (of algebra \mathbb{A} oor F) is 'n ring \mathbb{A} sodat:

1. $(\mathbb{A}, +)$ 'n unitêre (linker) F -module is;
2. $k(ab) = (ka)b = a(kb)$ vir alle $k \in F$ en $a, b \in \mathbb{A}$.

'n F -algebra \mathbb{A} , wat as 'n ring 'n delingsring is, word 'n delingsalgebra genoem.

Dit is belangrik om op te let dat uit die groepstruktuur van die ring \mathbb{A} en uit voorwaarde 1 in bostaande definisie volg dat \mathbb{A} 'n vektorruimte oor F is. 'n Algebra \mathbb{A} wat eindig dimensioneel as 'n vektorruimte oor F is, word 'n eindig dimensionele algebra oor F genoem.

Die ring $M_n(F)$ van $n \times n$ matrikse oor 'n liggaam F is 'n voorbeeld van 'n F -algebra. In die tesis gaan ons hierdie algebra van nader beskou.

Definisie 0.2 ([9], Hoofstuk 4, Def 7.3) Laat F 'n liggaam, en \mathbb{A} en \mathbb{B} F -algebras wees.

1. 'n Subalgebra van \mathbb{A} is 'n subring van \mathbb{A} wat ook 'n F -submodule van \mathbb{A} is.
2. 'n (Linker, Regter, Twee-sydige) algebra-ideaal van \mathbb{A} is 'n (linker, regter, twee-sydige) ideaal van die ring \mathbb{A} wat ook 'n F -submodule van \mathbb{A} is.

3. 'n Homomorfisme (onderskeidelik isomorfisme) $f : \mathbb{A} \rightarrow \mathbb{B}$ van F -algebras is 'n ring homomorfisme (onderskeidelik isomorfisme) wat ook 'n F -module homomorfisme (onderskeidelik isomorfisme) is.

Opmerking Gestel J is 'n linker (onderskeidelik regter) ideaal van die ring \mathbb{A} . Om te bewys dat J 'n linker (onderskeidelik regter) ideaal van die algebra \mathbb{A} is, moet ons slegs bewys dat $kJ \subseteq J$ vir elke $k \in F$. Gestel nou $1_{\mathbb{A}}$ is die identiteit van \mathbb{A} en $a \in \mathbb{A}$. Dan volg dat

$$ka = k(1_{\mathbb{A}}a) = (k1_{\mathbb{A}})a \quad \text{en} \quad ka = (ka)1_{\mathbb{A}} = a(k1_{\mathbb{A}}),$$

wat impliseer dat

$$kJ = (k1_{\mathbb{A}})J \subseteq J \quad (\text{onderskeidelik } kJ = J(k1_{\mathbb{A}}) \subseteq J).$$

Dus is J 'n linker (onderskeidelik regter) ideaal van die algebra \mathbb{A} . Aangesien 'n linker (onderskeidelik regter) ideaal van die algebra \mathbb{A} volgens definisie 'n linker (onderskeidelik regter) ideaal van die ring \mathbb{A} is, volg dat J 'n (linker, regter, twee-sydige) ideaal van die ring \mathbb{A} is as en slegs as J 'n (linker, regter, twee-sydige) ideaal van die algebra \mathbb{A} is.

Definisie 0.3 ([9], bladsy 426; Hoofstuk 9, Def 2.9 en bladsy 451) Laat \mathbb{A} 'n F -algebra (onderskeidelik ring) wees. Die Jacobson-radikaal van die algebra (onderskeidelik ring) \mathbb{A} is die deursnede van al die maksimale linker algebra- (onderskeidelik ring-) ideale. Ons sê die algebra (onderskeidelik ring) \mathbb{A} is semi-eenvoudig as die Jacobson-radikaal van die algebra (onderskeidelik ring) \mathbb{A} nul is.

Volgens die opmerking na Definisie 0.2 volg dat al die ideale van die algebra \mathbb{A} en die ring \mathbb{A} dieselfde is. Dus is die Jacobson-radikaal van die algebra \mathbb{A} en die ring \mathbb{A} dieselfde. In besonder is die algebra \mathbb{A} semi-eenvoudig as en slegs as die ring \mathbb{A} semi-eenvoudig is.

Definisie 0.4 ([9], bladsy 451) 'n (Linker, Regter) Artinse- (onderskeidelik Noetherse-) algebra is 'n F -algebra wat die afnemende (onderskeidelik toenemende) ketting voorwaardes op (linker, regter) algebra-ideale bevredig.

Die volgende twee definisies en resultaat handel oor spesifieke elemente met 'n besondere eienskap in 'n algebra.

Definisie 0.5 ([9], Hoofstuk 3, Oefening nr. 23 en bladsy 451) 'n Element a van 'n algebra \mathbb{A} is 'n idempotent as $a^2 = a$.

In hierdie tesis sal ons idempotente van die matriksalgebras $M_n(F)$ beskou.

Definisie 0.6 ([9], bladsy 122) Die versameling elemente van 'n algebra \mathbb{A} wat met al die elemente in \mathbb{A} kommuteer word die sentrum van \mathbb{A} genoem. Ons dui die sentrum van \mathbb{A} met $Z(\mathbb{A})$ aan. Met ander woorde,

$$Z(\mathbb{A}) := \{x \in \mathbb{A} \mid xa = ax, \text{ vir alle } a \in \mathbb{A}\}.$$

Proposisie 0.7 Die sentrum van 'n algebra \mathbb{A} is 'n subalgebra van \mathbb{A} .

Die volgende definisies en resultate dien as 'n oorsig van permutasiegroepe en spesifiek die groep S_n van alle permutasies van n letters.

Definisie 0.8 ([9], bladsy 46) Laat S 'n nie-leë versameling wees. 'n Bijeksie van $S \rightarrow S$ word 'n permutasie van S genoem. Laat $A(S)$ die versameling van alle permutasies van S wees. Onder die operasie van samestelling van funksies, $f \circ g$, is $A(S)$ 'n groep, genoem die groep van permutasies van S . As $S = \{1, 2, \dots, n\}$, dan word $A(S)$ die simmetriese groep van n letters genoem en aangedui as S_n .

Aangesien 'n element σ van S_n 'n bijeksie van die eindige versameling $S = \{1, 2, \dots, n\}$ na homself is, kan ons σ voorstel deur die lys van elemente van S_n langs mekaar te skryf en die beeld van elke element onder σ direk daaronder te skryf. Gestel byvoorbeeld $\sigma(i) = s_i$. Dan kan ons σ as

$$\begin{pmatrix} 1 & 2 & \dots & n \\ s_1 & s_2 & \dots & s_n \end{pmatrix}$$

voorstel.

Definisie 0.9 ([9], Hoofstuk 1, Def 6.1) Laat s_1, s_2, \dots, s_r ($r \leq n$) verskillende elemente van $S = \{1, 2, \dots, n\}$ wees. 'n Permutasie wat $s_1 \mapsto s_2, s_2 \mapsto s_3, \dots, s_{r-1} \mapsto s_r, s_r \mapsto s_1$ en elke ander element van S_n op homself afbeeld, word 'n r -siklus of 'n siklus van lengte r genoem en voorgestel as (s_1, s_2, \dots, s_r) . 'n 2-Siklus word 'n transposisie genoem.

Stelling 0.10 ([9], Hoofstuk 1, Gevolg 6.5) Elke permutasie in S_n kan geskryf word as 'n produk van (nie noodwendig disjunkte) transposisies.

Definisie 0.11 ([9], Hoofstuk 1, Def 6.6) 'n Permutasie $\sigma \in S_n$ word ewe (onderskeidelik onewe) genoem as σ geskryf kan word as 'n produk van 'n ewe (onderskeidelik onewe) getal transposisies.

Indien

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ s_1 & s_2 & \dots & s_n \end{pmatrix}$$

kan ons die aantal transposisies wat ons benodig om σ as 'n produk van transposisies te skryf as volg tel:

1. vind die getal heelgetalle in die geordende lys s_1, \dots, s_n wat kleiner is as s_1 en s_1 volg;
2. vind nou soortgelyk die getal heelgetalle wat kleiner as s_2 is en s_2 volg;
3. gaan voort met die telproses vir s_3, \dots, s_{n-1} .

Gestel die som van die getalle wat in (1),(2) en (3) bepaal is, is m . Dan kan σ as m transposisies voorgestel word.

Stelling 0.12 ([9], Hoofstuk 1, Stelling 6.7) 'n Permutasie in S_n ($n \geq 2$) kan nie beide ewe en onewe wees nie.

Definisie 0.13 ([9], bladsy 48) Die teken van 'n permutasie $\sigma \in S_n$, aangedui as $\text{sgn}(\sigma)$, is -1 as σ onewe is en 1 as σ ewe is.

Vervolgens definieer ons die begrip permutasiematriks. Aangesien die rye, of kolomme, van so 'n matriks slegs 'n permutasie van die rye en kolomme van die identiteitsmatriks is, is die bostaande definisies en resultate in verband met permutasies op hierdie matrikse van toepassing.

Definisie 0.14 ([4], bladsy 88) 'n Vierkantige matriks waarvan die elemente in enige ry, of enige kolom, almal nul is, behalwe vir een element wat gelyk is aan 1 word 'n permutasiematriks genoem.

Opmerking Let op dat ons 'n permutasie matriks as $\sum_{i=1}^n e_{\sigma(i),i}$ kan voorstel, waar $\sigma \in S_n$ die permutasie van die ryvektore is. Indien $\sigma(i) = k$, met ander woorde die i de ry van I_n is die k de ry van P , sal die i de ry van 'n willekeurige matriks, sê A , na die k de ry verskuif deur A van links met P te vermenigvuldig. Deur A van regs met P te vermenigvuldig sal die k de kolom na die i de kolom verskuif. Ons sal in Hoofstuk 1 die vermenigvuldiging met 'n spesifieke permutasie matriks algebraïes beskou.

Die volgende stelling handel oor polinome oor 'n liggaam F , met ander woorde elemente van die ring $F[x]$.

Stelling 0.15 (*DIE DELINGSALGORITME VIR POLINOME*) ([3], bladsy 76, nr. 99)
 As f en g polinome oor 'n liggaam F is en $g \neq 0$, dan bestaan daar unieke polinome q en r oor F sodat $f = qg + r$ en $r = 0$ of $\deg r < \deg g$.

Ons definieer volgende die begrip uitbreidingsliggaam en beskou daarna verskillende tipe uitbreidingsliggame, asook definisies en resultate wat daarvoor handel.

Definisie 0.16 ([3], bladsy 73, nr. 96) 'n Liggaam E word 'n uitbreidingsliggaam van 'n liggaam F genoem, en aangedui as E/F , as F 'n subliggaam van E is.

Let op dat E 'n vektorruimte oor F is, aangedui as E/F . Indien hierdie vektorruimte eindig dimensioneel is, dui ons die dimensie met $[E : F]$ aan en sê ons E is 'n eindig dimensionele uitbreiding van F . Andersins sê ons E is 'n oneindig dimensionele uitbreiding van F .

Laat F 'n liggaam en $f \in F[x]$ 'n polinoom van positiewe graad wees. Dan ontbind f oor F (of f ontbind in $F[x]$) as f geskryf kan word as 'n produk van lineêre faktore in $F[x]$; dit wil sê, $f = u_0(x - u_1)(x - u_2) \cdots (x - u_n)$, met $u_i \in F$.

Vervolgens definieer ons die begrip vervalliggaam.

Definisie 0.17 ([9], Hoofstuk 5, Def 3.1) Laat F 'n liggaam en $f \in F[x]$ 'n polinoom van positiewe graad wees. 'n Uitbreidingsliggaam E van F word 'n vervalliggaam oor F van die polinoom f genoem as f in $E[x]$ ontbind, en E die kleinste liggaam is wat F en al die wortels van f bevat. Laat S 'n versameling van polinome van positiewe graad in $F[x]$

wees. 'n Uitbreidingsliggaam E van F word 'n vervalliggaam oor F van die versameling S genoem as elke polinoom in S in $E[x]$ ontbind en E voortgebring word deur F en die wortels van al die polinome in S .

Ons beskou volgende die definisie van 'n algebraïese uitbreidingsliggaam.

Definisie 0.18 ([9], Hoofstuk 5, Def 1.4) Laat E 'n uitbreidingsliggaam van F wees. 'n Element u van E is algebraïes oor F as u 'n wortel van 'n nie-nul polinoom $f \in F[x]$ is. As u nie 'n wortel van enige nie-nul polinoom $f \in F[x]$ is nie, dan word u transendent oor F genoem. E word 'n algebraïese uitbreiding van F genoem as elke element van E algebraïes oor F is. E word 'n transendente uitbreiding genoem as daar ten minste een element in E is wat transendent oor F is.

Opmerking Indien E 'n eindig dimensionele uitbreiding van F is, sê $[E : F] = n$, volg vir enige $u \in E$ dat $1, u, u^2, \dots, u^n$ lineêr afhanklik is. Dit beteken daar bestaan $k_1, k_2, \dots, k_n, k_{n+1} \in F$, nie almal nul nie, sodat $k_1 + k_2u + k_3u^2 + \dots + k_{n+1}u^n = 0$. Maar dit impliseer dat daar 'n nie-nul polinoom $f(x) = k_1 + k_2x + k_3x^2 + \dots + k_{n+1}x^n \in F[x]$ bestaan sodat $f(u) = 0$, met ander woorde dat E 'n algebraïese uitbreiding van F is.

Soortgelyk aan bostaande definisie sê ons 'n element a van 'n algebra \mathbb{A} oor 'n liggaam F is algebraïes oor F as dit 'n wortel van 'n polinoom in $F[x]$ is. Ons sê ook soortgelyk dat \mathbb{A} algebraïes is oor F as elke element van \mathbb{A} algebraïes is oor F . Ons kan ook soortgelyk bewys dat 'n eindig dimensionele algebra oor 'n liggaam F algebraïes is oor F .

Ons gaan van die volgende ekwivalente stellings gebruik maak om 'n algebraïes geslote liggaam te definieer.

Stelling 0.19 ([9], Hoofstuk 5, Stelling 3.3) Die volgende voorwaardes op 'n liggaam E is ekwivalent.

1. Elke nie konstante polinoom $f \in E[x]$ het 'n wortel in E ;
2. elke nie konstante polinoom $f \in E[x]$ ontbind oor E ;
3. elke onherleibare polinoom in $E[x]$ het graad een;
4. daar is geen algebraïese uitbreidingsliggaam van E nie, behalwe E self;

5. daar bestaan 'n subliggaam F van E sodat E algebraïes oor F is en elke polinoom in $F[x]$ ontbind in $E[x]$.

Definisie 0.20 ([9], bladsy 258) 'n Liggaam wat die ekwivalente voorwaardes in Stelling 0.19 bevredig word algebraïes geslote genoem.

Opmerking Indien $F = \{a_0, a_1, \dots, a_n\}$ 'n willekeurige eindige liggaam is, waar $a_1 \neq 0$, dan volg dat die polinoom $f(x) = a_1 + (x - a_0) \cdots (x - a_n)$ nie 'n wortel in F het nie. Dus kan 'n eindige liggaam nie algebraïes geslote wees nie.

Ons maak van die volgende stelling gebruik om die begrip algebraïese afsluiting van 'n liggaam F te definieer.

Stelling 0.21 ([9], Hoofstuk 5, Stelling 3.4) As E 'n uitbreidingsliggaam van F is, dan is die volgende voorwaardes ekwivalent.

1. E is algebraïes oor F en E is algebraïes geslote;
2. E is 'n vervalliggaam oor F van die versameling van alle (onherleibare) polinome in $F[x]$.

Definisie 0.22 ([9], bladsy 259) As 'n uitbreidingsliggaam E van 'n liggaam F die ekwivalente kondisies in Stelling 0.21 bevredig, dan word E 'n algebraïese afsluiting van F genoem.

Stelling 0.23 ([9], Hoofstuk 5, Stelling 3.6) Elke liggaam het 'n algebraïese afsluiting.

Die volgende resultate handel oor eindige liggame

Die karakteristiek van 'n liggaam F is die kleinste positiewe heelgetal n sodat $na = \underbrace{a + \cdots + a}_{n \text{ keer}} = 0$ vir alle $a \in F$. Hierdie begrip word in die volgende stelling gebruik.

Stelling 0.24 ([9], Hoofstuk 5, Gevolg 5.2) 'n Eindige liggaam se karakteristiek is 'n priemgetal.

Stelling 0.25 ([1], bladsy 169) *Al die wortels van 'n onherleibare polinoom oor 'n eindige liggaam is verskillend.*

Stelling 0.26 ([3], bladsy 69, nr. 89β) *'n Liggaam F het karakteristiek p , waar p 'n priemgetal is, as en slegs as \mathbb{Z}_p in F ingebed kan word.*

Opmerking Laat F 'n eindige liggaam wees. Uit Stelling 0.24 en Stelling 0.26 volg dan dat daar 'n priemgetal p bestaan sodat \mathbb{Z}_p in F ingebed kan word.

Stelling 0.27 ([1], Stelling 4.5.8)

1. *Elke eindige liggaam het p^n elemente vir 'n priemgetal p en $n \in \mathbb{N}$. 'n Eindige liggaam met p^n elemente is isomorf aan $\frac{\mathbb{Z}_p[x]}{[f]}$, waar f 'n onherleibare polinoom van graad n in $\mathbb{Z}_p[x]$ is.*
2. *Vir elke priemgetal p en elke $n \in \mathbb{N}$ bestaan daar 'n eindige liggaam $\frac{\mathbb{Z}_p[x]}{[f]}$, waar f 'n onherleibare polinoom van graad n in $\mathbb{Z}_p[x]$ is.*

1 Die minimum aantal idempotente voortbringers van volledige matriksalgebras oor 'n liggaam

In hierdie hoofstuk ondersoek ons die minimum aantal idempotente wat nodig is om die F -algebra $M_n(F)$ van alle $n \times n$ matrikse oor 'n liggaam F as 'n algebra voort te bring. Ons tel nie die identiteitsmatriks I_n nie, aangesien I_n as 'n element van elke subring in die F -algebra $M_n(F)$ gesien word. Ons sal die antwoord in die volgende stelling vind.

Stelling 1.1 ([12], Stelling 1) *Laat F enige liggaam en $\nu = \nu(n, F)$ die kleinste getal wees sodat die algebra $M_n(F)$, met $n \geq 2$, deur ν idempotente voortgebring kan word. Dan volg dat*

$$\nu(n, F) = \begin{cases} 2 & \text{as } n = 2 \text{ en } F \neq \mathbb{Z}_2 \\ 3 & \text{andersins.} \end{cases}$$

Ons sal die stelling deur middel van vier lemmas bewys. Deur middel van Lemma 1.2 en Lemma 1.5 sal ons bewys dat

$$\nu(n, F) = 3 \quad \text{as } n \geq 3 \quad (\text{vir alle } F). \quad (1)$$

Deur middel van Lemma 1.2 en Lemma 1.8 sal ons bewys dat

$$\nu(2, \mathbb{Z}_2) = 3, \quad (2)$$

en deur middel van Lemma 1.9 dat

$$\nu(2, F) = 2 \quad \text{as } F \neq \mathbb{Z}_2. \quad (3)$$

Notasie Laat $n \in \mathbb{N}$, met $n \geq 2$. Ons sal deur p_n , q_n en r_n die volgende idempotente in $M_n(F)$ aandui:

Voordat ons Lemma 1.2 bewys, beskou ons eers die permutasiematriks

$$a_n := \begin{bmatrix} 0 & 1 & 0 & & \circ \\ & 0 & 1 & 0 & \\ \circ & & \ddots & \ddots & \ddots \\ & & & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 \end{bmatrix}. \quad (7)$$

Ons beskou eerstens die vermenigvuldiging van a_n met 'n willekeurige matriks $B = (b_{ij})$.

Laat K_i die i de kolom van B wees. Dan is

$$B = \begin{bmatrix} K_1 & \circ \end{bmatrix} + \begin{bmatrix} 0 & K_2 & \circ \end{bmatrix} + \dots + \begin{bmatrix} \circ & \overset{\text{kolom } i}{\downarrow} K_i & \circ \end{bmatrix} + \dots + \begin{bmatrix} \circ & K_n \end{bmatrix}.$$

Aangesien

$$\begin{aligned} \begin{bmatrix} \circ & \overset{\text{kolom } i}{\downarrow} K_i & \circ \end{bmatrix} a_n &= \begin{bmatrix} b_{1i} \\ b_{2i} \\ \vdots \\ \circ & \vdots & \circ \\ b_{ni} \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & & \circ \\ & 0 & 1 & 0 & \\ \circ & & \ddots & \ddots & \ddots \\ & & & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 \end{bmatrix} \\ &= (b_{1i}e_{1i} + \dots + b_{ni}e_{ni})(e_{12} + e_{23} + \dots + e_{n-1,n} + e_{n1}) \\ &= \begin{cases} b_{1i}e_{1,i+1} + \dots + b_{ni}e_{n,i+1} & \text{as } 1 \leq i \leq n-1 \\ b_{n1}e_{11} + \dots + b_{nn}e_{n1} & \text{as } i = n \end{cases} \\ &= \begin{cases} \begin{bmatrix} \circ & \overset{\text{kolom } i+1}{\downarrow} K_i & \circ \end{bmatrix} & \text{as } 1 \leq i \leq n-1 \\ \begin{bmatrix} K_n & \circ \end{bmatrix} & \text{as } i = n, \end{cases} \end{aligned}$$

volg dat

$$\begin{aligned} Ba_n &= \begin{bmatrix} K_1 & \circ \end{bmatrix} a_n + \dots + \begin{bmatrix} \circ & K_n \end{bmatrix} a_n \\ &= \begin{bmatrix} 0 & K_1 & \circ \end{bmatrix} + \dots + \begin{bmatrix} \circ & K_{n-1} \end{bmatrix} + \begin{bmatrix} K_n & \circ \end{bmatrix} \\ &= \begin{bmatrix} K_n & K_1 & \dots & K_{n-1} \end{bmatrix} \\ &= \begin{bmatrix} b_{1n} & b_{11} & \dots & b_{1,n-1} \\ \vdots & \vdots & & \vdots \\ b_{nn} & b_{n1} & \dots & b_{n,n-1} \end{bmatrix}. \end{aligned} \quad (8)$$

Soortgelyk volg dat

$$a_n B = \begin{bmatrix} b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \\ b_{11} & b_{12} & \cdots & b_{1n} \end{bmatrix}. \quad (9)$$

Ons kan a_n dus as 'n operator op 'n $n \times n$ matriks B sien wat deur vermenigvuldiging van regs die inskrywings van die eerste $n - 1$ kolomme een kolom aanskuif en die inskrywings van die n 'de kolom na die eerste verskuif. Deur vermenigvuldiging van links skuif die inskrywings van die laaste $n - 1$ rye een ry op en die inskrywings van die eerste ry na die laaste ry.

In die besonder volg vir willekeurige $j, l \in \{1, \dots, n\}$ dat

$$a_n e_{jl} = \begin{cases} e_{j-1,l} & \text{as } j \geq 2 \\ e_{nl} & \text{as } j = 1 \end{cases} \quad (10)$$

en dat

$$e_{jl} a_n = \begin{cases} e_{j,l+1} & \text{as } l \leq n - 1 \\ e_{j1} & \text{as } l = n. \end{cases} \quad (11)$$

Let op dat

$$a_n^2 = \begin{array}{c} \text{kolom 3} \\ \downarrow \\ \begin{bmatrix} 0 & 1 & & \bigcirc \\ & \ddots & \ddots & \\ 0 & \cdots & 0 & 1 \\ 1 & 0 & & \\ 0 & 1 & 0 & \end{bmatrix} \leftarrow \text{ry } n-2 \end{array}$$

$$a_n^3 = \begin{array}{c} \text{kolom 4} \\ \downarrow \\ \begin{bmatrix} 0 & 1 & & \bigcirc \\ & \ddots & \ddots & \\ 0 & \cdots & 0 & 1 \\ 1 & 0 & & \\ & 1 & 0 & \\ \bigcirc & 1 & 0 & \end{bmatrix} \leftarrow \text{ry } n-3 \end{array}$$

$$\vdots \quad (12)$$

$$\begin{aligned}
a_n^{n-1} &= \begin{bmatrix} 0 & \cdots & 0 & 1 \\ 1 & 0 & & \\ & 1 & 0 & \\ & & \ddots & \ddots \\ \circ & & & 1 & 0 \\ & & & & 1 & 0 \end{bmatrix} \begin{array}{l} \leftarrow \text{ry } n - (n - 1) \\ \text{kolom } n \\ \downarrow \end{array} \\
a_n^n &= \begin{bmatrix} 1 & \circ \\ & \ddots \\ \circ & 1 \end{bmatrix} = I_n.
\end{aligned}$$

Ons kan vermenigvuldiging deur bostaande matrikse as onderskeidelik $2, 3, \dots, n - 1, n$ keer die toepassing van a_n beskou.

Uit (10) en (11) volg dat ons deur middel van a_n en 'n matrikseenhed enige ander matrikseenhed kan voortbring, waaruit volg dat ons deur middel van a_n en 'n matrikseenhed die hele $M_n(F)$ kan voortbring. Die bewys van die volgende lemma is op hierdie waarneming gebaseer.

Lemma 1.2 ([12], Lemma 1) *Vir elke $n \geq 2$ en elke liggaam F is die F -subalgebra van $M_n(F)$ voortgebring deur die drie idempotente p_n, q_n en r_n die hele $M_n(F)$.*

Bewys Ons bewys eerstens dat ons a_n en 'n matrikseenhed deur middel van p_n, q_n en r_n kan voortbring, sodat dit dan maklik volg, soos reeds opgemerk, dat ons die hele $M_n(F)$ deur middel van p_n, q_n en r_n kan voortbring. Eerstens,

$$\begin{aligned}
& r_n(2I_n - p_n - q_n) \\
&= \begin{bmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \\ 1 & \cdots & \cdots & 1 \end{bmatrix} \left(\begin{bmatrix} 2 & & & \circ \\ & 2 & & \\ & & 2 & \\ & & & \ddots \\ \circ & & & \ddots \end{bmatrix} - \begin{bmatrix} 1 & 1 & & \circ \\ & 0 & 0 & \\ & & 1 & 1 \\ \circ & & & \ddots \\ & & & & \ddots \end{bmatrix} \right) \\
& \quad - \begin{bmatrix} 0 & 0 & & \circ \\ & 1 & 1 & \\ & & 0 & 0 \\ & & & \ddots \\ \circ & & & \ddots \end{bmatrix} \tag{13}
\end{aligned}$$

$$\begin{aligned}
&= \begin{bmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \\ 1 & \cdots & \cdots & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 & & \circ \\ & 1 & -1 & \\ & & 1 & -1 \\ & & & \ddots & \ddots \\ \circ & & & & \ddots & \ddots \end{bmatrix} \\
&= \begin{bmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{bmatrix} = e_{n1}. \tag{14}
\end{aligned}$$

Verder is

$$\begin{aligned}
&p_n + q_n - I_n + e_{n1} \\
&= \begin{bmatrix} 1 & 1 & & & \\ & 1 & 1 & & \circ \\ \circ & & 1 & 1 & \\ & & & \ddots & \ddots \\ & & & & \ddots & \ddots \end{bmatrix} - \begin{bmatrix} 1 & & & & \\ & 1 & & & \circ \\ \circ & & 1 & & \\ & & & \ddots & \\ & & & & \ddots & \ddots \end{bmatrix} + \begin{bmatrix} 0 & \cdots & \cdots & 0 \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{bmatrix} \\
&= a_n. \tag{15}
\end{aligned}$$

Vervolgens kies ons willekeurige $k, m \in \{1, 2, \dots, n\}$. Deur e_{n1} nou $n - k$ keer van links en $m - 1$ keer van regs met a_n te vermenigvuldig, volg dat

$$\begin{aligned}
a_n^{n-k} e_{n1} a_n^{m-1} &= e_{k1} a_n^{m-1} \\
&= e_{km}.
\end{aligned}$$

Omdat ons elke element A van $M_n(F)$ kan uitdruk as

$$A = \sum_{k,m=1}^n s_{km} e_{km} \quad \text{waar } s_{km} \in F,$$

kan ons sodoende $M_n(F)$ as 'n F -algebra voortbring.

□

Notasie In die tesis gaan ons 'n $n \times n$ matriks met 1'e in die k 'de posisies bo die hoofdiagonaal en 0'e in die ander posisies as $D_n^{(k)}$ aandui, byvoorbeeld

$$D_n^{(1)} = \begin{bmatrix} 0 & 1 & & \circ \\ & 0 & 1 & \\ & & \ddots & \ddots \\ & & & 0 & 1 \\ \circ & & & & 0 \end{bmatrix} \quad \text{en} \quad D_n^{(2)} = \begin{bmatrix} 0 & 0 & 1 & & \circ \\ & 0 & 0 & 1 & \\ & & \ddots & \ddots & \ddots \\ & & & 0 & 0 & 1 \\ & & & & 0 & 0 \\ \circ & & & & & 0 \end{bmatrix}. \quad (16)$$

Let op dat

$$I_n = D_n^{(0)}$$

en

$$p_n + q_n - I_n = \begin{bmatrix} 0 & 1 & & \circ \\ & 0 & 1 & \\ & & \ddots & \ddots \\ & & & 0 & 1 \\ \circ & & & & 0 \end{bmatrix} = D_n^{(1)}. \quad (17)$$

Let ook op dat

$$(D_n^{(k)})^m = \begin{cases} D_n^{(km)} & \text{as } km \leq n-1 \\ 0 & \text{andersins.} \end{cases} \quad (18)$$

Verder is

$$\begin{aligned} D_n^{(1)}e_{jl} &= (e_{12} + e_{23} + \cdots + e_{n-1,n})e_{jl} \\ &= \begin{cases} e_{j-1,l} & \text{as } 2 \leq j \leq n \\ 0 & \text{as } j = 1 \end{cases} \end{aligned} \quad (19)$$

en

$$\begin{aligned} e_{jl}D_n^{(1)} &= e_{jl}(e_{12} + e_{23} + \cdots + e_{n-1,n}) \\ &= \begin{cases} e_{j,l+1} & \text{as } l \leq n-1 \\ 0 & \text{as } l = n. \end{cases} \end{aligned} \quad (20)$$

vir willekeurige $j, l \in \{1, \dots, n\}$.

Aangesien

$$(p_n + q_n - I_n)^{n-1} = (D_n^{(1)})^{n-1} = D_n^{(n-1)} = e_{1n}$$

kan die matrikseenhed e_{mk} in die bewys van Lemma 1.2 ook as volg voortgebring word:

$$\begin{aligned} a_n^{n-m+1}(p_n + q_n - I_n)^{n-1}a_n^k &= a_n^{n-m+1}e_{1n}a_n^k \\ &= e_{mn}a_n^k \\ &= e_{mk}. \end{aligned} \tag{21}$$

Definisie 1.3 ([8], bladsy 154) *Ons definieer die standaard polinoomidentiteit van graad n as*

$$f(a_1, a_2, \dots, a_n) := \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{\sigma(1)} a_{\sigma(2)} \cdots a_{\sigma(n)} = 0, \tag{22}$$

waar S_n en sgn onderskeidelik in Definisie 0.8 en Definisie 0.13 gedefinieer is.

Ons benodig die volgende resultaat in Lemma 1.5.

Stelling 1.4 ([12], Stelling 8) *Enige algebra \mathbb{A} voortgebring deur twee idempotente bevredig die standaard polinoomidentiteit:*

$$f(a_1, a_2, a_3, a_4) = \sum_{\sigma \in S_4} \text{sgn}(\sigma) a_{\sigma(1)} a_{\sigma(2)} a_{\sigma(3)} a_{\sigma(4)} = 0$$

van graad 4.

Bewys Gestel \mathbb{A} word voortgebring deur die idempotente p en q , en laat e die identiteit van \mathbb{A} wees. Verder, laat $t = (p - q)^2 = p^2 - pq - qp + q^2 = p - pq - qp + q$. Dan volg dat

$$\begin{aligned} pt &= p(p - q)^2 & tp &= (p - q)^2 p \\ &= p - pq - pqp + pq & \text{en} & & &= p - pqp - qp + qp \\ &= p - pqp & & & &= p - pqp. \end{aligned}$$

Dus is $tp = pt$. Soortgelyk is $tq = qt$, sodat t in die sentrum van \mathbb{A} is. Nou,

$$\mathbb{A} = \{lp + mq + ke + \sum_i s_i (\text{'n eindige produk van die } p\text{'s en } q\text{'s}) \mid l, m, k, s_i \in F\}.$$

Maar

$$p + q - pq - t = p + q - pq - p + pq + qp - q = qp, \quad (23)$$

$$\begin{aligned} (1-t)p &= (1-p+pq+qp-q)p \\ &= p - p + pqp + qp - qp \\ &= pqp, \end{aligned} \quad (24)$$

en soortgelyk is

$$(1-t)q = qpq. \quad (25)$$

Aangesien die produk van j p 's of j q 's maar net p of q onderskeidelik is, vereenvoudig 'n produk van p 's en q 's dus na een van die volgende vorms:

1. Indien die som van die $\#p$'s en $\#q$'s in die produk (waar $\#$ die aantal aandui) onewe is, verkry ons die volgende vorms:

$$pqp \cdots qp \quad \text{en} \quad qpq \cdots pq.$$

Uit (24) volg dan dat

$$\begin{aligned} \underbrace{pqp}_{=(1-t)p} \cdots qp &= (1-t) \underbrace{pqp \cdots qp}_{\#p's + \#q's = j-2} \\ &= (1-t)^2 \underbrace{pqp \cdots qp}_{\#p's + \#q's = j-4} \\ &\vdots \\ &= (1-t)^{\lfloor \frac{j-1}{2} \rfloor} p \\ &= (1-t)^{\lfloor \frac{j-1}{2} \rfloor} p. \end{aligned} \quad (26)$$

Soortgelyk volg uit (25) dat

$$qpq \cdots pq = (1-t)^{\lfloor \frac{j-1}{2} \rfloor} q = (1-t)^{\lfloor \frac{j-1}{2} \rfloor} q. \quad (27)$$

2. Indien die som van die $\#p$'s en $\#q$'s in die produk ewe is, verkry ons die volgende vorms:

$$pqp \cdots qpq \quad \text{en} \quad qpq \cdots pqp.$$

Dan volg uit (26) dat

$$\begin{aligned} pqpqp \cdots qpq &= \underbrace{pqpqp \cdots qp}_{\#p's + \#q's = j-1 \text{ onewe}} q \\ &= (1-t)^{\frac{(j-1)-1}{2}} pq \\ &= (1-t)^{\lfloor \frac{j-1}{2} \rfloor} pq. \end{aligned} \quad (28)$$

Verder is

$$\begin{aligned}
qpqp \cdots qp &= \underbrace{qpqpq \cdots \cdots pq}_{\#p's + \#q's = j-1 \text{ onewe}} p \\
&= (1-t)^{\frac{(j-1)-1}{2}} qp \quad (\text{volg uit (27)}) \\
&= (1-t)^{\lfloor \frac{j-1}{2} \rfloor} qp \\
&= (1-t)^{\lfloor \frac{j-1}{2} \rfloor} (p+q-pq-t) \quad (\text{volg uit (23)}) \\
&= (1-t)^{\lfloor \frac{j-1}{2} \rfloor} p + (1-t)^{\lfloor \frac{j-1}{2} \rfloor} q - (1-t)^{\lfloor \frac{j-1}{2} \rfloor} pq - (1-t)^{\lfloor \frac{j-1}{2} \rfloor} t \cdot e \quad (29)
\end{aligned}$$

Dus volg uit (26), (27), (28) en (29) dat elke $x \in \mathbb{A}$ uitgedruk kan word as

$$x = h_1(t)e + h_2(t)p + h_3(t)q + h_4(t)pq, \quad (30)$$

waar h_1, h_2, h_3 en h_4 polinome in t is. Aangesien t in die sentrum van \mathbb{A} is en die sentrum van \mathbb{A} 'n subalgebra van \mathbb{A} is (Proposisie 0.7), is elke $h_i(t)$ in die sentrum van \mathbb{A} . Indien ons kan bewys dat die standaard polinoomidentiteit van graad 4 vir die elemente e, p, q en pq geld, is ons dus klaar.

Sonder die verlies aan algemeenheid, laat $a_1 = e$. Kom ons beskou die produkte van a_1, a_2, a_3 en a_4 waar a_2, a_3 en a_4 in 'n willekeurige vaste volgorde voorkom. Vir enige so 'n produk kan a_1 moontlik in posisie 1 of 2, of a_1 kan moontlik in posisie 3 of 4 voorkom. Die produkte van die elemente in al vier hierdie volgordes is gelyk. Die teken van die permutasie van die indekse van die elemente in hierdie produkte verskil egter indien e in die eerste en tweede posisie is, en indien e in die derde en vierde posisie is. Sodoende kanselleer die som van die vier produkte uit sodat die standaard polinoomidentiteit nul is. Byvoorbeeld: aangesien

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (123) = (13)(12), \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234) = (14)(13)(12),$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (21)(12)(31)(13)(41)(14) \quad \text{en} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12)$$

volg dat

$$\text{sgn}(\sigma)a_2a_3a_1a_4 = +a_2a_3ea_4 = a_2a_3a_4, \quad \text{sgn}(\sigma)a_2a_3a_4a_1 = -a_2a_3a_4e = -a_2a_3a_4,$$

$$\text{sgn}(\sigma)a_1a_2a_3a_4 = +ea_2a_3a_4 = a_2a_3a_4 \quad \text{en} \quad \text{sgn}(\sigma)a_2a_1a_3a_4 = -a_2ea_3a_4 = -a_2a_3a_4$$

sodat

$$\text{sgn}(\sigma)a_2a_3a_1a_4 + \text{sgn}(\sigma)a_2a_3a_4a_1 + \text{sgn}(\sigma)a_1a_2a_3a_4 + \text{sgn}(\sigma)a_2a_1a_3a_4 = 0.$$

Hierdie argument geld vir al $3! = 6$ volgordes van a_2 , a_3 en a_4 . Dus geld

$$\sum_{\sigma \in S_4} \text{sgn}(\sigma) a_{\sigma(1)} a_{\sigma(2)} a_{\sigma(3)} a_{\sigma(4)} = 0$$

vir e , p , q en pq .

□

Lemma 1.5 ([12], Lemma 2) *As $n \geq 3$, kan die F -algebra $M_n(F)$ nie deur twee idempotente voortgebring word nie.*

Bewys Beskou die matrikseenhede e_{11} , e_{12} , e_{22} en e_{23} . Die enigste nie-nul produk van die eenhede is $e_{11}e_{12}e_{22}e_{23} = e_{13}$. Dus is

$$\sum_{\sigma \in S_4} \text{sgn}(\sigma) a_{\sigma(1)} a_{\sigma(2)} a_{\sigma(3)} a_{\sigma(4)} = e_{13},$$

waar $a_1 = e_{11}$, $a_2 = e_{12}$, $a_3 = e_{22}$ en $a_4 = e_{23}$. Sodoende volg dat $M_n(F)$ nie die standaard polinoomidentiteit van graad 4 bevredig nie. Die resultaat volg dus uit Stelling 1.4.

□

In Lemma 1.7 sal ons vind dat $M_2(F)$ die standaard polinoomidentiteit van graad 4, vir enige liggaam F , bevredig. Ons sou dus die vraag kon vra of die omgekeerde van Stelling 1.4 geld en ons sodoende die gevolgtrekking kan maak dat $M_2(F)$ deur 2 idempotente voortgebring kan word. In die daaropvolgende lemma (Lemma 1.8) sal ons egter 'n voorbeeld van 'n liggaam F sien waarvoor $M_2(F)$ nie deur 2 idempotente voortgebring word nie. Die omgekeerde van Stelling 1.4 geld dus nie.

Aangesien $2n > 4$ indien $n \geq 3$, kon ons Lemma 1.5 ook deur middel van Stelling 1.4 en die volgende resultaat bewys het.

Lemma 1.6 ([8], Lemma 6.3.1) *$M_n(F)$ bevredig nie 'n polinoomidentiteit van graad kleiner as $2n$ nie.*

Die rede waarom ons die standaard polinoomidentiteit van graad 4 in Stelling 1.4 en Lemma 1.5 gebruik, en nie van graad 3 nie, is omdat $f(e_{11}, e_{12}, e_{22}) = e_{12} \neq 0$ en $M_2(F)$,

met $F \neq \mathbb{Z}_2$, deur 2 idempotente, soos ons in Lemma 1.9 sal sien, voortgebring kan word. Die kleinste graad l sodat 'n algebra voortgebring deur 2 elemente die standaard polinoomidentiteit van graad l bevredig, is dus 4.

Uit Lemma 1.2 en Lemma 1.5 volg dat

$$\nu(n, F) = 3 \quad \text{as} \quad n \geq 3.$$

Ons het dus (1) bewys.

Lemma 1.7 *Die F -algebra $M_2(F)$, vir enige liggaam F , bevredig die standaard polinoomidentiteit van graad 4.*

Bewys Aangesien e_{11} , e_{12} , e_{22} en e_{21} 'n basis vir $M_2(F)$ (gesien as 'n vektorruimte) is, kan enige $x \in M_2(F)$ in die vorm

$$x = me_{11} + le_{12} + se_{22} + ve_{21}$$

geskryf word, waar $m, l, s, v \in F$. Aangesien F in die sentrum van $M_2(F)$ lê, is dit slegs nodig om te bewys dat $M_2(F)$ die standaard polinoomidentiteit $f(a_1, a_2, a_3, a_4)$ vir $a_1 = e_{11}$, $a_2 = e_{12}$, $a_3 = e_{22}$ en $a_4 = e_{21}$ bevredig.

Die enigste nie-nul produkte van hierdie elemente is

$$\begin{aligned} a_1 a_2 a_3 a_4 &= e_{11} e_{12} e_{22} e_{21} = e_{11} & , & \quad a_2 a_1 a_4 a_3 = e_{21} e_{11} e_{12} e_{22} = e_{22} \\ a_3 a_4 a_1 a_2 &= e_{22} e_{21} e_{11} e_{12} = e_{22} & \text{en} & \quad a_2 a_3 a_4 a_1 = e_{12} e_{22} e_{21} e_{11} = e_{11}. \end{aligned}$$

Aangesien

$$\text{sgn}(1234) = +, \quad \text{sgn}(2143) = -, \quad \text{sgn}(3412) = + \quad \text{en} \quad \text{sgn}(2341) = -$$

volg dat

$$\sum_{\sigma \in S_4} \text{sgn}(\sigma) a_{\sigma(1)} a_{\sigma(2)} a_{\sigma(3)} a_{\sigma(4)} = e_{11} - e_{22} + e_{22} - e_{11} = 0.$$

Die resultaat is dus bewys.

□

Lemma 1.8 ([12], Lemma 3) *Die algebra $M_2(\mathbb{Z}_2)$ kan nie deur twee idempotente voortgebring word nie.*

Bewys Laat $p = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ 'n idempotent in $M_2(\mathbb{Z}_2)$ wees, sodat $p \neq 0$, $p \neq I_2$. Dan volg dat

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a^2 - bc & ab - bd \\ ca - dc & cb - d^2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

waar

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{en} \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Gevolgtik is

$$a^2 - bc = a \tag{31}$$

$$ab - bd = b \tag{32}$$

$$ca - dc = c \tag{33}$$

$$cb - d^2 = d. \tag{34}$$

Aangesien 0 en 1 idempotente is, volg dat alle elemente van \mathbb{Z}_2 idempotente is. Sodoende volg uit (31) dat $bc = 0$. Ons beskou die volgende moontlikhede:

1. **c = 0 en b = 1:** Uit (32) volg dan dat $d = a - 1$.
2. **b = 0 en c = 1:** Uit (33) volg dan dat $d = a - 1$.

In die eerste twee gevalle volg dus dat p van die volgende vorm is:

$$p = \begin{bmatrix} a & b \\ c & a - 1 \end{bmatrix}, \quad \text{met } bc = 0.$$

3. **b = 0 en c = 0:** Aangesien $p \neq 0, I_2$ volg dat

$$p = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{of} \quad p = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Uit al drie bostaande gevalle volg sodoende dat p van die volgende vorm is:

$$\begin{bmatrix} a & b \\ c & a - 1 \end{bmatrix}, \tag{35}$$

waar $a, b, c \in \mathbb{Z}_2$ en $bc = 0$.

Gestel nou p en q is twee idempotente van die vorm (35). Dan is daar die volgende twee moontlikhede:

1. **p en q is bo-driehoeks of p en q is onder-driehoeks:** Aangesien die som en produk van bo- of onder-driehoeks matrikse bo- of onder-driehoeks, onderskeidelik, is en I_2 beide bo- en onder-driehoeks is, volg dat die algebra \mathbb{A} voortgebring deur p en q eg in $M_2(\mathbb{Z}_2)$ bevat is.
2. **een van p en q is bo-driehoeks en die ander een is onder-driehoeks:** Sonder die verlies aan algemeenheid laat

$$p = \begin{bmatrix} a_1 & 1 \\ 0 & 1 - a_1 \end{bmatrix} \quad \text{en} \quad q = \begin{bmatrix} a_2 & 0 \\ 1 & 1 - a_2 \end{bmatrix}.$$

Nou,

$$\mathbb{A} = \{lp + mq + kI_2 + \sum_i s_i (\text{'n produk van } p\text{'s en } q\text{'s}) \mid l, m, k, s_i \in F\}. \quad (36)$$

Verder is

$$pq = \begin{bmatrix} a_1 & 1 \\ 0 & 1 - a_1 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ 1 & 1 - a_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 + 1 & 1 - a_2 \\ 1 - a_1 & (1 - a_1)(1 - a_2) \end{bmatrix}.$$

Omdat

$$\begin{aligned} & (1 - a_2)a_1 + (1 - a_1)a_2 + (1 - a_1)(1 - a_2) \\ &= a_1 - a_2 a_1 + a_2 - a_1 a_2 + 1 - a_1 - a_2 + a_1 a_2 \\ &= 1 - a_2 a_1 = a_1 a_2 + 1 \end{aligned}$$

en

$$\begin{aligned} (1 - a_2)(1 - a_1) + (1 - a_1)(a_2 - a_2) + (1 - a_1)(1 - a_2) &= 3(1 - a_2)(1 - a_1) \\ &= (1 - a_2)(1 - a_1) \end{aligned}$$

volg dat

$$\begin{aligned} pq &= \begin{bmatrix} (1 - a_2)a_1 & (1 - a_2) \\ 0 & (1 - a_2)(1 - a_1) \end{bmatrix} + \begin{bmatrix} (1 - a_1)a_2 & 0 \\ (1 - a_1) & (1 - a_1)(1 - a_2) \end{bmatrix} \\ &+ \begin{bmatrix} (1 - a_1)(1 - a_2) & 0 \\ 0 & (1 - a_1)(1 - a_2) \end{bmatrix} \\ &= (1 - a_2)p + (1 - a_1)q + (1 - a_1)(1 - a_2)I_2. \end{aligned} \quad (37)$$

Soortgelyk is

$$qp = \begin{bmatrix} a_2 & 0 \\ 1 & 1 - a_2 \end{bmatrix} \begin{bmatrix} a_1 & 1 \\ 0 & 1 - a_1 \end{bmatrix} = \begin{bmatrix} a_2 a_1 & a_1 \\ a_1 & 1 + (1 - a_2)(1 - a_1) \end{bmatrix}.$$

Omdat

$$a_2a_1 + a_1a_2 + a_1a_2 = 3a_1a_2 = a_2a_1$$

en

$$\begin{aligned} a_2(1 - a_1) + a_1(1 - a_2) + a_1a_2 &= a_2 - a_2a_1 + a_1 - a_1a_2 + a_1a_2 \\ &= -a_2 - a_1 + a_2a_1 \\ &= 1 + (1 - a_2)(1 - a_1) \end{aligned}$$

volg dat

$$\begin{aligned} qp &= \begin{bmatrix} a_2a_1 & a_2 \\ 0 & a_2(1 - a_1) \end{bmatrix} + \begin{bmatrix} a_1a_2 & 0 \\ a_1 & a_1(1 - a_2) \end{bmatrix} + \begin{bmatrix} a_1a_2 & 0 \\ 0 & a_1a_2 \end{bmatrix} \\ &= a_2p + a_1q + a_1a_2I_2. \end{aligned} \tag{38}$$

Uit (36), (37) en (38) volg sodoende dat \mathbb{A} as 'n lineêre kombinasie van p , q en I_2 uitgedruk kan word. Gevolglik is $\dim \mathbb{A} \leq 3$ en $\mathbb{A} \neq M_2(\mathbb{Z}_2)$. Dus kan $M_2(\mathbb{Z}_2)$ nie deur twee idempotente voortgebring word nie.

□

Alternatiewe bewys vir Lemma 1.8 Soos in die bostaande bewys kan bewys word dat 'n idempotent in $M_2(\mathbb{Z}_2)$ van die volgende vorm is:

$$\begin{bmatrix} a & b \\ c & a - 1 \end{bmatrix}, \tag{39}$$

waar $a, b, c \in \mathbb{Z}_2$ en $bc = 0$. 'n Idempotent p in $M_2(\mathbb{Z}_2)$ is dus een van die volgende matrikse:

$$\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}. \tag{40}$$

Vervolgens beskou ons die algebras voortgebring deur twee willekeurige idempotente p en q in (40). Aangesien 'n algebra voortgebring deur p en q , waar $p = q$, bevat is in 'n algebra voortgebring deur p en q , waar $p \neq q$, volg dat indien ons kan bewys dat al die algebras voortgebring deur p en q , waar $p \neq q$, eg in $M_2(\mathbb{Z}_2)$ bevat is, al die algebras voortgebring deur twee willekeurige elemente in (40) eg in $M_2(\mathbb{Z}_2)$ bevat is. Gestel dus nou dat p en q twee verskillende idempotente in (40) is.

Kom ons neem sonder die verlies aan algemeenheid aan dat $p = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ en q enige ander matriks in (40) is. Aangesien p en I_2 terselfdertyd bo- en onder-driehoeks is, volg dat p , q en I_2 dan al drie bo- of onder-driehoeks is. Aangesien die som en die produk van bo- of onder-driehoekse matrikse onderskeidelik bo- of onder-driehoeks is, volg dan dat die algebra \mathbb{A} voortgebring deur p en q eg in $M_2(\mathbb{Z}_2)$ bevat is. Soortgelyk volg dat die algebra voortgebring deur $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ en enige ander matriks in (40) eg in $M_2(\mathbb{Z}_2)$ bevat is.

Verder, aangesien

$$\begin{aligned} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} && \text{en} \\ \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \end{aligned}$$

volg dat die algebra voortgebring deur $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ (onderskeidelik $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$), en $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ (onderskeidelik $\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$) dieselfde sal wees. Dit is dus om te ewe om p of q as $\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$ (onderskeidelik $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$) of as $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ (onderskeidelik $\begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$) te kies. Dus volg, sonder die verlies aan algemeenheid, dat die volgende kombinasie die enigste kombinasie van p en q is wat ons nog moet beskou:

$$p = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{en} \quad q = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}.$$

Nou, aangesien

$$\begin{aligned} pq &= \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = p, \\ qp &= \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} = q, \end{aligned}$$

$p^2 = p$ en $q^2 = q$ volg dat enige produk van p 's en q 's maar net p of q is. Laat \mathbb{A} die algebra voortgebring deur p en q wees. Dan volg dat

$$\begin{aligned} \mathbb{A} &= \{mp + lq + kI_2 + \sum_i s_i (\text{'n produk van } p\text{'s en } q\text{'s}) \mid m, l, k, s_i \in \mathbb{Z}_2\} \\ &= \{mp + lq + kI_2 \mid m, l, k \in \mathbb{Z}_2\} \end{aligned}$$

van dimensie 3 en dus eg bevat is in $M_2(\mathbb{Z}_2)$. Dus kan $M_2(\mathbb{Z}_2)$ nie deur twee idempotente voortgebring word nie.

□

Uit bostaande lemma en Lemma 1.2 volg dat

$$\nu(2, \mathbb{Z}_2) = 3.$$

Dus is (2) bewys. In die volgende Lemma bewys ons (3).

Lemma 1.9 ([12], Lemma 4) *As $F \neq \mathbb{Z}_2$, dan kan die F -algebra $M_2(F)$ deur twee idempotente voortgebring word.*

Bewys Kies 'n $a \in F$, met $a \neq 0$ en $a \neq -1$. Stel

$$p_0 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{en} \quad q_0 = \begin{bmatrix} 1 & 0 \\ a & 0 \end{bmatrix}.$$

Laat \mathbb{A} die algebra voortgebring deur p_0 en q_0 wees. Nou,

$$p_0 q_0 = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ a & 0 \end{bmatrix} = \begin{bmatrix} 1+a & 0 \\ 0 & 0 \end{bmatrix} \in \mathbb{A}.$$

Aangesien F 'n liggaam is, het $1+a$ 'n inverse in F , sodat $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in \mathbb{A}$. Gevolglik is

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in \mathbb{A}, \quad p_0 - \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \in \mathbb{A}$$

en

$$q_0 - \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ a & 0 \end{bmatrix} \in \mathbb{A} \quad \text{sodat} \quad \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \in \mathbb{A}.$$

Aangesien $M_2(F)$ voortgebring word deur

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

volg dat $M_2(F) \subseteq \mathbb{A}$. Maar $p_0, q_0 \in M_2(F)$ sodat $M_2(F) = \mathbb{A}$.

Dus word $M_2(F)$ deur die idempotente p_0 en q_0 voortgebring.

□

Die bostaande bewys misluk indien $F = \mathbb{Z}_2$, aangesien ons aan die begin van die bewys die aanname maak dat $a \neq 0$ en $a \neq -1$. Aangesien $-1 = 1$ en 0 die enigste elemente van \mathbb{Z}_2 is, bestaan daar nie 'n $a \in \mathbb{Z}_2$ wat aan die gevraagde vereiste voldoen nie.

Stelling 1.1 is dus nou bewys.

2 Die minimum aantal idempotente voortbringers van direkte somme van volledige matriksalgebras oor 'n liggaam

Ons sal in hierdie hoofstuk poog om die resultate van die eerste hoofstuk na direkte somme van volledige matriksalgebras $M_n(F)$, waar F 'n willekeurige liggaam is, uit te brei. Ons eerste mikpunt sal wees om die volgende stelling te bewys.

Stelling 2.1 ([12], Stelling 3) *Laat $\mathbb{B} := M_{n_1}^{m_1}(F) \oplus M_{n_2}^{m_2}(F) \oplus \dots \oplus M_{n_k}^{m_k}(F)$ die direkte som van F -algebras van die vorm $M_{n_s}^{m_s}(F)$, waar $M_{n_s}^{m_s}(F)$ die direkte som van m_s kopieë van die F -algebra $M_{n_s}(F)$ voorstel, en $\nu(\mathbb{B})$ die minimum aantal idempotente voortbringers van \mathbb{B} wees. As $1 \leq n_1 < n_2 < \dots < n_k$, dan is*

$$\nu(\mathbb{B}) = \max_{1 \leq j \leq k} \nu(M_{n_j}^{m_j}(F)).$$

Vervolgens sal ons die direkte somme $M_n^m(F)$ beskou. Ons het reeds in Hoofstuk 1 die geval bewys indien $m = 1$. Ons sal hierdie resultate nou uitbrei na direkte somme $M_n^m(F)$, waar $m \geq 2$.

Aangesien $M_1(F) \cong F$ sal ons, om notasie te vergemaklik, $M_n^m(F)$ as F^m , m kopieë van F , aandui indien $n = 1$. Ons sal die volgende resultaat vir hierdie geval bewys.

Stelling 2.2 ([11], Stelling 2) *Laat F 'n liggaam en $m \geq 2$ wees. Dan is*

$$\nu(F^m) = \lceil \log_2 m \rceil.$$

Indien $n = 2$ sal ons deur middel van Stelling 2.3 die minimum aantal idempotente voortbringers vir $M_2^m(F)$ kan bepaal wanneer $m \geq 2$ en $|F| \geq m + 2$.

Stelling 2.3 ([12], Stelling 5) *Laat F 'n liggaam wees, met $m \geq 2$ en $|F| \geq m + 2$. Dan is*

$$\nu(M_2^m(F)) = 2.$$

In die geval waar $n \geq 3$ sal ons die presiese minimum aantal idempotente voortbringers kan bepaal indien $|F| \geq m + 1$ en $m \geq 2$. Ons sal dit deur middel van die volgende resultaat doen.

Stelling 2.4 ([12], Stelling 5) Laat $m \geq 2$ en $n \geq 3$. Vir enige liggaam F , met $|F| \geq m + 1$, is

$$\nu(M_n^m(F)) = 3.$$

Alhoewel ons nie daarin sal slaag om die minimum aantal idempotente voortbringers vir die direkte somme $M_2^m(F)$, met $m \geq 2$ en $|F| \leq m + 1$, en $M_n^m(F)$, met $m \geq 2$, $n \geq 3$ en $|F| \leq m$, te bepaal nie, sal ons wel 'n ondergrens vir hierdie gevalle vind deur middel van Gevolg 2.19, en 'n bogrens deur middel van Gevolg 2.13 en Gevolg 2.17, onderskeidelik. Alhoewel die ondergrens oor die algemeen nie direkte relevansie het nie, sal ons wel uit die ondergrens kan aflei dat die minimum aantal idempotente voortbringers in bostaande gevalle van $|F|$, n , asook m , afhanklik is.

Aangesien alle eindige direkte somme van volledige matriksalgebras oor 'n liggaam F , in die vorm

$$M_{n_1}^{m_1}(F) \oplus M_{n_2}^{m_2}(F) \oplus \cdots \oplus M_{n_k}^{m_k}(F),$$

geskryf kan word, waar $1 \leq n_1 < n_2 < \cdots < n_k$, volg dat ons deur middel van Stelling 2.1, Stelling 2.2, Stelling 2.3 en Stelling 2.4 die minimum aantal idempotente voortbringers van alle eindige direkte somme van volledige matriksalgebras oor 'n liggaam F kan bepaal, behalwe die gevalle waarin 'n direkte som $M_2^m(F)$, met $m \geq 2$ en $|F| \leq m + 1$, voorkom, of die gevalle waarin 'n direkte som $M_n^m(F)$, met $n \geq 3$, $m \geq 2$ en $|F| \leq m$, voorkom. Ons sal egter deur middel van Stelling 2.1, Gevolg 2.19, Gevolg 2.13 en Gevolg 2.17 'n ondergrens en 'n bogrens vir die minimum aantal idempotente voortbringers vir elk van hierdie oorblywende gevalle kan bepaal.

Ons sal die hoofstuk afsluit deur aan te toon hoe ons die resultate wat ons in die tesis bewys het op eindig dimensionele semi-eenvoudige algebras oor 'n algebraïes geslote liggaam kan toepas.

Ons beperk ons nou eers tot Stelling 2.1 voor ons die direkte somme $M_n^m(F)$ beskou. Ons gaan eers 'n spesifieke geval van Stelling 2.1, naamlik die geval wanneer $m_1 = m_2 = \cdots = m_k = 1$ en $n_1 > 1$ bewys voor ons, soortgelyk, die algemene resultaat gaan bewys. Ons gaan met ander woorde eerstens die volgende stelling bewys:

Stelling 2.5 ([12], Stelling 2) Laat F enige liggaam en $\mathbb{B} := M_{n_1}(F) \oplus M_{n_2}(F) \oplus \cdots \oplus M_{n_k}(F)$ wees. As $1 < n_1 < n_2 < \cdots < n_k$ dan is

$$\nu(\mathbb{B}) = \max_{1 \leq s \leq k} \nu(n_s, F) \leq 3.$$

Voor ons egter Stelling 2.5 of Stelling 2.1 kan bewys, het ons nodig om Lemma 2.8, waarin ons Definisie 2.6 en Stelling 2.7 gaan benodig, te bewys.

Definisie 2.6 ([4], bladsy 188) 'n Vandermonde matriks van orde n is 'n $n \times n$ matriks van die vorm

$$\begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & x_4 & \cdots & x_n \\ x_1^2 & x_2^2 & x_3^2 & x_4^2 & \cdots & x_n^2 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & x_4^{n-1} & \cdots & x_n^{n-1} \end{bmatrix}.$$

Ons dui die determinant van bostaande matriks, genoem die Vandermonde determinant, as $V(x_1, x_2, \dots, x_n)$ aan.

Stelling 2.7 (DIE VANDERMONDE DETERMINANT ARGUMENT) ([4], bladsy 188)
Die determinant van die Vandermonde matriks in Definisie 2.6 is

$$\prod_{1 \leq i < j \leq n} (x_j - x_i).$$

Bewys Ons gaan die stelling deur middel van induksie op n bewys. Gestel $n = 2$. Dan volg dat

$$\begin{vmatrix} 1 & 1 \\ x_1 & x_2 \end{vmatrix} = x_2 - x_1 = \prod_{1 \leq i < j \leq 2} (x_j - x_i).$$

Die resultaat geld dus vir $n = 2$.

Ons neem nou aan dat die resultaat vir $n = k - 1$ geld.

Ons beskou volgende die determinant van die $k \times k$ Vandermonde matriks. Deur middel van ry operasies (ons stel ry i as R_i voor), die gebruik van die ko-faktor ontwikkeling en ons induksie hipotese volg dat

$$V(x_1, x_2, \dots, x_k) = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_k \\ x_1^2 & x_2^2 & \cdots & x_k^2 \\ \vdots & \vdots & & \vdots \\ x_1^{k-1} & x_2^{k-1} & \cdots & x_k^{k-1} \end{vmatrix}$$

$$\begin{aligned}
&= \begin{vmatrix} 1 & 1 & \cdots & 1 \\ 0 & x_2 - x_1 & \cdots & x_k - x_1 \\ 0 & x_2(x_2 - x_1) & \cdots & x_k(x_k - x_1) \\ \vdots & \vdots & & \vdots \\ 0 & x_2^{k-2}(x_2 - x_1) & \cdots & x_k^{k-2}(x_k - x_1) \end{vmatrix} \begin{array}{l} \text{eers } R_k - x_1 R_{k-1} \\ \text{dan } R_{k-1} - x_1 R_{k-2} \\ \vdots \\ \text{dan } R_2 - x_1 R_1 \end{array} \\
&= 1 \begin{vmatrix} x_2 - x_1 & \cdots & x_k - x_1 \\ x_2(x_2 - x_1) & \cdots & x_k(x_k - x_1) \\ \vdots & & \vdots \\ x_2^{k-3}(x_2 - x_1) & \cdots & x_k^{k-3}(x_k - x_1) \\ x_2^{k-2}(x_2 - x_1) & \cdots & x_k^{k-2}(x_k - x_1) \end{vmatrix} \\
&= (x_2 - x_1)(x_3 - x_1) \cdots (x_k - x_1) \begin{vmatrix} 1 & 1 & \cdots & 1 \\ x_2 & x_3 & \cdots & x_k \\ x_2^2 & x_3^2 & \cdots & x_k^2 \\ \vdots & \vdots & & \vdots \\ x_2^{k-2} & x_3^{k-2} & \cdots & x_k^{k-2} \end{vmatrix} \\
&= (x_2 - x_1)(x_3 - x_1) \cdots (x_k - x_1) V(x_2, x_3, \dots, x_k) \\
&= (x_2 - x_1)(x_3 - x_1) \cdots (x_k - x_1) \prod_{2 \leq i < j \leq k} (x_j - x_i) \tag{41} \\
&= \prod_{1 \leq i < j \leq k} (x_i - x_j).
\end{aligned}$$

Die resultaat volg dus.

□

Lemma 2.8 ([12], Lemma 5) *Laat \mathbb{A} 'n F -subalgebra met identiteit e van 'n direkte som $\mathbb{B} = \mathbb{B}_1 \oplus \mathbb{B}_2 \oplus \cdots \oplus \mathbb{B}_k$ van F -algebras \mathbb{B}_m wees, en laat w_m die identiteit van \mathbb{B}_m wees. Dit wil sê $w_1 \oplus w_2 \oplus \cdots \oplus w_k = e$. Laat $\pi_m : \mathbb{B} \rightarrow \mathbb{B}_m$ die kanoniese projeksie wees en gestel dat*

1. $\pi_m(\mathbb{A}) = \mathbb{B}_m$ vir elke $m = 1, \dots, k$ en
2. daar 'n element $w = \alpha_1 w_1 \oplus \alpha_2 w_2 \oplus \cdots \oplus \alpha_k w_k$ in \mathbb{A} is, waar α_m ($m = 1, \dots, k$) verskillende elemente in F is.

Dan is $\mathbb{A} = \mathbb{B}$.

Bewys Aangesien \mathbb{A} 'n F -subalgebra van \mathbb{B} is, is $\mathbb{A} \subseteq \mathbb{B}$. Indien ons dus kan bewys dat $\mathbb{B} \subseteq \mathbb{A}$ is ons klaar. Ons stel die elemente $\delta_{1m}w_1 \oplus \delta_{2m}w_2 \oplus \cdots \oplus \delta_{km}w_k$, waar δ_{im} die Kronecker deltas is, as f_m ($m = 1, 2, \dots, k$) voor. Aangesien

$$\begin{aligned} w^s &= (\alpha_1 w_1 \oplus \alpha_2 w_2 \oplus \cdots \oplus \alpha_k w_k)^s \\ &= (\alpha_1 w_1)^s \oplus (\alpha_2 w_2)^s \oplus \cdots \oplus (\alpha_k w_k)^s \\ &= \alpha_1^s w_1^s \oplus \alpha_2^s w_2^s \oplus \cdots \oplus \alpha_k^s w_k^s \\ &= \alpha_1^s w_1 \oplus \alpha_2^s w_2 \oplus \cdots \oplus \alpha_k^s w_k \end{aligned}$$

vir alle $s \in \mathbb{N}$, het ons die volgende stelsel van vergelykings

$$\begin{aligned} e &= w_1 \oplus w_2 \oplus \cdots \oplus w_k \\ w &= \alpha_1 w_1 \oplus \alpha_2 w_2 \oplus \cdots \oplus \alpha_k w_k \\ w^2 &= \alpha_1^2 w_1 \oplus \alpha_2^2 w_2 \oplus \cdots \oplus \alpha_k^2 w_k \\ &\vdots \\ w^{k-1} &= \alpha_1^{k-1} w_1 \oplus \alpha_2^{k-1} w_2 \oplus \cdots \oplus \alpha_k^{k-1} w_k. \end{aligned}$$

Of anders gestel is

$$\begin{aligned} e &= f_1 + f_2 + \cdots + f_k \\ w &= \alpha_1 f_1 + \alpha_2 f_2 + \cdots + \alpha_k f_k \\ w^2 &= \alpha_1^2 f_1 + \alpha_2^2 f_2 + \cdots + \alpha_k^2 f_k \\ &\vdots \\ w^{k-1} &= \alpha_1^{k-1} f_1 + \alpha_2^{k-1} f_2 + \cdots + \alpha_k^{k-1} f_k, \end{aligned}$$

waar "+" die optellingsoperasie van die algebra \mathbb{B} is. Ons kan bostaande vergelykings as

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots & \alpha_k \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \alpha_3^{k-1} & \cdots & \alpha_k^{k-1} \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_k \end{bmatrix} = \begin{bmatrix} e \\ w \\ \vdots \\ w^{k-1} \end{bmatrix}$$

in matriks vorm uitdruk. Volgens die Vandermonde determinant argument (Stelling 2.7)

is $V(\alpha_1, \alpha_2, \dots, \alpha_k) = \prod_{1 \leq i < j \leq k} (\alpha_j - \alpha_i)$. Volgens aanname is $\alpha_i \neq \alpha_j$ vir $i \neq j$ sodat

$V(\alpha_1, \alpha_2, \dots, \alpha_k) \neq 0$. Deur van Cramer se reël en die ko-faktor uitbreiding gebruik te

maak volg sodoende dat

$$\begin{aligned}
f_1 &= \frac{\begin{vmatrix} e & 1 & \dots & 1 \\ w & \alpha_2 & \dots & \alpha_k \\ \vdots & \vdots & & \vdots \\ w^{k-1} & \alpha_2^{k-1} & \dots & \alpha_k^{k-1} \end{vmatrix}}{V(\alpha_1, \alpha_2, \dots, \alpha_k)} \\
&= e \frac{\begin{vmatrix} \alpha_2 & \dots & \alpha_k \\ \vdots & & \vdots \\ \alpha_2^{k-1} & \dots & \alpha_k^{k-1} \end{vmatrix}}{V(\alpha_1, \alpha_2, \dots, \alpha_k)} + w \frac{\begin{vmatrix} 1 & \dots & 1 \\ \alpha_2^2 & \dots & \alpha_k^2 \\ \vdots & & \vdots \\ \alpha_2^{k-1} & \dots & \alpha_k^{k-1} \end{vmatrix}}{V(\alpha_1, \alpha_2, \dots, \alpha_k)} + \dots + w^{k-1} \frac{\begin{vmatrix} 1 & \dots & 1 \\ \alpha_2 & \dots & \alpha_k \\ \vdots & & \vdots \\ \alpha_2^{k-2} & \dots & \alpha_k^{k-2} \end{vmatrix}}{V(\alpha_1, \alpha_2, \dots, \alpha_k)} \\
&= e \frac{c_1}{V(\alpha_1, \alpha_2, \dots, \alpha_k)} + w \frac{c_2}{V(\alpha_1, \alpha_2, \dots, \alpha_k)} + \dots + w^{k-1} \frac{c_{k-1}}{V(\alpha_1, \alpha_2, \dots, \alpha_k)}, \quad (42)
\end{aligned}$$

waar $c_1, \dots, c_{k-1} \in F$. Uit (42) volg sodoende dat f_1 geskryf kan word as 'n lineêre kombinasie van $e, w, w^2, \dots, w^{k-1}$ oor F . Aangesien $w \in \mathbb{A}$ volg dat $f_1 \in \mathbb{A}$. Soortgelyk volg dat $f_2, f_3, \dots, f_k \in \mathbb{A}$.

Laat m 'n willekeurige element van $\{1, \dots, k\}$ wees. Aangesien $\pi_m(\mathbb{B}) = \mathbb{B}_m = \pi_m(\mathbb{A})$, volgens aanname, bestaan daar vir elke $b \in \mathbb{B}$ 'n $a \in \mathbb{A}$ sodat $\pi_m(b) = \pi_m(a)$. Dus volg vir 'n willekeurige $b \in \mathbb{B}$ dat

$$\begin{aligned}
bf_m &= \bigoplus_{i=1}^k \delta_{im} \pi_m(b) w_m \\
&= \bigoplus_{i=1}^k \delta_{im} \pi_m(a) w_m \\
&= af_m \in \mathbb{A}.
\end{aligned}$$

Dus volg dat $b = \sum_{m=1}^k (bf_m) \in \mathbb{A}$. Gevolglik is $\mathbb{B} \subseteq \mathbb{A}$.

□

Ons is nou in staat om Stelling 2.5 en Stelling 2.1 te bewys.

Die bewys van Stelling 2.5 Gestel $k = 1$. Dan volg uit Stelling 1.1 dat

$$\nu(\mathbb{B}) = \nu(M_{n_1}(F)) = \max_{1 \leq s \leq 1} \nu(n_1, F) \leq 3.$$

Die stelling geld dus vir $k = 1$.

Gestel nou $k > 1$. Let op dat aangesien $n_1 > 1$ volg dat $n_2 \geq 3$ sodat uit Stelling 1.1 volg dat $\nu(n_m, F) = 3$ vir alle $m \geq 2$. Dit wil sê $\max_{1 \leq s \leq k} \nu(n_s, F) = 3$ vir $k > 1$. Indien ons dus kan bewys dat $\nu(\mathbb{B}) = 3$ vir alle $k > 1$ is ons klaar.

Aangesien die kanoniese projeksie π_2 van \mathbb{B} op $M_{n_2}(F)$ 'n surjektiewe homomorfisme is en homomorfismes optelling en vermenigvuldiging behou, volg dat indien b_1, \dots, b_l vir \mathbb{B} voortbring, $\pi_2(b_1), \dots, \pi_2(b_l)$ vir $M_{n_2}(F)$ voortbring. Aangesien $\nu(n_2, F) = 3$ volg dus dat $\nu(\mathbb{B}) \geq 3$. Indien ons bewys dat \mathbb{B} deur drie idempotente voortgebring kan word, volg dat $\nu(\mathbb{B}) = 3$ en ons is klaar.

Laat

$$p = p_{n_1} \oplus p_{n_2} \oplus \dots \oplus p_{n_k}, \quad q = q_{n_1} \oplus q_{n_2} \oplus \dots \oplus q_{n_k} \quad \text{en} \quad r = r_{n_1} \oplus r_{n_2} \oplus \dots \oplus r_{n_k},$$

met p_n, q_n en r_n die idempotente in (4), (5) en (6), onderskeidelik. Ons sal deur middel van induksie op k bewys dat die F -subalgebra \mathbb{A} voortgebring deur p, q en r gelyk aan \mathbb{B} , vir alle k , en dus in die besonder vir $k > 1$, is.

Ons het die geval $k = 1$ in Lemma 1.2 bewys. Ons neem nou aan dat die algebra voortgebring deur p, q en r , waar $1 \leq k \leq j - 1$, gelyk aan $\mathbb{B} = M_{n_1}(F) \oplus \dots \oplus M_{n_k}(F)$ is. Indien ons kan bewys dat die algebra voortgebring deur p, q en r , waar $k = j$, gelyk aan $\mathbb{B} = M_{n_1}(F) \oplus \dots \oplus M_{n_j}(F)$ is, is die induksie voltooi en het ons bewys dat $\mathbb{A} = \mathbb{B}$ vir alle k .

Laat

$$\mathbb{B}_1 := M_{n_1}(F) \oplus M_{n_2}(F) \oplus \dots \oplus M_{n_{j-1}}(F), \quad \mathbb{B}_2 := M_{n_j}(F),$$

en \mathbb{A} die F -subalgebra van $\mathbb{B} = M_{n_1}(F) \oplus \dots \oplus M_{n_j}(F)$ voortgebring deur

$$p = p_{n_1} \oplus \dots \oplus p_{n_j}, \quad q = q_{n_1} \oplus \dots \oplus q_{n_j} \quad \text{en} \quad r = r_{n_1} \oplus \dots \oplus r_{n_j}$$

wees. Verder, laat π_1 die kanoniese projeksie van \mathbb{B} op \mathbb{B}_1 en π_2 die kanoniese projeksie van \mathbb{B} op \mathbb{B}_2 wees. Dan is $\pi_1(\mathbb{A})$ die algebra voortgebring deur

$$p_{n_1} \oplus p_{n_2} \oplus \dots \oplus p_{n_{j-1}}, \quad q_{n_1} \oplus q_{n_2} \oplus \dots \oplus q_{n_{j-1}} \quad \text{en} \quad r_{n_1} \oplus r_{n_2} \oplus \dots \oplus r_{n_{j-1}}$$

en $\pi_2(\mathbb{A})$ is die algebra voortgebring deur

$$p_{n_j}, q_{n_j} \quad \text{en} \quad r_{n_j}.$$

Volgens ons induksie hipotese is

$$\pi_1(\mathbb{A}) = \mathbb{B}_1 \quad \text{en} \quad \pi_2(\mathbb{A}) = \mathbb{B}_2.$$

Laat $b = r(2e - p - q)$ en $a = p + q - e + b$, waar $e = I_{n_1} \oplus \cdots \oplus I_{n_j}$ die identiteit van \mathbb{B} is, sodat $b, a \in \mathbb{A}$. Dan volg uit (14) en (15) dat

$$b = e_{n_{11}} \oplus \cdots \oplus e_{n_{j1}} \quad \text{en} \quad a = a_{n_1} \oplus a_{n_2} \oplus \cdots \oplus a_{n_j},$$

waar a_n die permutasie matriks in (7) is. Deur van (17) gebruik te maak volg dat

$$\begin{aligned} p + q - e &= (p_{n_1} \oplus p_{n_2} \oplus \cdots \oplus p_{n_j}) + (q_{n_1} \oplus q_{n_2} \oplus \cdots \oplus q_{n_j}) - (I_{n_1} \oplus I_{n_2} \oplus \cdots \oplus I_{n_j}) \\ &= (p_{n_1} + q_{n_1} - I_{n_1}) \oplus \cdots \oplus (p_{n_j} + q_{n_j} - I_{n_j}) \\ &= D_{n_1}^{(1)} \oplus D_{n_2}^{(1)} \oplus \cdots \oplus D_{n_j}^{(1)}, \end{aligned}$$

waar " + " die optellingsoperasie in \mathbb{B} is, sodat uit (18) volg dat

$$(p + q - e)^{n_j - 1} = 0 \oplus 0 \oplus \cdots \oplus 0 \oplus D_{n_j}^{(n_j - 1)}$$

of in terme van \mathbb{B}_1 en \mathbb{B}_2 dat

$$(p + q - e)^{n_j - 1} = 0 \oplus e_{1, n_j} \quad (0 \in \mathbb{B}_1 \text{ en } e_{1, n_j} \in \mathbb{B}_2).$$

Laat $w_1 := I_{n_1} \oplus \cdots \oplus I_{n_{j-1}}$ en $w_2 := I_{n_j}$. Dan is w_1 die identiteit van \mathbb{B}_1 en w_2 die identiteit van \mathbb{B}_2 . Sodoende volg dan uit (21) dat

$$\begin{aligned} 0w_1 + 1w_2 &= 0 \oplus \cdots \oplus 0 \oplus \sum_{m=1}^{n_j} e_{mm} \\ &= 0 \oplus \cdots \oplus 0 \oplus \sum_{m=1}^{n_j} a_{n_j}^{n_j - m + 1} e_{1, n_j} a_{n_j}^m \\ &= \sum_{m=1}^{n_j} a^{n_j - m + 1} (0 \oplus \cdots \oplus e_{1, n_j}) a^m \in \mathbb{A}. \end{aligned}$$

Volgens Lemma 2.8 is $\mathbb{A} = \mathbb{B} = M_{n_1}(F) \oplus \cdots \oplus M_{n_j}(F)$. Dit wil sê $\mathbb{B} = M_{n_1}(F) \oplus \cdots \oplus M_{n_k}(F)$ kan vir alle k , en dus vir $k > 1$, deur drie idempotente voortgebring word.

□

Die bewys van Stelling 2.1 Om die stelling te bewys, gebruik ons Lemma 2.8, induksie op k en sentrale polinome. Sentrale polinome word in Hoofstuk 3 behandel.

Daar is niks om te bewys as $k = 1$ nie. Dus, laat $k > 1$ wees en gestel die resultaat is waar vir alle k' sodat $k' < k$. Laat

$$\mathbb{B}_1 := M_{n_1}^{m_1}(F) \oplus \cdots \oplus M_{n_{k-1}}^{m_{k-1}}(F) \quad \text{en} \quad \mathbb{B}_2 := M_{n_k}^{m_k}(F)$$

sodat

$$\mathbb{B} = \mathbb{B}_1 \oplus \mathbb{B}_2.$$

Ons weet volgens die induksie hipotese dat

$$\nu(\mathbb{B}_1) = \max_{1 \leq j \leq k-1} \nu(M_{n_j}^{m_j}(F)). \quad (43)$$

Laat π_1 die kanoniese projeksie van \mathbb{B} op \mathbb{B}_1 en π_2 die kanoniese projeksie van \mathbb{B} op \mathbb{B}_2 wees. Aangesien π_1 en π_2 dan surjektiewe homomorfismes is en homomorfismes optelling en vermenigvuldiging behou, volg dat indien b_1, b_2, \dots, b_s vir \mathbb{B} voortbring, $\pi_1(b_1), \pi_1(b_2), \dots, \pi_1(b_s)$ vir \mathbb{B}_1 en $\pi_2(b_1), \pi_2(b_2), \dots, \pi_2(b_s)$ vir \mathbb{B}_2 voortbring.

Sodoende volg dat

$$\nu(\mathbb{B}) \geq \max(\nu(\mathbb{B}_1), \nu(\mathbb{B}_2)) \geq \nu(\mathbb{B}_1), \nu(\mathbb{B}_2). \quad (44)$$

Laat $t = \max(\nu(\mathbb{B}_1), \nu(\mathbb{B}_2))$. Aangesien $t \geq \nu(\mathbb{B}_1), \nu(\mathbb{B}_2)$, volg dat \mathbb{B}_1 en \mathbb{B}_2 onderskeidelik deur t , nie noodwendig verskillende, idempotente voortgebring kan word. Sê

$$e_1, e_2, \dots, e_t \quad \text{en} \quad E_1, E_2, \dots, E_t \quad (45)$$

bring, onderskeidelik, \mathbb{B}_1 en \mathbb{B}_2 voort. Laat \mathbb{A} die F -subalgebra van \mathbb{B} voortgebring deur

$$e_1 \oplus E_1, e_2 \oplus E_2, \dots, e_t \oplus E_t$$

wees. Dan is $\pi_1(\mathbb{A}) = \mathbb{B}_1$ en $\pi_2(\mathbb{A}) = \mathbb{B}_2$ volgens (45). Indien ons kan bewys dat

$$0 \oplus e \in \mathbb{A}, \quad (46)$$

met 0 die nulelement van \mathbb{B}_1 en e die identiteitselement van \mathbb{B}_2 , dan volg uit Lemma 2.8 dat $\mathbb{A} = \mathbb{B}$, en dus dat \mathbb{B} deur t idempotente voortgebring kan word. Met ander woorde dat

$$\nu(\mathbb{B}) \leq t. \quad (47)$$

Uit (43), (44) en (47) kan ons dan die gevolgtrekking maak dat

$$\begin{aligned} \nu(\mathbb{B}) &= t = \max(\nu(\mathbb{B}_1), \nu(\mathbb{B}_2)) \\ &= \max\left(\max_{1 \leq j \leq k-1} \nu(M_{n_j}^{m_j}(F)), \nu(M_{n_k}^{m_k}(F))\right) \\ &= \max_{1 \leq j \leq k} \nu(M_{n_j}^{m_j}(F)). \end{aligned}$$

As ons dus (46) kan bewys, is ons klaar.

Volgens Stelling 3.5 bestaan daar 'n nie-nulwordende sentrale polinoom f (soos in Definisie 3.1 gedefinieer) vir $M_{n_k}(F)$. Dus bestaan daar matrikse $X_1, X_2, \dots, X_l \in M_{n_k}(F)$ sodat

$$f(X_1, \dots, X_l) = aI_{n_k}$$

vir 'n $a \in F$, $a \neq 0$. Gevolglik is

$$\begin{aligned} f(\underbrace{X_1 \oplus \dots \oplus X_1}_{m_k \text{ kopieë}}, \dots, \underbrace{X_l \oplus \dots \oplus X_l}_{m_k \text{ kopieë}}) &= aI_{n_k} \oplus \dots \oplus aI_{n_k} \\ &= aI_{n_k}^{m_k}. \end{aligned}$$

Omdat

$$X_1 \oplus \dots \oplus X_1, \dots, X_l \oplus \dots \oplus X_l \in M_{n_k}^{m_k}(F) = \mathbb{B}_2 = \pi_2(\mathbb{A})$$

bestaan daar $A_1, A_2, \dots, A_l \in \mathbb{A}$ sodat

$$\pi_2(A_1) = X_1 \oplus \dots \oplus X_1, \quad \pi_2(A_2) = X_2 \oplus \dots \oplus X_2, \quad \dots, \quad \pi_2(A_l) = X_l \oplus \dots \oplus X_l.$$

Verder is

$$\pi_1(A_1), \dots, \pi_1(A_l) \in \mathbb{B}_1 = M_{n_1}^{m_1}(F) \oplus \dots \oplus M_{n_{k-1}}^{m_{k-1}}(F) \quad \text{met} \quad n_1, \dots, n_{k-1} < n_k.$$

Beskou nou die 1 – 1 homomorfisme

$$\alpha_j : M_{n_j}(F) \rightarrow M_{n_k}(F) \quad (j = 1, 2, \dots, k-1)$$

gedefinieer deur

$$\alpha_j(Y) := \left[\begin{array}{c|c} Y & 0 \\ \hline 0 & 0 \end{array} \right].$$

Ons kan dus deur van α_j gebruik te maak $M_{n_j}(F)$ in $M_{n_k}(F)$ inbed of, anders gestel, kan ons $M_{n_j}(F)$ as 'n subalgebra

$$\mathbb{D} = \left\{ \left[\begin{array}{c|c} Y & 0 \\ \hline 0 & 0 \end{array} \right] : Y \in M_{n_j}(F) \right\}$$

van $M_{n_k}(F)$ beskou. Sodoende volg, vir willekeurige $Y_1, \dots, Y_l \in M_{n_j}(F)$, aan die een kant dat

$$\alpha_j(\underbrace{f(Y_1, Y_2, \dots, Y_l)}_{\in M_{n_j}(F)}) \in \mathbb{D}$$

en, met behulp van Stelling 3.2, aan die ander kant dat

$$\begin{aligned} \alpha_j(f(Y_1, Y_2, \dots, Y_l)) &= f(\underbrace{\alpha_j(Y_1)}_{\in M_{n_k}(F)}, \dots, \underbrace{\alpha_j(Y_l)}_{\in M_{n_k}(F)}) \in Z(M_{n_k}(F)) \\ &= \begin{bmatrix} d & & \circ \\ & \ddots & \\ \circ & & d \end{bmatrix} \quad \text{vir 'n } d \in F. \end{aligned}$$

Gevollik is $d = 0$ wat impliseer dat $f(Y_1, Y_2, \dots, Y_l) = 0$. Daarom is

$$f(\pi_1(A_1), \pi_1(A_2), \dots, \pi_1(A_l)) = 0$$

in \mathbb{B}_1 , en dus volg dat

$$\mathbb{A} \ni f(A_1, A_2, \dots, A_l) = 0 \oplus (aI_{n_k} \oplus \dots \oplus aI_{n_k}),$$

met $0 \in \mathbb{B}_1$ en $aI_{n_k} \oplus \dots \oplus aI_{n_k} \in \mathbb{B}_2$. Gevollik is

$$\frac{1}{a}f(A_1, A_2, \dots, A_l) = 0 \oplus e \in \mathbb{A}.$$

□

Let daarop dat die geval $n_1 = 1$ ook gedek word deur die bewys van Stelling 2.1, maar nie deur die bewys van Stelling 2.5 nie.

Alhoewel ons $\nu(M_n(F))$ (in Stelling 1.1) en $\nu(M_{n_1}^{m_1}(F) \oplus \dots \oplus M_{n_k}^{m_k}(F))$ (in Stelling 2.1) in terme van $\nu(M_{n_1}^{m_1}(F)), \dots, \nu(M_{n_k}^{m_k}(F))$ bepaal het, weet ons nog nie wat $\nu(M_n^m(F))$ is nie. Ons beskou dus nou direkte somme van die vorm $M_n^m(F)$.

Ons beskou eerstens die geval indien $n = 1$, met ander woorde, direkte somme van die vorm F^m .

In ([12], Stelling 5) beweer Krupnik foutiewelik, soos in [11] uitgewys, dat $\nu(F^m) = m - 1$, waar F 'n oneindige liggaam is. Hier volg 'n teenvoorbeeld.

Volgens Krupnik is $\nu(F^4) = 3$, waar F 'n oneindige liggaam is. Beskou nou die idempotente

$$(1, 1, 0, 0) \quad \text{en} \quad (1, 0, 1, 0). \quad (48)$$

Aangesien $(1, 1, 1, 1)$ die identiteit van F^4 is en

$$\begin{aligned}(1, 0, 0, 0) &= (1, 1, 0, 0)(1, 0, 1, 0); \\(0, 1, 0, 0) &= (1, 1, 0, 0) - (1, 0, 0, 0); \\(0, 0, 1, 0) &= (1, 0, 1, 0) - (1, 0, 0, 0); \\(0, 0, 0, 1) &= (1, 1, 1, 1) - (1, 0, 0, 0) - (0, 1, 0, 0) - (0, 0, 1, 0),\end{aligned}$$

volg dat die twee idempotente in (48) die hele F^4 as F -algebra voortbring. Dus is $\nu(F^4) \leq 2$. Trouens, uit Lemma 2.10 volg dat $\nu(F^4) = 2$.

Indien ons F^m as 'n vektorruimte oor F in plaas van 'n F -algebra beskou, volg dat aangesien F^m dimensie m het ons al m hierdie elemente kan voortbring deur $m - 1$ elemente van die basis

$$(1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1)$$

en e , waar e die identiteit van F^m is, te gebruik. Dus volg dat ons die vektorruimte F^m deur $m - 1$ elemente kan voortbring. Aangesien die aantal elemente van 'n basis, met ander woorde die dimensie van 'n vektorruimte, uniek is kan ons die vektorruimte F^m nie deur minder as $m - 1$ elemente voortbring nie. Dus volg dat die minimum aantal idempotente voortbringers vir die vektorruimte F^m , $m - 1$ is. Krupnik se resultaat, naamlik dat $\nu(F^m) = m - 1$, waar F 'n oneindige liggaam is, sou dus wel waar gewees het indien hy F^m as 'n vektorruimte beskou het.

As regstelling van die fout in [12] word inderwaarheid iets sterker as Stelling 2.2 in ([11], Stelling 2) bewys, naamlik dat

$$\nu(R^m) = \lceil \log_2 m \rceil,$$

waar R 'n kommutatiewe ring is en Stelling 2.2 dus direk volg. Die volgende Lemmas en resultate is 'n uiteensetting van die bewys van Stelling 2 in [11].

Notasie Laat $m \geq 2$. Ons dui die element van R^m met 'n 1 in die k de posisie en 0'e andersins as e_k^m , die identiteit van R^m as 1_{R^m} en die nulelement van R^m as 0_{R^m} aan. Laat $n \geq 1$. Ons definieer die idempotente $u_i^{2^n}$ ($i = 1, \dots, n$) in R^{2^n} as

$$u_i^{2^n} := \sum_{j=0}^{2^{i-1}-1} \sum_{k=1+j \cdot 2^{n-i+1}}^{j \cdot 2^{n-i+1} + 2^{n-i}} e_k^{2^n}. \quad (49)$$

Vir $n = 3$ beteken dit byvoorbeeld dat

$$u_1^8 = (1, 1, 1, 1, 0, 0, 0, 0) \quad u_2^8 = (1, 1, 0, 0, 1, 1, 0, 0) \quad u_3^8 = (1, 0, 1, 0, 1, 0, 1, 0).$$

Nog 'n manier om die $u_i^{2^n}$'s te beskou is as volg. Stel eerstens vir $u_1^2 := e_1^2 = (1, 0)$. Breek dan $R^{2^{n+1}}$, vir $n \geq 1$, op as $R^{2^n} \oplus R^{2^n}$ en stel $u_1^{2^{n+1}} := (1_{R^{2^n}}, 0_{R^{2^n}})$ en $u_j^{2^{n+1}} := (u_{j-1}^{2^n}, u_{j-1}^{2^n})$ vir $j = 1, 2, \dots, n+1$.

Lemma 2.9 ([11], Lemma 1) *Vir elke $n \geq 1$ is die versameling $\{u_1^{2^n}, \dots, u_n^{2^n}\}$ 'n versameling idempotente voortbringers van R^{2^n} , waar R 'n kommutatiewe ring en $u_1^{2^n}, \dots, u_n^{2^n}$ in (49) gedefinieer is.*

Bewys Ons bewys die lemma deur middel van induksie op n .

As $n = 1$, dan is $u_1^2 := e_1^2 = (1, 0)$. Verder is $1_{R^2} - e_1^2 = (1, 1) - (0, 1) = (1, 0)$. Aangesien $(1, 0)$ en $(0, 1)$ vir R^2 voortbring volg sodoende dat u_1^2 vir R^2 voortbring.

Gestel nou die versameling $\{u_1^{2^n}, \dots, u_n^{2^n}\}$ bring R^{2^n} voort vir 'n $n \geq 1$. Laat \mathbb{A} die R -subalgebra van $R^{2^{n+1}}$ voortgebring deur $\{u_1^{2^{n+1}}, \dots, u_{n+1}^{2^{n+1}}\}$ wees. Dan volg dat

$$\begin{aligned} (u_{j-1}^{2^n}, 0_{R^{2^n}}) &= (u_{j-1}^{2^n}, u_{j-1}^{2^n})(1_{R^{2^n}}, 0_{R^{2^n}}) \\ &= u_j^{2^{n+1}} u_1^{2^{n+1}} \in \mathbb{A} \end{aligned} \tag{50}$$

en dat

$$\begin{aligned} (0_{R^{2^n}}, u_{j-1}^{2^n}) &= (u_{j-1}^{2^n}, u_{j-1}^{2^n})(0_{R^{2^n}}, 1_{R^{2^n}}) \\ &= u_j^{2^{n+1}} (1_{R^{2^{n+1}}} - (1_{R^{2^n}}, 0_{R^{2^n}})) \\ &= u_j^{2^{n+1}} (1_{R^{2^{n+1}}} - u_1^{2^{n+1}}) \in \mathbb{A}, \end{aligned} \tag{51}$$

vir $j = 1, \dots, n+1$. Aangesien $\{(0_{R^{2^n}}, u_1^{2^n}), \dots, (0_{R^{2^n}}, u_n^{2^n})\}$ en $\{(u_1^{2^n}, 0_{R^{2^n}}), \dots, (u_n^{2^n}, 0_{R^{2^n}})\}$ vir $0_{R^{2^n}} \oplus R^{2^n}$ en vir $R^{2^n} \oplus 0_{R^{2^n}}$, onderskeidelik, volgens ons induksie hipotese, voortbring volg uit (50) en (51) dat $R^{2^{n+1}} = R^{2^n} \oplus R^{2^n} = (0 \oplus R^{2^n}) + (R^{2^n} \oplus 0) = \mathbb{A}$, waar "+" die optellingsoperasie van $R^{2^{n+1}}$ is. Die induksie is dus voltooi en die lemma is bewys.

□

Lemma 2.10 ([11], bladsy 607) *Die R -algebra R^m , met $m \geq 2$, waar R 'n kommutatiewe ring is, kan nie deur minder as $\lceil \log_2 m \rceil$ idempotente voortgebring word nie.*

Bewys Laat $p_1, \dots, p_{\lceil \log_2 m \rceil - 1}$ enige $\lceil \log_2 m \rceil - 1$ idempotente in R^m en P die versameling wat uit die identiteit van R^m en al die produkte van hierdie elemente bestaan, wees. Aangesien die produk van j van die p_i 's maar net p_i is en R kommutatief is, kan ons die elemente van P as die produkte van al $\lceil \log_2 m \rceil - 1$ elemente $p_1, \dots, p_{\lceil \log_2 m \rceil - 1}$, elk tot die mag 0 of 1 verhef, sien. Ons kan, byvoorbeeld, indien $m = 32$ en p_1, p_2, p_3 en p_4 idempotente in R^{32} is, die produk $p_1 p_3 p_4$ as die produk

$$(p_1)^1 (p_2)^0 (p_3)^1 (p_4)^1$$

sien. Die maksimum moontlike aantal elemente van P is dus $2^{\lceil \log_2 m \rceil - 1} < 2^{\log_2 m} = m$. Dit wil sê $|P| < m$. Laat \mathbb{A} die R -subalgebra van R^m voortgebring deur $p_1, \dots, p_{\lceil \log_2 m \rceil - 1}$ wees. Dan is

$$\mathbb{A} = \left\{ \begin{array}{l} a_1 p_1 + \dots + a_{\lceil \log_2 m \rceil} p_{\lceil \log_2 m \rceil - 1} + k 1_{R^m} + \sum_i s_i \cdot \mathbf{1}_i \\ \text{produk van elemente in } \{p_1, \dots, p_{\lceil \log_2 m \rceil - 1}\} \end{array} \mid a_1, \dots, a_{\lceil \log_2 m \rceil - 1}, k, s_i \in F \right\}.$$

Aangesien P uit die elemente en alle moontlike produkte van die versameling $\{p_1, \dots, p_{\lceil \log_2 m \rceil - 1}, 1_{R^m}\}$ bestaan, bestaan \mathbb{A} slegs uit somme en skalaarprodukte van P . Gevolglik is \mathbb{A} die R -submoduul voortgebring deur P . Die rang van \mathbb{A} is dus kleiner as m . Omdat die rang van R^m gelyk aan m is, volg dat $\mathbb{A} \subsetneq R^m$.

□

Stelling 2.11 ([11], Stelling 2) Laat R 'n kommutatiewe ring en $m \geq 2$ wees. Die minimum aantal idempotente $\nu = \nu(R^m)$ sodat R^m as 'n R -algebra deur ν idempotente voortgebring kan word, is $\lceil \log_2 m \rceil$.

Bewys Laat $m \geq 2$ wees. Dan is $m = 2^n$ of $2^{n-1} < m < 2^n$ vir 'n $n \in \mathbb{N}$.

Indien $m = 2^n$ volg uit Lemma 2.9 dat R^m deur $n = \log_2 m = \lceil \log_2 m \rceil$ elemente voortgebring kan word.

Indien $2^{n-1} < m < 2^n$, dan is R^m die homomorfe beeld van R^{2^n} onder die kanoniese afbeelding $\pi_{2^n, m}$ gedefinieer deur

$$\pi_{2^n, m} : (x_1, \dots, x_m, \dots, x_{2^n}) \mapsto (x_1, \dots, x_m).$$

Aangesien die kanoniese afbeelding 'n homomorfisme is en optelling en vermenigvuldiging sodoende behoue bly, volg uit Lemma 2.9 dat R^m ook in hierdie geval dan deur $n = \log_2 2^n = \lceil \log_2 m \rceil$ idempotente voortgebring kan word.

Volgens Lemma 2.10 kan R^m nie deur minder as $\lceil \log_2 m \rceil$ elemente voortgebring word nie. Gevolglik is $\nu(R^m) = \lceil \log_2 m \rceil$.

□

Aangesien Stelling 2.2 direk uit Stelling 2.11 volg, kan ons dus nou die minimum aantal idempotente om die F -algebras F^m voort te bring bepaal.

Vervolgens beskou ons die direkte somme $M_n^m(F)$, met $m \geq 2$ en $n \geq 2$, waar F 'n willekeurige liggaam is. Krupnik bepaal in ([12], Stelling 5) deur middel van die volgende resultaat die minimum aantal idempotente voortbringers vir die direkte somme $M_n^m(F)$, met $m \geq 2$ en $n \geq 2$, waar F 'n oneindige liggaam is.

Stelling 2.12 ([12], Stelling 5) *Laat F 'n oneindige liggaam en $n \geq 2$ wees. Dan is*

$$\nu(M_n^m(F)) = \begin{cases} 2 & \text{as } n = 2 \\ 3 & \text{as } n \geq 3. \end{cases}$$

Hierdie resultaat geld egter, soos ons aan die begin van die hoofstuk in Stelling 2.3 en Stelling 2.4 aangedui het, ook vir sekere eindige liggame. Hier volg die bewys van Stelling 2.3.

Die bewys van Stelling 2.3 Laat a_1, \dots, a_m , met $a_j \neq 0, 1$, verskillende elemente in F wees. Ons stel

$$P = \tilde{p}_1 \oplus \dots \oplus \tilde{p}_m \quad \text{en} \quad Q = \tilde{q}_1 \oplus \dots \oplus \tilde{q}_m$$

waar

$$\tilde{p}_j = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{en} \quad \tilde{q}_j = \begin{bmatrix} 1 & 0 \\ -a_j & 0 \end{bmatrix}, \quad j = 1, \dots, m.$$

Laat $\mathbb{B}_j = M_2(F)$, vir alle j , sodat

$$\mathbb{B} := \mathbb{B}_1 \oplus \dots \oplus \mathbb{B}_m = \underbrace{M_2(F) \oplus \dots \oplus M_2(F)}_{m \text{ kopieë}} = M_2^m(F)$$

en laat \mathbb{A} die F -subalgebra van \mathbb{B} voortgebring deur P en Q wees.

Omdat $|F| \geq m + 2$ en $m \geq 2$ volg dat $|F| \geq 4$ en dus dat $F \neq \mathbb{Z}_2$. Aangesien $\pi_j(\mathbb{A})$, waar $\pi_j : \mathbb{B} \rightarrow \mathbb{B}_j$ die kanoniese projeksie is, die algebra voortgebring deur \tilde{p}_j en \tilde{q}_j is, volg, vir alle j , uit Lemma 1.9 dat $\pi_j(\mathbb{A}) = M_2(F)$. Gevolglik is

$$\pi_j(\mathbb{A}) = M_2(F) = \pi_j(\mathbb{B})$$

vir alle j . Verder is

$$\begin{aligned}
(P - Q)^2 &= (\tilde{p}_1 - \tilde{q}_1)^2 \oplus \cdots \oplus (\tilde{p}_m - \tilde{q}_m)^2 \\
&= \begin{bmatrix} 0 & 1 \\ a_1 & 0 \end{bmatrix}^2 \oplus \cdots \oplus \begin{bmatrix} 0 & 1 \\ a_m & 0 \end{bmatrix}^2 \\
&= \begin{bmatrix} a_1 & 0 \\ 0 & a_1 \end{bmatrix} \oplus \cdots \oplus \begin{bmatrix} a_m & 0 \\ 0 & a_m \end{bmatrix} \\
&= a_1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \oplus \cdots \oplus a_m \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
\end{aligned}$$

waar $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ die identiteitselement van $\mathbb{B}_j = M_2(F)$, vir alle j , is. Omdat $(P - Q)^2 \in \mathbb{A}$, volg uit Lemma 2.8 dat $\mathbb{A} = \mathbb{B}$, sodat \mathbb{B} deur die idempotente P en Q voortgebring word.

□

Ons het die volgende resultaat gevind, wat ons in staat stel om 'n bogrens vir die minimum aantal idempotente voortbringers van 'n direkte som $M_2^m(F)$, met $|F| \leq m + 1$, te bepaal.

Gevolg 2.13 *Laat F 'n eindige liggaam wees, met $m \geq 2$ en $|F| \leq m + 1$. Dan is*

$$\nu(M_2^m(F)) \leq \begin{cases} \left\lceil \log_2 \left\lceil \frac{m}{|F|-2} \right\rceil \right\rceil + 2 & \text{as } |F| \geq 3 \\ \lceil \log_2 m \rceil + 3 & \text{as } F = \mathbb{Z}_2. \end{cases}$$

Bewys Gestel $|F| \geq 3$. Laat $\left\lfloor \frac{m}{|F|-2} \right\rfloor = l$, $\left\lceil \frac{m}{|F|-2} \right\rceil = k$, $\mathbb{B}_1 = \underbrace{M_2(F) \oplus \cdots \oplus M_2(F)}_{|F|-2 \text{ keer}}$ en, indien $m - l(|F| - 2) > 0$, $\mathbb{B}_2 = \underbrace{M_2(F) \oplus \cdots \oplus M_2(F)}_{m-l(|F|-2) \text{ keer}}$ wees. Dan volg dat

$$M_2^m(F) = \underbrace{\mathbb{B}_1 \oplus \cdots \oplus \mathbb{B}_1}_{l \text{ keer}} \oplus \mathbb{B}_2 \quad \text{indien } m - l(|F| - 2) > 0$$

of

$$M_2^m(F) = \underbrace{\mathbb{B}_1 \oplus \cdots \oplus \mathbb{B}_1}_{l \text{ keer}} \quad \text{indien } m - l(|F| - 2) = 0.$$

Eerstens, aangesien $(|F| - 2) + 2 = |F|$ volg uit Stelling 2.3 dat \mathbb{B}_1 deur 2 idempotente, sê p_1 en p_2 , voortgebring kan word. Tweedens, aangesien

$$m = l(|F| - 2) + r, \quad \text{met } 0 \leq r < |F| - 2,$$

volgens die delingsalgoritme, volg dat $(m - l(|F| - 2)) + 2 = r + 2 < (|F| - 2) + 2 = |F|$. Sodoende volg uit Stelling 2.3 dat \mathbb{B}_2 ook deur 2 idempotente, sê q_1 en q_2 , voortgebring kan word.

Ons beskou nou die subalgebra \mathbb{A} van $M_2^m(F)$, voortgebring deur

$$1_{\mathbb{B}_1} \oplus 0 \oplus \cdots \oplus 0, \quad \dots, \quad 0 \oplus \cdots \oplus 0 \oplus 1_{\mathbb{B}_1} \oplus 0, \quad 0 \oplus \cdots \oplus 0 \oplus 1_{\mathbb{B}_2}, \quad (52)$$

indien $m - l(|F| - 2) > 0$, of deur

$$1_{\mathbb{B}_1} \oplus 0 \oplus \cdots \oplus 0, \quad \dots, \quad 0 \oplus \cdots \oplus 0 \oplus 1_{\mathbb{B}_1}, \quad (53)$$

indien $m - l(|F| - 2) = 0$, waar $1_{\mathbb{B}_1}$ en $1_{\mathbb{B}_2}$ die identiteitselemente van \mathbb{B}_1 en \mathbb{B}_2 , onderskeidelik, is. Aangesien \mathbb{A} slegs bestaan uit skalaar produkte van die elemente in (52), indien $m - l(|F| - 2) > 0$, of die elemente in (53), indien $m - l(|F| - 2) = 0$, is \mathbb{A} inderwaarheid slegs k kopieë van F en dus isomorf aan F^k . Volgens Stelling 2.11 kan \mathbb{A} deur $\lceil \log_2 k \rceil$ idempotente, sê $v_1, \dots, v_{\lceil \log_2 k \rceil}$, voortgebring word. Dit wil sê $v_1, \dots, v_{\lceil \log_2 k \rceil}$ kan in die besonder die elemente in (52), indien $m - l(|F| - 2) > 0$, of in (53), indien $m - l(|F| - 2) = 0$, voortbring. Gevolglik, indien $m - l(|F| - 2) > 0$, kan die idempotente,

$$v_1, \dots, v_{\lceil \log_2 k \rceil}, \quad p_1 \oplus \cdots \oplus p_1 \oplus q_1 \quad \text{en} \quad p_2 \oplus \cdots \oplus p_2 \oplus q_2,$$

die idempotente,

$$\begin{aligned} p_1 \oplus 0 \oplus \cdots \oplus 0, \quad 0 \oplus p_1 \oplus 0 \oplus \cdots \oplus 0, \quad \dots, \quad 0 \oplus \cdots \oplus 0 \oplus p_1 \oplus 0, \\ p_2 \oplus 0 \oplus \cdots \oplus 0, \quad 0 \oplus p_2 \oplus 0 \oplus \cdots \oplus 0, \quad \dots, \quad 0 \oplus \cdots \oplus 0 \oplus p_2 \oplus 0, \\ 0 \oplus \cdots \oplus 0 \oplus q_1, \quad 0 \oplus \cdots \oplus 0 \oplus q_2, \end{aligned}$$

en dus die hele $M_2^m(F)$ voortbring; of, indien $m - l(|F| - 2) = 0$, kan die idempotente,

$$v_1, \dots, v_{\lceil \log_2 k \rceil}, \quad p_1 \oplus \cdots \oplus p_1 \quad \text{en} \quad p_2 \oplus \cdots \oplus p_2,$$

die idempotente,

$$\begin{aligned} p_1 \oplus 0 \oplus \cdots \oplus 0, \quad 0 \oplus p_1 \oplus 0 \oplus \cdots \oplus 0, \quad \dots, \quad 0 \oplus \cdots \oplus 0 \oplus p_1, \\ p_2 \oplus 0 \oplus \cdots \oplus 0, \quad 0 \oplus p_2 \oplus 0 \oplus \cdots \oplus 0, \quad \dots, \quad 0 \oplus \cdots \oplus 0 \oplus p_2, \end{aligned}$$

en dus die hele $M_2^m(F)$ voortbring. Dit beteken

$$\nu(M_2^m(F)) \leq \lceil \log_2 k \rceil + 2 = \left\lceil \log_2 \left\lceil \frac{m}{|F| - 2} \right\rceil \right\rceil + 2.$$

Gestel nou $F = \mathbb{Z}_2$. Dan kan $M_2(\mathbb{Z}_2)$ volgens Stelling 1.1 deur drie idempotente, sê p , q en r , voortgebring word.

Ons beskou nou die subalgebra \mathbb{A} van $M_2^m(\mathbb{Z}_2)$, voortgebring deur

$$I_2 \oplus 0 \oplus \cdots \oplus 0, \quad \dots, \quad 0 \oplus \cdots \oplus 0 \oplus I_2. \quad (54)$$

Aangesien ons \mathbb{A} as m kopieë van F kan sien en dus volg dat \mathbb{A} isomorf is aan F^m , kan \mathbb{A} , en dus in die besonder die elemente in (54), volgens Stelling 2.11 deur $\lceil \log_2 m \rceil$ idempotente, sê $v_1, \dots, v_{\lceil \log_2 m \rceil}$, voortgebring word.

Sodoende volg dat die idempotente,

$$v_1, \dots, v_{\lceil \log_2 m \rceil}, \quad p \oplus \cdots \oplus p, \quad q \oplus \cdots \oplus q, \quad r \oplus \cdots \oplus r,$$

die idempotente,

$$\begin{aligned} p \oplus 0 \oplus \cdots \oplus 0, & \quad 0 \oplus p \oplus 0 \oplus \cdots \oplus 0, & \dots, & \quad 0 \oplus \cdots \oplus 0 \oplus p, \\ q \oplus 0 \oplus \cdots \oplus 0, & \quad 0 \oplus q \oplus 0 \oplus \cdots \oplus 0, & \dots, & \quad 0 \oplus \cdots \oplus 0 \oplus q, \\ r \oplus 0 \oplus \cdots \oplus 0, & \quad 0 \oplus r \oplus 0 \oplus \cdots \oplus 0, & \dots, & \quad 0 \oplus \cdots \oplus 0 \oplus r, \end{aligned}$$

en dus die hele $M_2^m(\mathbb{Z}_2)$ voortbring. Gevolglik is

$$\nu(M_2^m(\mathbb{Z}_2)) \leq \lceil \log_2 m \rceil + 3.$$

□

Voorbeelde Ons beskou 'n paar voorbeelde waar ons van Stelling 1.1, Stelling 2.3 en Gevolg 2.13 gebruik maak.

Laat $F = \mathbb{Z}_2$. Aangesien die kanoniese afbeelding π_i van $M_2^m(\mathbb{Z}_2)$ op $M_2(\mathbb{Z}_2)$ 'n surjektiewe homomorfisme is en uit Stelling 1.1 volg dat $\nu(2, \mathbb{Z}_2) = 3$ weet ons reeds dat $\nu(M_2^m(F)) \geq 3$. Deur nou van die bogenoemde resultate gebruik te maak, volg, byvoorbeeld, dat

$$\begin{aligned} \nu(M_2(\mathbb{Z}_2)) &= 3 \\ 3 &\leq \nu(M_2^2(\mathbb{Z}_2)) \leq \lceil \log_2 2 \rceil + 3 = 4 \\ 3 &\leq \nu(M_2^3(\mathbb{Z}_2)) \leq \lceil \log_2 3 \rceil + 3 = 5 \\ 3 &\leq \nu(M_2^4(\mathbb{Z}_2)) \leq \lceil \log_2 4 \rceil + 3 = 5 \\ 3 &\leq \nu(M_2^5(\mathbb{Z}_2)) \leq \lceil \log_2 5 \rceil + 3 = 6 \end{aligned}$$

Laat $|F| \geq 3$. Aangesien uit Stelling 1.1 volg dat $\nu(M_2(F)) = 2$ volg, soortgelyk as in die geval waar $F = \mathbb{Z}_2$, dat $\nu(M_2^m(F)) \geq 2$. Deur nou weereens van die bogenoemde resultate gebruik te maak, volg, byvoorbeeld, dat

$$\begin{aligned}
\nu(M_2(\mathbb{Z}_3)) &= 2 \\
2 \leq \nu(M_2^2(\mathbb{Z}_3)) &\leq \lceil \log_2 2 \rceil + 2 = 3 \\
2 \leq \nu(M_2^3(\mathbb{Z}_3)) &\leq \lceil \log_2 3 \rceil + 2 = 4 \\
2 \leq \nu(M_2^4(\mathbb{Z}_3)) &\leq \lceil \log_2 4 \rceil + 2 = 4 \\
2 \leq \nu(M_2^5(\mathbb{Z}_3)) &\leq \lceil \log_2 5 \rceil + 2 = 5 \\
\nu(M_2(GF(4))) &= 2 \\
\nu(M_2^2(GF(4))) &= 2 \\
2 \leq \nu(M_2^3(GF(4))) &\leq \lceil \log_2 \lceil \frac{3}{2} \rceil \rceil + 2 = 3 \\
2 \leq \nu(M_2^4(GF(4))) &\leq \lceil \log_2 \lceil \frac{4}{2} \rceil \rceil + 2 = 3 \\
2 \leq \nu(M_2^5(GF(4))) &\leq \lceil \log_2 \lceil \frac{5}{2} \rceil \rceil + 2 = 4 \\
2 \leq \nu(M_2^6(GF(4))) &\leq \lceil \log_2 \lceil \frac{6}{2} \rceil \rceil + 2 = 4 \\
2 \leq \nu(M_2^7(GF(4))) &\leq \lceil \log_2 \lceil \frac{7}{2} \rceil \rceil + 2 = 4 \\
2 \leq \nu(M_2^8(GF(4))) &\leq \lceil \log_2 \lceil \frac{8}{2} \rceil \rceil + 2 = 4 \\
2 \leq \nu(M_2^9(GF(4))) &\leq \lceil \log_2 \lceil \frac{9}{2} \rceil \rceil + 2 = 5,
\end{aligned}$$

waar $GF(4)$ die galois liggaam met vier elemente is.

□

Ons beskou nou volgende die direkte somme $M_n^m(F)$, met $m \geq 2$ en $n \geq 3$. Voor ons Stelling 2.4 bewys, beskou ons eers magte van die matrikse $D_{n,\alpha}^{(1)}, a_{n,\alpha} \in M_n(F)$, waar $\alpha \neq 0$ 'n element van die liggaam F is, wat ons as volg definieer:

$$\begin{aligned}
D_{n,\alpha}^{(1)} &= D_n^{(1)} + (\alpha - 1)e_{12} & a_{n,\alpha} &= a_n + (\alpha - 1)e_{12} \\
&= \begin{bmatrix} 0 & \alpha & & & \circ \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ \circ & & & & 0 \end{bmatrix} & & = \begin{bmatrix} 0 & \alpha & 0 & & \circ \\ & 0 & 1 & 0 & \\ \circ & & \ddots & \ddots & \ddots \\ & & & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 \end{bmatrix}, & (55)
\end{aligned}$$

waar a_n in (7) en $D_n^{(1)}$ in (16) gedefinieer is. In die volgende twee lemmas sal ons algebraïes bewys dat

$$D_{n,\alpha}^{(2)} := (D_{n,\alpha}^{(1)})^2 = \begin{array}{c} \text{kolom 3} \\ \downarrow \\ \left[\begin{array}{cccc} 0 & 0 & \alpha & \circ \\ & 0 & 0 & 1 \\ & & \ddots & \ddots \\ & & & 0 & 0 & 1 \\ & & & & 0 & 0 \\ \circ & & & & & 0 \end{array} \right] \end{array} = D_n^{(2)} + (\alpha - 1)e_{13}$$

$$D_{n,\alpha}^{(3)} := (D_{n,\alpha}^{(1)})^3 = \begin{array}{c} \text{kolom 4} \\ \downarrow \\ \left[\begin{array}{cccc} 0 & \alpha & & \circ \\ & 0 & 1 & \\ & & \ddots & \ddots \\ & & & 0 & 1 \\ & & & & 0 \end{array} \right] \end{array} = D_n^{(3)} + (\alpha - 1)e_{14}$$

$$\vdots \quad \quad \quad \vdots$$

$$D_{n,\alpha}^{(n-1)} := (D_{n,\alpha}^{(1)})^{(n-1)} = \begin{array}{c} \text{kolom } n \\ \downarrow \\ \left[\begin{array}{cccc} 0 & 0 & \dots & 0 & \alpha \\ & 0 & & & 0 \\ & & \ddots & & \\ \circ & & & & 0 \end{array} \right] \end{array} = D_n^{(n-1)} + (\alpha - 1)e_{1n}$$

$$D_{n,\alpha}^{(n)} := (D_{n,\alpha}^{(1)})^{(n)} = \left[\circ \right]$$

$$\text{en dat } a_{n,\alpha}^2 = \begin{array}{c} \text{kolom 3} \\ \downarrow \\ \left[\begin{array}{cccc} 0 & \alpha & & \circ \\ & 0 & 1 & \\ & & \ddots & \ddots \\ 0 & \dots & & 0 & 1 \\ 1 & 0 & & & \\ 0 & \alpha & 0 & & \end{array} \right] \end{array} \quad \leftarrow \text{ry } n-2$$

$$\begin{aligned}
&= \underbrace{\begin{bmatrix} & & \text{kolom 3} & & \\ & & \downarrow & & \\ & 0 & 1 & & \circ \\ & & 0 & 1 & \\ & & & \ddots & \ddots \\ 0 & & & \cdots & 0 & 1 \\ 1 & 0 & & & & \\ 0 & 1 & 0 & & & \end{bmatrix}}_{=a_n^2} + (\alpha - 1) \underbrace{\begin{bmatrix} & & \text{kolom 3} & & \\ & & \downarrow & & \\ & 0 & 1 & & \circ \\ & & 0 & 0 & \\ & & & \ddots & \ddots \\ 0 & & & \cdots & 0 & 0 \\ 0 & 0 & & & & \\ 0 & 1 & 0 & & & \end{bmatrix}}_{e_{13}+e_{n2}} \leftarrow \text{ry } n-2 \\
a_{n,\alpha}^3 &= \begin{bmatrix} & & & & \text{kolom 4} & & \\ & & & & \downarrow & & \\ & & 0 & \alpha & & & \circ \\ & & 0 & 1 & & & \\ & & & \ddots & \ddots & & \\ 0 & & & \cdots & 0 & 1 & \\ 1 & 0 & & & & & \\ & \alpha & 0 & & & & \\ \circ & & \alpha & 0 & & & \end{bmatrix} \leftarrow \text{ry } n-3 \\
&= \underbrace{\begin{bmatrix} & & & & \text{kolom 4} & & \\ & & & & \downarrow & & \\ & & 0 & 1 & & & \circ \\ & & 0 & 1 & & & \\ & & & \ddots & \ddots & & \\ 0 & & & \cdots & 0 & 1 & \\ 1 & 0 & & & & & \\ & 1 & 0 & & & & \\ \circ & & 1 & 0 & & & \end{bmatrix}}_{=a_n^3} + (\alpha - 1) \underbrace{\begin{bmatrix} & & & & \text{kolom 4} & & \\ & & & & \downarrow & & \\ & & 0 & 1 & & & \circ \\ & & 0 & 0 & & & \\ & & & \ddots & \ddots & & \\ 0 & & & \cdots & 0 & 0 & \\ 0 & 0 & & & & & \\ & 1 & 0 & & & & \\ \circ & & 1 & 0 & & & \end{bmatrix}}_{e_{14}+e_{n3}+e_{n-1,2}} \leftarrow \text{ry } n-3 \\
&\vdots \\
a_{n,\alpha}^{n-1} &= \begin{bmatrix} & & & & \text{kolom } n & & \\ & & & & \downarrow & & \\ 0 & \cdots & & 0 & \alpha & & \\ 1 & 0 & & & & & \\ & \alpha & 0 & & & & \\ & & \ddots & \ddots & & & \\ \circ & & & \alpha & 0 & & \\ & & & & \alpha & 0 & \end{bmatrix} \leftarrow \text{ry } n-(n-1)
\end{aligned}$$

$$\begin{aligned}
&= \underbrace{\begin{bmatrix} 0 & \cdots & 0 & 1 \\ 1 & 0 & & \\ & 1 & 0 & \\ & & \ddots & \ddots \\ \circ & & & 1 & 0 \\ & & & & 1 & 0 \end{bmatrix}}_{=a_n^{n-1}} + (\alpha - 1) \underbrace{\begin{bmatrix} 0 & \cdots & 0 & 1 \\ 0 & 0 & & \\ & 1 & 0 & \\ & & \ddots & \ddots \\ \circ & & & 1 & 0 \\ & & & & 1 & 0 \end{bmatrix}}_{e_{1n}+e_{n,n-1}+e_{n-1,n-2}+\cdots+e_{32}} \leftarrow \text{ry } n - (n - 1) \\
a_{n,\alpha}^n &= \begin{bmatrix} \alpha & \circ \\ & \ddots \\ \circ & \alpha \end{bmatrix} = I_n + (\alpha - 1)I_n = \alpha I_n.
\end{aligned}$$

Lemma 2.14 *Laat $D_{n,\alpha}$ soos in (55) gedefinieer wees. Dan volg dat*

$$D_{n,\alpha}^{(k)} = \begin{cases} D_n^{(k)} + (\alpha - 1)e_{1,k+1} & \text{as } 1 \leq k \leq n - 1 \\ 0 & \text{as } k = n. \end{cases}$$

Bewys Ons bewys die resultaat deur middel van induksie op k . Volgens die definisie van $D_{n,\alpha}^{(1)}$ is die stelling waar vir $k = 1$. Gestel die stelling is waar vir 'n $1 \leq k \leq n - 1$. Dan is

$$\begin{aligned}
D_{n,\alpha}^{(k+1)} &= (D_n^{(k)} + (\alpha - 1)e_{1,k+1})(D_n^{(1)} + (\alpha - 1)e_{12}) \\
&= D_n^{(k+1)} + (\alpha - 1)e_{1,k+1}D_n^{(1)} + \underbrace{(\alpha - 1)D_n^{(k)}e_{12}}_{=0} + \underbrace{(\alpha - 1)^2e_{1,k+1}e_{12}}_{=0} \\
&= \begin{cases} D_n^{(k+1)} + (\alpha - 1)e_{1,(k+1)+1} & \text{as } 2 \leq k + 1 \leq n - 1 \\ 0 & \text{as } k + 1 = n \end{cases} \quad (56)
\end{aligned}$$

waar (56) volg uit (18), (19) en (20). Die induksie is dus voltooi en die lemma bewys. □

Lemma 2.15 *Laat $a_{n,\alpha}$ soos in (55) gedefinieer wees. Dan volg dat*

$$a_{n,\alpha}^k = \begin{cases} a_n^k + (\alpha - 1)(e_{1,k+1} + e_{nk} + e_{n-1,k-1} + \cdots + e_{n-(k-2),2}) & \text{as } 1 \leq k \leq n - 1 \\ \alpha I_n & \text{as } k = n. \end{cases}$$

Bewys Ons bewys die resultaat deur middel van induksie op k . Volgens die definisie van $a_{n,\alpha}$ is die stelling waar vir $k = 1$. Gestel die stelling is waar vir 'n k sodat $1 \leq k \leq n - 1$. Dan is

$$\begin{aligned}
a_{n,\alpha}^{k+1} &= a_{n,\alpha}^k a_{n,\alpha} \\
&= (a_n^k + (\alpha - 1)(e_{1,k+1} + e_{nk} + e_{n-1,k-1} + \cdots + e_{n-(k-2),2}))(a_n + (\alpha - 1)e_{12}) \\
&= \begin{cases} a_n^{k+1} + (\alpha - 1)(e_{1,k+2} + e_{n,k+1} + e_{n-1,k} + \cdots + e_{n-(k-2),3}) & \text{as } 1 < k \leq n - 2 \\ +(\alpha - 1)e_{n-k+1,2} & \end{cases} \quad (57) \\
&= \begin{cases} a_n^n + (\alpha - 1)(e_{11} + e_{nn} + e_{n-1,n-1} + \cdots + e_{33}) & \text{as } k = n - 1 \\ +(\alpha - 1)e_{22} & \end{cases} \\
&= \begin{cases} a_n^{k+1} + (\alpha - 1)(e_{1,(k+1)+1} + e_{n,(k+1)} + e_{n-1,(k+1)-1} + \cdots & \text{as } 2 \leq k + 1 < n \\ \cdots + e_{n-((k+1)-2),2}) & \\ \alpha I_n & \text{as } k + 1 = n, \end{cases}
\end{aligned}$$

waar (57) volg uit (10), (11) en (12). Die induksie is dus voltooi en die lemma bewys. □

Ons gebruik die volgende welbekende formule, genoem Lagrange se Interpolasie Formule, in Stelling 2.4.

Stelling 2.16 (*LAGRANGE SE INTERPOLASIE FORMULE*) ([9], Hoofstuk 6, Oefening nr. 12) As F 'n liggaam, a_0, a_1, \dots, a_n verskillende elemente van F en c_0, c_1, \dots, c_n enige elemente van F is, dan is

$$f(x) = \sum_{i=0}^n \frac{(x - a_0) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n)}{(a_i - a_0) \cdots (a_i - a_{i-1})(a_i - a_{i+1}) \cdots (a_i - a_n)} c_i$$

die unieke polinoom van graad hoogstens n in $F[x]$ sodat $f(a_i) = c_i$ vir alle i .

Die bewys van Stelling 2.4 Laat $\alpha \neq 0$ enige element in F wees. Ons stel

$$p_{n,\alpha} = p_n + (\alpha - 1)e_{12}$$

$$q_{n,\alpha} = q_n$$

$$= \begin{bmatrix} 1 & \alpha & & & \\ & 0 & 0 & & \circ \\ & & 1 & 1 & \\ & & & 0 & 0 \\ & & & & \ddots \\ \circ & & & & \ddots \end{bmatrix}, \quad = \begin{bmatrix} 0 & 0 & & & \\ & 1 & 1 & & \circ \\ & & 0 & 0 & \\ & & & 1 & 1 \\ & & & & \ddots \\ \circ & & & & \ddots \end{bmatrix}$$

en

$$r_{n,\alpha} = e_{n1} + e_{nn}$$

$$= \begin{bmatrix} & & & & \\ & & \circ & & \\ & & & & \\ 1 & 0 & \cdots & 0 & 1 \end{bmatrix},$$

waar p_n en q_n in (4) en (5), onderskeidelik, gedefinieer is.

Aangesien

$$\begin{aligned} p_{n,\alpha} + q_{n,\alpha} - I_n &= p_n + q_n - I_n + (\alpha - 1)e_{12} \\ &= D_n^{(1)} + (\alpha - 1)e_{12} \\ &= D_{n,\alpha}^{(1)} \end{aligned}$$

volg deur van Lemma 2.14 gebruik te maak dat

$$\begin{aligned} & r_{n,\alpha} \left(I_n - \frac{1}{\alpha} (p_{n,\alpha} + q_{n,\alpha} - I_n)^{n-1} \right) \\ &= r_{n,\alpha} \left(I_n - \frac{1}{\alpha} D_{n,\alpha}^{(n-1)} \right) \\ &= \begin{bmatrix} & & & & \\ & & \circ & & \\ & & & & \\ 1 & 0 & \cdots & 0 & 1 \end{bmatrix} \left(\begin{bmatrix} 1 & & & & \circ \\ & \ddots & & & \\ & & 1 & & \\ \circ & & & & 1 \end{bmatrix} - \frac{1}{\alpha} \begin{bmatrix} & & & & \alpha \\ & & & & \\ & & & & \\ & & & & \circ \end{bmatrix} \right) \end{aligned}$$

$$\begin{aligned}
&= \begin{bmatrix} & & & & \\ & & \circ & & \\ & & & & \\ & 1 & 0 & \cdots & 0 & 1 \\ & & & & & \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 & -1 \\ & 1 & & & \\ & & \ddots & & \circ \\ & & & 1 & \\ \circ & & & & 1 \end{bmatrix} \\
&= \begin{bmatrix} & \circ \\ 1 & \end{bmatrix} = e_{n1}. \tag{58}
\end{aligned}$$

Verder is

$$\begin{aligned}
e_{n1} + p_{n,\alpha} + q_{n,\alpha} - I_n &= e_{n1} + D_n^{(1)} + (\alpha - 1)e_{12} \\
&= a_n + (\alpha - 1)e_{12} \\
&= a_{n,\alpha} \tag{59}
\end{aligned}$$

en volg uit (10), (11) en Lemma 2.15 , vir willekeurige $j, l \in \{1, \dots, n\}$, dat

$$\begin{aligned}
&a_{n,\alpha}^{n-j} e_{n1} \\
&= \begin{cases} a_n^{n-j} e_{n1} + (\alpha - 1)(e_{1,n-j+1} + e_{n,n-j} + e_{n-1,n-j-1} + \cdots \\ \cdots + e_{n-(n-j-2),2}) e_{n1} & \text{as } 1 \leq j \leq n-1 \\ a_{n,\alpha}^0 e_{n1} = I_n e_{n1} = e_{n1} & \text{as } j = n \end{cases} \\
&= \begin{cases} e_{n-(n-1),1} + (\alpha - 1)e_{11} = e_{11} + (\alpha - 1)e_{11} & \text{as } j = 1 & \text{(uit (10))} \\ a_n^{n-j} e_{n1} + 0 = e_{n-(n-j),1} = e_{j1} & \text{as } 2 \leq j \leq n-1 & \text{(uit (10))} \\ e_{n1} & \text{as } j = n \end{cases} \\
&= \begin{cases} \alpha e_{11} & \text{as } j = 1 \\ e_{j1} & \text{as } 2 \leq j \leq n \end{cases}
\end{aligned}$$

en sodoende dat

$$\begin{aligned}
&a_{n,\alpha}^{n-j} e_{n1} a_{n,\alpha}^{l-1} \\
&= \begin{cases} a_{n,\alpha}^{n-j} e_{n1} a_n^{l-1} + a_{n,\alpha}^{n-j} e_{n1} (\alpha - 1)(e_{1l} + e_{n,l-1} + \cdots + e_{n-(l-1-2),2}) & \text{as } 2 \leq l \leq n \\ a_{n,\alpha}^{n-j} e_{n1} & \text{as } l = 1 \end{cases} \\
&= \begin{cases} \alpha e_{11} a_n^{l-1} + \alpha e_{11} (\alpha - 1)(e_{1l} + e_{n,l-1} + \cdots + e_{n-l+3,2}) & \text{as } j = 1 & \text{en } 2 \leq l \leq n \\ e_{j1} a_n^{l-1} + e_{j1} (\alpha - 1)(e_{1l} + e_{n,l-1} + \cdots + e_{n-l+3,2}) & \text{as } 2 \leq j \leq n & \text{en } 2 \leq l \leq n \\ \alpha e_{11} & \text{as } j = 1 & \text{en } l = 1 \\ e_{j1} & \text{as } 2 \leq j \leq n & \text{en } l = 1 \end{cases}
\end{aligned}$$

$$\begin{aligned}
&= \begin{cases} \alpha e_{1l} + \alpha(\alpha - 1)e_{1l} & \text{as } j = 1 & \text{en } 2 \leq l \leq n & \text{(uit (11))} \\ e_{jl} + (\alpha - 1)e_{jl} & \text{as } 2 \leq j \leq n & \text{en } 2 \leq l \leq n & \text{(uit (11))} \\ \alpha e_{11} & \text{as } j = 1 & \text{en } l = 1 \\ e_{j1} & \text{as } 2 \leq j \leq n & \text{en } l = 1 \end{cases} \\
&= \begin{cases} \alpha^2 e_{1l} & \text{as } j = 1 & \text{en } 2 \leq l \leq n \\ \alpha e_{jl} & \text{as } 2 \leq j \leq n & \text{en } 2 \leq l \leq n \\ \alpha e_{11} & \text{as } j = 1 & \text{en } l = 1 \\ e_{j1} & \text{as } 2 \leq j \leq n & \text{en } l = 1. \end{cases} \tag{60}
\end{aligned}$$

Aangesien F 'n liggaam is en $\alpha^2, \alpha \in F$ dus 'n inverse in F het (want $\alpha \neq 0$ en dus $\alpha^2 \neq 0$), volg uit (58), (59) en (60) dat ons e_{jl} ($j, l = 1, \dots, n$) deur middel van $p_{n,\alpha}$, $q_{n,\alpha}$ en $r_{n,\alpha}$ kan voortbring.

Omdat ons elke element A van $M_n(F)$ kan uitdruk as

$$A = \sum_{j,l=1}^n s_{jl} e_{jl}, \quad \text{waar } s_{jl} \in F,$$

volg sodoende dat $p_{n,\alpha}$, $q_{n,\alpha}$ en $r_{n,\alpha}$ vir $M_n(F)$ voortbring.

Laat $\alpha_1, \dots, \alpha_m$, met $\alpha_j \neq 0$, verskillende elemente in F wees. Ons stel nou

$$P_n = p_{n,\alpha_1} \oplus \dots \oplus p_{n,\alpha_m}, \quad Q_n = q_{n,\alpha_1} \oplus \dots \oplus q_{n,\alpha_m} \quad \text{en} \quad R_n = r_{n,\alpha_1} \oplus \dots \oplus r_{n,\alpha_m}.$$

Laat $\mathbb{B}_j := M_n(F)$ ($j = 1, \dots, m$) sodat $\mathbb{B} := \mathbb{B}_1 \oplus \dots \oplus \mathbb{B}_m = \underbrace{M_n(F) \oplus \dots \oplus M_n(F)}_{m \text{ kopieë}}$ en laat \mathbb{A} die subalgebra van \mathbb{B} voortgebring deur P_n , Q_n en R_n wees.

Aangesien $\pi_j(\mathbb{A})$ die algebra voortgebring deur p_{n,α_j} , q_{n,α_j} en r_{n,α_j} is, volg dat $\pi_j(\mathbb{A}) = M_n(F)$. Indien ons kan bewys dat $\alpha_1 I_n \oplus \dots \oplus \alpha_m I_n \in \mathbb{A}$ volg uit Lemma 2.8 dat $\mathbb{A} = \mathbb{B}$ en ons is klaar.

Aangesien $0, \alpha_1, \dots, \alpha_m$ verskillende elemente van F is, bestaan daar volgens Lagrange se Interpolasie Formule (Stelling 2.16) 'n polinoom $f(x) \in F[x]$ van graad m , naamlik

$$f(x) = \frac{(x - \alpha_1) \cdots (x - \alpha_m)}{(-\alpha_1) \cdots (\alpha_m)} \cdot 0 + \sum_{j=1}^m \frac{x(x - \alpha_1) \cdots (x - \alpha_{j-1})(x - \alpha_{j+1}) \cdots (x - \alpha_m)}{\alpha_j(\alpha_j - \alpha_1) \cdots (\alpha_j - \alpha_{j-1})(\alpha_j - \alpha_{j+1}) \cdots (\alpha_j - \alpha_m)} \cdot 1$$

sodat $f(\alpha_j) = 1$. (Ons het $c_0 = 0$ en $c_j = 1$ vir $j = 1, \dots, m$ gekies.)

Aangesien

$$r_{n,\alpha}(p_{n,\alpha} + q_{n,\alpha} - I_n)^{n-1} = (e_{n1} + e_{nn})\alpha e_{1n} = \alpha e_{nn}$$

vir alle $\alpha \in F$, volg dat

$$R_n(P_n + Q_n - e)^{n-1} = \alpha_1 e_{nn} \oplus \cdots \oplus \alpha_m e_{nn},$$

waar $e = \underbrace{I_n \oplus \cdots \oplus I_n}_{m \text{ keer}}$ die identiteit van $M_n^m(F)$ is. Omdat $\theta : F \rightarrow M_n(F)$ gedefinieer deur

$$\theta(y) = ye_{nn} = \begin{bmatrix} \circ & & & \\ & & & \\ & & & \\ & & & y \end{bmatrix}$$

'n homomorfisme is, volg dat

$$\begin{aligned} f(R_n(P_n + Q_n - e)^{n-1}) &= f(\alpha_1 e_{nn} \oplus \cdots \oplus \alpha_m e_{nn}) \\ &= f(\alpha_1 e_{nn}) \oplus \cdots \oplus f(\alpha_m e_{nn}) \\ &= f(\theta(\alpha_1)) \oplus \cdots \oplus f(\theta(\alpha_m)) \\ &= \theta(f(\alpha_1)) \oplus \cdots \oplus \theta(f(\alpha_m)) \\ &= \underbrace{\theta(1) \oplus \cdots \oplus \theta(1)}_{m \text{ keer}} \\ &= \underbrace{e_{nn} \oplus \cdots \oplus e_{nn}}_{m \text{ keer}}. \end{aligned}$$

Met behulp van (59) volg sodoende dat

$$\begin{aligned} &(P_n + Q_n - e + R_n - f(R_n(P_n + Q_n - I_n)^{n-1}))^n \\ &= (P_n + Q_n - e + \underbrace{e_{n1} \oplus \cdots \oplus e_{n1}}_{m \text{ keer}})^n \\ &= \begin{bmatrix} 0 & \alpha_1 & 0 & & \circ \\ & 0 & 1 & 0 & \\ \circ & & \ddots & \ddots & \ddots \\ & & & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 \end{bmatrix}^n \oplus \cdots \oplus \begin{bmatrix} 0 & \alpha_m & 0 & & \circ \\ & 0 & 1 & 0 & \\ \circ & & \ddots & \ddots & \ddots \\ & & & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 \end{bmatrix}^n \\ &= a_{n,\alpha_1}^n \oplus \cdots \oplus a_{n,\alpha_m}^n \\ &= \alpha_1 I_n \oplus \cdots \oplus \alpha_m I_n \in \mathbb{A}. \end{aligned}$$

□

Ons kan vir 'n direkte som $M_n^m(F)$, met $n \geq 3$, $m \geq 2$ en $|F| \leq m$, soortgelyk aan die geval waar $n = 2$, $m \geq 2$ en $|F| \leq m + 1$, deur middel van die volgende resultaat, 'n bogrens vir die minimum aantal idempotente voortbringers bepaal. Aangesien die bewys van Gevolg 2.17 soortgelyk aan die bewys van Gevolg 2.13 is, formuleer ons slegs die resultaat sonder bewys.

Gevolg 2.17 Laat $m \geq 2$ en $n \geq 3$. Vir enige eindige liggaam F , met $|F| \leq m$ is

$$\nu(M_n^m(F)) \leq \left\lceil \log_2 \left\lceil \frac{m}{|F| - 1} \right\rceil \right\rceil + 3.$$

Voorbeelde Ons beskou 'n paar voorbeelde waar ons van Stelling 1.1, Stelling 2.4 en Gevolg 2.17 gebruik maak.

Aangesien die kanoniese afbeelding π_i van $M_n^m(F)$, met $n \geq 3$, op $M_n(F)$ 'n surjektiewe homomorfisme is en uit Stelling 1.1 volg dat $\nu(n, F) = 3$ weet ons reeds dat $\nu(M_n^m(F)) \geq 3$. Deur nou van die bogenoemde resultate gebruik te maak, volg, byvoorbeeld, dat

$$\begin{aligned} \nu(M_3(GF(4))) &= 3 \\ \nu(M_3^2(GF(4))) &= 3 \\ \nu(M_3^3(GF(4))) &= 3 \\ 3 &\leq \nu(M_3^4(GF(4))) \leq \lceil \log_2 \lceil \frac{4}{3} \rceil \rceil + 3 = 4 \\ 3 &\leq \nu(M_3^5(GF(4))) \leq \lceil \log_2 \lceil \frac{5}{3} \rceil \rceil + 3 = 4 \\ 3 &\leq \nu(M_3^6(GF(4))) \leq \lceil \log_2 \lceil \frac{6}{3} \rceil \rceil + 3 = 4 \\ 3 &\leq \nu(M_3^7(GF(4))) \leq \lceil \log_2 \lceil \frac{7}{3} \rceil \rceil + 3 = 5, \end{aligned}$$

waar $GF(4)$ die galois liggaam met vier elemente is.

□

Ons kan die volgende resultaat vir eindige algebras in die algemeen bewys.

Stelling 2.18 Laat \mathbb{B}^m m kopieë van die eindige algebra \mathbb{B} wees. Dan kan \mathbb{B}^m nie deur k elemente voortgebring word as $m > |\mathbb{B}|^k$ nie.

Bewys Ons beskou enige k elemente van \mathbb{B}^m , sê

$$\begin{aligned} X_1 &= (x_{11}, x_{12}, \dots, x_{1m}), \\ X_2 &= (x_{21}, x_{22}, \dots, x_{2m}), \\ &\vdots \\ X_k &= (x_{k1}, x_{k2}, \dots, x_{km}). \end{aligned}$$

Dan kan ons die "kolomme"

$$K_1 = \begin{bmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{k1} \end{bmatrix}, K_2 = \begin{bmatrix} x_{12} \\ x_{22} \\ \vdots \\ x_{k2} \end{bmatrix}, \dots, K_m = \begin{bmatrix} x_{1m} \\ x_{2m} \\ \vdots \\ x_{km} \end{bmatrix},$$

vorm deur die n 'de komponente van X_1, \dots, X_k , van bo na onder in "kolom" K_n te plaas. Hierdie "kolomme" is m elemente van \mathbb{B}^k .

Indien $m > |\mathbb{B}|^k$ volg dat twee van die bostaande "kolomme" dieselfde moet wees, sê "kolom" l en j is dieselfde. Maar dit beteken dat die l 'de en j 'de komponent van enige element van die subalgebra \mathbb{A} van \mathbb{B}^m , voortgebring deur X_1, \dots, X_k , altyd dieselfde is. Aangesien \mathbb{B}^m elemente bevat waarvan die l 'de en j 'de komponente verskil, is $\mathbb{A} \subsetneq \mathbb{B}^m$. Dit wil sê \mathbb{B}^m kan nie deur k elemente voortgebring word nie.

□

Let op dat die bostaande stelling vir enige k elemente van die algebra \mathbb{B}^m geld, en nie slegs enige k idempotente van die algebra \mathbb{B}^m nie.

Ons kan bostaande stelling as volg op 'n direkte som van die vorm $M_n^m(F)$ waar F eindig is toepas.

Gevolg 2.19 ([12], Stelling 4) *Laat F 'n eindige liggaam wees. As $m > |F|^{kn^2}$ dan kan die algebra $M_n^m(F)$ nie deur k elemente voortgebring word nie.*

Bewys Dit volg direk uit bostaande stelling dat $M_n(F)$ nie deur k elemente voortgebring kan word as $m > |M_n(F)|^k = (|F|^{n^2})^k = |F|^{kn^2}$ is nie.

□

Opmerking Uit Gevolg 2.19 volg dat indien 'n direkte som $M_n^m(F)$ deur k elemente voortgebring word, dan is $|F|^{kn^2} \geq m$ wat impliseer dat $\frac{\log m}{n^2 \log |F|} \leq k$. Gevolglik is $\frac{\log m}{n^2 \log |F|}$ 'n ondergrens van die aantal (idempotente) voortbringers van $M_n^m(F)$ indien F eindig is en dus, in die besonder, indien $n = 2$ en $|F| \leq m + 1$ of indien $n \geq 3$ en $|F| \leq m$.

Aangesien die kanoniese afbeelding π_i van $M_n^m(F)$ op $M_n(F)$ 'n surjektiewe homomorfisme is en uit Stelling 1.1 volg dat $\nu(n, F) = 3$ indien $n \geq 3$ weet ons reeds dat $\nu(M_n^m(F)) \geq 3$. Ons kan dus in die geval waar $n \geq 3$ slegs nuwe inligting omtrent die grootte van $\nu(M_n^m(F))$ uit Gevolg 2.19 bekom indien $\frac{\log m}{n^2 \log |F|} > 3 \Rightarrow \log m > \log |F|^{3n^2} \Rightarrow m > |F|^{3n^2}$. Aangesien $|F| \geq 2$ moet

$$m > 2^{3n^2} = 8^{n^2} = l \text{ (sê)}$$

wees, vir $\frac{\log m}{n^2 \log |F|}$ om moontlik groter as die reeds bekende ondergrense te wees. Vir $n = 3$ is $l = 8^9 = 134217728$ en vir waardes van $n > 3$ is $l > 134217728$. Soortgelyk moet $m > 8^4 = 4096$ indien $n = 2$ en $F = \mathbb{Z}_2$, en moet $m > 9^4 = 6561$ indien $n = 2$ en $F \neq \mathbb{Z}_2$ voordat $\frac{\log m}{n^2 \log |F|}$ moontlik 'n nuwe onbekende ondergrens vir $\nu(M_n^m(F))$ kan wees. Gevolglik is $\frac{\log m}{n^2 \log |F|}$ oor die algemeen nie nuttig as 'n ondergrens vir $\nu(M_n^m(F))$ nie.

Ons kan egter wel ook uit Gevolg 2.19 die afleiding maak dat $\nu(M_n^m(F))$ van n , $|F|$, asook m , afhanklik is.

Voorbeelde Hier volg voorbeelde waar Gevolg 2.19 wel gebruik kan word om 'n nuwe onbekende ondergrens vir $\nu(M_n^m(F))$ te bepaal. Ons maak ook in die voorbeelde van Gevolg 2.13 gebruik om 'n bogrens vir $\nu(M_n^m(F))$ te bepaal.

Laat $F = \mathbb{Z}_2$, $n = 2$ en $m = 70000$. Aangesien $\frac{\log 70000}{\log 2^{2^2}} > 4$ volg dat

$$5 \leq \nu(M_2^{70000}(\mathbb{Z}_2)) \leq \lceil \log_2 70000 \rceil + 3 = 20.$$

Laat $F = GF(4)$, waar $GF(4)$ die galois liggaam met vier elemente is, $n = 2$ en $m = 70000$. Aangesien $\frac{\log 70000}{\log 4^{2^2}} > 2$ volg dat

$$3 \leq \nu(M_2^{70000}(GF(4))) \leq \lceil \log_2 \lceil \frac{70000}{2} \rceil \rceil + 2 = 18.$$

□

Gevolg 2.19 word in [12] as Stelling 4 bewys. In die bewys van Krupnik word die stelling gemaak dat 'n subalgebra \mathbb{A} van $M_n^m(F)$ voortgebring deur k elemente van orde $\leq |F|^{kn^2}$ is. Hierdie stelling geld egter nie vir $n = 1$ nie. Hier volg 'n teenvoorbeeld.

Laat $F = \mathbb{Z}_5$, $m = 5$, $n = 1$ en $k = 3$. Dan is $F^m = \mathbb{Z}_5^5$ (5 kopieë van \mathbb{Z}_5). Aangesien $|F|^{kn^2} = 5^3$ het enige subalgebra van \mathbb{Z}_5^5 voortgebring deur 3 elemente volgens Krupnik se bewys minder as 5^3 elemente. Volgens Stelling 2.2 bring

$$(1, 1, 1, 1, 0), (1, 1, 0, 0, 1) \text{ en } (1, 0, 1, 0, 1) \quad (59)$$

egter die hele \mathbb{Z}_5^5 voort. Aangesien \mathbb{Z}_5^5 5⁵ elemente het, is die orde van die F -subalgebra voortgebring deur die $k = 3$ elemente in (59) groter as $|F|^{kn^2}$.

Dit is wel waar dat die subruimte van die vektorruimte $M_n^m(F)$ voortgebring deur k elemente van orde $\leq |F|^k \leq |F|^{kn^2}$ is. Gevolg 2.19 geld dus ook vir vektorruimtes.

Voorbeelde Deur van Stelling 2.1, Stelling 2.2, Stelling 2.3 en Stelling 2.4 gebruik te maak kan ons nou, byvoorbeeld, die minimum aantal idempotente voortbringers van die volgende direkte som van volledige matriksalgebras oor 'n oneindige liggaam F bepaal:

$$\begin{aligned} & \nu(M_2^3(F) \oplus M_3^2(F) \oplus M_4^8(F) \oplus F^6) \\ &= \max(\nu(M_2^3(F)), \nu(M_3^2(F)), \nu(M_4^8(F)), \nu(F^6)) \\ &= \max(2, 3, 3, 3) = 3. \end{aligned}$$

Deur van Stelling 2.1, Gevolg 2.19, Gevolg 2.13 en Gevolg 2.17 gebruik te maak, kan ons nou, byvoorbeeld, 'n ondergrens en 'n bogrens vir die minimum aantal idempotente voortbringers van die volgende direkte som van volledige matriksalgebras oor 'n eindige liggaam $GF(4)$, waar $GF(4)$ die galois liggaam met vier elemente is, bepaal:

$$\begin{aligned} & \nu(M_2^7(GF(4)) \oplus M_3^2(GF(4)) \oplus M_2^{70000}(GF(4)) \oplus (GF(4))^9) \\ &= \max(\nu(M_2^7(GF(4))), \nu(M_3^2(GF(4))), \nu(M_2^{70000}(GF(4))), \nu((GF(4))^9)). \end{aligned}$$

Aangesien

$$\begin{aligned} 2 &\leq \nu(M_2^7(GF(4))) &&\leq 4 \\ 3 &= \nu(M_3^2(GF(4))) &&= 3 \\ 3 &\leq \nu(M_2^{70000}(GF(4))) &&\leq 18 \\ 4 &= \nu((GF(4))^9) &&= 4 \end{aligned}$$

volg dat

$$4 \leq \nu(M_2^7(GF(4)) \oplus M_3^2(GF(4)) \oplus M_2^{70000}(GF(4)) \oplus (GF(4))^9) \leq 18.$$

□

Ons sluit die hoofstuk af deur te wys dat ons deur middel van die resultate wat ons in die tesis bespreek het die minimum aantal idempotente voortbringers van 'n eindig-dimensionele semi-eenvoudige algebra kan bepaal.

Volgens die welbekende Wedderburn-Artin Stelling kan 'n semi-eenvoudige Artinse-algebra as 'n direkte som van matriksalgebras oor delingsalgebras uitgedruk word.

Stelling 2.1 (WEDDERBURN-ARTIN STELLING) ([9], Hoofstuk 5, Stelling 5.4)
'n Algebra \mathbb{A} oor 'n liggaam F is 'n semi-eenvoudige linker Artinse-algebra as en slegs as daar 'n isomorfisme van F -algebras, naamlik

$$\mathbb{A} \cong M_{n_1}(\mathbb{D}_1) \oplus M_{n_2}(\mathbb{D}_2) \oplus \cdots \oplus M_{n_t}(\mathbb{D}_t), \quad (60)$$

waar $n_1 \leq n_2 \leq \cdots \leq n_t$ positiewe heelgetalle en \mathbb{D}_i 'n delingsalgebra oor F is, bestaan.

Ons gebruik die volgende konvensie en resultate om deur middel van die Wedderburn-Artin Stelling te bewys dat 'n eindig-dimensionele semi-eenvoudige algebra \mathbb{A} oor 'n algebraïes geslote liggaam F as die direkte som van volledige $n \times n$ matriksalgebras oor F uitgedruk kan word.

Konvensie Laat \mathbb{A} 'n F -algebra wees. Dan kan F deur middel van die 1-1 F -algebra homorfisme $\alpha : F \rightarrow \mathbb{A}$ gedefinieer deur $k \mapsto k1_{\mathbb{A}}$ in \mathbb{A} ingebed word. Ons neem sodoende die konvensie aan dat ons F as die subalgebra $\text{Im}(\alpha)$, waar $\text{Im}(\alpha)$ die beeld van α is, van \mathbb{A} sien. Aangesien vir elke $a \in \mathbb{A}$ en elke $k \in F$ volg dat

$$\alpha(k)a = (k1_{\mathbb{A}})a = k(1_{\mathbb{A}}a)1_{\mathbb{A}} = (1_{\mathbb{A}}a)(k1_{\mathbb{A}}) = a\alpha(k),$$

is $\alpha(F)$ oftewel F , volgens die konvensie, in die sentrum van \mathbb{A} geleë.

Lemma 2.20 ([9], Hoofstuk 5, Lemma 5.6) *As \mathbb{D} 'n algebraïese delingsalgebra oor 'n algebraïes geslote liggaam F is, dan is $\mathbb{D} = F$.*

Bewys Volgens die bostaande konvensie volg dat F in die sentrum van \mathbb{D} geleë is.

Omgekeerd, laat $a \in \mathbb{D}$ en $a \neq 0$ wees. Aangesien \mathbb{D} algebraïes oor F is, volg dat daar 'n $f \in F[x]$ bestaan sodat $f(a) = 0$. Omdat F algebraïes geslote is, is

$$f(x) = k(x - k_1)(x - k_2) \cdots (x - k_n) \quad \text{waar} \quad k, k_i \in F, k \neq 0$$

sodat

$$0 = f(a) = k(a - k_1)(a - k_2) \cdots (a - k_n).$$

Aangesien \mathbb{D} 'n delingsalgebra is, volg dat een van die faktore van $f(a)$ nul is, met ander woorde, dat $a - k_i = 0$ vir 'n i . Sodoende is $a = k_i \in F$ vir 'n i . Gevolglik is $\mathbb{D} = F$.

□

Die volgende welbekende resultaat word in die daaropvolgende lemma gebruik.

Stelling 2.21 ([2], Hoofstuk 5, Stelling 5.4.7) *As W 'n subruimte van 'n eindig dimensionele vektorruimte V is, dan is $\dim W \leq \dim V$. Inderwaarheid, as $\dim W = \dim V$ dan is $W = V$.*

Lemma 2.22 ([9], Hoofstuk 5, Oefening nr. 2) *'n Eindig-dimensionele algebra \mathbb{A} oor 'n liggaam F bevredig beide die afnemende en toenemende ketting voorwaardes op die linker en regter algebra-ideale, en is dus 'n Artinse- en Noetherse algebra.*

Bewys Gestel $L_1 \supseteq L_2 \supseteq \cdots$ (onderskeidelik $L_1 \subseteq L_2 \subseteq \cdots$) is 'n afnemende (onderskeidelik toenemende) ketting van (linker, regter) algebra-ideale. Aangesien 'n algebra-ideaal, gesien as 'n vektorruimte, 'n subruimte van die algebra, volgens definisie, is, volg uit Stelling 2.21 dat $\dim L_i \geq \dim L_{i+1}$ (onderskeidelik $\dim L_i \leq \dim L_{i+1}$) en dat $\dim L_i = \dim L_{i+1}$ as en slegs as $L_i = L_{i+1}$. Aangesien \mathbb{A} eindig dimensioneel is, moet die ketting sodoende stop.

□

Indien \mathbb{A} 'n semi-eenvoudige eindig-dimensionele algebra oor 'n liggaam F is, volg uit Lemma 2.22 dat \mathbb{A} 'n linker Artinse-algebra oor F is. Volgens die Wedderburn-Artin Stelling kan \mathbb{A} soos in (60) uitgedruk word. Aangesien \mathbb{A} eindig-dimensioneel is, volg dat elke \mathbb{D}_i eindig-dimensioneel is. Volgens die opmerking na Definisie 0.18 is elke \mathbb{D}_i algebraïes oor F . Uit Lemma 2.20 volg sodoende dat indien F 'n algebraïes geslote liggaam is, dat $F = \mathbb{D}_i$. Ons het dus die volgende skerper weergawe van die Wedderburn-Artin Stelling bewys.

Stelling 2.23 ([9], Hoofstuk 5, Stelling 5.7) Laat \mathbb{A} 'n eindig-dimensionele algebra oor 'n algebraïes geslote liggaam F wees. Dan bestaan daar positiewe heelgetalle $n_1 \leq n_2 \leq \dots \leq n_t$ en 'n isomorfisme van F -algebras, naamlik

$$\mathbb{A} \cong M_{n_1}(F) \oplus \dots \oplus M_{n_t}(F). \quad (61)$$

Indien \mathbb{A} 'n eindig-dimensionele semi-eenvoudige algebra oor 'n algebraïes geslote liggaam F is, kan ons sodoende, volgens Stelling 2.23, \mathbb{A} soos in (61), met ander woorde as 'n eindige direkte som van volledige $n \times n$ matriksalgebras, uitdruk. Dit beteken dat ons van die resultate wat ons in die tesis bespreek het gebruik kan maak om die minimum aantal idempotente voortbringers van \mathbb{A} te bepaal. Aangesien F algebraïes geslote is, volg uit die opmerking na Stelling 0.19 dat F oneindig is. Uit Stelling 2.1, Stelling 2.2 en Stelling 2.12 volg sodoende dat

$$\nu(\mathbb{A}) = \max_{1 \leq i \leq t} \nu(M_{n_i}^{m_i}(F)),$$

waar

$$\nu(M_{n_i}^{m_i}(F)) = \begin{cases} \lceil \log_2 m_i \rceil & \text{as } n_i = 1 \\ 2 & \text{as } n_i = 2 \\ 3 & \text{as } n_i \geq 3. \end{cases}$$

Indien daar 'n i bestaan sodat $n_i = 1$ volg dat \mathbb{A} 'n tweesydigte ideaal van die vorm $0 \oplus \dots \oplus 0 \oplus F^{m_i} \oplus 0 \oplus \dots \oplus 0$ het. Indien \mathbb{A} geen tweesydigte ideale het nie, volg dus dat $n_i > 1$, vir alle i , en dus in die besonder dat

$$\nu(\mathbb{A}) \leq 3.$$

3 Sentrale Polinome

In hierdie hoofstuk bespreek ons die vraag of daar 'n nie-nulwordende sentrale polinoom vir $M_n(F)$, met $n \geq 2$, waar F enige liggaam is, bestaan. Ons benodig so 'n polinoom om Stelling 2.1 te bewys. Voordat ons hierdie aangeleentheid verder ondersoek, definieer ons eers die begrip sentrale polinoom en bepaal ons die sentrum van $M_n(F)$.

Definisie 3.1 ([6], bladsy 9, Def) Laat F 'n liggaam, \mathbb{A} 'n F -algebra en $F[X_1, X_2, \dots, X_n]$ die polinoomring in nie-kommuterende veranderlikes X_1, X_2, \dots, X_n oor F wees.

- 'n Polinoomidentiteit vir \mathbb{A} is 'n polinoom $P(X_1, X_2, \dots, X_n) \in F[X_1, X_2, \dots, X_n]$ sodat $P(a_1, a_2, \dots, a_n) = 0$ vir elke $a_1, a_2, \dots, a_n \in \mathbb{A}$.
- 'n Sentrale polinoom vir \mathbb{A} is 'n polinoom $P(X_1, X_2, \dots, X_n) \in F[X_1, X_2, \dots, X_n]$ sodat $P(a_1, a_2, \dots, a_n) \in Z(\mathbb{A})$, met $Z(\mathbb{A})$ die sentrum van \mathbb{A} , vir elke $a_1, a_2, \dots, a_n \in \mathbb{A}$.
- 'n Sentrale polinoom is nie-nulwordend as dit nie 'n polinoomidentiteit is nie.

Stelling 3.2 Die sentrum van $M_n(F)$, met $n \geq 2$, is FI_n . Met ander woorde

$$Z(M_n(F)) = \left\{ \begin{bmatrix} a & & \circ \\ & \ddots & \\ \circ & & a \end{bmatrix} : a \in F \right\}.$$

Bewys Gestel

$$X_1 = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \in Z(M_n(F)).$$

Dan volg dat $X_1 X = X X_1$ vir alle $X \in M_n(F)$. In die besonder volg dat $e_{ii} X_1 = X_1 e_{ii}$ ($1 \leq i \leq n$). Aangesien

$$X_1 e_{ii} = \begin{matrix} \text{kolom } i \\ \downarrow \\ \begin{bmatrix} a_{1i} \\ \circ & \vdots & \circ \\ a_{ni} \end{bmatrix} \end{matrix} \quad \text{en} \quad e_{ii} X_1 = \begin{bmatrix} \circ & & \\ a_{i1} & \cdots & a_{in} \\ \circ & & \end{bmatrix} \leftarrow \text{ry } i$$

volg dat $a_{ij} = 0$ as $i \neq j$.

Verder is $e_{ij}X_1 = X_1e_{ij}$. Aangesien

$$e_{ij} \begin{bmatrix} a_{11} & & \circ \\ & \ddots & \\ \circ & & a_{nn} \end{bmatrix} = \begin{bmatrix} \circ & & \circ \\ & a_{jj} & \\ \circ & & \circ \end{bmatrix} \begin{matrix} \text{kolom } j \\ \downarrow \\ \leftarrow \text{ry } i \end{matrix}$$

en

$$\begin{bmatrix} a_{11} & & \circ \\ & \ddots & \\ \circ & & a_{nn} \end{bmatrix} e_{ij} = \begin{bmatrix} \circ & & \circ \\ & a_{ii} & \\ \circ & & \circ \end{bmatrix} \begin{matrix} \text{kolom } j \\ \downarrow \\ \leftarrow \text{ry } i \end{matrix}$$

volg dat $a_{11} = a_{22} = \dots = a_{nn}$. Gevolglik is

$$Z(M_n(F)) \subseteq \left\{ \begin{bmatrix} a & & \circ \\ & \ddots & \\ \circ & & a \end{bmatrix} : a \in F \right\}.$$

Omgekeerd, volg dat

$$\begin{aligned} \begin{bmatrix} a & & \circ \\ & \ddots & \\ \circ & & a \end{bmatrix} X &= aI_n X \\ &= aX I_n \\ &= X a I_n \\ &= X \begin{bmatrix} a & & \circ \\ & \ddots & \\ \circ & & a \end{bmatrix} \end{aligned}$$

vir alle $a \in F$ en alle $X \in M_n(F)$. Die resultaat is dus bewys.

□

W. Wagner het reeds in 1937 in [17] opgelet dat $f(X, Y) = (XY - YX)^2$ 'n nie-nulwordende sentrale polinoom vir die volledige matriksalgebra $M_2(F)$ is, met F enige liggaam. Ons het die volgende bekende resultaat nodig om die stelling te bewys.

Stelling 3.3 (CAYLEY-HAMILTON) ([2], Hoofstuk 7, "Supplementary Exercises" nr. 7)
'n Vierkantige matriks oor 'n liggaam F bevredig sy karakteristieke polinoom.

Stelling 3.4 ([17], bladsy 533) As F 'n liggaam is, dan is $f(X, Y) = (XY - YX)^2$ 'n
nie-nulwordende sentrale polinoom vir $M_2(F)$.

Bewys Laat $A := \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ en $B := \begin{bmatrix} e & f \\ g & h \end{bmatrix}$ willekeurige matrikse in $M_2(F)$ wees.

Dan volg dat

$$\begin{aligned} \operatorname{tr}(AB - BA) &= \operatorname{tr} \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} - \begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) \\ &= \operatorname{tr} \left(\begin{bmatrix} ae + bg & * \\ * & cf + dh \end{bmatrix} - \begin{bmatrix} ae + fc & * \\ * & gb + hd \end{bmatrix} \right) \\ &= \operatorname{tr} \left(\begin{bmatrix} bg - fc & * \\ * & fc - gb \end{bmatrix} \right) \\ &= bg - fc + fc - gb \\ &= 0, \end{aligned}$$

waar $\operatorname{tr}(X)$ die spoor van 'n willekeurige matriks X aandui. Gevolglik is die karakteristieke polinoom $p(\lambda)$ van $AB - BA$ van die vorm

$$p(\lambda) = \lambda^2 + c, \quad \text{waar } c \in F.$$

Uit die Cayley-Hamilton Stelling (Stelling 3.3) volg sodoende dat

$$\begin{aligned} (AB - BA)^2 + cI_n &= 0 \\ \Rightarrow (AB - BA)^2 &= -cI_n. \end{aligned}$$

Dus, volgens Stelling 3.2 is $(AB - BA)^2 \in Z(M_n(F))$. Gevolglik is $(XY - YX)^2$ 'n sentrale polinoom vir $M_2(F)$.

Indien ons $A = e_{12}$ en $B = e_{21}$ kies, volg dat

$$\begin{aligned} (AB - BA)^2 &= (e_{12}e_{21} - e_{21}e_{12})^2 \\ &= (e_{11} - e_{22})^2 \\ &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}^2 \\ &= I_n \neq 0. \end{aligned}$$

Dus is $(XY - YX)^2$ 'n nie-nulwordende sentrale polinoom vir $M_2(F)$.

□

Die vraag of daar 'n nie-nulwordende sentrale polinoom vir $M_n(F)$, met $n \geq 3$ en F 'n liggaam, bestaan, is vir die eerste keer deur I. Kaplansky in [10] gevra. Die vraag is gedeeltelik deur V.N. Latyshev en A.L. Shmelkin in [13] beantwoord, waarin bewys is dat daar wel 'n nie-nulwordende sentrale polinoom bestaan indien F 'n eindige liggaam is. E. Formanek en Y.P. Razmyslov het egter spoedig in [5] en [15], onderskeidelik, deur middel van die volgende stelling 'n antwoord op Kaplansky se vraag gevind.

Stelling 3.5 ([5], Stelling) *Vir elke $n \geq 2$ bestaan daar 'n nie-nulwordende sentrale polinoom vir $M_n(F)$, waar F 'n liggaam is.*

Die res van die hoofstuk gaan ons wy aan 'n uiteensetting van die bewys van E. Formanek in [5]. Ons beskou eers 'n aantal voorafgaande resultate en notasie wat ons in die bewys gaan benodig.

Lemma 3.6 ([2], Hoofstuk 7, "Supplementary Exercises" nr. 12) *Die karakteristieke polinoom van die $n \times n$ matriks*

$$A_p := \begin{bmatrix} 0 & & & & -c_0 \\ 1 & 0 & & \circ & -c_1 \\ & 1 & 0 & & -c_2 \\ & & 1 & 0 & \vdots \\ & & & \ddots & \ddots & \vdots \\ \circ & & & \ddots & 0 & -c_{n-2} \\ & & & & 1 & -c_{n-1} \end{bmatrix}$$

is $p(\lambda) = \lambda^n + c_{n-1}\lambda^{n-1} + \dots + c_0$.

Bewys Ons bewys die stelling deur middel van induksie op n . Vir $n = 2$ volg dat

$$\begin{aligned} p(\lambda) &= \det(\lambda I_2 - A_p) \\ &= \begin{vmatrix} \lambda & c_0 \\ -1 & \lambda + c_1 \end{vmatrix} \\ &= \lambda^2 + c_1\lambda + c_0. \end{aligned}$$

Gestel die stelling is waar vir $n = k - 1$.

Ons beskou nou die karakteristieke polinoom van die $k \times k$ matriks A_p . Deur middel van kolom-operasies (ons stel kolom i as K_i voor) en die gebruik van die ko-faktor-ontwikkeling volg dat

$$\begin{aligned}
p(\lambda) &= \det(\lambda I_k - A_p) \\
&= \begin{vmatrix} \lambda & & & & c_0 \\ -1 & \lambda & & \circ & c_1 \\ & -1 & \lambda & & c_2 \\ & & -1 & \lambda & \vdots \\ & & & \ddots & \ddots & \vdots \\ & \circ & & & \ddots & \lambda & c_{k-2} \\ & & & & & -1 & \lambda + c_{k-1} \end{vmatrix} \\
&= \lambda \begin{vmatrix} \lambda & & & c_1 \\ -1 & \lambda & & c_2 \\ & -1 & \lambda & c_3 \\ \circ & & \ddots & \vdots \\ & & & -1 & \lambda + c_{k-1} \end{vmatrix} + (-1)^{k+1} c_0 \begin{vmatrix} -1 & \lambda & & \\ & -1 & \lambda & \circ \\ & & -1 & \lambda \\ \circ & & & \ddots & \ddots \\ & & & & -1 \end{vmatrix} \\
&= \lambda(\lambda^{k-1} + \lambda^{k-2}c_{k-1} + \cdots + c_1) + (-1)^{k+1}c_0 \begin{vmatrix} -1 & \lambda & & \\ & -1 & \lambda & \circ \\ & & -1 & \lambda \\ \circ & & & \ddots & \ddots \\ & & & & -1 \end{vmatrix} \tag{62} \\
&= \lambda(\lambda^{k-1} + \lambda^{k-2}c_{k-1} + \cdots + c_1) + (-1)^{k+1}c_0 \begin{vmatrix} -1 & 0 & & \circ \\ & \ddots & \ddots & \\ \circ & & -1 & 0 \\ & & & -1 \end{vmatrix} \begin{array}{l} \text{eers } K_2 + \lambda K_1 \\ \text{dan } K_3 + \lambda K_2 \\ \vdots \\ \text{dan } K_k + \lambda K_{k-1} \end{array} \\
&= \lambda^k + \lambda^{k-1}c_{k-1} + \cdots + \lambda c_1 + (-1)^{k+1}(-1)^{k-1}c_0 \\
&= \lambda^k + \lambda^{k-1}c_{k-1} + \cdots + \lambda c_1 + c_0,
\end{aligned}$$

waar (62) uit die induksie-hipotese volg. Die induksie is dus voltooi.

□

Opmerking Die matriks A_p in Lemma 3.6 word die meegaande matriks van die polinoom p genoem.

Lemma 3.7 Die ring $M_n(F)$, waar F 'n liggaam en $n \geq 2$ is, bevat 'n matriks waarvan al die eiewaardes verskillend is.

Bewys Indien F oneindig is, neem ons die matriks

$$A := \begin{bmatrix} k_1 & & & \circ \\ & k_2 & & \\ & & \ddots & \\ \circ & & & k_n \end{bmatrix}$$

waar k_1, k_2, \dots, k_n verskillende elemente in F is. Indien F 'n eindige liggaam is, volg uit Stelling 0.26 dat daar 'n priemgetal p bestaan sodat \mathbb{Z}_p in F ingebed kan word. Volgens Stelling 0.27(2) bestaan daar 'n eindige liggaam K van die vorm $\frac{\mathbb{Z}_p[x]}{[f]}$, waar f 'n onherleibare polinoom van graad n oor \mathbb{Z}_p is. Uit Stelling 0.25 volg dat al die wortels van f verskillend is. Aangesien \mathbb{Z}_p in F ingebed kan word, kan ons \mathbb{Z}_p as 'n subliggaam van F sien. Sodoende kan f as 'n polinoom oor F beskou word. Volgens Lemma 3.6 is $f(x)$ die karakteristieke polinoom van die meegaande matriks $A_f \in M_n(F)$. Aangesien al die wortels van f verskillend is, is al die eiewaardes van A_f verskillend. Dus bestaan daar 'n matriks in $M_n(F)$ waarvan al die eiewaardes verskillend is.

□

Notasie Laat x_1, x_2, \dots, x_{n+1} kommuterende veranderlikes, X, Y_1, Y_2, \dots, Y_n nie kommuterende veranderlikes, en $F[x_1, x_2, \dots, x_{n+1}]$ en $F[X, Y_1, Y_2, \dots, Y_n]$ die algebras oor F , voortgebring deur x_1, x_2, \dots, x_{n+1} en X, Y_1, Y_2, \dots, Y_n , onderskeidelik, wees. Ons definieer die funksie

$$\theta : F[x_1, x_2, \dots, x_{n+1}] \rightarrow F[X, Y_1, Y_2, \dots, Y_n]$$

deur

$$\sum c_a x_1^{a_1} x_2^{a_2} \dots x_{n+1}^{a_{n+1}} \mapsto \sum c_a X^{a_1} Y_1 X^{a_2} Y_2 \dots X^{a_n} Y_n X^{a_{n+1}}.$$

Dit beteken byvoorbeeld vir $n = 5$ dat

$$\theta(9x_1x_6^4x_3x_2^2) = 9XY_1X^2Y_2XY_3Y_4Y_5X^4$$

en vir $n = 2$ dat

$$\theta(x_2^2) = Y_1 X^2 Y_2.$$

Laat g die polinoom

$$g(x_1, x_2, \dots, x_{n+1}) := \prod_{2 \leq i \leq n} (x_1 - x_i)(x_{n+1} - x_i) \prod_{2 \leq j < k \leq n} (x_j - x_k)^2 \quad (63)$$

wees. Ons definieer G as die beeld van g onder θ , met ander woorde

$$G(X, Y_1, Y_2, \dots, Y_n) := \theta(g(x_1, x_2, \dots, x_{n+1})),$$

en die polinoom P as

$$P(X, Y_1, \dots, Y_n) := G(X, Y_1, \dots, Y_n) + G(X, Y_2, \dots, Y_n, Y_1) + \dots + G(X, Y_n, Y_1, \dots, Y_{n-1}).$$

□

Ons sal bewys dat $P(X, Y_1, \dots, Y_n)$ 'n nie-nulwordende sentrale polinoom vir $M_n(F)$ is.

In Lemma 3.8 bewys ons eers dat $P(X, Y_1, \dots, Y_n)$ in die sentrum van $M_n(F)$ is vir beperkte waardes van X, Y_1, \dots, Y_n , naamlik wanneer X 'n diagonaal matriks en Y_1, \dots, Y_n matrikseenhede is.

In Lemma 3.17 en Lemma 3.18 bewys ons dat die beperkte waardes van X, Y_1, \dots, Y_n in Lemma 3.8 alle waardes in $M_n(F)$ dek, met ander woorde dat

$$P(X, Y_1, \dots, Y_n) \in Z(M_n(F)), \quad \text{vir alle } X, Y_1, \dots, Y_n \in M_n(F);$$

en laastens bewys ons in Lemma 3.20 dat $P(X, Y_1, \dots, Y_n)$ nie-nulwordend is, met ander woorde dat daar 'n $X, Y_1, \dots, Y_n \in M_n(F)$ bestaan, sodat

$$P(X, Y_1, \dots, Y_n) \neq 0.$$

Lemma 3.8 *Die polinoom $P(X, Y_1, \dots, Y_n)$ is in die sentrum van $M_n(F)$, wanneer X 'n diagonaal matriks en Y_1, \dots, Y_n matrikseenhede is.*

Bewys Laat

$$X = (\delta_{ij}x_i) = \begin{bmatrix} x_1 & & & \circ \\ & x_2 & & \\ & & \ddots & \\ \circ & & & x_n \end{bmatrix}$$

'n diagonaal matriks en Y_1, \dots, Y_n willekeurige matrikseenhede, sê $e_{i_1j_1}, e_{i_2j_2}, \dots, e_{i_nj_n}$, wees.

Ons beskou eerstens die polinoom $G(X, Y_1, \dots, Y_n)$. Aangesien

$$\begin{aligned} X^{a_1} e_{i_1j_1} \dots X^{a_n} e_{i_nj_n} X^{a_{n+1}} &= (\delta_{ij}x_i^{a_1})e_{i_1j_1} \dots (\delta_{ij}x_i^{a_n})e_{i_nj_n}(\delta_{ij}x_i^{a_{n+1}}) \\ &= x_{i_1}^{a_1} e_{i_1j_1} \dots x_{i_n}^{a_n} e_{i_nj_n} (\delta_{ij}x_i^{a_{n+1}}) \\ &= x_{i_1}^{a_1} e_{i_1j_1} \dots x_{i_n}^{a_n} e_{i_nj_n} x_{j_n}^{a_{n+1}} \\ &= x_{i_1}^{a_1} \dots x_{i_n}^{a_n} x_{j_n}^{a_{n+1}} e_{i_1j_1} \dots e_{i_nj_n} \end{aligned} \quad (64)$$

volg, deur $a_1, a_2, \dots, a_n, a_{n+1}$ so te kies dat $g(x_{i_1}, \dots, x_{i_n}, x_{j_n}) = \sum c_a x_{i_1}^{a_1} \dots x_{i_n}^{a_n} x_{j_n}^{a_{n+1}}$, dat

$$\begin{aligned} G(X, Y_1, \dots, Y_n) &= \theta(g(x_{i_1}, \dots, x_{i_n}, x_{j_n})) \\ &= \theta\left(\sum c_a x_{i_1}^{a_1} \dots x_{i_n}^{a_n} x_{j_n}^{a_{n+1}}\right) \\ &= \sum c_a X^{a_1} e_{i_1j_1} \dots X^{a_n} e_{i_nj_n} X^{a_{n+1}} \\ &= \sum c_a x_{i_1}^{a_1} \dots x_{i_n}^{a_n} x_{j_n}^{a_{n+1}} e_{i_1j_1} \dots e_{i_nj_n} \quad (\text{volg uit (64)}) \\ &= \left(\sum c_a x_{i_1}^{a_1} \dots x_{i_n}^{a_n} x_{j_n}^{a_{n+1}}\right) e_{i_1j_1} \dots e_{i_nj_n} \\ &= g(x_{i_1}, \dots, x_{i_n}, x_{j_n}) e_{i_1j_1} \dots e_{i_nj_n}. \end{aligned} \quad (65)$$

Om $G(X, Y_1, \dots, Y_n)$ verder te vereenvoudig, beskou ons die polinoom $g(x_{i_1}, \dots, x_{i_n}, x_{j_n})$. Ons het die volgende twee moontlike gevalle:

1. (i_1, \dots, i_n) is nie 'n permutasie van $\{1, 2, \dots, n\}$ nie:

In hierdie geval het ons die volgende moontlikhede:

- (a) $x_{i_1} = x_{i_l}$, waar $l \neq 1$:

Dan vereenvoudig g tot

$$\begin{aligned} &g(x_{i_1}, \dots, x_{i_n}, x_{j_n}) \\ &= \prod_{2 \leq k \leq n} (x_{i_1} - x_{i_k})(x_{j_n} - x_{i_k}) \prod_{2 \leq k < r \leq n} (x_{i_k} - x_{i_r})^2 \\ &= (x_{i_1} - x_{i_2}) \dots \underbrace{(x_{i_1} - x_{i_l})}_{=0} \dots (x_{i_1} - x_{i_n}) \prod_{2 \leq k \leq n} (x_{j_n} - x_{i_k}) \prod_{2 \leq k < r \leq n} (x_{i_k} - x_{i_r})^2 \\ &= 0. \end{aligned}$$

(b) $x_{i_m} = x_{i_l}$ waar $l, m \neq 1$ en $l \neq m$:

Ons neem, sonder die verlies aan algemeenheid, aan dat $l < m$. Dan vereenvoudig g tot

$$\begin{aligned} g(x_{i_1}, \dots, x_{i_n}, x_{j_n}) &= \prod_{2 \leq k \leq n} (x_{i_1} - x_{i_k})(x_{j_n} - x_{i_k}) \prod_{2 \leq k < r \leq n} (x_{i_k} - x_{i_r})^2 \\ &= (x_{i_2} - x_{i_m})^2 \cdots \underbrace{(x_{i_l} - x_{i_m})^2}_{=0} \cdots (x_{i_{m-1}} - x_{i_m})^2 \cdot \\ &\quad \prod_{2 \leq k \leq n} (x_{i_1} - x_{i_k})(x_{j_n} - x_{i_k}) \prod_{\substack{2 \leq k < r \leq n \\ r \neq m}} (x_{i_k} - x_{i_r})^2 \\ &= 0. \end{aligned}$$

2. (i_1, \dots, i_n) is 'n permutasie van $\{1, 2, \dots, n\}$:

Aangesien die hoofdiagonaal van X slegs n moontlik verskillende waardes het, volg dat indien (i_1, \dots, i_n) 'n permutasie van $\{1, \dots, n\}$ is, dat $j_n \in \{i_1, \dots, i_n\}$. Ons het dus in geval 2 die volgende moontlikhede:

(a) $j_n = i_1$:

Dan vereenvoudig g tot

$$\begin{aligned} g(x_{i_1}, \dots, x_{i_n}, x_{i_1}) &= \prod_{2 \leq k \leq n} (x_{i_1} - x_{i_k})(x_{i_1} - x_{i_k}) \prod_{2 \leq k < r \leq n} (x_{i_k} - x_{i_r})^2 \\ &= \prod_{2 \leq k \leq n} (x_{i_1} - x_{i_k})^2 \prod_{2 \leq k < r \leq n} (x_{i_k} - x_{i_r})^2 \\ &= \prod_{1 \leq k < r \leq n} (x_{i_k} - x_{i_r})^2 \\ &= d \text{ (sê)}. \end{aligned}$$

(b) $j_n = i_l$, waar $1 < l \leq n$:

In hierdie geval vereenvoudig g tot

$$\begin{aligned} g(x_{i_1}, \dots, x_{i_n}, x_{j_n}) &= \prod_{2 \leq k \leq n} (x_{i_1} - x_{i_k})(x_{j_n} - x_{i_k}) \prod_{2 \leq k < r \leq n} (x_{i_k} - x_{i_r})^2 \\ &= (x_{j_n} - x_{i_2}) \cdots \underbrace{(x_{j_n} - x_{i_l})}_{=0} \cdots (x_{j_n} - x_{i_n}) \prod_{2 \leq k \leq n} (x_{i_1} - x_{i_k}) \prod_{2 \leq k < r \leq n} (x_{i_k} - x_{i_r})^2 \\ &= 0. \end{aligned}$$

Uit bostaande moontlikhede volg dat

$$g(x_{i_1}, \dots, x_{i_n}, x_{j_n}) = \begin{cases} d & \text{as } i_1 = j_n \text{ en } (i_1, \dots, i_n) \text{ 'n permutasie} \\ & \text{van } \{1, 2, \dots, n\} \text{ is} \\ 0 & \text{andersins.} \end{cases} \quad (66)$$

Aangesien $e_{jk}e_{lm} = \delta_{kl}e_{jm}$ volg dat

$$e_{i_1j_1} \cdots e_{i_nj_n} = \begin{cases} e_{i_1j_n} & \text{as } j_1 = i_2, \dots, j_{n-1} = i_n \\ 0 & \text{andersins.} \end{cases} \quad (67)$$

Uit (66) en (67) volg sodoende dat

$$\begin{aligned} G(X, e_{i_1j_1}, \dots, e_{i_nj_n}) &= g(x_{i_1}, \dots, x_{i_n}, x_{j_n}) e_{i_1j_1} \cdots e_{i_nj_n} \quad (\text{volg uit (65)}) \\ &= \begin{cases} & \text{as } j_1 = i_2, \dots, j_{n-1} = i_n, j_n = i_1 \\ de_{i_1j_n} = de_{i_1i_1} & \text{en } (i_1, \dots, i_n) \text{ 'n permutasie van} \\ & \{1, 2, \dots, n\} \text{ is} \\ 0 & \text{andersins.} \end{cases} \quad (68) \end{aligned}$$

Aangesien $e_{i_1j_1}, \dots, e_{i_nj_n}$ willekeurige matrikseenhede is, volg vir alle $1 < k \leq n$ uit (68) dat

$$\begin{aligned} &G(X, e_{i_kj_k}, \dots, e_{i_nj_n}, e_{i_1j_1}, \dots, e_{i_{k-1}j_{k-1}}) \\ &= \begin{cases} & \text{as } j_k = i_{k+1}, \dots, j_{n-1} = i_n, j_n = i_1, j_1 = i_2, \dots, \\ de_{i_kj_{k-1}} = de_{i_ki_k} & j_{k-1} = i_k \text{ en } (i_1, \dots, i_n) \text{ 'n permutasie van} \\ & \{1, 2, \dots, n\} \text{ is} \\ 0 & \text{andersins.} \end{cases} \quad (69) \end{aligned}$$

Ons noem $e_{i_1j_1}, \dots, e_{i_nj_n}$ 'n siklus van matrikseenhede indien (i_1, \dots, i_n) 'n permutasie van $\{1, \dots, n\}$ is en $j_1 = i_2, \dots, j_{n-1} = i_n, j_n = i_1$. Uit (68) en (69) volg sodoende dat

$$\begin{aligned} P(X, e_{i_1j_1}, \dots, e_{i_nj_n}) &= \begin{cases} de_{i_1i_1} + \cdots + de_{i_ni_n} & \text{as die matrikseenhede 'n siklus is} \\ 0 & \text{andersins} \end{cases} \\ &= \begin{cases} dI_n & \text{as die matrikseenhede 'n siklus is} \\ 0 & \text{andersins.} \end{cases} \quad (70) \end{aligned}$$

Dus lê $P(X, Y_1, \dots, Y_n)$, volgens Stelling 3.2, in die sentrum van $M_n(F)$ wanneer X 'n diagonaal matriks en Y_1, \dots, Y_n matrikseenhede is.

□

Die volgende lemma word benodig om Lemma 3.18 en Lemma 3.20 te bewys.

Lemma 3.9 *Laat F 'n liggaam en $Q \in M_n(F)$ 'n inverteerbare matriks wees. Dan volg dat*

$$Q^{-1}P(X, Y_1, \dots, Y_n)Q = P(Q^{-1}XQ, Q^{-1}Y_1Q, \dots, Q^{-1}Y_nQ).$$

Bewys Ons kies a_1, \dots, a_{n+1} so dat $g(x_{i_1}, \dots, x_{i_n}, x_{j_n}) = \sum c_a x_{i_1}^{a_1} \dots x_{i_n}^{a_n} x_{j_n}^{a_{n+1}}$. Aangesien dan volg dat

$$\begin{aligned} & Q^{-1}G(X, Y_1, \dots, Y_n)Q \\ &= Q^{-1}\left(\sum c_a X^{a_1} Y_1 X^{a_2} Y_2 \dots X^{a_n} Y_n X^{a_{n+1}}\right)Q \\ &= \sum c_a (Q^{-1}XQ)^{a_1} Q^{-1}Y_1Q (Q^{-1}XQ)^{a_2} \dots (Q^{-1}XQ)^{a_n} Q^{-1}Y_nQ (Q^{-1}XQ)^{a_{n+1}} \\ &= G(Q^{-1}XQ, Q^{-1}Y_1Q, \dots, Q^{-1}Y_nQ) \end{aligned}$$

volg dat

$$\begin{aligned} & Q^{-1}P(X, Y_1, \dots, Y_n)Q \\ &= Q^{-1}(G(X, Y_1, \dots, Y_n) + \dots + G(X, Y_n, Y_1, \dots, Y_{n-1}))Q \\ &= Q^{-1}G(X, Y_1, \dots, Y_n)Q + \dots + Q^{-1}G(X, Y_n, Y_1, \dots, Y_{n-1})Q \\ &= G(Q^{-1}XQ, Q^{-1}Y_1Q, \dots, Q^{-1}Y_nQ) + \dots \\ &\quad \dots + G(Q^{-1}XQ, Q^{-1}Y_nQ, Q^{-1}Y_1Q, \dots, Q^{-1}Y_{n-1}Q) \\ &= P(Q^{-1}XQ, Q^{-1}Y_1Q, \dots, Q^{-1}Y_nQ). \end{aligned}$$

□

Ons het ook die volgende welbekende definisies en resultate in die bewys van Lemma 3.18 en Lemma 3.20 nodig.

Definisie 3.10 ([2], bladsy 347, Def) *'n Vierkantige matriks A is diagonaliseerbaar as daar 'n inverteerbare matriks Q bestaan sodat $Q^{-1}AQ$ 'n diagonaalmatriks is. Ons sê Q diagonaliseer A .*

Stelling 3.11 ([2], bladsy 347 en bladsy 348) *Indien 'n vierkantige matriks Q 'n matriks A diagonaliseer, dan is die kolomvektore van Q eiektore van A en $Q^{-1}AQ$ is 'n diagonaalmatriks met die eiewaardes van A op die hoofdiagonaal.*

Opmerking Gestel $A \in M_n(F)$, waar F 'n liggaam is. Dan het die karakteristieke polinoom van A koeffisiënte in F , sodat die wortels daarvan en dus die eiewaardes van A elemente van \overline{F} is, waar \overline{F} die algebraïese afsluiting van F is. Dit beteken, volgens Stelling 3.11, dat $Q^{-1}AQ \in M_n(\overline{F})$ is. Verder sal die verskillende komponente van die eievektore van A sodoende ook in \overline{F} wees. Aangesien die kolomvektore van Q eievektore van A is, sal Q en Q^{-1} gevolglik ook elemente van $M_n(\overline{F})$ wees.

Stelling 3.12 ([2], Stelling 7.2.3) 'n Vierkantige matriks A waarvan al die eiewaardes verskillend is, is diagonaliseerbaar.

Stelling 3.13 ([1], Stelling 3.10.3) Laat D 'n integraalgebied wees. Dan bestaan daar 'n liggaam F_D wat 'n subring D^* , isomorf aan D , bevat sodat elke element in F_D van die vorm uv^{-1} is, waar $u, v \in D^*$ en $v \neq 0$.

Definisie 3.14 ([1], Notas 3.10.5(i)) Die liggaam F_D in Stelling 3.13 word die kwosiënt-liggaam van die integraalgebied D genoem.

Definisie 3.15 ([16], bladsy 238) Laat F 'n liggaam en $f \in F[x]$ 'n polinoom van graad n met verskillende wortels, u_1, \dots, u_n in die vervalliggaam E van f oor F wees. Laat

$$\Delta = \prod_{i < j} (u_i - u_j) = (u_1 - u_2)(u_1 - u_3) \cdots (u_{n-1} - u_n).$$

Die diskriminant van f is die element $\Delta^2 \in E$.

Proposisie 3.16 ([16], Proposisie 4.57) Laat F, E, f en Δ soos in Definisie 3.15 wees. Dan volg dat die diskriminant van f 'n element van F is.

Vervolgens bewys ons Lemma 3.17, Lemma 3.18 en Lemma 3.20.

Lemma 3.17 Die polinoom $P(X, Y_1, \dots, Y_n)$ lê in die sentrum van $M_n(F)$, waar X 'n diagonaal matriks en Y_1, \dots, Y_n enige willekeurige matrikse in $M_n(F)$ is.

Bewys Gestel X is 'n diagonaalmatriks in $M_n(F)$. Aangesien die matrikseenhede $M_n(F)$ span, kan enige willekeurige $Y \in M_n(F)$ uitgedruk word as

$$Y = \sum_{i,j} b_{ij} e_{ij}, \quad \text{waar } b_{ij} \in F.$$

Gestel $Y_k = \sum_{i_k, j_k} b_{i_k j_k}^{(k)} e_{i_k j_k}$. Dan volg, indien ons a_1, \dots, a_{n+1} so kies dat $g(x_{i_1}, \dots, x_{i_n}, x_{j_n}) = \sum c_a x_{i_1}^{a_1} \cdots x_{i_n}^{a_n} x_{j_n}^{a_{n+1}}$, dat

$$\begin{aligned} & G(X, Y_1, \dots, Y_n) \\ &= \sum_a c_a X^{a_1} Y_1 X^{a_2} Y_2 \cdots X^{a_n} Y_n X^{a_{n+1}} \\ &= \sum_a c_a X^{a_1} \left(\sum_{i_1, j_1} b_{i_1 j_1}^{(1)} e_{i_1 j_1} \right) X^{a_2} \left(\sum_{i_2, j_2} b_{i_2 j_2}^{(2)} e_{i_2 j_2} \right) \cdots X^{a_n} \left(\sum_{i_n, j_n} b_{i_n j_n}^{(n)} e_{i_n j_n} \right) X^{a_{n+1}} \\ &= \sum_a \sum_{i_1, j_1} \cdots \sum_{i_n, j_n} c_a X^{a_1} b_{i_1 j_1}^{(1)} e_{i_1 j_1} X^{a_2} b_{i_2 j_2}^{(2)} e_{i_2 j_2} \cdots X^{a_n} b_{i_n j_n}^{(n)} e_{i_n j_n} X^{a_{n+1}} \\ &= \sum_{i_1, j_1} \cdots \sum_{i_n, j_n} \sum_a c_a X^{a_1} b_{i_1 j_1}^{(1)} e_{i_1 j_1} X^{a_2} b_{i_2 j_2}^{(2)} e_{i_2 j_2} \cdots X^{a_n} b_{i_n j_n}^{(n)} e_{i_n j_n} X^{a_{n+1}} \\ &= \sum_{i_1, j_1} \cdots \sum_{i_n, j_n} b_{i_1 j_1}^{(1)} \cdots b_{i_n j_n}^{(n)} \left(\sum_a c_a X^{a_1} e_{i_1 j_1} X^{a_2} e_{i_2 j_2} \cdots X^{a_n} e_{i_n j_n} X^{a_{n+1}} \right) \\ &= \sum_{i_1, j_1} \cdots \sum_{i_n, j_n} b_{i_1 j_1}^{(1)} \cdots b_{i_n j_n}^{(n)} G(X, e_{i_1 j_1}, \dots, e_{i_n j_n}). \end{aligned} \tag{71}$$

Aangesien $e_{i_1 j_1}, e_{i_2 j_2}, \dots, e_{i_n j_n}$ willekeurige matrikseenhede is, volg uit (71) dat

$$\begin{aligned} & G(X, Y_k, \dots, Y_n, Y_1, \dots, Y_{k-1}) \\ &= \sum_{i_k, j_k} \cdots \sum_{i_n, j_n} \sum_{i_1, j_1} \cdots \sum_{i_{k-1}, j_{k-1}} b_{i_k j_k}^{(k)} \cdots b_{i_n j_n}^{(n)} b_{i_1 j_1}^{(1)} \cdots b_{i_{k-1} j_{k-1}}^{(k-1)} \cdot \\ & \quad G(X, e_{i_k j_k}, \dots, e_{i_n j_n}, e_{i_1 j_1}, \dots, e_{i_{k-1} j_{k-1}}) \\ &= \sum_{i_1 j_1} \cdots \sum_{i_n j_n} b_{i_1 j_1}^{(1)} \cdots b_{i_n j_n}^{(n)} G(X, e_{i_k j_k}, \dots, e_{i_n j_n}, e_{i_1 j_1}, \dots, e_{i_{k-1} j_{k-1}}), \end{aligned}$$

waar $1 < k \leq n$. Gevolglik is

$$\begin{aligned} & P(X, Y_1, \dots, Y_n) \\ &= \sum_{i_1, j_1} \cdots \sum_{i_n, j_n} b_{i_1 j_1}^{(1)} \cdots b_{i_n j_n}^{(n)} (G(X, e_{i_1 j_1}, \dots, e_{i_n j_n}) + \cdots + G(X, e_{i_n j_n}, e_{i_1 j_1}, \dots, e_{i_{n-1} j_{n-1}})) \\ &= \sum_{i_1, j_1} \cdots \sum_{i_n, j_n} b_{i_1 j_1}^{(1)} \cdots b_{i_n j_n}^{(n)} P(X, e_{i_1 j_1}, \dots, e_{i_n j_n}), \end{aligned} \tag{72}$$

waar $b_{i_1 j_1}^{(1)} \cdots b_{i_n j_n}^{(n)} \in F$. Aangesien $Z(M_n(F))$ 'n subalgebra van $M_n(F)$, volgens Proposisie 0.7, is en $P(X, e_{i_1 j_1}, \dots, e_{i_n j_n})$ in die sentrum van $M_n(F)$, volgens Lemma 3.8, is, volg dat $P(X, Y_1, \dots, Y_n)$ in die sentrum van $M_n(F)$, vir alle $Y_1, \dots, Y_n \in M_n(F)$ en enige diagonaalmatriks X in $M_n(F)$, is.

□

Lemma 3.18 *Die polinoom $P(X, Y_1, \dots, Y_n)$ lê in die sentrum van $M_n(F)$, waar X, Y_1, \dots, Y_n enige willekeurige matrikse in $M_n(F)$ is.*

Bewys Ons bewys eerstens dat $P(X, Y_1, \dots, Y_n)$, waar X 'n diagonaliseerbare matriks in $M_n(F)$ is, in die sentrum van $M_n(F)$ is.

Laat $X \in M_n(F)$ enige diagonaliseerbare matriks in $M_n(F)$ wees. Dit beteken daar bestaan 'n inverteerbare matriks Q , sodat $Q^{-1}XQ$, volgens Stelling 3.11, 'n diagonaalmatriks met die eiewaardes van X op die hoofdiagonaal is. Volgens die opmerking na Stelling 3.11 is $Q, Q^{-1}, Q^{-1}AQ \in M_n(\overline{F})$, waar \overline{F} die algebraïese afsluiting van F is.

Aangesien $Q^{-1}AQ \in M_n(\overline{F})$ 'n diagonaalmatriks is en $Q^{-1}Y_1Q, \dots, Q^{-1}Y_nQ \in M_n(\overline{F})$, volg uit Lemma 3.8 dat $P(Q^{-1}XQ, Q^{-1}Y_1Q, \dots, Q^{-1}Y_nQ) \in Z(M_n(\overline{F}))$. Deur van hierdie feit en Lemma 3.9 gebruik te maak, volg dat

$$\begin{aligned} & P(X, Y_1, \dots, Y_n) \\ &= QQ^{-1}P(X, Y_1, \dots, Y_n)QQ^{-1} \\ &= Q \underbrace{P(Q^{-1}XQ, Q^{-1}Y_1Q, \dots, Q^{-1}Y_nQ)}_{\in Z(M_n(\overline{F}))} Q^{-1} \end{aligned} \tag{73}$$

$$\begin{aligned} &= QQ^{-1}P(Q^{-1}XQ, Q^{-1}Y_1Q, \dots, Q^{-1}Y_nQ) \\ &= P(Q^{-1}XQ, Q^{-1}Y_1Q, \dots, Q^{-1}Y_nQ) \in Z(M_n(\overline{F})). \end{aligned} \tag{74}$$

Omdat $X, Y_1, \dots, Y_n \in M_n(F)$, en dus volg dat $P(X, Y_1, \dots, Y_n) \in M_n(F)$, volg sodoende uit (74) dat

$$P(X, Y_1, \dots, Y_n) \in M_n(F) \cap Z(M_n(\overline{F})) = Z(M_n(F)). \tag{75}$$

Uit Stelling 3.2 volg dus dat

$$P(X, Y_1, \dots, Y_n) = \begin{bmatrix} k & & \circ \\ & \ddots & \\ \circ & & k \end{bmatrix}, \quad \text{waar } k \in F. \tag{76}$$

Vervolgens brei ons X na 'n willekeurige matriks in $M_n(F)$ uit. Gestel nou X is 'n matriks waarvan die inskrywings onafhanklike, kommuterende veranderlikes is, sê

$$X := \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{bmatrix}.$$

Dan is die inskrywings van X monome in die polinoomring $F[x_{ij}]_{i,j=1}^n$ en $X \in M_n(F[x_{ij}]_{i,j=1}^n)$.

Ons bewys nou dat X diagonaliseerbaar is deur te bewys dat al die wortels van die karakteristieke polinoom $p_X(\lambda)$ van X verskillend is, wat beteken dat al die eiewaardes van X verskillend is, en X sodoende volgens Stelling 3.12 diagonaliseerbaar is.

Laat $A = (a_{ij})$ 'n willekeurige matriks in $M_n(F)$, met karakteristieke polinoom $p_A(\lambda)$, wees. Ons definieer nou die homomorfisme $\alpha_A : F[x_{ij}]_{i,j=1}^n \rightarrow F$ deur

$$\alpha_A : f(x_{ij})_{i,j=1}^n \mapsto f(a_{ij})_{i,j=1}^n.$$

Met ander woorde, α_A vervang elke onafhanklike veranderlike x_{ij} met die matriksinskrywing a_{ij} en laat die koëffisiënte in F vas.

Volgens Stelling 3.13 kan die integraalgebied $F[x_{ij}]_{i,j=1}^n$ in sy kwosientliggaam, $F(x_{ij})_{i,j=1}^n$ ingebed word. Aangesien die elemente van $F(x_{ij})_{i,j=1}^n$ van die vorm fg^{-1} is, waar $f, g \in F[x_{ij}]_{i,j=1}^n$ en $g \neq 0$, volg dat ons α_A na die homomorfisme $\alpha'_A : F(x_{ij})_{i,j=1}^n \rightarrow F$ gedefinieer deur

$$\alpha'_A : f \mapsto \alpha_A(f), \quad \alpha'_A : g^{-1} \mapsto (\alpha_A(g))^{-1}, \quad \text{waar } f, g \in F[x_{ij}]_{i,j=1}^n, \quad g \neq 0,$$

kan uitbrei.

Aangesien $p_X(\lambda)$ 'n polinoom van graad n in $F[x_{ij}]_{i,j=1}^n$, en dus in $F(x_{ij})_{i,j=1}^n$, is, het die polinoom $p_X(\lambda)$ n (moontlik herhaalde) wortels in die algebraïese afsluiting L (sê) van $F(x_{ij})_{i,j=1}^n$. Gestel $\gamma_1, \dots, \gamma_n$ is die n wortels van $p_X(\lambda)$. Dan is $\gamma_1, \dots, \gamma_n$ almal funksies in die onafhanklike veranderlikes $\{x_{ij}\}_{i,j=1}^n$ en die diskriminant (Definisie 3.15) $\Delta^2(p_X(\lambda))$ van $p_X(\lambda)$ is

$$\Delta^2(p_X(\lambda)) = (\gamma_1 - \gamma_2) \cdots (\gamma_{n-1} - \gamma_n),$$

waar $\Delta^2(p_X(\lambda)) \in F(x_{ij})_{i,j=1}^n$ volgens Proposisie 3.16. Aangesien die beeld van $\Delta^2(p_X(\lambda))$ die diskriminant $\Delta^2(p_A(\lambda))$ van die karakteristieke polinoom $p_A(\lambda)$ van A onder α'_A is, volg dat $\Delta^2(p_A(\lambda)) = 0$ indien $\Delta^2(p_X(\lambda)) = 0$. Dus volg dat $p_A(\lambda)$ minstens twee gelyke

wortels het indien $p_X(\lambda)$ minstens twee gelyke wortels het. Omdat ons A willekeurig gekies het, volg dan dat die karakteristieke polinoom van alle matrikse in $M_n(F)$ twee gelyke wortels het, en dus dat alle matrikse in $M_n(F)$ twee gelyke eiewaardes het. Volgens Lemma 3.7 bestaan daar 'n matriks in $M_n(F)$ waarvan al die eiewaardes verskillend is. Dus is al die eiewaardes van $p_X(\lambda)$ verskillend. Gevolglik is X diagonaliseerbaar.

Ons brei nou α'_A (waar A 'n willekeurige matriks in $M_n(F)$ is) uit na die homomorfisme $\overline{\alpha'_A} : M_n(F[x_{ij}]_{i,j=1}^n) \rightarrow M_n(F)$ gedefinieer deur

$$\overline{\alpha'_A} : (u_{kl}) \mapsto (\alpha'_A(u_{kl})), \quad \text{waar } u_{kl} \in F[x_{ij}]_{i,j=1}^n.$$

Let op dat

$$\overline{\alpha'_A}(X) = \overline{\alpha'_A}((x_{kl})) = (\alpha'_A(x_{kl})) = (\alpha_A(x_{kl})) = (a_{kl}) = A.$$

Aangesien $Y_i \in M_n(F)$ vir alle $i \in \{1, \dots, n\}$ volg dat al die inskrywings van Y_i in F is. Sodoende volg dat

$$\overline{\alpha'_A}(Y_i) = (\alpha'_A(y_{kl})) = (\alpha_A(y_{kl})) = (y_{kl}) = Y_i, \quad \text{waar } y_{kl} \in F \text{ die inskrywings van } Y_i \text{ is.}$$

Verder volg uit (75) dat $P(X, Y_1, \dots, Y_n) \in Z(M_n(F[x_{ij}]_{i,j=1}^n))$ sodat

$$P(X, Y_1, \dots, Y_n) = \begin{bmatrix} h & & \circ \\ & \ddots & \\ \circ & & h \end{bmatrix}, \quad \text{waar } h \in M_n(F[x_{ij}]_{i,j=1}^n).$$

Gevolglik is

$$\begin{aligned} \overline{\alpha'_A}(P(X, Y_1, \dots, Y_n)) &= \overline{\alpha'_A} \left(\begin{bmatrix} h & & \circ \\ & \ddots & \\ \circ & & h \end{bmatrix} \right) \\ \Rightarrow P(\overline{\alpha'_A}(X), \overline{\alpha'_A}(Y_1), \dots, \overline{\alpha'_A}(Y_n)) &= \begin{bmatrix} \alpha'_A(h) & & \circ \\ & \ddots & \\ \circ & & \alpha'_A(h) \end{bmatrix} \\ \Rightarrow P(A, Y_1, \dots, Y_n) &= \begin{bmatrix} \alpha_A(h) & & \circ \\ & \ddots & \\ \circ & & \alpha_A(h) \end{bmatrix}. \end{aligned}$$

Aangesien $\alpha_A(h) \in F$ volg dat $P(A, Y_1, \dots, Y_n) \in Z(M_n(F))$. Omdat A 'n willekeurige

matriks in $M_n(F)$ was, kan ons alle beperkings op X verwyder.

□

Ons gebruik die volgende bekende resultaat in die bewys van Lemma 3.20.

Lemma 3.19 *Indien F 'n subliggaam van 'n liggaam E is, dan het F en E dieselfde identiteit.*

Lemma 3.20 *Die polinoom $P(X, Y_1, \dots, Y_n)$ is nie-nulwordend.*

Bewys Laat $X \in M_n(F)$ 'n vaste diagonaliseerbare matriks waarvan al die eiewaardes verskillend is, wees. Uit Lemma 3.7 weet ons daar bestaan so 'n matriks in $M_n(F)$. Indien ons nou kan bewys dat daar $Y_1, \dots, Y_n \in M_n(F)$ bestaan, sodat $P(X, Y_1, \dots, Y_n) \neq 0$, is ons klaar.

Gestel nou $P(X, Y_1, \dots, Y_n) = 0$ vir alle $Y_1, \dots, Y_n \in M_n(F)$. Dan volg in die besonder dat $P(X, e_{i_1 j_1}, \dots, e_{i_n j_n}) = 0$, waar $e_{i_1 j_1}, \dots, e_{i_n j_n}$ willekeurige matrikseenhede in $M_n(F)$ is. Laat \bar{F} die algebraïese afsluiting van F wees. Aangesien F 'n subliggaam van \bar{F} is, volg uit Lemma 3.19 dat F en \bar{F} dieselfde identiteit het. Sodoende volg dat die matrikseenhede van $M_n(F)$ vir $M_n(\bar{F})$ span. Laat X, Y_1, \dots, Y_n nou willekeurige elemente van $M_n(\bar{F})$ wees. Aangesien $P(X, e_{i_1 j_1}, \dots, e_{i_n j_n}) = 0$ en uit (72) volg dat

$$P(X, Y_1, \dots, Y_n) = \sum_{i_1, j_1} \cdots \sum_{i_n, j_n} b_{i_1 j_1}^{(1)} \cdots b_{i_n j_n}^{(n)} P(X, e_{i_1 j_1}, \dots, e_{i_n j_n}),$$

waar $b_{i_1 j_1}^{(1)} \cdots b_{i_n j_n}^{(n)} \in \bar{F}$, volg dat $P(X, Y_1, \dots, Y_n) = 0$. Gevolglik is $P(X, Y_1, \dots, Y_n) = 0$ vir alle $Y_1, \dots, Y_n \in M_n(\bar{F})$.

Indien ons dus kan bewys dat daar $Y_1, \dots, Y_n \in M_n(\bar{F})$ bestaan sodat $P(X, Y_1, \dots, Y_n) \neq 0$, volg dat daar $Y_1, \dots, Y_n \in M_n(F)$ bestaan sodat $P(X, Y_1, \dots, Y_n) \neq 0$.

Laat $Q \in M_n(\bar{F})$ 'n matriks, met inverse $Q^{-1} \in M_n(\bar{F})$, wees wat X diagonaliseer en laat $Y_1 = Qe_{12}Q^{-1}, Y_2 = Qe_{23}Q^{-1}, \dots, Y_{n-1} = Qe_{n-1,n}Q^{-1}, Y_n = Qe_{n1}Q^{-1}$ wees. Dan is $e_{12}, e_{23}, \dots, e_{n-1,n}, e_{n1}$ 'n siklus van matrikseenhede, $Y_1, \dots, Y_n \in M_n(\bar{F})$ en $Q^{-1}XQ \in M_n(\bar{F})$ is 'n diagonaal matriks met verskillende inskrywings op die diagonaal. Dus volg

dat

$$P(X, Y_1, \dots, Y_n) = QP(Q^{-1}XQ, Q^{-1}Y_1Q, \dots, Q^{-1}Y_nQ)Q^{-1} \quad (77)$$

$$\begin{aligned} &= QP(Q^{-1}XQ, e_{12}, e_{23}, \dots, e_{n-1,n}, e_{n1})Q^{-1} \\ &= QdI_nQ^{-1} = dI_n \neq 0, \end{aligned} \quad (78)$$

waar (77) uit Lemma 3.9 en (78) uit (70) volg.

□

Uit Lemma 3.8, Lemma 3.18 en Lemma 3.20 volg dat $P(X, Y_1, \dots, Y_n)$ 'n nie-nulwordende sentrale polinoom vir $M_n(F)$, met $n \geq 2$, is. Stelling 3.5 is dus bewys.

Voorbeeld Kom ons beskou die sentrale polinoom $P(X, Y_1, Y_2)$ vir 2×2 matrikse wat ons in bostaande stelling gekonstrueer het.

Aangesien

$$\begin{aligned} g(x_1, x_2, x_3) &= (x_1 - x_2)(x_3 - x_2) \\ &= x_1x_3 - x_1x_2 - x_2x_3 + x_2^2 \end{aligned}$$

volg dat

$$G(X, Y_1, Y_2) = XY_1Y_2X - XY_1XY_2 - Y_1XY_2X + Y_1X^2Y_2$$

en dat

$$G(X, Y_2, Y_1) = XY_2Y_1X - XY_2XY_1 - Y_2XY_1X + Y_2X^2Y_1.$$

Sodoende volg dat

$$\begin{aligned} P(X, Y_1, Y_2) &= G(X, Y_1, Y_2) + G(X, Y_2, Y_1) \\ &= XY_1Y_2X - XY_1XY_2 - Y_1XY_2X + Y_1X^2Y_2 \\ &\quad + XY_2Y_1X - XY_2XY_1 - Y_2XY_1X + Y_2X^2Y_1. \end{aligned}$$

Indien ons $Y_1 = Y_2$ stel volg dat

$$\begin{aligned} P(X, Y, Y) &= 2(XY^2X - XYXY - YXYX + YX^2Y) \\ &= -2(XY - YX)^2. \end{aligned}$$

Aangesien -2 slegs 'n skalaar is, volg dat $(XY - YX)^2$ 'n nie-nulwordende sentrale polinoom in $M_2(F)$, vir enige liggaam F , is. Dit is presies die polinoom wat ons in Stelling 3.4 beskou het en wat in 1937 deur W. Wagner in [17] gekonstrueer is.

Verwysings

- [1] R.B.J.T. Allenby, *Rings, Fields and Groups – An Introduction to Abstract Algebra*, Second Edition, Butterworth-Heinemann, Oxford, 2001.
- [2] H. Anton, C. Rorres, *Elementary Linear Algebra*, Eighth Edition, John Wiley and Sons, New York, 2000.
- [3] A. Clark, *Elements of Abstract Algebra*, Dover Publications, New York, 1984.
- [4] P.M. Cohn, *Classic Algebra*, John Wiley and Sons, New York, 2000.
- [5] E. Formanek, *Central polynomials for matrix rings*, J. Algebra **23** (1972), 129-132.
- [6] E. Formanek, *The polynomial identities and invariants of $n \times n$ matrices*, Amer. Math. Soc., Providence, R.I., 1991.
- [7] E. Formanek, *The polynomial identities of matrices.*, Contemp. Math., 13, Amer. Math. Soc, Providence, R.I., 1982.
- [8] I.N. Herstein, *Noncommutative rings*, Third Printing, The Mathematical Association of America, Number Fifteen, 1973.
- [9] T.W. Hungerford, *Algebra*, Springer-Verlag, New York, 1991.
- [10] I. Kaplansky, *Problems in the theory of rings*, Amer. Math. Monthly **77** (1970), 445-454.
- [11] A.V. Kelarev, A.B. van der Merwe, L. van Wyk, *The Minimum Number of Idempotent Generators of an Upper Triangular Matrix Algebra*, J. Algebra **205** (1998), 605-616.
- [12] N. Krupnik, *Minimal number of idempotent generators of matrix algebras over arbitrary field*, Comm. Algebra **20** (1992), 3251-3257.
- [13] V.N. Latyshev and A.L. Shmelkin, *On a problem of Kaplansky*, Algebra i Logika **8** (1969), 447-448; (translation), Algebra and Logic **8** (1969), 257.
- [14] N.H. McCoy, *The Theory of Rings*, Chelsea Publishing Company, New York, 1973.
- [15] Y.P. Razmyslov, *On a problem of Kaplansky*, Izv. Akad. Nauk SSSR **37** (1973), 483-501; (translation), Math. USSR-Izv. **7** (1973), 479-496.

- [16] J. Rotman, *Advanced Modern Algebra*, Pearson Education, Upper Saddle River, 2002.
- [17] W. Wagner, *Über die Grundlagen der projektiven Geometrie und allgemeine Zahlssysteme*, Math. Ann. **113** (1937), 528-567.

Lys van Simbole

\subseteq	is 'n subversameling van
$\#$	aantal
$\mathbb{B}_1 \oplus \mathbb{B}_2$	direkte som van \mathbb{B}_1 en \mathbb{B}_2
$\lceil a \rceil$	kleinste heelgetal wat $\geq a$
$\lfloor a \rfloor$	grootste heelgetal wat $\leq a$
\mathbb{Z}	versameling van heelgetalle
\mathbb{N}	versameling van positiewe heelgetalle
\mathbb{Z}_m	ring van heelgetalle modulo m
$\deg f$	graad van die polinoom f
\max	maksimum van
$\dim V$ of $\dim \mathbb{A}$	$\begin{cases} \text{dimensie van die vektorruimte } V \\ \text{dimensie van die algebra } \mathbb{A} \end{cases}$
$\det A$	determinant van die matriks A
$V(x_1, \dots, x_n)$	die Vandermonde determinant van x_1, \dots, x_n
E/F	die liggaam E is 'n uitbreidingsliggaam van die liggaam F
$[E : F]$	dimensie van die liggaam E as 'n F -vektorruimte
$ A $ of $ F $	$\begin{cases} \text{kardinaalgetal van die versameling } A \\ \text{orde van die liggaam } F \end{cases}$
$F[x]$	polinoomring van polinome oor F
$F[x_1, \dots, x_n]$	polinoomring van alle polinome in die n veranderlikes x_1, \dots, x_n oor F
$F(x)$	kwosiëntliggaam van $F[x]$
$F(x_1, \dots, x_n)$	kwosiëntliggaam van $F[x_1, \dots, x_n]$
S_n	simmetriese groep van n letters
(s_1, s_2, \dots, s_r)	'n r -siklus
$\text{sgn}(\sigma)$	teken van die permutasie σ
δ_{ij}	Kronecker delta
$\pi_i(\mathbb{B})$	kanoniese afbeelding op die i 'de komponent van die direkte som \mathbb{B}
$\Delta^2(f)$	diskriminant van die polinoom f
e_{ij}	matrikseenheid met 'n 1 in posisie (ij)
I_n	die $n \times n$ identiteitsmatriks
(b_{ij})	matriks met inskrywing b_{ij} in posisie (ij)
$\text{tr}(A)$	spoor van die matriks A
$M_n(F)$	volledige $n \times n$ matriksalgebra oor 'n liggaam F
$M_n^m(F)$	direkte som van m kopieë van die matriksalgebra $M_n(F)$

F^m	direkte som van m kopieë van die liggaam F
$\nu(n, F)$	minimum aantal idempotente voortbringers van $M_n(F)$
$\nu(\mathbb{B})$	minimum aantal idempotente voortbringers van die algebra \mathbb{B}
$Z(\mathbb{A})$	sentrum van die algebra \mathbb{A}
\overline{F}	algebraïese afsluiting van die liggaam F

Indeks

- Algebra, 2
 - Artinse-, 3
 - Delings-, 2
 - Dimensie, 2
 - Homomorfisme, 3
 - Ideaal, 2
 - Isomorfisme, 3
 - Noetherse-, 3
 - Sub-, 2
- Algebraïes geslote, 8
- Algebraïese
 - Afsluiting, 8
 - Element, 7
 - Uitbreidingsliggaam, 7
- Caley-Hamilton Stelling, 64
- Diagonaliseerbaar, 72
- Diskriminant, 73
- Idempotent, 4
- Jacobson-radikaal, 3
- Karakteristiek, 8
- Kwasiëntliggaam, 73
- Lagrange se Interpolasie Formule, 50
- Matrikseenhede, 2
- Meegaande Matriks, 67
- Permutasie, 4
 - Ewe, 5
 - Onewe, 5
 - Teken, 5
- Permutasiegroep, 4
 - Simmetriese groep van n letters, 4
- Permutasiematriks, 5
- Polinoom
 - Delingsalgoritme, 6
 - Onherleibaar, 9
 - Ontbinding, 6
- Polinoomidentiteit, 62
 - Standaard, 17
- Semi-eenvoudig, 3
- Sentrale Polinoom, 62
 - Nie-nulwordend, 62
- Sentrum, 4
- Siklus, 4
- Transendente
 - Element, 7
 - Uitbreidingsliggaam, 7
- Transposisie, 4
- Uitbreidingsliggaam, 6
 - Dimensie, 6
- Vandermonde
 - Determinant, 30
 - Determinant Argument, 30
 - Matriks, 30
- Vervalliggaam, 6
- Weddeburn-Artin Stelling, 59